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

Study of efficacy and proposal of implementation method of Live Forensics

今野 直樹† 田中 英彦†
Naoki Konno Hidehiko Tanaka

1. はじめに

これまで，ライブフォレンジックはインシデントレスポンスにおける手法の１つとして知られてきたが，実際は調査担当者のスキル不足や有効性の認識不足等の理由からほとんど実施されてこなかった．

しかしながら，現在，サイバー犯罪が多発しているため，ライブフォレンジックは被害端末に対するインシデントレスポンスにおいてだけでなく，攻撃者端末に対する解析においても欠かすことのできない技術となっている．

したがって，現場からのニーズに応えるため，ライブフォレンジックにおける有効性を明らかにした上でその具体的実施手法を体系的にまとめ，それを指針として示すことが研究者には求められている．

2. 研究背景

2.1 研究の必要性

近年，ファイルシステムに証拠を残さないタイプの攻撃手法が出現したことや，アプリケーションやシステム自体が暗号化されるようになったことで，従来のようにハードディスクを調べても必要な情報が得られないケースが増加している．

また，クラウドサービスの普及によって，データそのものがハードディスクに保存されない場合も多い．

このような状況では，従来からあるデジタルフォレンジックの手法だけに頼っていては，充分な解析を行うことが困難である．

これは，攻撃者に有利な状況であり，調査担当者にとっては極めて不利な状況といえる．

したがって，従来の手法だけでは対応できない部分について，新たにライブフォレンジックの手法を確立し，充分なインシデント調査や攻撃者の割り出し，犯行の裏付けを可能にする必要がある．

2.2 研究の目的

従来のデジタルフォレンジックでは，現場での解析を避け，一旦，保全作業者が現場から証拠品端末を持ち帰り，その後，解析センターにおいて高度なスキルを持った調査担当者が時間を掛けて解析を行ってきた．

しかし，こういった従来の手法では調査が立ち行かなくなっていることから，現場でできることは可能な限り現場で行うという新しいフォレンジックの手法が必要とされている．

そこで，本研究では，近年有力な解析手法として注目されているライブレスポンスやメモリフォレンジックの技術に着目し，稼働状態の端末に対するライブフォレンジックを実施することの有効性を検討し，さらに，ライブフォレンジックの手法を体系的に整備して具体的実施手法を提案することを目的とする．

なお，本稿の章構成は，

2 章－4 章：研究背景等

5 章－8 章：ライブフォレンジック概要

9 章－10 章：有効性の検討及び具体的実施手法の提案

としている．

3. デジタルフォレンジック

3.1 デジタルフォレンジックの概要

デジタルフォレンジックとは，コンピューター（端末）に関する犯罪等が生じた際に，被害の原因究明をしたり，捜査に必要なデータを収集分析して攻撃者を割り出したり，攻撃者の端末等を解析して犯行を裏付けたりする，法的な証拠を明らかにするための技術の総称である．

具体的には，被害サーバーのログファイルから不正アクセスの記録を割り出したり，攻撃者の端末を押収してハードディスクから証拠となるファイルを探し出したり，消去されたデータを復元したりすることで，証拠となるデータを押収する技術が該当する．

目的別によるフォレンジックの主な違いを**表 1** に示す．

企業の情報システム部員やセキュリティベンダーの技術者が行う復旧を目的としたフォレンジックは，被害端末を調査対象としたインシデントレスポンスとしての意味合いが強いが，法執行機関の捜査員が行う攻撃者検挙を目的としたフォレンジックは，主に攻撃者の端末を調査対象としており，その目的も作業内容も大きく異なる．

表1 目的別によるフォレンジックの主な違い

	復旧を目的としたフォレンジック	攻撃者検挙を目的としたフォレンジック
調査対象	被害を受けた端末	被害を受けた端末， 攻撃者の端末
作業内容	被害範囲の特定， 原因の特定， 脆弱性の対応， 復旧	攻撃者を割り出すための痕跡の調査， 犯行の立証，裏付けとなる痕跡の調査

†情報セキュリティ大学院大学, IISEC

3.2 デジタルフォレンジックの現状

3.2.1 海外の現状

米国の法執行機関では，フォレンジックラボと呼ばれるフォレンジック専用施設で解析を行っている．

フォレンジックラボでは，フォレンジック調査専用のサーバーを中心としたネットワークを形成しており，捜査官ごとに専用の解析ブースを設けている．

主な解析対象はハードディスク上のデータであり，ハードディスク全領域のイメージファイルを作成し，それをフォレンジックファイルサーバーに保存する．

これによって，データを改変することのない解析を可能にし，効率的に調査を行っている[1]．

3.2.2 国内の現状

日本においても，主な解析対象はハードディスク上のデータである．

調査対象端末からハードディスクを取り出し，別に用意したハードディスクに 100%物理複写した後，複写したハードディスクを解析用パソコンに接続して，フォレンジックツールを用いて解析を行う手法が主流である[2]．

