アンチ・フォレンジックツールの痕跡検出方式に関する初期的検討

浦野 晃 †　　橋本 正樹 †　　辻 秀典 †‡　　田中 英彦 †

† 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
mgs125503@iisec.ac.jp

‡ 株式会社情報技研
103-0024 東京都中央区日本橋小舟町 3-1 クレイドル日本橋 3 階
contact2012@iit.jp

あらまし　証拠隠蔽やデータの改ざんなどを簡単に実行できるアンチ・フォレンジックツールと呼ばれるソフトウェアが多数インターネット上に公開されている．デジタル・フォレンジックにおいて，アンチ・フォレンジックツールがデータを操作したことを看破できなければ，重要な証拠の見落とし，間違った情報に基づく調査につながる．本稿では，こうした影響を軽減させるため，デジタル・フォレンジックの作業プロセスに関する基本モデルと，アンチ・フォレンジックツール実行の痕跡検出方式についての初期的検討を行う．

Preliminary Studies of Detection System for Anti-Forensics Tool Execution

Akira Urano†　　Masaki Hashimoto†　　Hidenori Tsuji†‡　　Hidehiko Tanaka†

†Graduate School of Information Security, Institute of Information Security
2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama, Kanagawa 221-0835, JAPAN
mgs125503@iisec.ac.jp

‡Institute of Information Technology, Inc.
3F Cradle Nihonbashi 3-1 Kobuna-cho, Nihonbashi, Chuo-ku, Tokyo 103-0024, JAPAN
contact2012@iit.jp

Abstract　Recently, many anti forensic tools can be downloaded from the Internet easily, and the social influences by these tools are increasing. In this paper, we show our preliminary studies of the basic model for digital forensic process and the detection system for anti forensic tool execution in order to make these tools' influence reduce.

1　はじめに

デジタル・フォレンジックの作業プロセスや専用ツールによる分析を妨害する手法をアンチ・フォレンジックという．現在，アンチ・フォレンジックを簡単な操作で行うことができる，様々なアンチ・フォレンジックツール (以下,「AFT」) がインターネット上に公開されている．一般に AFT は，電子的証拠の削除，改ざん，隠蔽等を行う機能を有している．さらに AFT に加えて，アンチ・フォレンジックを目的として開発されたツールではないが，その機能面からアンチ・フォレンジックの用途として用いた場合，フォレンジック作業プロセスに対して AFT と同様

な影響を及ぼすツールも多く存在する．例えば，暗号化ソフトや通信路秘匿化ツールである．

一方，フォレンジックを実施する側の立場から見ると，アンチ・フォレンジック手法が用いられたかどうかを高い精度で検出するためには，高度なスキルと適切なツールの選択が要求される．

AFT の存在あるいは AFT が実行された痕跡が検出することができれば，当該 AFT が影響を及ぼしうる箇所に注意を促すことができ，分析作業の精度を向上させることが期待できる．

本稿では，デジタル・フォレンジックの作業プロセスに，AFT 実行の痕跡検査を導入する意義について考察し，検出方式の概要について述べる．

2　研究の背景

本章では，アンチ・フォレンジックとデジタル・フォレンジックの作業プロセスについて概説し，AFT の影響について述べる．

2.1　アンチ・フォレンジックの概要

Harris[1] は，アンチ・フォレンジックを「any attempt to compromise the availability or usefulness of evidence in the forensic process」と定義している．フォレンジックの作業プロセスにおける証拠の可用性や有益性を損なうための試みがアンチ・フォレンジックに相当する．

アンチ・フォレンジックを実行するツールはアンチ・フォレンジックツール（本稿では「AFT」と表記）と呼ばれる．Rekhis ら [2] は，AFT を次の 6 つに分類した．

Encryption
: Encryption は，ファイル単位またはファイルシステム全体の暗号化を意味する．

Steganography
: Steganography は，データ隠匿技術の一種であり，画像ファイルなどに秘密の情報を隠して，第三者からその存在を認識できなくする技術である．ステガノグラフィを検出できたとしても，そこから秘密の情報を取り出すことは難しいと言われている．

Covert channels
: Covert channels は，ネットワーク上の隠蔽された通信路をいう．情報を隠蔽して送受信する方法には，一般の通信に直接割り込んで読み書きするタイプや，特殊な変調方式を用いるタイプがある．

Data hiding in storage space
: Data hiding in storage space もデータ隠匿技術の一種であるが，HDD のスラックスペースなどに情報を隠すことで，通常の OS のコマンドやプログラムから見えないようにする行為である．

