Vol.2022-CSEC-97 No.14
Vol.2022-IOT-57 No.14
2022/5/20

解析者インタビューに基づくマルウェア動的解析業務の明文化と支援事項の検討

山岸 伶[1,a)]　藤井 翔太[1]　佐藤 隆行[1]

概要：マルウェア動的解析の実態は暗黙知となっており，解析者の効率的な育成やツール開発の障壁となっている．本研究では，解析者の実施したタスク，タスク完了条件，タスク実施上の問題点の明確化を目的とし，11 名の実験協力者へのインタビューを実施した．その結果，解析者が実施した 63 種類のタスク，25 種類の解析業務の完了条件を明らかにするとともに，解析手順に関する支援を主目的とした基本的な解析フローを作成した．また，解析者の教育の効率化や自己研鑽に貢献することを目的に，経験の異なる解析者の実施タスクや完了条件の傾向を明らかにした．加えて，28 点の解析者の抱える問題点を明らかにし，動的解析環境の安全性確保の支援の必要性等について示した．これらの本研究の成果は，マルウェア解析者の教育指針の検討や今後の動的解析に関わる研究開発の検討の一助になるものと考える．

Clarification of malware dynamic analysis work based on analyst interviews and consideration of support items

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 SOC（Security Operation Center）の業務であり，効率的な監視や対処の実現に貢献すると述べている [1]．

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．

マルウェアを実行・分析する動的解析の実施には，専門性が必要である．ゆえに，解析者はこの専門性を獲得するために教育を受け，経験を積む必要があることから，解析者の効率的な育成が求められている．また，増加するサイバー攻撃に対処するため，解析者の負担を可能な限り削減することが望ましい．こうした解析者の効率的な育成や解析者の負担削減のために，動的解析で実施する作業（タスク）を整理して解析者に示すことや，動的解析の問題点への支援が求められるが，前提となる動的解析のタスクや問題点が十分に理解されてない．

このような背景を受けて，以前の研究 [2] では，解析者の実施するタスクや問題点の明文化のため，3 名の協力者に調査を依頼した．調査では，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インタビューを実施した．ただし，文献 [2] では，協力者は単一組織の 3 名であり限定的であった．そこで本研究では，より深い洞察を得るため，当該調査を拡張し，4 つの組織の 11 名の協力者に動的解析の実施およびインタビューを依頼した．また，インタビューでは実施するタスクやタスク遂行上の問題点に関する質問に加え，タスクを完了する条件に関する問を設定した．

本研究における貢献は以下の通りである．

- 解析者が動的解析で実施するタスクとその完了条件を明文化した．また，明文化した結果をもとに，典型的な解析フローを作成した．これにより，暗黙知となっていったタスクが明らかになり，属人性の低減や解析手順に悩む初学者の支援につながる．
- 経験の異なる解析者の実施タスクや完了条件の差異を分析し，完了条件を意識した解析の遂行，マルウェア

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

全般の挙動や機能，より俯瞰的な視点をもった解析に関する教育の提供が重要であることを示した．これにより，解析者の教育の効率化や自己研鑽に貢献する．

- インタビューを通して，28 の問題点を明らかにした．これにより動的解析業務の課題を示すとともに，動的解析環境の安全性確保の支援の必要性等について示した．

2. 研究背景

2.1 マルウェア動的解析

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．動的解析は，静的解析と比較して低コストで実施可能であり，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，マルウェア感染による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有用である．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], [4]．例えば，文献 [3] 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，動的解析の業務において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．

動的解析に関する調査として，Wong ら [5] は，マルウェア解析のワークフローの理解不足を背景に，解析者の目的の違い，ワークフロー，動的解析環境構築の考慮事項の明確化を研究的課題に設定し，21 名の解析者に半構造化インタビューを実施した．その結果，解析者の目的は収集する IOCs(Indicator of Compromises) で分類可能なことを明らかにし，当該分類ごとに解析のワークフローを作成した．また，当該フローで多くの解析者が動的解析を実施することから，動的解析環境の準備について追加のインタビューを実施し，設定手順や注意点を明らかにした．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．

SOC 業務に関する調査として，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．

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，オンラインアンケートでデベロッパとマネージャのセキュリティ意識を調査した．

2.3 研究課題

上述した通り，文献 [5] では，マルウェア解析全体の目的やワークフローを調査し，マルウェア解析で動的解析は共通して実施される重要な位置づけであることを示している．一方で，同研究で導出されたワークフローは動的解析や静的解析の実施といった粒度であり，動的解析全体の詳細な実施タスクを主題とはしていない．このため，解析者の効率的な育成や解析者の負担削減に向けて異なる観点も必要だと考え，本研究では 3 つの研究課題（以下, RQ と表記）を設定する．