これは，物理的に複写することで証拠品管理を容易にするといった意味合いが強い．

米国と日本では，証拠形式上の違いはあるものの，ハードディスク上の不揮発性データを中心としてデジタルフォレンジックを実施してきたという点では同じである．

3.3 ライブフォレンジックの必要性

従来からのデジタルフォレンジックでは，ハードディスク上のデータ保全を最優先とし，不揮発性データを中心とした解析を実施してきた．

この方法が有効とされてきた理由は，証拠データのほとんどがハードディスク上の不揮発性データに残されていることが多く，このデータを保全し，解析することが重要であったからである．

しかしながら，近年では様々な要因から不揮発性データに頼った手法だけでは充分な証拠を得ることができないケースが増加しており，その対応策として，稼働中のシステムに対するライブフォレンジックを実施する必要がある．

従来手法による解析が難しくなっている要因としては以下のものがある．

・メモリにしか証拠が残らないマルウェアの増加
・クラウドサービスの普及
・OS 等のセキュリティ機能の強化
・セキュリティチップ搭載のハードディスクの普及
・大容量化による複写時間の問題
・踏み台サーバーを利用した攻撃の増加
・RAID のデータ保全問題
・モバイル端末の急速な普及

4. デジタルフォレンジックの研究動向

4.1 海外の研究動向

米国では 2005 年の DFRWS 2005 Forensics Challenge を契機に，メモリデータの保全解析手法が提案され，研究が広まった．

2007 年にオープンソースのメモリフォレンジックツール Volatility がリリースされたことで，メモリフォレンジック分野の研究が急速に進んでいる[3]．

4.2 国内の研究動向

ビッグデータに対応したデジタルフォレンジックが注目されており，大量のデータを効率よく解析するための研究が行われている．

また，人口知能をベースにした機械学習技術による自動解析ツールの研究が行われており，商用ツールとしての製品化も行われている[4]．

5. ライブフォレンジック

5.1 ライブフォレンジックの概要

ライブフォレンジックとは，システムが稼動状態のまま揮発性データまたは不揮発性データを取得し，収集した情報を解析する手法や技術のことである．

この手法自体はそれほど新しいものではなく，被害システムに対するインシデントレスポンスにおいては，稼働中のシステムから必要な情報を取得する手法が知られてきた[5]．

しかし，近年の攻撃手法の高度化によって，従来の手法だけでは必要な証拠を得ることができない事件が増加していることから，その対応策としてあらためてライブフォレンジックが注目されている[6]．

ライブフォレンジックにおける主な技術要素としては，

・ライブレスポンス
・メモリダンプ

がある．

また，ライブレスポンスで用いる代表的なツール群としては，

・Windows Sysinternals

があり，様々な調査で活用することができる．

5.2 揮発性データの重要性

調査対象端末の最新のシステム情報は揮発性データとしてメモリ上に保持されているため，デジタルフォレンジックではこの揮発性データを取得して解析することが非常に重要となる．

揮発性データは端末の電源断によって失われてしまうため，ライブフォレンジックによって確実に取得する必要がある．

6. ライブレスポンス

6.1 ライブレスポンスの概要

ライブレスポンスとは，コンソールにアクセスしてコマンドやツールを実行することにより，稼働中のシステム上で証拠収集を行う手法である．

主に，メモリ上に展開されているカーネル，プロセス，ファイル，レジストリ，ネットワーク等の最新情報を取得対象とする[7]．

また，ハードディスクが暗号化されている場合は，稼働中にディスクイメージの作成を行う．

調査対象端末内のコマンドは改ざんされている可能性があるため，安全なコマンド等をあらかじめ CD-ROM や外付けハードディスク等に記録して用意する必要がある．

6.2 ライブレスポンス時の注意事項

ライブレスポンス時の主な注意事項としては，次のものがある．

・調査対象端末のツール，コマンドを実行しない
・調査対象端末上のディスクに結果を保存しない
・マルウェアスキャン等の処理をしない
・OS アップデートやパッチの適用をしない
・検討せずにネットワークを切断しない
・検討せずにシャットダウン，電源断しない
・画面ロックを発生させない

なお，解析をする際に，証跡が攻撃者によるものなのか，ライブレスポンスによるものなのか分からなくなることを防ぐために，必ず「いつ（作業時間），何をしたか（作業内容）」を記録する必要がある．

