ユーザ調査によるマルウェア動的解析タスクの明文化

山岸 伶 [1, a)] 藤井 翔太 [1] 佐藤 隆行 [1]

概要：サイバー攻撃対策において，マルウェアの動的解析は効率的な監視や対処を実現する重要な業務の一つである．一方で，動的解析業務における解析項目は体系的には明文化されておらず，分析官の知見に依存している部分もあり，解析における問題点の洗い出しや解析者の育成の障壁となっている．このような背景を受け，本研究では暗黙知となっている解析時のタスクの明文化や問題点の洗い出しを目的としたユーザ調査を実施した．当該調査では， 3 名の解析者に対して動的解析を依頼し，実施したタスクやその問題点に関してヒアリングを実施した．調査の結果， 事前の OSINT 調査，表層解析，および実際の動的解析で構成される 40 種類のタスクを抽出し，当該タスク実施上の 7 個の問題点を明らかにした．加えて，解析者の効率的な育成に向けた知見を得るため，経験の異なる解析者の実施タスクの違いを分析した．分析の結果，経験の長い解析者はマルウェアファミリや TTPs を考慮し，検体自体やその挙動を一般化した視点で解析することを知見として残した．

キーワード：セキュリティ運用，マルウェア動的解析，ユーザ調査

Clarification of Malware Dynamic Analysis Tasks by User Investigation

Rei Yamagishi[1, a)]　Shota Fujii[1]　Takayuki Sato[1]

Abstract: A malware dynamic analysis is one of the most important works to ensure efficient monitoring and incident responses. However, analysis items in the analysis are not systematically documented. Hence, analysts rely on their own knowledge, and this becomes the barriers which are the identification of the problems in analysis and the training of the analyst. In this research, to clarify the tasks and problems in a dynamic analysis, we conducted a user investigation. In the investigation, we requested the analysis to three analysts and conducted hearings about the tasks and problems. As the result, we extracted forty tasks and clarified seven problems. In addition, to obtain the knowledge for efficient training, we consider the difference of the tasks between the analysts. As the result of the considerations, we found that long-experienced analysts analyze not only a malware and its behavior but also generalized information such as the malware family.

Keywords: Security Operation, Malware Dynamic-Analysis, User Survey

1. はじめに

サイバー攻撃対策において，マルウェア解析はインシデントの検知や対処をサポートする重要な業務の一つである．例えば，MITRE は，マルウェア解析がサイバー攻撃に対処する組織 SOC（Security Operation Center）の業務の一つであり，効率的な監視や対処を実現に貢献すると述べている [1]．また，JNSA のセキュリティ対応組織（SOC/CSIRT: Computer Security Incident Response Team）の教科書では，インシデント発生後の深堀分析の一つとして，マルウェアの検体解析を挙げている [2].

マルウェア解析手法の一つにマルウェアを実行してその挙動を分析する動的解析が存在している．他の手法にファイル名や種別といった簡易情報を分析する表層解析，マルウェアのコードやアセンブリ言語を分析する静的解析が存在するが，動的解析には比較的低コストで挙動や通信先といった有用な情報を得られる点にメリットが存在する．

動的解析では解析者が手動で分析を実施しており，分析には専門性が求められる．専門性の習得のため，様々な既存の文献や書籍が提供されているが，サイバー攻撃に対処する現場でどのように動的解析が実施されているかの情報は十分に提供されておらず，明らかになっていない．これに伴い，動的解析で実施する作業（タスク）だけでなく当該タスクの問題点も明文化されておらず，解析者の効率的な育成や解析者の障壁となっている．

こうした背景を受けて，本研究では，解析者や各組織内の暗黙知となっている解析者の実施するタスクの明文化を目的とする．目的の実現のため，解析者の動的解析を録画し，録画した解析の様子を振り返りながらタスクやその問題点に関するヒアリング調査を実施した．加えて，実施したタスクを比較することで，経験の異なる解析者のもつ観点の違いを分析した．

本論文における貢献を以下に示す．

- 3 名の解析者の動的解析にヒアリングを実施し，解析者の実施する 40 種類のタスクを抽出，明文化した．
- ヒアリングを通し，動的解析タスク実施上の問題点を

1 株式会社日立製作所 Hitachi, Ltd.
a) rei.yamagishi.ss@hitachi.com

7 個明らかにした．特に，タスクが明確になっていない点が問題であることを明らかにし，タスク遂行をサポートする手順書等のツールの開発が求められていることを示した．また，これは本研究で取り組むタスクの明文化の有用性を示す結果でもあった．

- 抽出したタスクを比較することで，経験の長い解析者は，(a)得られた情報をマルウェアファミリなどの一般化した視点で分析すること，(b)多角的に検体が動作しない可能性を検討することを明らかにした．加えて，これらの観点をもつよう教育的に促すことの重要性を示した．