RQ1）　解析者は動的解析でどのようなタスクを実施するか．また，それは解析者の経験でどのように異なるか
詳細な実施タスクを明文化することで，属人性の低減や動的解析の一つの指標となり解析者に向けた教育的な効果が期待されるため，本課題を設定した．加えて，経験の異なる解析者のタスクの比較から，傾向を把握し教育的な知見を得る．

RQ2）　解析者は動的解析のタスクの実施の際に，どのような完了条件を設けているか．また，それは解析者の経験でどのように異なるか
一部のタスクでは解析者が完了条件や目的を設定し取り組んでいることが想定される，完了条件を明確にすることで，タスク遂行継続の判断に貢献し，属人性の低減や教育的な効果が期待されるため，本課題を設定した．加えて，経験の異なる解析者の完了条件の比較から，傾向を把握し教育的な知見を得る．

RQ3）　解析者が動的解析のタスク遂行する際にはどのような問題点が存在するか
タスク実施上の問題点を明文化することで，解析者に必要な支援を明確化し，解析者の負担削減につながると考え，本課題を設定した．

3. ユーザ調査

3.1 調査設計

RQ を解明するため，解析者を実験協力者として募り，ユーザ調査として動的解析の録画と動画に基づいたインタビューを実施した．関連研究 [6] では，実際の動的解析を依頼せず，通常の業務に関する半構造化インタビューを実施したが，本研究はより詳細なタスクの明確化を目的とし

ているため，実際の解析に基づくことで，協力者に解析タスクを想起させ，インタビューの内容を充実できると判断した．一方で，動的解析を実施した検体によるバイアスがかかり，汎用的な解析タスクが得られない懸念があるため，インタビューの際に「今回は実施しなかったが普段他に実施することはないか」と質問することで，汎用的なタスクを調査した．

協力者には情報窃取を行う Formbook マルウェアの一検体（全員共通）を通常の業務や手順に準じ，録画しながら動的解析作業をするよう依頼した．また，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に加え，検体や解析の流れといった内容を含むものであった．なお，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停止を許容し，停止した場合はインタビュー時に口頭でタスクを補足するよう依頼した．

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と考えられるためである．また，RQ1 と RQ2 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，調査手順に関して説明する．事前準備として，著者は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．併せて，協力者は所属組織や業務歴に関わるアンケートを記入した．記入後，協力者は指定された検体を画面を録画しながら解析した．

インタビューでは，録画したビデオを主著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で抽出した．なお，主著者に限定したのはインタビューの一貫性を保つためである．次に当該テキストを参照しながら，解析の流れを振り返り，著者は協力者に対しインタビューを実施した．インタビューでは，タスクごとに実施理由，有効性，完了条件，問題点，今回は実施/録画しなかったが本来なら実施する関連タスクの質問を行い，その回答を得た．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．

インタビュー後の集計では，主著者がコードブックとして，タスク，完了条件，問題点を列挙した．次に，主著者を含む著者 2 名それぞれが解析とインタビューの録画を確認した後，協力者それぞれのコードブック内の事項の回答有無を判断した．著者らの判断に対して，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 0.81 未満であれば，不一致とみなして再度議論し，コードブックを編集することで意識の統一を図った．以上を繰り返し，カッパー値が 0.947 になった段階で，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．最後に，協力者にコードブックと当該協力者の回答有無を送付し，誤りや発言漏れの訂正を依頼した．

表 1 調査協力者

協力者 ID	組織 ID	解析歴	セキュリティ業務歴	分類
P1	A	0–1 年	0–1 年	初学者
P2	B	1–2 年	1–2 年	初学者
P3	A	0–1 年	0–1 年	初学者
P4	C	0–1 年	2–3 年	初学者
P5	C	2–3 年	2–3 年	経験者
P6	A	3–4 年	3–4 年	経験者
P7	D	4–5 年	15–20 年	経験者
P8	D	0–1 年	3–4 年	初学者
P9	B	2–3 年	3–4 年	経験者
P10	B	3–4 年	4–5 年	経験者
P11	C	0–1 年	4–5 年	初学者

3.3 結果

3.3.1 実験協力者に関するアンケート結果

表 1 では，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，本調査では同じプロジェクトに関わる 11 名の協力者に調査を実施した．便宜上，実験協力者に一意の ID を与え，P1–P11 とした．11 名は A から D の 4 組織にそれぞれ所属している．マルウェア解析歴は最長 4–5 年で最短 1 年未満，セキュリティ分野での業務歴は最長 15–20 年で最短は 1 年未満であった．なお，P3 はセキュリティ分野での業務は 1 年未満であったが，大学での研究も含めると 2–3 年間セキュリティ分野に従事している．