6.3 ライブレスポンスによる情報収集

ライブレスポンスにおいては，事前に必要なコマンド及びツールの実行命令を記述したバッチファイルを作成しておくことで，調査本番ではバッチファイルを利用した自動取得が可能となる．

バッチファイルによる自動取得は，手作業による入力ミスを防ぎ，作業時間を短縮する上で有効である．

収集すべき情報は次のとおりである．

・システム時刻情報
・ネットワーク関連情報
・ログオンユーザー関連情報
・プロセス関連情報
・サービス及びドライバー関連情報
・システム構成関連情報
・レジストリ及びログ関連情報

7. メモリダンプ

7.1 メモリダンプの概要

メモリダンプとは，専用のツールを利用することによって，メモリ上に存在する揮発性データを取得する手法である[8]．

メモリダンプを行うことで，揮発性データに含まれるマルウェアや認証情報，最新のレジストリ情報，ディスクに書き出されない直近のキャッシュ等の有用な情報を取得することが可能である．

ダンプしたメモリデータは，Volatility 等のメモリフォレンジックツールによって解析を行う．

ライブレスポンスによって取得する情報の多くはメモリ内に存在するため，メモリフォレンジックによって得られる情報と比較すると，その種類に関してはほとんど差がないが，メモリフォレンジックはライブレスポンスと比較して次のようなメリットがある．

・システムに対する影響を最小限に抑えることができる
・ルートキットの影響を受けにくい
・再現可能性の確保
・作業終了後に追加情報を得ることができる

7.2 メモリフォレンジックツール

様々な OS 用のメモリフォレンジックツールが存在しているが，特に Windows のメモリフォレンジックツールは充分に実用可能な段階にある．

メモリダンプ専用のものから，ダンプと解析の両方が行えるもの等，様々なツールが存在する．

この分野に関しては，オープンソースの Volatility コミュニティの活動が大きく影響している．

Volatility は，Windows，Linux，OS X に対応しているオープンソースのメモリフォレンジックツールであり，メモリフォレンジックツールの中ではもっとも開発が進んでいることから，ほとんどのフォレンジック技術者がメモリフォレンジックに Volatility を使用している．

7.3 その他のメモリ情報取得方法

専用ツールを用いたダンプの他にも，以下に示す手法や機能を用いることで，メモリ情報を取得することが可能である．

・FireWire（IEEE1394)
・Cold Boot Attack
・ハイバネーションファイル
・Windows ハイブリッドスリープ
・OS X セーフスリープ
・クラッシュダンプ
・スワップファイル

8. Windows Sysinternals

8.1 Windows Sysinternals の概要

Windows Sysinternals とは，Microsoft によって提供されているツール群であり，Windows 標準ツールでは調査することができない詳細な情報を収集することが可能である[9][10]．

例えばタスクマネージャーでは調べることができない詳細なプロセス情報やファイルへのアクセス状態を得ることができる．

一般的に Windows Sysinternals は，サーバーマシン等でシステム監視に使われるが，その機能を活かすことで，ライブフォレンジックに利用することができる．

8.2 代表的なツール

Windows Sysinternals には，様々なツールがあるが，特に使われる機会が多いものに，次のものがある．

（1）Process Explorer

タスク マネージャーの高機能版であり，プロセスの詳細情報を取得することが可能である．

（2）Process Monitor

プロセスがアクセスしているファイルやレジストリ，ネットワークに関する情報を取得することが可能である．

（3）Autoruns

システムの起動時に実行されるプログラムの情報をリスト表示でき，レジストリによって起動設定されているプログラムや読み込まれるコーデックについても取得可能である．

9. 有効性の検討

9.1 システムに与える影響

稼動状態での証拠取得作業は，ツール及びコマンドの実行プロセスがメモリ内のデータに影響を与えることが避けられない．

しかし，その影響範囲は無視できるほどに小さい．

ライブフォレンジックによる主な影響を**表 2** に示す．

調査対象端末の稼動状態を保持することによって，システムを維持するための通常タスクが継続されるが，これによって証拠データが失われてしまうことは稀である．

懸念されるのは，ライブフォレンジック対応を原因とするシステムへの影響である．

しかし，**表 2** に示したとおり，持込ディスクの接続履歴がログ等に記録されたり，実行ツールのプロセスがメモリ上に生成されたりする程度であるため，ライブフォレンジック対応によって証拠データが失われてしまうことは稀であり，システムに与える影響は非常に小さいといえる．

表 2　ライブフォレンジックによる主な影響

原因		影響の範囲
稼動状態の保持		スケジュール処理の継続， サービスや常駐プログラムの処理の継続， ログの出力
ライブフォレンジック対応	持込ディスクの接続	デバイスドライバーのロード， レジストリの更新， ログの出力
	ツールの実行	プロセスの生成， イベントログの出力， プリフェッチファイルの更新， レジストリの更新