2. 研究背景

本章では，研究背景とし，マルウェアの動的解析の現状や関連研究を整理する．最後に背景を受けて研究課題を設定する．

2.1 マルウェアの動的解析

マルウェアの動的解析では，解析者が解析環境内で観測対象のマルウェア（以降，検体と表記）を動作させ，ログ中に含まれる挙動や解析環境の様子を観測し分析する．動的解析では静的解析と比較して低コストで解析可能であり，検体の挙動や通信先といった情報を入手可能である．こうした情報は有用であり，マルウェア感染影響の調査や組織内からの通信遮断といったインシデントへの対応業務に活用される．その一方で，実際の動的解析業務ではどのようなタスクが実施されているのか明らかになっていない．

先述した通り，マルウェアの動的解析に関するタスク一つ一つに関しては，様々な既存の文献や書籍が提供されている [3-5]．例えば，Learning Malware Analysis [4] では，プロセスやネットワークトラフィックの調査方法が説明されている．しかし，これらの様々な既存の文献や書籍は，体系的にどのようなタスクが実施されるのかといった視点を含んでいない．

2.2 関連研究

関連研究として動的解析や SOC 業務に関する実態の調査やタスクの明確化に取り組んだ研究が挙げられる．

Wagner ら [6] は，未知のマルウェアファミリの動作の分析支援システムの要件を検討するために，当該タスクに関する文献の調査や専門家に対する半構造化インタビューを実施した．ただし，マルウェアの動的解析全般でなく特定目的での業務に限定している．

Kokulu ら [7] は，SOC 業務に関する固有の問題点が組織内部で閉じており明らかになっていないことを指摘し，SOC の分析官とマネージャに対し半構造化インタビューを実施し，問題点を明らかにした．Zhong ら [8] は SOC のトリアージタスクの負担を削減するため，トリアージのタスクをトラッキングし，タスクのオートマトンを作成するシステムを提案した．鐘本ら [9] は，SOC のアラート対応業務の暗黙知を明らかにするため，アナリストの行動を記録し共通部分を取り出すことでタスクを抽出した．いずれの研究も広い視点で SOC を対象としているが，動的解析における具体的なタスクを対象としていない．

金井ら [10] はソフトウェア開発現場でセキュリティを妨げる要因を明らかにするため，デベロッパーとマネージャのセキュリティ意識をオンラインアンケートで調査，分析した．一方で，開発現場を対象としており，セキュリティ運用の調査とは対象が異なる．

2.3 研究課題

こうした研究背景を受け，以下の 3 つの研究課題（以下，RQ と表記）を設定する．本研究では各 RQ への回答を目的として調査および分析を実施する．

RQ1: 動的解析で解析者はどのようなタスクを実施するか．
RQ2: 動的解析のタスク遂行時にはどのような問題点が存在するか．
RQ3: 経験の異なる解析者間でタスクは異なるか．また，どのような観点で異なるか．

3. ユーザ調査

本章では，本研究で実施したユーザ調査について，調査方針，調査手順，調査で利用した解析シナリオ，調査結果の順で述べる．

3.1 調査方針

RQ を解明するため，解析者を実験協力者として募り，ユーザ調査を実施する．別のアプローチとして，関連研究 [8, 9] のような，解析動作をシステム的にトラッキングすることによる調査も考えられるが，どのようなタスクがあるのか不明瞭な現状においてはトラッキング対象を絞り込むことが困難である点や RQ2 のタスク遂行時の問題点の調査といった解析者の思考をヒアリングしたいモチベーションからユーザ調査を選択した．

ユーザ調査では，タスクの確認，ヒアリング，事後分析を実施し，RQ を解明することとした．RQ1 を解明するため，実験協力者に動的解析の録画を依頼し，録画後に実験協力者と実験実施者で映像を確認しながら解析タスクを確認する．次に，RQ2 を解明するため，解析タスクの問題点に関するヒアリングを実施する．最後に，全実験協力者のタスクを比較することで RQ3 を解明する．

実験協力者の募集に際して，マルウェアの動的解析の業務経験がある解析者に直接依頼した．動的解析の業務経験を募集の条件としたのは，動的解析の業務経験がない実験協力者はタスクに関する暗黙知も持たず，本研究のモチベーションに合致しないためである．また，RQ3 を解明するため，解析歴が異なるメンバに対して，調査への協力を依頼した．

3.2 調査手順

本節では，図 1 を用いて，調査手順に関して説明する．図

1 の左の列で示す通り，実験手順は事前準備，解析実施，ユーザ調査，事後分析，およびデータ承諾のフェーズから成り，各フェーズは全て同日に実施した．次に，図 1 の右側に示す各フェーズの具体的な手順を説明する．また，図 1 では実験協力者と実験実施者がそれぞれ/共同で行う作業がわかるように 2 列に分けて示す．なお，実験実施者は著者ら 2 名から成る．

