セキュリティ業務におけるマルウェア解析の調査

- White Paper -

国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所　サイバーセキュリティネクサス

目次

1. はじめに

1.1. 背景

政府機関、企業、大学等を標的とするサイバー攻撃は、年々巧妙化かつ複雑化している。ランサムウェアによるデータの暗号化や、不正アクセスに起因する情報漏洩といった被害は後を絶たず、攻撃を受けた場合には経済的損失や社会的信用の失墜といった深刻な影響を及ぼす可能性がある。このような背景から、サイバー攻撃への対策は組織にとって喫緊の課題である。

サイバー攻撃対策には多岐にわたる取り組みが求められるが、その中でも重要な手段の一つが、マルウェアに関する情報の収集および分析である。マルウェアは攻撃者が主に用いるツールであり、その挙動や構造を把握することは、攻撃手法の理解および防御策の検討において有益である。

マルウェア解析には高度なセキュリティ知識が求められるため、解析手法に特化した書籍や資料は数多く存在する。一方で、セキュリティ専門家が実務の現場において、どのようにマルウェア解析を進め、いかなる工夫を施しているのかに焦点を当てた資料は限られている。たとえば、限られた時間内で迅速に脅威を特定するための解析の優先順位決定手法や、特定機能に着目した効率的な抽出・分析技法などが挙げられる。実務の現場においては、単なる詳細な解析ではなく、インシデント対応や脅威ハンティングの観点から、いかに効率的かつ実用的に有益な情報を得るかが重要である。

しかしながら、このような実務上の工夫や知見は、体系的に共有されているとは言い難いのが現状である。マルウェア解析に関する実務的ノウハウの共有は、今後のセキュリティ対策の高度化に資する重要な課題である。

1.2. 目的

本資料では、**マルウェア解析者の業務に焦点をあてて、解析の事例や工夫についてインタビューを実施して、その結果を共有すること**を目的にする。

1.3. 想定対象読者

本資料は、以下を想定対象読者とする。

- 業務でマルウェア解析を実施している方
- マルウェア解析者のマネジメントを行う方

1.4. 本資料の作成方法

16 名のマルウェア解析者の方（マネージドサイバーセキュリティサービスなどセキュリティのサービスを提供する業務の方 8 名、自組織のセキュリティ業務担当の方 7 名（企業規模：5,000-10,000 人 3 名、10,000 人以上、4 名）、非公開 1 名）にインタビューを実施し、当該インタビューの回答を中心に本資料を執筆した。インタビューにご協力いただいた方々に深く感謝します。

2. マルウェア解析の概要

2.1. マルウェアとは

マルウェアとは、悪意のある動作を実行するソフトウェアの総称である。攻撃者は、情報の窃取、データの破壊（削除や暗号化）、システムの不正制御、さらには攻撃基盤の維持・拡散など、様々な目的に応じてマルウェアを利用する。マルウェアの対象は、パソコン、スマートフォン、サーバ、ネットワーク機器など多岐にわたり、感染したデバイスは攻撃者の意図する動作を強制的に実行させられる。

2.2. マルウェア解析とは

前述のとおり、攻撃者は自身の目的達成のためにマルウェアを用いる。したがって、マルウェア解析を通じてマルウェアの機能や挙動に関する情報を取得・活用することは、サイバー攻撃への対策検討やインシデント対応といったセキュリティ業務を効率化するうえで有効である。

マルウェア解析には複数の手法が存在し、代表的なものとして以下の三つが挙げられる。

表層解析：マルウェアを実行せず、ファイルのヘッダ情報などのメタデータを分析する手法。
動的解析：サンドボックスなどの隔離した専用の解析環境上でマルウェアを実行し、その挙動を観察する手法。
静的解析：マルウェアのコードを逆アセンブル・逆コンパイルし、その内部処理を解析する手法。

加えて、本資料ではデバッグ手法についても紹介する。デバッグとは、専用の解析環境上でマルウェアのコードを逐次的に実行し、その動作をリアルタイムで観察・分析する手法である。これら各解析手法の詳細については、第 3 章にて解説する。