したがって，調査担当者が作業記録を取りながら慎重にライブフォレンジックを進めることで，システムに与える影響を無視できる程度に抑えることが可能である．

9.2 再現可能性

ライブフォレンジックは稼働状態で証拠収集を実施する性質上，調査結果の再現性を保証することが難しい．

しかし，メモリダンプを行うことによってデータ解析を繰り返し試行することが可能となる．

9.3 ダンプデータから得られる情報

ダンプデータを解析することで得られる有用な情報としては，

・ファイルとして残らないマルウェア
・鍵やパスワード等の認証情報
・ネットワーク接続状況（IP アドレス/ポート）
・ディスクに書き出されない直近のキャッシュ

等がある．

これらの情報はディスク解析から得ることはできないが，メモリフォレンジックを行うことで情報を得ることが可能となるため，ライブフォレンジックの有効性として評価できる．

したがって，これらの情報が収集可能であれば，原則としてライブフォレンジックを実施すべきである．

9.4 追加情報の取得可能性

ダンプデータを取得しておくことで，後日，追加情報を得られる場合が多い．

例えば，ライブフォレンジック実施時に未知のマルウェアを特定できなかったとしても，その後，更新された定義ファイルを用いてダンプデータをスキャンすることによって，マルウェアを特定できる場合がある．

また，ダンプデータの取得からしばらく時間が経過した後に，特定の暗号化データに対応した解析ツールが開発される場合があり，それを用いることで，それまでは解析をすることができなかった暗号化データから，有用な証拠データを得られることがある．

したがって，ダンプデータを取得しておくことは，その後も様々な追加情報を得ることを可能にするため，証拠収集において非常に有効であるといえる．

9.5 証拠性の担保

各フローにおいて，作業メモ，デジタルカメラ，画面キャプチャソフト等を活用して確実に記録を取る必要がある．

記録すべきものとしては，

・作業日時
・調査対象端末の状況（故障の有無等）
・持込ディスク等の接続
・ライブレスポンス（実行ツール，コマンド等）
・ファイルへのアクセス
・データの複写作業

等がある．

これらの記録は，調査対象端末のログに記録された処理等が，攻撃者の操作によって行われたものなのか，それとも調査担当者のライブフォレンジックによって行われたものなのか判別するために必要である．

記録によってこれらの判別を可能にすることで，調査対象端末の証拠性を担保することが可能となる．

9.6 具体的事案における有効性

次の事案では，ライブフォレンジックによって有益な情報を得られる可能性があり，有効性が高いと認められる．

（1）マルウェア感染の可能性が高い標的型攻撃事案及びオンラインバンキング不正送金事案では，ライブレスポンスやメモリダンプを実施することによって，未知のマルウェア検体の特定が可能となる．

（2）クラウドサービスを利用している可能性が高い組織犯罪事案では，リモートアクセスを実施することによって，クラウド上の証拠データを取得する手法が有効である．

（3）データ暗号化の可能性が高い児童ポルノ事案では，ライブレスポンスによって回復キーを取得したり，メモリダンプによってマスターキーを取得したりすることによって，暗号化データを復号し，証拠データを取得することが可能となる．

9.7 普及によって得られるアドバンテージ

現在，国内でデジタルフォレンジックを活用している組織は主に法執行機関とセキュリティベンダーに限られているのが実情である．

しかし，法執行機関が実施するフォレンジックは，主に攻撃者の端末を対象にしたものである．

インシデント発生時，被害者端末に対するフォレンジックの実施者は，第一次的には被害を受けた組織の技術者であり，第二次対応をセキュリティベンダーの技術者が実施した後，最終的に法執行機関の捜査員が調査を実施するというのが一般的な流れになる．

つまり，インシデント発生時に重要な証拠データをライブフォレンジックで保全しなければならないのは，被害を受けた組織の技術者であり，システムを乱してしまった後では，いかに法執行機関の捜査員がライブフォレンジックの高度なスキルを持っていたとしても対応することができない．

このとき，ライブフォレンジックで保全することなく，重要な揮発性データを失ってしまった場合，解析することが不可能となってしまう．

したがって，ライブフォレンジックの有効性及び手法が広く一般に普及することで，被害組織の技術者がメモリダンプだけでも実施することが当たり前になれば，その後のセキュリティベンダーによる被害調査や法執行機関による事件捜査を進める上で大きなアドバンテージを得ることができる．

10. 具体的実施手法の提案

ライブフォレンジックは，本稿でこれまでに述べてきたツールや技術によって実施する．

しかし，事前準備や現場での判断はどうすべきなのか，どのような手順を踏めばよいのか，といった様々な問題が生じるため，ライブフォレンジックを実施することは容易ではない．