(1)　実験説明

事前準備として，実験実施者が実験協力者に対して実験の目的や手順について説明し，実験参加の合意を得た．

(2)　アンケート配布

実験協力者の属性把握を目的として，アンケート紙を配布し，実験協力者に記入を依頼した．アンケート内容は名前，所属，動的解析業務の従事歴，およびセキュリティ関係の業務や研究の従事歴とした．

(3)　解析実施

実験協力者が自身の解析環境で解析シナリオ(3.3 節で詳述）に基づいて検体を実行し，画面を録画しながら解析を実行した．また，過度に解析負担が増加する場合や組織のノウハウに抵触する場合には録画を停止してもよいことを説明した．その場合，(4）のヒアリング時に，録画停止時の活動を可能な限り補足してもらうよう依頼した．

(4)　解析タスクの確認

(3）で録画したビデオを実験実施者と実験協力者で確認しながら，実施した解析タスクやその流れをテキスト形式に抽出した．

(5)　タスクに関するヒアリング

(4）のテキストを参照しながら，各タスクの実行理由を半構造化インタビューの形式でヒアリングを実施した．具体的には，解析の流れを振り返りながら，タスクごとに後述する 4 つの観点の質問を行い，その回答を得た．なお，質問の中で，(4）の段階でタスクの実行理由を実験協力者が述べている場合，(5)で繰り返し質問することは避けた．また，実験実施者は，回答内容に関して不明点があった場合，追加の質問を行い，対話形式で調査を深めた．

質問内容

- 当該タスクは有効であったか．
- なぜ当該タスクを実行したか．
- 当該タスク実施にあたり、困ったことはあったか．
- その他，何か懸念事項等はあるか．

(6)　タスク一覧表の作成

(4）で抽出したテキスト形式の解析タスクは，実験協力者それぞれの表現や説明に依存しており，統一的な形式となっていない．これらのタスクを統一的に扱うため，解析タスクの項目を作成し，各実験協力者が項目に該当するタスクを実施したか判定した．具体的な手順は以下の通りである．

(6-a)　タスク項目の作成

まず実験実施者 2 名それぞれが，(4）でとったテキスト形式のメモからタスクを抽出し，タスク一覧表の項目を作成した．次に，それぞれが作成した項目を 2 名で確認し，表現が共通するものをまとめることで，一つの解析タスク一覧表を作成した．

(6-b)　タスク実施の有無の判定

実験実施者 2 名それぞれが，再度，実験協力者の解析を確認し，(6-a）で作成したタスク項目を実行したか否かの判定を行った．例えば，実験協力者 A が項目「レジストリの確認」を実行した場合 1，実行しない場合は 0 とし，これをすべての項目，すべての実験協力者分繰り返した．実験実施者 2 名がそれぞれ判定を行った後，一覧表を持ち寄り，各実験協力者の判定に対し Cohen's kappa 検定を実施し，一致度を確認した．この際，カッパー値が 0.61 未満であれば，不一致とみなし，再度タスク実施の有無の判定を実施した．カッパー値が 0.61 以上の場合は，おおよその項目の判定は一致したとみなし，残りの一致しない項目に関して議論して統一させた．なお， Kokulu ら [11] がカッパー値 0.61 以上の場合に 2 群はかなり一致していると定義しており，これを参考にし，閾値を 0.61 以上とした．

(7)　内容の確認・合意

(6）で作成した一覧表を実験協力者に展開し，内容に差異がないことを確認した．併せて，匿名化処理したうえで実験データとして活用することの合意を得た．これは，動画停止中に実施したタスクを伝えきれていなかった場合や，公開により実験協力者が不利益を講じる場合を懸念したためである．

3.3　解析シナリオ

3.2 節の（3）解析実施で実験協力者に依頼した解析のシナリオについて，解析の目的，解析検体，および解析報告書に分けて述べる．

3.3.1 解析の目的

RQ を解明すべく，検体の挙動を明らかにすることを目的とし，解析対象の検体に対して通常の業務と同様の動的解析を実施することを依頼した．

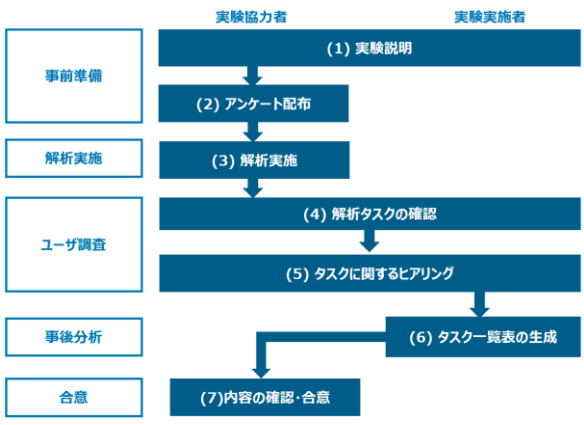

図 1　ユーザ調査の手順

Figure 1　The Flow of User Survey

3.3.2 解析検体

解析を依頼したマルウェアは, 情報窃取を行う Formbook（名称は malpedia [12] に登録されているもの）マルウェアの一検体であった．この検体は，実際の実験協力者の動的解析業務に近づけるため，実験協力者の組織に届いたマルウェアを選定した．