便宜上，マルウェア解析歴が 2 年未満の人を初学者と，2 年以上の協力者を経験者とみなし比較する．一方で，マルウェア解析以外のセキュリティ業務には長年携わっている協力者も存在し，この以前の業務の種別や解析実施数といった年数以外の要素が実施タスクに影響を及ぼす可能性は否定できない．ただ，マルウェア解析のスキルを定量化するのが困難であったため，年数を区切りとした．

3.3.2 実施時間

本節では，解析の録画時間およびインタビュー実施時間について示す．解析の録画時間は，最大 735.00 分，最小 0.00 分，平均 269.86 分，標準偏差 252.17 分であった．なお，最小 0.00 分は P8 であり，録画負担の都合から解析録画ができず，報告書やメモをベースとしたインタビューを実施した．また，検体の実行中やログ分析中など，解析者の作業がないあるいは単調なタスクで録画を停止したケースもあったため，録画時間にばらつきが存在し，標準偏差が大きくなった．こうした録画時間のばらつきはタスク抽出に影響が懸念されるが，解析者の負担を考慮した調査に

は必要であり，インタビューでの質問や一覧表作成後の確認で制約を緩和している．

インタビューの実施時間は最大 87.97 分，最小 60.63 分，平均 74.14 分，標準偏差 9.22 分であった．インタビューはオンライン会議設定や解析者負担の都合から 90 分を目途に実施したため，60.63 分から 87.97 分の間となり，標準偏差が比較的小さくなった．

3.3.3 タスク一覧

表 2 に，抽出した 63 種類のタスクを示す．また，タスクは，検体情報をあらかじめ収集する事前調査，動的解析環境の準備に関わる環境準備，実際の動的解析，検体の情報を確認する表層解析，動的解析で収集した情報を分析する事後分析，事後分析の結果を踏まえて動的解析以外の手法で情報を収集する事後調査の 6 フェーズに分類できた．

3.3.4 タスクの完了条件

表 3 に，インタビューしたタスクでの完了条件を示す．完了条件は 25 個であり，事前調査，動的解析，事後分析の 3 フェーズの完了条件となっている．なお，環境準備は各々が決めた手順を実行していることが大半であったため，表層解析や事後分析は実施した解析者が一部であったため，完了条件を本研究ではまとめなかった．

3.3.5 タスク実施上の問題点

表 4 にインタビューしたタスク実施上での問題点を示す．問題点は 28 個であり，これらは 13 種類のカテゴリに分類できた．

4. 結果分析

4.1 RQ1: 動的解析の実施タスクについて

先述の通りタスクは，順に，検体情報をあらかじめ収集する事前調査，動的解析環境の準備に関わる環境準備，実際の動的解析，検体の情報を確認する表層解析，動的解析で収集した情報を分析する事後分析，事後分析の結果を踏まえて動的解析以外の手法で情報を収集する事後調査の 6 フェーズに分類できた．このうち最多は 26 種類の事前調査であり，次点以降で 14 種類の事後分析，13 種類の動的解析，6 種類の環境準備，2 種類の表層解析および事後調査と続く．実施率をみても事前調査，環境準備，動的解析，事後分析は 100.00%であったが，表層解析は 54.55%で事後調査は 63.64%であった．これらのことから，事前調査，環境準備，動的解析，事後分析の 4 フェーズはマルウェア動的解析業務において重要な役割をもつと考える．

タスク個別の実施率では，100.00%のものが 6 種類存在し，レピュテーション共有サイトでの「ファイルの表層情報の確認」と「検知シグネチャ名・数の確認」，解析実行準備での「検体入手」，事後分析時の端末ログでの「プロセスツリーの把握」と「特定イベントをキーにした詳細の調査」，通信パケットでの「通信先の確認」であった．レピュテーション共有サイトでの 2 点に関しては，報告書の内容にレピュテーションサイトでの検知名やファイル名といった情報が存在したため，また検体入手に関しては今回の実験設定でハッシュ値を指定し自身で検体を入手していただいたため，バイアスが生じたと考えられ，本研究の制約として残る．事後分析の 3 点に関しては，ログ分析の中で共通してみられる点だということが考えられる．事実，組織Cでは，一部必須の解析の手順を共有しており，ログ分析において中心としているタスクは，検体の関わるプロセスツリーと特定プロセス，イベントをキーとした調査であると述べていた．他にも，端末ログや通信パケットの分析では 80.00%以上の解析者が実施したタスクが 6/9 であり，解析者にとって端末ログや通信パケットの分析は重要であると考えられる．