そこで，これらの問題を解決するため，ライブフォレンジックの具体的実施手法について考察した結果を以下に述べる．

10.1 持込ディスク作成フロー

10.1.1 持込ディスクについて

ライブフォレンジックの過程において，ライブレスポンスを実施するには，あらかじめ持込ディスク（ツールキット）を作成し，準備しておく必要がある．

本研究の考察結果から，持込ディスクの作成手順を図式化し，新規に考案したフローチャートを**図 1** に示す．

持込ディスクは，外付けハードディスクや CD-ROM 等の記録媒体に，各種ツールやコマンドを保存して作成する．

調査対象端末の USB ポートが使用可能な場合は，外付けハードディスクを利用した方が，1 台で実行プログラムの保存と収集データの保存ができるため便利である．

しかし，調査対象端末において USB ポートが使えない場合には，調査対象端末の CD ドライブに CD-ROM で作成した持込ディスクを挿入し，CD-ROM に保存したツールを使用してライブレスポンスを実施する．

その場合，収集データを LAN 経由で解析用ノート PC に保存する必要がある．

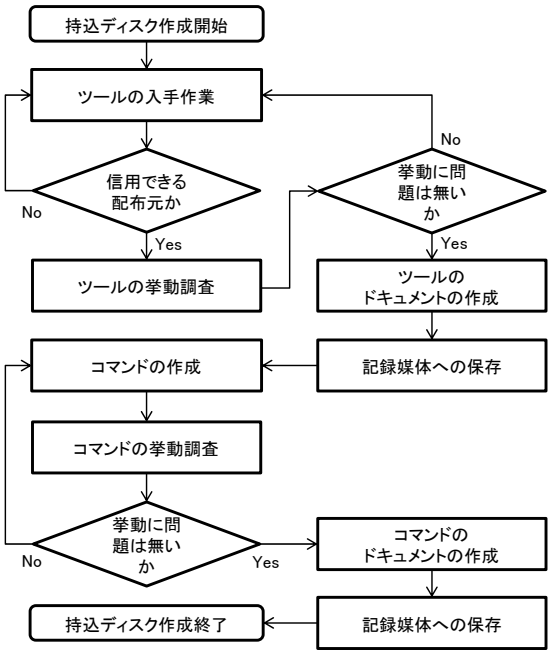

図 1　持込ディスク作成のフローチャート

10.1.2 ツールの入手について

ツールを入手する際は，必ず公式サイト等の信頼できる配布元を利用し，二次配布サイトを利用することがないように注意すべきである．

また，ツールを実行する際に調査対象内のライブラリに依存しないように，信頼できる DLL をツールと併せて可能な限り用意する必要がある．

安全なコマンド類の作成時は，クリーンな OS 環境上で作業を行い，環境の管理記録（OS バージョン，インストールしたアプリケーション）を残す必要がある．

標準コマンド（exe ファイル）や DLL は OS バージョンやアーキテクチャごとに用意しておくことが望ましい．

10.1.3 挙動調査の重要性

各ツールは，必ず事前に挙動調査を行い，出力結果やパフォーマンスを確認しておく必要がある．

商用製品であっても，検証評価を行っていないツールを本番で使用しないように注意しなければならない．

具体的には，Windows Sysinternals 等を利用してライブレスポンスツールの挙動調査を実施し，どのような動作をするのか事前に把握しておくことが重要である．

その調査内容としては，

・メモリ使用量（実行プログラムのロード）
・ネットワーク通信の発生
・キャッシュの生成
・レジストリキー，エントリの生成
・既存ファイルへのアクセス，更新

等を確認する．

同じ機能を持つツールが複数ある場合は，上記処理による調査対象端末への影響を比較し，できるだけ影響が少ないものを選定する．

また，ツールごとに入手場所，説明，要件（依存関係，実行権限，影響範囲）等のドキュメントを作成しておく必要がある．

10.2 ライブフォレンジックフロー

10.2.1 ライブフォレンジックフローの必要性

現在，ライブフォレンジックが積極的に行われていない原因の 1 つとして，判断基準や作業手順が整備されていないことによる解析事故の不安から，調査担当者が実施を敬遠していることがあげられる．