3.3.3 解析報告書

実験協力者の動的解析業務の再現を目的とし，解析結果を解析報告書としてまとめることを実験協力者に依頼した．この報告書は通常の業務のフォーマットで利用するものに従い, ファイル名, アイコン, 通信先情報等の検体情報や，検体および解析の流れといった内容を含むものであった．

3.4 調査結果

本節では調査結果として，実験協力者に関するアンケート結果，タスク一覧表，およびタスク実施上の問題点をそれぞれまとめる．

3.4.1 実験協力者に関するアンケート結果

表 1 に，実験協力者に関するアンケートの結果を示す．表 1 が示す通り，本調査では 3 名の実験協力者に調査を実施した．便宜上，3 名を以降 P1-3 と表記．3 名とも同一組織の所属であり，動的解析業務の従事歴は最長 4 年で最短 1 年未満，セキュリティ関係の業務や研究の従事歴は最長 7-10 年で最短は 1 年未満であった．

3.4.2 タスク一覧表

表 2 に，タスク一覧表を示す．表 2 が示す通り，3.2 節の（6-a）タスク項目の作成によって 40 種類のタスクを抽出することができた．タスクは，OSINT 調査により検体情報をあらかじめ収集する事前調査，検体の情報を確認する表層解析, および実際の動的解析の 3 フェーズに分類できた．40 種類のタスクのうち，29 種類が事前調査，1 種類が表層解析，10 種類が動的解析に属することが分かった．

事前調査と動的解析はさらに細かく分類することができた．事前調査は, VirusTotal [13] といったレピュテーションサイトで検体に関する情報の検索，Google [14] を用いた Web 検索エンジンでの検索，Twitter [15] などの SNS を用いた検索，解析情報を提供するブログ記事の閲覧，ANY.RUN [16] や JoeSandbox [17] といったオンラインサンドボックスでの解析結果の確認, Shodan [18] などを用いた通信先確認サービスで通信先の特徴を確認に分類できた．また，動的解析は通信のログを分析，端末のログを分析に分類できた．

表 1 実験協力者の情報

Table 1 Information of Participants in Our Research Study.

実験協力者 ID	動的解析業務の従事歴	セキュリティ関係の業務や研究の従事歴
P1	4 年	7-10 年
P2	2 年	5-7 年
P3	1 年未満	1 年未満

各タスクについては表 2 の 3 列目にまとめた．なお，21 行目の” TTPs を確認（ATT&CK [19] マッピング）”にある TTPs（Tactics, Techniques, and Procedures）は攻撃者の戦術，戦法，行動を表す攻撃のパターンを示す情報であり，例えばスピアフィッシングやプロセスインジェクションが攻撃者の戦法にあたる．TTPs は IP アドレスやハッシュ値といった情報と比較し攻撃者による変更が困難であるため，分析にとって有用である [20]．また，ATT&CK はこの TTPs を体系化したナレッジベースのデータベースである．

3.2 節の（6-b）タスク実施の有無の判定で，各実験協力者が当該タスクを実施したか否かを判定し，表 2 の 4-6 列目にまとめた. なお, ここでは実施した場合に 1 と記載し，実施していない場合に 0 と記載した. なお, P1 が実施したタスクは 33 種類，P2 が実施したタスクは 33 種類，P3 が実施したタスクは 21 種類であった．

各タスクを実施した実験協力者の割合を実施率として表 2 の 7 列目にまとめた．なお，100%の実施率であったタスクが 19 種類，66.7%の実施率であったタスクが 9 種類，33.3%の実施率であったタスクが 12 種類であった．

本節の残りで，抽出したタスクに関して取り上げ，タスクの詳細を補足する．実験協力者はレピュテーション共有サイトで「投稿日を確認」（表 2 の 2 行目）した．P2 は中でも初投稿日に着目し，解析記事を探す際に活用した．具体的には，初投稿日と記事の書かれた日を比較し，参考にする解析記事の選定に用いた. P2 はレピュテーション共有サイトで「strings を確認」（表 2 の 4 行目）し，マルウェアの内容を把握していた. 具体的には, adobe のコピーライトの文字列が存在していることから pdf の埋め込みがあることを懸念した．実験協力者はレピュテーション共有サイトでの「detection（検知数・名）を確認」（表 2 の 5 行目）を通して，マルウェアファミリを推定した．レピュテーション共有サイトでの検知名はベンダ毎に命名規則や示すファミリが異なっているにもかかわらず, Formbook というファミリ名を全実験協力者が指定した．