次に，初学者と経験者の間の実施率の差について述べる．実施率の差が大きいタスクはいずれも経験者の実施数が大きく，初学者の実施数が小さいケースであった．これは実施タスクの数に違いがあったこと（初学者の実施タスク数は平均 26.17 個，経験者は平均 40.6 個）が一因だと考える．最も大きい差は 66.67%であり，「オンラインサンドボックスでのその他挙動や設定情報の確認」であった．その他に関しては，mutex やインポートテーブルといった情報が含まれ，当該タスクを遂行した解析者の中でも異なる．これらを一つに集約したため最も大きな差になったと考えるが，一方で，経験者はファイルやプロセスといった共通的な情報以外も確認し，実施タスク総数が増加することを裏付ける結果となっている．また，同様に，レピュテーション共有サイトの調査を除く，事前調査の実施率は他のフェーズと比較し，実施率の差が大きく，専門家の暗黙知化が進んでいる傾向が示唆された．

4.2 RQ2: 動的解析タスクの完了条件について

全体を通して，時間を解析終了の基準とすることが多く，事前調査，動的解析，事後分析ではそれぞれ 81.82%，100.00%，72.73%の解析者が時間を完了条件としていた．多くの解析者が動的解析業務は時間をかけてもわからないことがあるため，区切りとなる時間をあらかじめ考えて実施することが大切だと述べていた．特に動的解析実行時は，100.00%の解析者が時間を完了条件としていた．これは実行している検体が動的解析環境で十分に動いているか定量的に判断することが難しく，時間を基準とすることが推察される．これは，表 4 の問題点の 16 行目にある検体実行成功の判断が難しいという点にもつながる．一方で，攻撃者の解析回避手段として検体の一時停止も挙げられるため，適切な動的解析の時間設定は困難であり，今後の課題として残る．事実，今回の解析検体でも 15 分後に UAC が出現し実行許可を与えた場合に不審な挙動を取るという報告結果を得た．したがって，動的解析時間を 15 分未満に設定していた場合は十分な解析結果を得られないことを