したがって，本研究の考察結果から，ライブフォレンジックの判断基準や作業手順を図式化し，新規に考案したフローチャートを**図 2** に示す．

10.2.2 ライブフォレンジックの可否に関する判断基準

ライブフォレンジックを開始する際には，次の点から可否の判断を行う．

（1）端末が操作可能，かつ，管理者権限のパスワードが判明している場合は，ライブフォレンジックが可能である．

（2）端末が操作可能，かつ，非管理者権限のパスワードが判明している場合は，制限があることを踏まえた上で，ライブフォレンジックが可能である．

（3）端末が操作可能だがパスワードが不明の場合は，無操作時間の経過による画面ロックに注意した上で，ライブフォレンジックが可能である．

自動ロックの設定を解除するか，MouseJiggler 等のツールの利用を検討する．

（4）画面ロック状態で操作不能の場合は，パスワードが判明しなければ電源断を検討する．

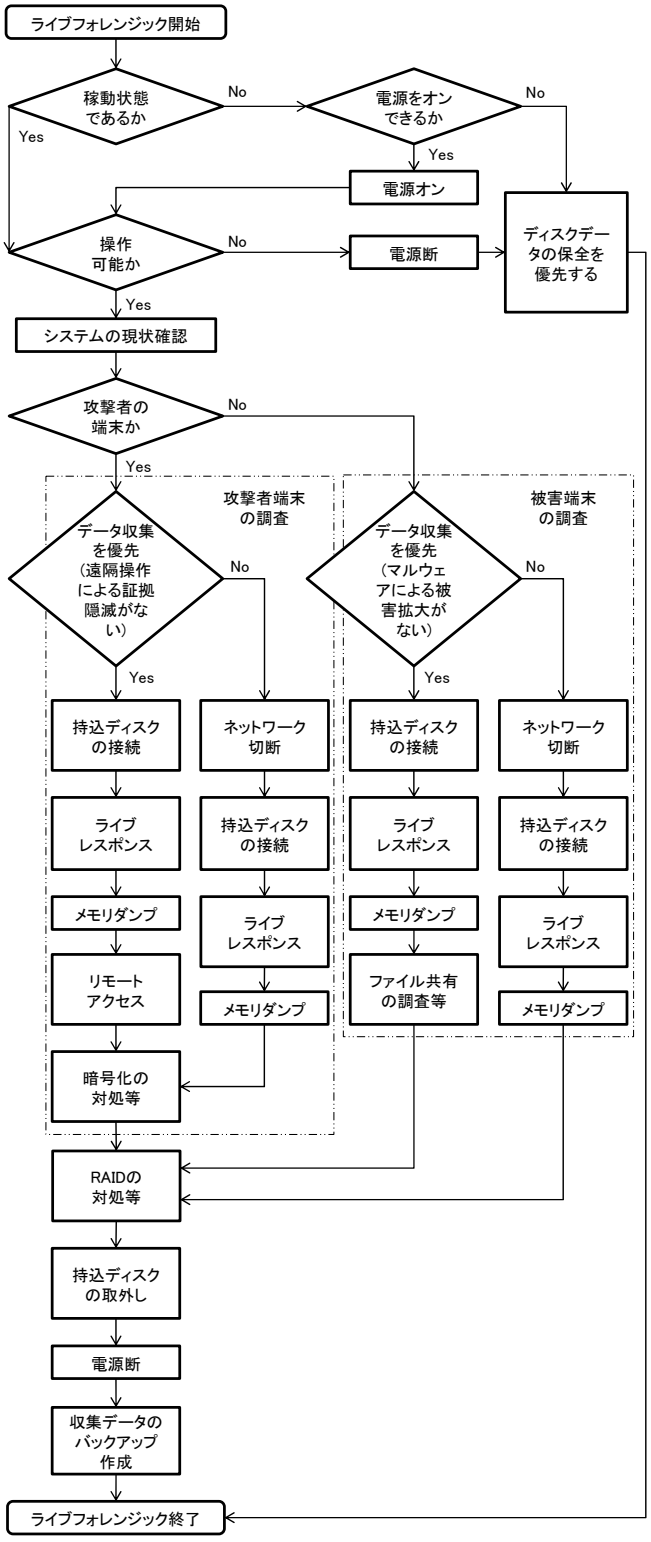

図 2　ライブフォレンジックのフローチャート

10.2.3 端末が電源オフの場合の注意事項

既に調査対象端末が電源オフの状態であっても，リモートアクセス等による証拠保全を実施する必要がある場合は，端末の電源をオンにしなければならない．

その際，一定の操作手順を実施しなければデータが消去される等の細工による証拠隠滅のおそれがある場合には，ディスクデータの保全を優先して，ライブフォレンジックを断念することも検討する．