実験協力者はオンラインサンドボックスで「プロセスの関係性を確認」（表 2 の 14 行目）し，プロセスの親子関係や各プロセスの主な挙動を確認した．P1 は JoeSandbox の提供するプロセスと主な挙動の可視化グラフを挙げ，当該タスク遂行時に有用だと述べた．P1 と P2 は，オンラインサンドボックスで「スクリーンショットを確認」（表 2 の 17 行目）したが，動画形式でのスクリーンショットが，タイミングも把握可能であることから有用であると述べた．

表 2　実験協力者のタスク一覧表

Table 2　The List of Paticipants' Tasks.

フェーズ	分類	タスク	タスク実施者内訳			実施率 [%]
			P1	P2	P3	
事前調査（OSINT 調査）	レピュテーション共有サイトで検索	投稿日を確認	1	1	1	100
		ファイル種別を確認	1	1	0	66.7
		コミュニティを確認	1	1	1	100
		strings を確認	0	1	0	33.3
		detection（検知数・名）を確認	1	1	1	100
	web 検索	ハッシュ値で検索	1	1	1	100
		ファミリ名で検索	1	1	0	66.7
		ドメイン名の売却状況を検索	1	0	0	33.3
		ファイル名で検索	1	0	1	66.7
	SNS 検索	ハッシュ値で検索	1	0	0	33.3
		ファミリ名で検索	1	0	0	33.3
	解析記事	ファミリの挙動を確認	1	1	0	66.7
	オンラインサンドボックスで挙動を確認	インポートされている API を確認	0	1	0	33.3
		プロセスの関係性を確認	1	1	1	100
		シェルコマンドを確認	1	1	1	100
		ファイル操作を確認	1	1	1	100
		スクリーンショットを確認	1	1	0	66.7
		通信先を確認	1	1	1	100
		解析回避に関する挙動の確認	0	1	0	33.3
		TTPs を確認（ATT&CK マッピング）	0	1	0	33.3
		オンラインサンドボックス間で結果に差異がないか確認	1	1	0	66.7
		レジストリ操作を確認	1	1	1	100
		オンラインサンドボックス上で二次検体に対して上記のタスクを再帰的に実施	1	1	1	100
	通信先確認サービス（shodan 等）で通信先の特徴を確認	レピュテーションを確認	1	1	1	100
		稼働状況を確認	1	1	1	100
		ポートの開閉状況を確認	1	1	1	100
		WHOIS 情報を確認	1	0	0	33.3
		DNS 情報を確認	1	0	0	33.3
		同じドメインに紐づく IP アドレス, 同じ IP アドレスに紐づくドメインを確認	1	1	1	100
表層解析	表層解析	ファイルの種別を確認	0	0	1	33.3
動的解析	通信のログを分析	発生した通信の確認	1	1	1	100
		DNS リクエストが事前調査と一致するか確認	1	1	0	66.7
	端末のログを分析	ファイル操作を確認	1	1	1	100
		プロセスの挙動を確認	1	1	1	100
		ネットワークイベントを確認	1	1	1	100
		API 呼び出し履歴を確認	0	1	0	33.3
		レジストリ操作を確認	1	1	0	66.7
		シェルコマンドを確認	1	1	0	66.7
		メモリダンプを確認	0	1	0	33.3
		二次検体に対して、上記のタスクを再帰的に実施	1	1	1	100
実行タスク合計数			**33**	**33**	**21**	

通信先確認に関して，実験協力者間で調査手法に差異が見られた．具体的には，Shodan やその他ドメイン状況確認の web サービスを利用したり，当該ドメインをキーに Google 検索を実施したり，手法や利用サービスは様々であった．一方で，dig コマンドや whois コマンドを用いた直接的な接続による調査は実施せず，代行サービスを用いる点は共通していた．また，「稼働状況を確認」や「同じドメインに紐づく IP アドレス，同じ IP アドレスに紐づくドメイ

ンを確認」では，通信先として取得できた短縮 URL の現在の状況も確認した．現在の通信先の情報を正しく把握することは，動的解析後に通信先遮断といった対応の判断に有用であると P1 は述べた．

3.4.3 タスク実施上の問題点

表 3 では（5）でヒアリングしたタスク実施上での問題点をまとめた。問題点は 7 個であり，分類をすると，事前調査に関するもの 4 個，動的解析に関するもの，報告書作成に関するもの，解析者のスキルに関するものがそれぞれ 1 個であった．また 表 3 の 3 列目に指摘した実験協力者の識別子をまとめた．