表 2 動的解析において実施されるタスクと各タスクの実施率

フェーズ	カテゴリ	タスク	累計実施率	初学者	経験者
事前調査	レピュテーション共有サイト（ファイルキー）	ファイルの表層情報の確認	100.00%	100.00%	100.00%
		検知シグネチャ名・数の確認	100.00%	100.00%	100.00%
		投稿日時の確認	81.82%	83.33%	80.00%
		ファイルの構成情報の確認	18.18%	16.67%	20.00%
		コミュニティの確認	36.36%	16.67%	60.00%
		関連検体に対して再帰的に実行	63.64%	50.00%	80.00%
	セキュリティベンダサイト（検知名キー）	作成するファイルのパス確認	9.09%	16.67%	0.00%
	オンラインサンドボックス（ファイルキー）	スクリーンショットの確認	27.27%	33.33%	20.00%
		検知シグネチャの確認	45.45%	50.00%	40.00%
		ファイル関連情報の確認	72.73%	66.67%	80.00%
		レジストリ関連情報の確認	72.73%	50.00%	100.00%
		コマンド情報の確認	54.55%	33.33%	80.00%
		プロセス関連情報の確認	72.73%	66.67%	80.00%
		通信関連情報の確認	90.91%	83.33%	100.00%
		ファミリ，類似検体情報の確認	45.45%	50.00%	40.00%
		その他挙動・設定情報の確認	63.64%	33.33%	100.00%
		TTPs の確認	27.27%	16.67%	40.00%
		関連検体に対して再帰的に実行	36.36%	33.33%	40.00%
	関連サービス（通信先キー）	通信先のレピュテーションの確認	63.64%	50.00%	80.00%
		通信先の詳細情報の確認	45.45%	50.00%	40.00%
		生死の情報の確認	36.36%	16.67%	60.00%
	解析レポート（ファミリキー）	挙動の確認	36.36%	16.67%	60.00%
		解析検知回避機能の確認	27.27%	16.67%	40.00%
	関連情報をキーとした情報収集	検索エンジン検索	90.91%	83.33%	100.00%
		SNS での検索	54.55%	33.33%	80.00%
		脅威情報データベースで検索	9.09%	16.67%	0.00%
環境準備	監視準備	ロギング準備	90.91%	83.33%	100.00%
		環境の状況確認	45.45%	33.33%	60.00%
	実行準備	検体入手	100.00%	100.00%	100.00%
		実行に必要なアプリの準備	18.18%	16.67%	20.00%
		実環境の模倣	54.55%	50.00%	60.00%
		検体配置の工夫	18.18%	33.33%	0.00%
動的解析	検体実行	ユーザ権限での検体実行	45.45%	33.33%	60.00%
		管理者権限での検体実行	81.82%	83.33%	80.00%
		上記の両権限での実行	27.27%	16.67%	40.00%
	監視	設定情報の監視	90.91%	83.33%	100.00%
		画面の監視	54.55%	50.00%	60.00%
		通信の監視	81.82%	66.67%	100.00%
		検体が情報窃取しうる動作の実行	18.18%	16.67%	20.00%
	実行後処理	実行前後の状態の変化の確認	81.82%	66.67%	100.00%
		ログの取得	90.91%	83.33%	100.00%
		再起動とその後の状態の変化の確認	36.36%	16.67%	60.00%
	複数回，再帰的な実行	複数環境での実行	45.45%	33.33%	60.00%
		複数回の実行	54.55%	33.33%	80.00%
		二次検体の実行	18.18%	16.67%	20.00%
表層解析	表層解析	ハッシュ値の確認	36.36%	33.33%	40.00%
		表層情報の確認	36.36%	33.33%	40.00%
事後分析	端末ログの分析	プロセスツリーの把握	100.00%	100.00%	100.00%
		特定イベントをキーにした調査	100.00%	100.00%	100.00%
		特定ファイル名・パスをキーにした調査	90.91%	83.33%	100.00%
		特定プロセスをキーにした調査	90.91%	83.33%	100.00%
		端末 EDR のアラート・シグネチャ確認	45.45%	33.33%	60.00%
	通信パケットの確認	通信先の把握	100.00%	100.00%	100.00%
		通信のヘッダ情報の確認	81.82%	66.67%	100.00%
		通信内容の確認	72.73%	50.00%	100.00%
		通信内容のデコード	54.55%	33.33%	80.00%
	その他ログの確認	プロキシログの確認	9.09%	16.67%	0.00%
		FW ドロップログの確認	18.18%	16.67%	20.00%
		DNS の確認	63.64%	50.00%	80.00%
		偽装サーバへの通信内容の確認	27.27%	16.67%	40.00%
		OSINT の追加調査	45.45%	33.33%	60.00%
事後調査	結果の深堀	事前調査結果と比較	54.55%	50.00%	60.00%
		静的解析の実施	18.18%	0.00%	40.00%

示唆している．

事前調査では，特定の情報の収集を完了条件とする解析者が多い傾向にあった．収集対象となる情報も多様であり，計 12 種類の情報が挙げられ，情報収集の対象となる情報は，解析に必要なためあるいは解析を高度化するための情報，解析効率化のための情報，解析後の業務への活用を見据えた情報に分類された．なお，解析後の業務への活用を見据えた情報は事前調査だけでなく本来動的解析後の

表 3 動的解析の実施タスクの完了条件と回答率

フェーズ	カテゴリ	完了条件	累計回答率	初学者	経験者
事前調査	解析に必要/高度化するための情報	検体の実行形式	27.27%	16.67%	40.00%
		検体の関わるファイルパス	45.45%	50.00%	40.00%
		検体の関わるレジストリ	45.45%	33.33%	60.00%
		検体のパッカー	9.09%	0.00%	20.00%
		検体の検知回避方法	27.27%	0.00%	60.00%
		検体が窃取する情報	18.18%	0.00%	40.00%
	解析効率化のための情報	検体の関わるプロセスツリー	54.55%	50.00%	60.00%
		検体の挙動に関する概要情報	36.36%	16.67%	60.00%
	解析後の業務への活用を見据えた情報	検体が用いる永続化方法	27.27%	0.00%	60.00%
		検体の通信先	63.64%	33.33%	100.00%
		検体に関連する攻撃の目的	18.18%	0.00%	40.00%
		検体の関与が疑われる攻撃者	9.09%	0.00%	20.00%
	その他	新規情報がなくなるまでの再帰的な調査	27.27%	16.67%	40.00%
	強制終了	事前調査の時間	81.82%	100.00%	60.00%
動的解析	ある情報の収集	不審なプロセスの観測	63.64%	50.00%	80.00%
		不審な通信の観測	36.36%	0.00%	80.00%
	強制終了	検体の実行時間	100.00%	100.00%	100.00%
事後分析	ある情報の収集	レジストリ	63.64%	33.33%	100.00%
		検体の関わるファイル	54.55%	16.67%	100.00%
		検体のプロセスツリー	63.64%	50.00%	80.00%
		検体の通信先とその通信内容	81.82%	66.67%	100.00%
		検体の永続化方法	54.55%	16.67%	100.00%
		事前調査で収集した情報と事後分析結果の差異	72.73%	50.00%	100.00%
	その他	新規情報がなくなるまでの再帰的な分析	45.45%	33.33%	60.00%
	強制終了	分析時間	72.73%	50.00%	100.00%