10.2.4 システムの現状確認

調査対象端末が操作可能な場合，ハードウェアやシステムについて確認し，現状を把握する．

（1）ハードウェアの現状確認

次の点を観察し，ハードウェアの現状を確認する．

・ハードウェアの電源ランプ
・ディスクのアクセスランプ
・NIC のアクセスランプ

（2）システムの現状確認

タスクマネージャーを起動し，次の点からシステムの稼働状況を確認する．

・各プロセスの I/O 読み取り（書き込み）バイト数
・CPU の使用率，メモリの使用率
・ネットワークの使用率，送受信バイト数

10.2.5 調査対象別による作業の優先順位の判断基準

調査対象端末が攻撃者のものなのか，あるいは被害者のものなのかによって，ライブフォレンジックの目的が変化するため，それに合わせて取るべき作業の優先順位を判断しなければならない．

調査対象端末が攻撃者のものである場合，リモートアクセス等によって重要な証拠データを得られる可能性が高いことから，原則としてネットワーク接続を維持した状態で，証拠データ収集を優先すべきである．

しかし，組織的な攻撃であって，ネットワーク接続を継続することによって遠隔操作による証拠隠滅のおそれがある場合には，リモートアクセス等によって得られる可能性がある証拠データの価値と比較検討して，証拠隠滅を防ぐ方の価値が高いと判断すれば，ネットワーク切断を優先すべきである．

また，調査対象が被害者のものである場合も原則として証拠データの収集を優先すべきである．

しかし，端末がワーム等のマルウェアに感染している可能性が高い場合等，ネットワーク接続を継続することによって被害拡大のおそれが高い場合には，ネットワーク切断を優先すべきである．

10.3 ライブレスポンスによる未知のマルウェア検出

アンチマルウェアソフトでは検知できない未知のマルウェアをライブレスポンスの手法を活用して検出する手法を提案する．

多くのマルウェアは，感染後に次回以降の起動時にもプログラムが自動起動されるようにシステムの設定を変更するため，自動起動が設定されているプログラムに不審なものがないかをライブレスポンスで調査する手法が未知のマルウェアを発見する上で有効となる．

バンキングトロイ系マルウェアは，システムのネットワーク設定を変更することで不正な Web サイトへと導くため，最新のネットワーク設定（キャッシュ情報含む）を確認して，不審点を調査することで，マルウェアの特定につなげることができる．

マルウェアは，C&C サーバーから指令を受け取ったり，収集した情報を送信したりするなど，バックグラウンドで通信するものが多いため，ライブフォレンジックによって通信中のプロセスを調査することが検出方法として非常に有効である．

マルウェアの多くは，通常のプログラムが動作するために必要となる，

・ＣＰＵ命令の実行
・実行するためのメモリ領域
・データの送受信（I/O）

等の痕跡を隠ぺいする機能があるため，複数の観点から実行中のプログラムを解析し，不審な挙動を明らかにすることで，マルウェアを特定することが可能である．

具体的には，マルウェアの感染が疑われる調査対象端末に対して，以下のライブレスポンスとメモリフォレンジックを併せて実施することにより，結果の差異から不審な挙動を明らかにする．

・バッチファイルによる証拠データの収集
・ライブレスポンスの結果確認
・Volatility 等によるマルウェアの検出

10.4 Windows Sysinternals による未知のマルウェア検出

未知のマルウェアを Windows Sysinternals 等の GUI ツールを用いて検出する手法を提案する．

GUI ツールは，CUI ツールのように作業をバッチファイルで自動化する手法が使えないというデメリットがあるが，その反面，リアルタイムでプロセスや通信を確認することができるメリットがある．

また，コマンドラインに不慣れであっても使用できる点もメリットである．

特に Windows Sysinternals のツールは，プロセスの中から文字列を抽出したり，プロセスの一時停止が可能であったりと非常に高機能であり，さらにインターフェースが使いやすいため，CUI ツールには無いメリットが多い．

ツールによる調査手順としては，次のとおりとなる．

・自動起動設定の調査
・ネットワーク状態の調査
・プロセス，サービスの調査
・フォレンジックツールによる調査

10.5 クラウド上に保存された証拠データの取得

クラウド上に保存された証拠データをリモートアクセスによって取得する手法を提案する．

クラウド上のデータは証拠隠滅が容易なため，ライブフォレンジックを実施し，直ちに保全する必要がある．

攻撃者がオンラインストレージや Web メール等のクラウドサービスを利用しており，なおかつ，調査対象端末がネットワーク接続状態にある場合，クラウド上に保存され

ている証拠データに対してリモートアクセスを実施し，それをダウンロードして取得することが可能である．

クラウドサービスの調査方法としては，事前に確認済みの情報に加えて，調査対象端末のデスクトップ上のショートカット，「すべてのプログラム」の一覧，Web ブラウザのブックマーク及び履歴等を調査し，利用サービスを特定する．