4. 分析結果

本章では，3.4 節で得た実験結果を分析し RQ に対する回答をそれぞれ述べる．

4.1 RQ1: 動的解析で実施されるタスクについて

RQ1 に関連して，ユーザ調査の結果，表 2 で示す 40 種類のタスクが存在した．実験協力者は共通して，オンラインサンドボックスを中心とした OSINT の事前調査を実施し，次に実際の動的解析を実施した．

OSINT 調査として，実験協力者は主に侵害の痕跡を示す IoC（Indicator of Compromise）の情報や，挙動に関する情報を調査した．またヒアリングでは，動的解析で得られる情報の事前入手や動的解析環境で検体がうまく動作しない可能性の検討を目的として，実験協力者が OSINT 調査を実施することが明らかになった．通常の環境で検体がうまく動作しない場合，特定の条件で動作させたり動的解析でなく静的解析を実施したりする必要がある．そのため，実験協力者は，通信先の死活状況や，オンラインサンドボックス間で得られた情報の差異，検体の持つ検知回避に関する挙動や機能の有無といった観点で情報を収集した．また，一部の実験協力者は，検体だけでなくマルウェアファミリ（Formbook）の特徴や代表的な挙動も把握し，事前情報を入手した．

表 3　タスク実施上での問題点

Table 3　The problems in Tasks of Dynamic Analysis.

分類	問題点	指摘者
事前調査（OSINT 調査）	OSINT 調査時に英語以外の情報である場合に把握が困難	P1
	OSINT 調査はどこまで深く調査するかの判断が困難	P1
	情報の食い違いがあると深堀が必要になりコスト増加	P2
	何をしていいのかわからなくなるときが存在（手順書が欲しい）	P3
動的解析	ログの横断的に分析・検索することが困難	P1
報告書作成	自信のない分析結果の報告が困難	P1
解析者スキル	静的解析のスキルがないと動的解析で情報を得られない場合，解析で得られる情報が不十分	P1

動的解析で，実験協力者は OSINT 調査との違いを意識しながら，通信ログと端末ログを調査した．なお，今回の検体は既に通信先が停止しており，OSINT 調査で判明していた実行形式のファイルが入手できなかった．そのため，実験協力者は，OSINT 調査で得られた情報がすべて得られない理由（今回の場合は通信先の停止）を確認することが主な分析内容であった．この原因が分かった上で，他の異常な痕跡を調査するために，sysmon を用いた端末ログ分析やパケットの分析を実施した．また，OSINT 調査では実施した観点でのタスクを動的解析では実施しなかった場合もあった．

4.2 RQ2: タスク実施上の問題点について

RQ2 に関連して，ヒアリングを通して 7 個の問題点を抽出した．問題点は動的解析時よりも，事前調査の OSINT 調査に多く見られた．OSNT 調査に関して，P3 は「OSINT 調査はどこまで深く調査するかの判断が困難」，P1 は「何をしていいのかわからなくなるときが存在(手順書が欲しい)」と述べ，タスクの種類や調査の深さといったタスクに関する問題点をあげた．タスクの種類に関しては，本研究で取り組むタスクの明文化の有用性を裏付ける結果であり，タスクの手順書といったツールによる支援が必要だと考えられる．また，調査の深さに関連して，P1 は調査の目的を意識し調査継続の判断を心がけていても，調査に過不足があると述べた．したがって，タスクの種類だけでなくその十分性についても明文化し，解析者を支援する手法を検討することが今後の課題として残る．

動的解析に関する問題点として，「ログの横断的に分析・検索することが困難」という点が挙げられた．これは動的解析で通信ログや端末ログを横断的に分析していたが，同一 IP アドレスの検索をそれぞれのログ分析ツールで実施していたことに起因する．解決策として，SIEM（Security Information and Event Management）といったログ分析管理ツールとの連携が挙げられる．

解析者スキルに関連する問題点として，P1 は「静的解析のスキルがないと動的解析で情報を得られない場合，解析で得られる情報が不十分」と述べた．P1 は動的解析だけでなく静的解析の実施も必要であり，両方のスキルを研鑽するのが望ましいとしたうえで，実際の業務では動的解析だけでは不十分な場合，得意な専門家に静的解析を依頼しチームとして活動すると述べた．加えて，P1 はその場合，静的解析への引継ぎを意識した OSINT 調査や報告が必要だと補足した．したがって，動的解析と静的解析の両スキルでの教育や，異なるスキルをもつ人材が補完しあえる業務体制が重要である．また，動的解析から静的解析に引き継ぐ際のタスクや情報を明文化することが今後の課題として挙げられる．