表 4 動的解析の実施上の問題点と回答率

分類	問題点	累計回答率	初学者	経験者
能力	静的解析の選択肢がないこと	18.18%	33.33%	0.00%
解析進行の不安	何が分からないのかが不明	45.45%	83.33%	0.00%
	調査・解析手順が不明/不安なこと	54.55%	100.00%	0.00%
	情報収集先・ツールの情報不足	45.45%	66.67%	20.00%
	新しい/慣れない情報収集先・ツールの使い方が不明	72.73%	100.00%	40.00%
実行判断	解析前に死活状態の確認が困難	18.18%	0.00%	40.00%
	想定する環境で検体が動きそうかの判断をするのが困難	27.27%	16.67%	40.00%
情報収集	解析前に調査できた情報が乏しいと苦戦	18.18%	0.00%	40.00%
用語	C&C，ダウンロード，アップデート等の役割の違う接続先を統一した用語が不足	9.09%	0.00%	20.00%
仕組み	解析者間の情報共有が不足	18.18%	16.67%	20.00%
解析環境	収集情報のエンリッチメント・効率化と解析検知のバランスの調整が困難	36.36%	33.33%	40.00%
	解析環境の準備・用意が困難	54.55%	50.00%	60.00%
	解析環境の安全性の担保が困難	27.27%	16.67%	40.00%
	出社が必要	18.18%	0.00%	40.00%
検体実行	検体実行時の適切な実行権限	27.27%	33.33%	20.00%
	実行成功の判断が困難	36.36%	0.00%	80.00%
	停止理由の検討とカバレッジ向上が困難	9.09%	16.67%	0.00%
ログ分析	不審，特徴的な動きの判断が困難	36.36%	50.00%	20.00%
	ログの相関的な分析が大変	18.18%	16.67%	20.00%
	検体の挙動とログのマッピングが困難	18.18%	33.33%	0.00%
	通信先が多い場合に分析が困難	54.55%	50.00%	60.00%
	解析終了の判断が困難	18.18%	16.67%	20.00%
	ログのフィルタ時に重要な情報を落としていないか不安	9.09%	16.67%	0.00%
	手順書を作って共有しているが，手順書に最新の状態に対応していない部分が存在	18.18%	16.67%	20.00%
報告	場合によっては報告書作成が困難	18.18%	16.67%	20.00%
著名な特定ツール	イベントビューワーは利用が困難	45.45%	33.33%	0.00%
教育	後進の育成が困難．勘やコツに関する言語化・マニュアル化が不十分	18.18%	0.00%	40.00%
その他	暗黙知（常識）を知らないため，解析手順等を聞いて動的解析を実施しても困難	9.09%	16.67%	0.00%

事後分析で調査し，動的解析でない本来の業務への活用を見据えた情報である．P6 は，「インシデントレスポンスの観点において動的解析で特に収集したい情報は感染端末の回復に用いる永続化方法と通信ブロックに活用する通信先であり，これらを優先して調査し把握する」と述べている．

先述した通り，動的解析フェーズの完了条件として時間を 100.00%の解析者が挙げていた．その一方で，不審なプロセスの観測や不審な通信の観測を挙げている解析者も多く，解析者はこれらの不審なプロセスや通信を観測することで，マルウェアが動いていて情報が取れていると判断し，動的解析を終了している．

次に，動的解析歴が与える完了条件の違いについて考察する．初学者と経験者ごとに完了条件の回答数に関して，初学者は平均値 7.83 個，中央値 8.0 個であり，経験者は平均値 17.0 個，中央値 17.0 個であり，マンホイットニーの u 検定で有意差が存在した（$p = 0.008 < 0.05$）．また，平