リモートアクセスによる取得手順としては，次のとおりとなる．

・事前確認
・クラウドサービスの確認
・リモートアクセス
・証拠データの取得

10.6 暗号化データの保全，暗号鍵の取得

暗号化機能が有効になっている調査対象端末に対して，ライブフォレンジックを用いて証拠データや暗号鍵を取得する手法を提案する．

調査対象端末において暗号化機能が利用されていた場合，後のディスク解析が困難になるため，ライブフォレンジックによって暗号化データへの対処を講じなければならない．

稼働中の調査対象端末を確認した結果，暗号化ソフトウェア等の利用状況が判明した場合，暗号化データは復号状態となっているため，論理複写によるデータ保全を行う．

なお，暗号化ソフトウェアによっては，稼働中に復号キーの再取得が可能である．

また，ログオンユーザーが暗号化データへアクセスするために認証情報を入力している場合，認証中はマスターキーがメモリ上に存在するため，メモリフォレンジックによってマスターキーを取得することで暗号化データの復号が可能となる[11]．

しかし，メモリダンプを実施した場合であっても，その後のダンプデータ解析によって必ず復号キーを取得できるとは限らないため，必ず稼動状態での論理複写等を実施すべきである．

主な暗号化技術としては，次のもの等があり，ライブフォレンジックでのデータ保全を実施する必要がある．

・EFS
・BitLocker
・FileVault
・TrueCrypt

11. おわりに

本研究の結論として，調査担当者は積極的にライブフォレンジックを実施すべきである．

本研究では，ライブレスポンスやメモリフォレンジックの技術に着目し，ライブフォレンジックの有効性の検討及び具体的実施手法の提案を行った．

有効性の検討結果から，ライブフォレンジックには，マルウェアの検出，クラウド上のデータ取得や暗号鍵の取得等が可能になる大きなメリットがあり，標的型攻撃事案，組織犯罪事案，児童ポルノ事案等の具体的事案に関して有効であることを示した．

また，持込ディスクを作成するためのフローチャート及びライブフォレンジックを実施するためのフローチャートを新規に提案するとともに，具体的実施手法として，

・ライブレスポンスによる未知のマルウェア検出手法
・Windows Sysinternals による未知のマルウェア検出手法
・クラウド上に保存された証拠データの取得手法
・暗号化データの保全，暗号鍵の取得手法

等を整備して，ライブフォレンジックの指針として新たに提案することができた．

今後の課題としては，新しく開発されるツールや法律改正等の状況変化に対して，調査担当者が後れを取ることなく対応していかなければならない点があげられる．

したがって，調査担当者同士が今以上にお互いの情報交換を行い，技術力並びに対応力を高めていく必要がある．

最後に将来の展望として，様々な組織でライブフォレンジックの有効性が評価され，実施手法が整備されていくことで，多くのインシデント現場でライブフォレンジックが実践されるようになり，被害範囲の特定，攻撃者の割り出し等で今以上の優れた結果を出すことが期待できる．

参考文献

[1] デジタル･フォレンジック研究会 , “ 改訂版デジタル･フォレンジック事典 ” ,日科技連出版社,(2014)

[2] 特定非営利活動法人デジタル・フォレンジック研究会 , “ 証拠保全ガイドライン第 3 版 ” (オンライン) , 入手先〈http://www.digitalforensic.jp/eximgs/20130930gijutsu.pdf〉(参照 2014-10-14)

[3] *The Volatility Framework* (Website), available from〈https://code.google.com/p/volatility/〉(accessed 2014-10-14)

[4] 上原哲太郎 , ” デジタル・フォレンジックの動向と今後の趨勢および人材育成 ” (オンライン) , 第 10 回デジタル・フォレンジック・コミュニティ 2013 in TOKYO , 入手先〈https://digitalforensic.jp/wp-content/uploads/2014/06/16ebb6b5ac09776478fd9a5b02771cb4.pdf〉 (参照 2015-3-11)

[5] CERT , ” First Responders Guide to Computer Forensics ” , available from〈https://resources.sei.cmu.edu/asset_files/Handbook/2005_002_001_14429.pdf〉(accessed 2014-11-2)

[6] 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)

[7] Jason Luttgens, Matthew Pepe , ” Incident Response & Computer Forensics, Third Edition ” , McGraw-Hill Osborne Media , (2014)

[8] Michael Hale Ligh, Andrew Case et al , ” The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory ” , Wiley , (2014)

[9] *Windows Sysinternals* (Website), available from〈https://technet.microsoft.com/ja-jp/sysinternals〉 (accessed 2014-10-14)

[10] Mark Russinovich , Aaron Margosis , ” Windows Sysinternals Administrator's Reference ” , Microsoft Press , (2011)

[11] 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復号技術の開発 ” 情報処理学会, マルチメディア通信と分散処理研究会報告 , 2015-DPS-162(38)