Residual data wiping
: Residual data wiping は，痕跡を消去する目的で，一時的に生成されるファイルや復元される可能性がある削除データを完全に消去する行為である．

Tail obfuscation
: Tail obfuscation は，フォレンジック調査員を混乱あるいは誤解させる目的で，偽のメールヘッダを生成したり，タイムスタンプやログ情報を書き換えたりする行為を指す．

さらに，アンチ・フォレンジックを目的として開発されたツールではないが，アンチ・フォレンジックの用途で利用することができ，かつその結果がデジタル・フォレンジックへの作業プロセスへ十分な悪影響を与えるツールが数多く存在している．本研究では，これらのツールに対しても必要に応じて検査できるような実装を目指す．

2.2　デジタル・フォレンジックの作業プロセス

デジタル・フォレンジックの手順を理解するために，複数のプロセスに分けて解説される場合が多い．

NIST[3] によれば，収集 (Collection)，検査 (Examination)，分析 (Analysis)，報告 (Report-

ing) の 4 つのプロセスで構成されるとしている (図 1) .

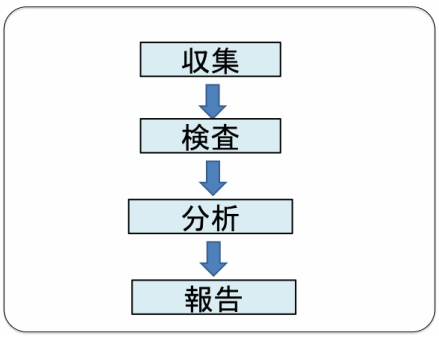

図 1: デジタル・フォレンジックの作業プロセス

2.3 AFT による影響

アンチ・フォレンジックがデジタルフォレンジックの作業プロセスに与える影響として，次のようなものが挙げられる.

1. 改ざんされた電子的証拠を真正な証拠として採用してしまう.
2. 電子的証拠の抽出に要する時間とコストを増加させる.
3. 電子的証拠の抽出そのものが不可能になる.

上記 2，3 では，他のデバイスを調査する，あるいは関係者への聞き取り調査といった別のアプローチを選択する判断の余地があるが，上記 1 ではアンチ・フォレンジックの影響に気づかず改ざんされた証拠を提出してしまう重大なリスクがある.

3 研究の目的

AFT の影響を軽減するには，AFT が影響を及ぼした箇所を特定することが効果的な対策である．しかし，巧妙にアンチ・フォレンジックが行われた場合，影響を受けた箇所を特定することは容易ではない．したがって，AFT が実行されたかどうかを検出できれば，フォレンジック調査員の負担を軽減できる可能性がある.

例えば，JPEG 形式の画像ファイルにメッセージを埋め込むことが可能なステガノグラフィーツールである○○.exe が検出された場合には，HDD 内の画像ファイルやメールに添付された画像ファイルの検査を慎重に実施する等である.

そこで，本研究では，従来のデジタル・フォレンジックの作業プロセスに AFT 実行の痕跡検査を導入することで，デジタル・フォレンジック調査の有効性向上を目的とする．特に本研究では，この提案の現実的適応に向けて，以下の 2 点について検討する.

検査の実行時間

AFT が実行されている PC が検査対象となる確率は，定量的な根拠はないが，直感的には未だそれほど高くないと考えられる．そのため，全ての検査対象の PC に対して，AFT 実行の痕跡検査の導入を考えると，痕跡検査自体の実行に時間がかかりすぎ，作業プロセス全体に悪影響を与えてしまう恐れがある．その影響を軽減するため，検査実行を自動化する必要があると考えられる.

AFT に関する継続的情報収集・解析活動

現時点においても AFT は多種多様なものが存在し，将来的にはその数量は増大し，その機能もより巧妙なものに発展することが予想される．現存する AFT に対しては，その入手先や実行時の挙動などについて広範囲に及ぶ情報収集と解析作業を継続して行い，可能な限りあらゆる AFT に対抗できるようなデータベースを構築することが望ましいと考える．これは，マルウェア検知のためのシグネチャ情報作成に類似している面がある.