均値，中央値ともに 9 以上差があることからも，初学者と比較し経験者の設定する完了条件は多い（Find1）．

初学者と経験者の間の回答率の差について述べる．まず全体を通して，経験者と初学者の差が大きい傾向にあり，回答率の差が大きい完了条件はいずれも経験者の回答数が大きく，初学者の回答数が小さいケースであった．特に情報収集を完了条件とするケースにこの差が顕著であり，事前調査や事後分析のタスク遂行自体の差は少ないことから，初学者は何の情報を集めるのかを意識せず解析を遂行する傾向にあることが推察される（Find2）．また，収集する情報の傾向に関しても経験者と初学者の差が見られた．レジストリやファイルパスといった比較的定型化しやすい項目については，初学者・経験者共に収集していた一方で，検知回避方法，窃取情報，攻撃目的，および攻撃者のような抽象度の高い項目の収集については，初学者の実施率は 0.00%であり，経験者のみが実施していた．このことから，抽象度が高く，定型化することが難しい項目の収集については，解析経験に基づくスキルが必要であることが示唆された．なお，先述した P6 によるインシデントレスポンスへの活用を見据えた情報収集に関する回答例のように，経験者は，目的意識をもって情報収集を実施する傾向にあるため，抽象度の高い項目を集めていることが推察された（Find3）．

4.3 RQ3: 動的解析実施上の問題点について

全体を通して解析進行に関する不安が問題点として挙がった．72.73%の解析者が新しく慣れない情報収集先やツールの使い方が分からないことが問題であると挙げた．また，同様に 45.45%が情報収集先やツールを知らないということを挙げた．また，同様の解析進行に関する不安として，何が分からないのかわからないや解析手順に不安を抱えているという問題点もあげられた．後進の育成が困難でマニュアル化できていないという専門家の問題点や暗黙知を知らないために苦労しているという初学者の問題点も含めて，本研究で明文化したタスクや暗黙知や今後の研究が本問題の解消に貢献しうると考える．

また，解析環境の準備や用意が負担になっているという問題点も挙げられた．サンドボックスの利用等で簡略化できる点もあるがこれに関しても自由度の高い環境と解析検知のトレードオフに帰着すると考える．また，解析環境がどのくらい安全かどうかが把握できていないと不安といった問題点も挙げられた（Find4）．ログ分析において，初学者を中心に不審な点や検体の特徴的な動きをログから見つけるのが困難という点や，挙動がログに落とし込まれた時の見え方が分からない点が挙げられた（Find5）．

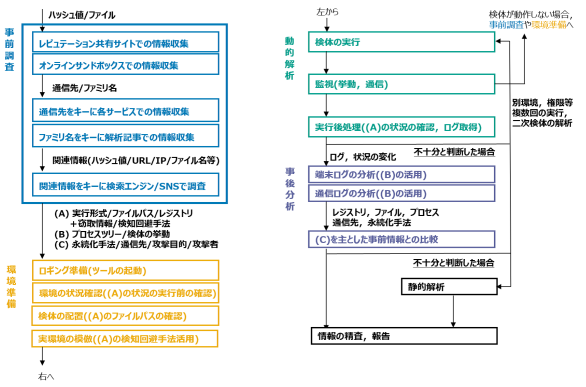

図 1 典型的な動的解析の解析フロー

5. 議論

5.1 動的解析のフロー

解析方法に関して初学者を含む解析者の指標となることを目的とし，調査結果をもとに解析フローを作成した（図 1）．四角形内の文字が実施タスクを，黒色の太字が取得する情報を，下線を含む文字が条件を，細字はその他補足説明を表している．なお，本フローは，目的に基づき，解析者の実施率が高いタスクやその分類を主に選択することで作成した．また，本フローは，前述の初学者の解析支援に加えて，教育への活用や分析漏れの抑制等にも応用できると推察される．

5.2 解析者の教育に関わる知見

本節では初学者の教育の指針や解析者の自己研鑽への貢献を目的に，4 章の結果をもとに教育的知見を 3 点述べる．

完了条件を意識した解析の遂行

（Find1），（Find2）で示す通り，初学者と比較し，解析者は完了条件を多く設定し，目的意識をもってタスクを遂行している．特に経験者は，当該業務に割り当てられる時間を考慮しつつ，どういった情報が最終的なセキュリティ業務や報告に必要なのか，動的解析の実行/高度化/効率化に必要なのかを意識してから実施していた．

マルウェア全般の挙動や機能に関する教育の提供

（Find5）で示す通り，解析歴やセキュリティ従事歴自体が浅い初学者はマルウェアの特徴的な挙動やその挙動がどのようにログとして現れるのかの把握することに苦戦すると述べていた．したがって，マルウェアの機能や挙動を体系的に伝え，それがどういった形でログに現れるのか例を含めて伝えるのが重要となる．