4.3 RQ3: 経験による実施タスクの違いについて

RQ3 に関連して，経験の異なる解析者の実施したタスク

を比較することで，タスクの傾向に違いが存在していたことが確認できた．特に P3 はセキュリティ業務や動的解析の経験が浅く，ヒアリングでも「何をしていいのかわからなくなるときがあった」と回答していた．以降では，動的解析業務やセキュリティ関係業務の長さから，P1，P2 を経験者，P3 を初心者として，両者のタスクの共通点や差異について考察する．プロセス，通信先，コマンド，レジストリの確認といった挙動に関する調査は 3 名とも実施しており，報告書作成に関する情報は十分収集していた．一方で，P1 と P2 は検体の一般化や多角的に検体が動作しない可能性の検討を行っていた．

検体の一般化に関して，P1 と P2 はマルウェアファミリ（Formbook）をキーとした Google 検索や当該ファミリの解析記事の調査を実施し，検体の挙動の把握をしていた．また，P2 は TTPs を考慮した情報収集を実施していた．具体的には，Formbook が情報窃取を目的とし，メーラやブラウザの情報を窃取する機能を有すると把握し，検体の実行時にメーラやブラウザを立ち上げておくといった工夫が見られた．

多角的な検体が動かない可能性の検討では，オンラインサンドボックスでの解析結果の比較やマルウェアの解析回避機能の有無といった観点で分析をしていた．解析環境が異なる場合に異なる挙動をするマルウェアが存在するため，オンラインボックスでの解析結果の比較することでこの観点での情報収集を実施した．マルウェアの解析回避機能の有無に関しては，JoeSandbox に存在する解析回避のシグネチャの確認や Formbook が TTPs の観点（ATT&CK の defence evasion の tactics など）でどういった検知回避を行うマルウェアなのかを調査していた．一方で，通信先の状況確認し，二次検体のダウンロードが可能かという観点での検討はすべての実験協力者が実施していた．

また，P1 と P2 は，動的解析のタスク実施時に，異常なレジストリ操作がないか，異常な通信がないかを確認したというように，タスクを実施しながら「異常」を確認していることがヒアリングで判明した．異常に関して深堀したところ，P2 は解析を重ねるうちに Windows システム固有の通信等がわかり，解析環境固有の通信に関する情報と組み合わせることで異常が判明すると述べた．こうした解析者の感じる異常と正常を言語化することが今後の課題であると考える．

5. 議論

本章では，調査結果から得た提言事項と本調査の制約および本研究の倫理について議論する．

5.1 提言事項

本節では，ツール的観点と教育的観点から提言事項を述べる．

ツール的観点に関しては，解析タスク実施を明確化し，サポートする手順書等のツールの開発が求められている．実験協力者へのヒアリングで P3 が「何をしていいのかわからなくなるときがあった」と述べ，主に OSINT 調査の際にタスクを整理することによる支援を求めていた．また，タスクを整理し示すことは P1 が「OSINT 調査はどこまで深く調査するかの判断が困難」と述べていた問題点の部分的解決にもつながると考える．また，こうしたタスクを明らかにして支援してほしいといった要望は，本研究の有用性を示しているとも考えている．

教育的観点では，解析に慣れてきた解析歴 1 年程度の実験協力者には，マルウェアファミリや TTPs といった観点での検体情報の一般化や多角的に検体が動作しない可能性の検討を教育的に促すことが重要であると考える．特に検体情報の一般化は，P2 が述べたオンラインサンドボックス間で情報の食い違いがあるときの検体情報の深堀や，検体単体の情報だけでは十分な情報が得られなかった場合の対応の一手法として重要であると考える．

5.2 制約

本研究では，主に実験協力者の募集に関して，解析検体や環境に関して，ユーザ調査手法に関しての 3 点が制約として挙げられる．

実験協力者の募集に関しては，人数の少なさや所属組織の偏りが挙げられる．実験協力者が少ないことで，一人ひとりに深くヒアリングできたことは良いが，3 名は少なく実験結果を一般的にとらえがたい．また，3 名とも同じ組織に所属しているため，組織固有の要因でタスクが限られた可能性がある．

2 点目は解析検体や解析環境に関して，その数が限られていたことである．検体の数や種別が変化すると，検体の挙動が変化し，解析者の行うタスクが変化することは十分考えられる．また，同様に解析環境が変われば扱うツールや得られる情報が変化するため，解析者のタスクにも影響を与える．こうした，検体や環境の変化に伴うタスクの変化をとらえるのは今後の課題であり，本調査の制約となる．

最後に，ユーザ調査手法に関して，実験協力者の認識に基づくタスク調査やヒアリングであるため，実験協力者が認識していないことは調査できない点にある．例を挙げると，4.2 節で述べた異常の確認といった実験協力者でも言語化しがたい場合やそもそもタスクや問題点としてとらえられていない場合が考えられ，制約となる．

5.3 研究倫理

本研究ではユーザ調査にあたり個人を特定可能な情報として，実験協力者の氏名とメールアドレスや本人の声や動作が入った録画映像を収集した．実験協力者には，実験の説明をしたうえで，これらの情報を組織内で管理することに同意を得ている．また，本稿では匿名化処理をしてデータを記載している．