しかし，単一の組織内のみで，データベースを維持，拡充していくことに人的リソースを割り当てることは容易ではない．そこで，外部組織を含めたフォレンジック関係者から構成されるコミュニティを形成し，その中で AFT に関して情報共有を可能にする枠組みを作ると，データベースの維持，拡充に要する負担を分担することができる．そのためには，共通した記述ルールの策定

が望ましいと考える．

また，AFT の多様性や潜在的個体数を考えると，全ての AFT を網羅することは困難が予想され，検査範囲を広げすぎると対応中のインシデントに関連性の薄い AFT も多数検出してしまうと思われる．これではフォレンジック調査員を混乱させるだけになってしまう．したがってデータベース構築の過程において，AFT の影響度や機能面などの観点から分類を行い，検査実行時に対応中のインシデントに適した検出範囲を設定できるような設計が要求されると考えられる．

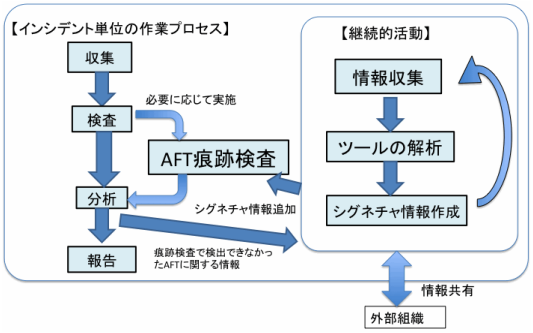

図 2: AFT 検査を取り入れた運用体制の例

これらを踏まえた上で，図 1 を拡張し，AFT 存在痕跡検査とシグネチャ作成，情報共有の仕組みを取り入れた運用体制の基本モデルを図 2 に示す．

本モデルでは，通常のフォレンジック作業プロセスとは別に，継続的活動として，AFT 検出のためのシグネチャ情報作成を行い，新たに作成されたシグネチャ情報は，適宜検査ツールに追加する．また，外部組織とも密接に連携し，常に最新の AFT に関する情報を共有し，さらに，通常のフォレンジック作業プロセスで痕跡検査により検出できなかった AFT，誤検出したツールをシグネチャ作成プロセスに反映させることで，AFT 痕跡検査の精度向上を図る．

4 AFT 検出方式の検討

本章では，前章で述べた基本モデルに求められる，AFT の実行痕跡を検出する方式について検討する．

4.1 AFT の実行に至るまでの痕跡

PC 利用者が AFT を実行するまでに至る段階はおおむね次のようになると推測できる．

第 1 段階 情報収集

Web ブラウザを用いて検索，あるいは雑誌等を通じて情報収集を行う．IP 電話やメール，インターネット上の質問掲示板などで質問することも考えられる．

第 2 段階 AFT の入手

インターネットを通じてダウンロードするほか，コンピュータ雑誌の付録，パッケージソフトの購入などの手段を用いて，AFT を入手する．プログラミングの知識があれば，ツールを自作，あるいは他者が公開したソースコードを参考に改良を加えるといったことも考えられる．

第 3 段階 AFT の実行

圧縮ファイルの解凍，インストーラーの起動を含め，AFT 本体が起動され，何らかのデータの作成，更新，削除などが行われる可能性がある．

第 4 段階 痕跡の削除

この段階まで至るかどうかは利用者次第ではあるが，当該 PC 利用者が悪意のある行為を実行しようとしていた場合，何らかの隠蔽工作を講じる可能性を十分考慮すべきである．また，痕跡を意図せず，純粋に不要になったため AFT を削除した場合も考えられる．このケースだと，情報収集した痕跡はそのまま残されていることが期待できる．

参考として，各段階において想定される痕跡の例を表 1 に示す．

表 1: AFT の実行に至る各段階での痕跡の例

段階区分	想定される痕跡の例
情報収集	ブラウザ検索履歴 質問掲示板への書き込み メール
AFT の入手	オンライン決済 ファイルのダウンロード
AFT の実行	解凍ソフトの利用 インストーラーの起動 レジストリの内容変更 アクティベーション ユーザ登録 API の呼び出し システムコール ファイル生成／変更 メールへのファイル添付
痕跡の削除	アンインストーラーの起動 レジストリの内容変更

ここで，PC 利用者が巧妙に AFT の実行の痕跡を削除していたと仮定すると，第 1 段階の情報収集による痕跡のみ検出できるかもしれない．しかし，このケースでは調査員の視点からは，PC 利用者が AFT に関する情報収集のみ行ったのか，AFT を実行したのち削除したのか区別できない．