より俯瞰的な視点をもった解析を促す教育の提供

（Find3）で挙げた通り，経験の長い解析者は，より俯瞰的な視点を持った解析を実施する．具体的には，検体でなくファミリを意識し，MITRE ATT&CK などの TTPs を考慮し，ファイルパスやレジストリといった具体的な項目

に加えて解析検体の永続化方法や検知回避機能，窃取情報は何かといった観点で分析を実施する．初学者から次のステップへ進もうとする解析者には，このような俯瞰的な視点を持つように促すことが，解析の幅を広げると考える．

5.3 研究機会に関わる提言事項

本節では，解析者が挙げた問題点の中でも，現在解決されておらず，今後の研究を通して解析者を支援すべき点について，提言事項として述べる．

動的解析環境の安全性確保の支援

（Find4）の通り，解析者は解析環境であっても安全性が担保されているか意識する必要があるが，その判断が困難あるいは負担となっていることが分かった．特にオープンソースや商用でないカスタマイズされた動的解析環境では，キーロギングされ通信で情報が送られていないか，解析終了後に正しくリカバリーできているか，検体を送るため解析環境と組織内ネットワークをつなぐ際，外部との通信が停止できているかに，細心の注意を払っていた．一方で，確認漏れの懸念がつきまとい安全性確保が負担となっていたため，カスタマイズされた動的解析環境でも解析に影響を与えずに安全性を確保する支援が必要となっている．この問題への取り組みにより，客観的に見た安全な解析を提供するだけでなく，解析者の不安の払拭や安全性を確保するために掛けていた負担の低減が期待される．

5.4 制約

本研究における制約として，解析検体や解析環境数が限られていたことが挙げられる．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．本研究では，検体数が 1 件と限られていたものの，3 章で述べたように，インタビューの際に「今回は実施しなかったが普段他に実施することはないか」と質問することにより，可能な範囲で対象検体に限らないタスクを調査し，本制約の緩和を図っている．

もう一つの制約は，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，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，明文化できない点にある．この制約はインタビュー形式の研究に共通する [11] が，本研究では動的解析の録画により制約の緩和を図った．

5.5 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，実験および管理方法の説明をしたうえで同意を得ている．また，本稿では匿名化処理をしてデータを記載している．

6. おわりに

マルウェア動的解析の実態は暗黙知となっており，解析者の効率的な育成やツール開発の障壁となっている．本研究では，解析者の実施したタスクやその完了条件，問題点の明確化を目的とし，4 つの組織の 11 名の実験協力者へのインタビューを実施した．その結果，解析者が実施したタスクや完了条件，問題点を明らかにするとともに，基本的な解析フローを作成した．また，経験の異なる解析者の実施タスクや完了条件の傾向を明らかにし，問題点のうち後の研究を通して解析者を支援すべき点等について提言事項として述べた．これらの本研究の成果は，マルウェア解析者の教育指針の検討や今後の動的解析に関わる研究開発の検討の一助になるものと考える．

謝辞 本研究を推進するにあたり，調査にご協力頂いた解析者の方々に感謝します．

参考文献

[1] Zimmerman, C.: Ten strategies of a world-class cybersecurity operation scenter (2014).
[2] 山岸 伶, 藤井翔太, 佐藤隆行：ユーザ調査によるマルウェア動的解析タスクの明文化, CSS2021 論文集, pp. 112–119 (2021).
[3] Monnappa, K. A.: *Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware*, Packt Publishing (2018).
[4] Kleymenov, A. and Thabet, A.: *Mastering Malware Analysis: The Complete Malware Analyst's Guide to Combating Malicious Software, APT, Cybercrime, and IoT Attacks*, Packt Publishing (2019).
[5] Yong W., M., Landen, M., Antonakakis, M. et al.: An Inside Look into the Practice of Malware Analysis, *Proc, of the 2021 ACM CCS*, pp. 3053–3069 (2021).
[6] Wagner, M., Aigner, W., Rind, A. et al.: Problem Characterization and Abstraction for Visual Analytics in Behavior-Based Malware Pattern Analysis, *Proc. of VizSec '14*, 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 CCS*, pp. 1955–1970 (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, No. 1, pp. 603–614 (2019).
[9] 鐘本 楊, 芝原俊樹, 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, CSS2020 論文集，pp. 645–652 (2020).
[10] Kanei, F., Hasegawa, A. A., Shioji, E. et al.: A Cross-Role and Bi-National Analysis on Security Efforts and Constraints of Software Development Projects, *Proc. of Annual Computer Security Applications Conference (ACSAC)*, pp. 349–364 (2021).
[11] Hollnagel, E.: *Handbook of cognitive task design*, CRC Press (2003).