加えて，本研究では解析者の秘匿したいノウハウを開示

することで実験協力者に不利益を被ることが想定される．実験協力者には，研究目的が個人のノウハウの開示ではなく，暗黙知となっている動的解析のタスクの明文化であることを説明し，秘匿したい部分では録画停止を依頼した．加えて，実験終了後に本人に関連する実験結果を共有し，公開が本人の不利益に当たらないことやオプトアウト可能であることを確認した．

6. おわりに

動的解析における解析タスクは体系的にまとめられておらず，暗黙知となっている．本研究では，暗黙知となっている解析者の実施するタスクの明文化を目的とし，3 名の解析者の動的解析を録画した．その後，録画した解析の様子を振り返りながらタスクやその問題点に関するヒアリング調査を実施した．加えて，実施したタスクを比較することで, 経験の異なる解析者のもつ観点の違いを分析した．この結果，40 種類のタスクを抽出し，7 個の問題点を明らかにした．加えて，経験の長い解析者は，マルウェアファミリや TTPs の考慮といった検体自体やその挙動を一般化することが明らかになった．さらに本研究ではタスクの列挙に加え，タスク遂行を支援するツールの開発や教育的指針を提言することで貢献した．今後の課題として，より多くの実験協力者や異なる検体，異なる解析環境での調査実施や提言事項を活用した解析支援ツールや教育コンテンツの開発が挙げられる．

謝辞　本研究を推進するにあたり，HIRT（Hitach Incident Response Team）の方々に調査のご協力を頂きました．ここに感謝します．

参考文献

[1] Carson Zimmerman: Ten strategies of a world-class cybersecurity operation　scenter. MITRE Corporate Communications and Public Affairs. Appendices(2014).
[2] NPO 日本ネットワークセキュリティ協会（JNSA）：セキュリティ対応組織（SOC/CSIRT） の教科書 ～ 機能・役割・人材スキル・成熟度 ～，入手先〈https://isog-j.org/output/2017/Textbook_soc-csirt_v2.1.pdf＞（参照 2021-07-01）．
[3] Michael, S. and Andrew H.: Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press (2012).
[4] Monnappa, K. A.: Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, Packt Publishing(2018).
[5] Alexey, K. and Amr, T.:Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoT attacks, Packt Publishing(2019).
[6] Wagner, M. , Aigner, W., Rind, A., et al.: Problem Characterization and Abstraction for Visual Analytics in Behavior-Based Malware Pattern Analysis, Proc. of the Eleventh Workshop on Visualization for Cyber Security, pp.9-16 (2014).
[7] Kokulu, F. B., Soneji, A., Bao, T., et al.: Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues, Proc. of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 1955-1970, ACM(2019)
[8] Zhong, C., Yen, J., Liu, P., et al.: Learning From Experts' Experience: Toward Automated Cyber Security Data Triage, IEEE Systems Journal, vol.13,issue 1, pp.603-614(2018).
[9] 鐘本 楊, 長谷川彩子, 塩治榮太郎, 秋山満昭: セキュリティオペレーションの効率化に向けた SOC アナリストの共通行動抽出, コンピュータセキュリティシンポジウム 2020 論文集, pp.645-652(2020).
[10] 金井文宏, 長谷川彩子, 塩治榮太郎, 秋山満昭: セキュアなソフトウェア開発の阻害要因分析, コンピュータセキュリティシンポジウム 2020 論文集, pp.681-688(2020).
[11] Landis, J.R. and Koch, G.G.: The Measurement of Observer Agreement for Categorical Data, Biometrics, Vol. 33, No. 1 pp. 159-174(1977).
[12] Fraunhofer: malpedia, available from〈https://malpedia.caad.fkie.fraunhofer.de/〉(accessed 2021-07-01).
[13] Chronicle Security Ireland Limited: VirusTotal, available from〈https://www.virustotal.com/gui/〉(accessed 2021-07-01).
[14] Google: Google, available from〈https://www.google.com/〉(accessed 2021-07-01).
[15] Twitter, Inc.: Twitter, available from〈https://twitter.com/〉(accessed 2021-07-01).
[16] ANY.RUN: ANY.RUN:, available from〈https://any.run/〉(accessed 2021-07-01).
[17] Joe security LLC: JoeSandbox cloud basic, available from〈https://www.joesandbox.com/#windows〉(accessed 2021-07-01).
[18] Shodan: Shodan, available from〈https://www.shodan.io/〉(accessed 2021-07-01).
[19] MITRE: ATT&CK, available from〈https://attack.mitre.org/〉(accessed 2021-07-01).
[20] David J Bianco: The Pyramid of Pain, available from〈http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html> (accessed 2021-07-26).