したがって，以下のいずれかを検出する仕組みが必要である．

- AFT に関する情報収集
- AFT の実行

次節で，これらの痕跡を検出する方式の素案について述べる．

4.2 マルウェア検出を応用した検出方式の検討

本研究では，AFT 実行の痕跡を検出するために，既存のマルウェアの検出方式を応用する．すなわち，AFT の実行は，PC 利用者が意識的に行っているものであり，マルウェアと比較すると，前節で述べたとおり検出に利用できる痕跡は多いと推定される．

一般にマルウェア解析におけるシグネチャとは，実行ファイル内の特徴的なコードや振る舞いを意味するが，想定されるあらゆる痕跡を利用して AFT を検出するには，マルウェアを対象とした既存のシグネチャ情報記述ルールを拡張する必要がある．そこで，本研究において，AFT 検出の基礎とするために，記述ルールが公開されており，かつ拡張が可能なオープンソースのフレームワークとして，以下の 2 つを比較した．

- OpenIOC[4]
  OpenIOC は，Mandiant 社 [5] がマルウェアの脅威存在を検出するためのシグネチャ情報記述ルールを公開したものである．シグネチャ情報は XML 形式で記述される．シグネチャ情報の GUI 編集ツールとして IOCEditor，検査ツールとして IOCFinder が提供されている．一方で，実行できる環境は Windows に限られるという制約がある．

- YARA-project[6]
  YARA-project は，マルウェアの識別や分類するための研究コミュニティであり，シグネチャ情報の記述ルールと検査ツール，API を公開している．テキストエディタなどを用いてシグネチャを記述する必要があるが，正規表現を利用できるため柔軟な表現が可能である．また，Windows 以外でも，Linux，MacOSX 上でも実行できる利点がある．

なお，両者ともシグネチャ情報のデータベースは公開されていないため，自ら作成するか，研究コミュニティに参加し提供してもらう必要がある．これらは，マルウェアを対象としたものであり，AFT を対象とした記述ルールやシグネチャ情報ではない．よって，本研究に利用するためには，既存の記述ルールをベースにして AFT 検出に最適化したルールを設計し，そのルールに従ってシグネチャ情報を作成する必要がある．

しかし，既存のフレームワークを活用することで検出ツール自体を作成する必要はなく，シ

グネチャ情報の記述ルールとシグネチャ情報に焦点を絞った評価が容易に実施できる利点がある．

本研究では，記述ルールの拡張性，編集ツールの使いやすさを評価し，OpenIOC を用いて今後の研究を進めることにした．

5　期待される成果と今後の方針

本研究は外部組織との連携が前提となっているが，AFT のシグネチャ情報のアップデートが効果的に機能することで，AFT の検出精度が向上し，デジタル・フォレンジックの作業プロセス全体の信頼性向上に貢献できると考える．

今後は，OpenIOC のフレームワークをベースにして，AFT 実行の痕跡検査のためのシグネチャ記述ルールを設計し，実在の AFT を解析してシグネチャ情報を作成し，評価試験を行う予定である．

6　まとめ

本稿では，アンチ・フォレンジック手法がデジタル・フォレンジックの作業プロセスに与える影響を軽減させるための体制構築について考察した．また，分析作業に先だって AFT 実行の痕跡検査を行うことで，一定の効果が期待できることを述べた．

今後の研究では，フォレンジックの現場で活用できるよう実行速度や導入しやすさ，他組織との情報共有の具体化についても考慮しつつ進めていきたい．

参考文献

[1] Ryan Harris. 2006. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. Digit. Investig. 3 (September 2006), 44-49. DOI=10.1016/j.diin.2006.06.005 http://dx.doi.org/10.1016/j.diin.2006.06.005

[2] Slim Rekhis and Noureddine Boudriga. 2010. Formal Digital Investigation of Anti-forensic Attacks. In Proceedings of the 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE '10). IEEE Computer Society, Washington, DC, USA, 33-44. DOI=10.1109/SADFE.2010.9 http://dx.doi.org/10.1109/SADFE.2010.9

[3] Karen Kent, Suzanne Chevalier, Timothy Grance, and Hung Dang. 2006. SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Technical Report. NIST, Gaithersburg, MD, United States.

[4] The OpenIOC Framework, Mandiant Corporation (online), available from `http://www.openioc.org` (accessed 2013-08-10).

[5] Mandiant® - Detect. Respond. Contain, Mandiant Corporation (online), available from `http://www.mandiant.com` (accessed 2013-08-10).

[6] yara-project - A malware identification and classification tool - Google Project Hosting (online), available from `http://code.google.com/p/yara-project/` (accessed 2013-08-10).