2.3. マルウェア解析におけるリスクと安全性確保の重要性

マルウェアの取り扱いには以下のようなリスクが伴うため、十分な注意を払いつつ、マルウェアを管理・解析する必要がある。

- **意図しないマルウェア感染のリスク**：マルウェアを誤って実行した場合、解析者のデバイスが感染し、機密情報の漏洩や組織外への被害拡大といった深刻な事態に発展するおそれがある。そのため、マルウェアを扱う際には細心の注意を払うとともに、隔離された仮想環境等を利用し、万が一の事態に備えることが重要である。
- **マルウェアや情報共有による機密情報漏洩のリスク**：マルウェア本体および関連ファイルには、機密情報が含まれている可能性がある。VirusTotal をはじめとする外部サービスでは、アップロードされたファイルの情報が第三者に公開され、場合によってはマルウェアの取得すら可能となることがある。そのため、これらのサービスにファイルをアップロードする際には、情報漏洩のリスクを慎重に評価し、必要に応じてアップロードを控えるべきである。

以上のようなリスクを正確に認識し、適切な対策を講じたうえでマルウェア解析を実施することが肝要である。判断が難しい場合には、解析を行わないという選択肢を取ることが、安全性を確保する上で望ましい対応である。

3. インタビューについて

本資料の内容は、主に解析者へのインタビューに基づいて作成している。本章では、インタビューの協力者、手法、限界について説明する。

3.1. 協力者情報

16 名のマルウェア解析者の方にご協力いただいた。彼らの業務は、自組織のためのセキュリティ業務と他組織に向けたセキュリティ業務（サービス）に分類できた。7 名が自組織のセキュリティ業務の担当者、8 名がマネージドサイバーセキュリティサービスといったセキュリティサービスを提供する業務の担当者、1 名が非公開であった。また、自組織のセキュリティ業務の担当者に関しては、3 名の担当者の企業規模が 5,000-10,000 人、4 名の企業規模が 10,000 人以上であった。

セキュリティ業務、マルウェア解析業務の経験に関して、0-1 年が 1 名、2-3 年が 2 名、4-6 年が 7 名、7-9 年が 2 名、10-14 年が 2 名、15-20 年が 2 名であった。ポジションに関して、12 名が実務者、1 名がマネージャ、3 名が実務者とマネージャの兼任であった。

彼らが所属する組織は 12 組織であり、2 名の所属する組織が従業員数 100 名未満、6 名の所属する組織が従業員数 1,001-2,000 名、2 名の所属する組織が従業員数 2,001-5,000 名、1 名の所属する組織が従業員数 5,001-10,000-名、4 名の所属する組織が従業員数 10,001 名以上、1 名が非公開であった。

3.2. 手法

インタビューは半構造化インタビューの形式でメンロレポート※に記載された倫理的配慮に遵守して設計され、以下の手順で実施した。

※The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research
https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf

(1) 協力者募集

直接的な依頼、イベントでの告知、協力者からの紹介といった形式で協力者を募集した。なお、募集ポスターを作成し、当該ポスターもとにインタビュー依頼について説明した。このポスターにより、協力者への依頼の説明が統一された。

(2) インタビュー

インタビューは、Microsoft Teams を用いたオンライン形式で実施した。なお、後述のデータ分析に資するため、協力者の同意を得たうえで、Microsoft Teams の録音機能を用いて音声を記録した。インタビューは半構造化インタビューの形式で実施した。半構造化インタビューとは、あらかじめ用意したインタビュー台本を基にしつつ、協力者の発言内容に応じて適宜質問を深掘りする柔軟性を有したインタビュー手法である。本研究におけるインタビュー台本は、作成後に関係者間で事前にレビューを実施したものである。

- インタビュー期間：2023/11-2024/03
- インタビュー時間：1 時間から 1 時間半程度（協力者の負担軽減のため、開始から 45 分程度で一度休憩）
- インタビュー者：同一の 1 名（一貫性を保つため）

インタビューの内容は、（分析目的で質問した）協力者自身の情報・経歴、マルウェア解析を実施する事例・業務、主要な解析手順、解析技術であった。ここで協力者より得られた回答をもとに、4 章、5 章、7 章を執筆する。

なお、解析環境については、時間の都合上全員に解析環境に関する詳細な質問をインタビューすることができなかった。そのため、3 名の協力者に別途 30 分程度のインタビューを再度依頼し、データを収集した。そのため、6 章の解析環境の準備の内容は限定的な結果となっている。

(3) データ分析

インタビュー時に録音した音声データを自動文字起こし機能でテキストに変換し、当該テキストの誤りを手動で修正した。インタビューの内容のテキストを 2 名によるコーディング(定性的なデータのパターンや意味を見出すために、データをラベル付けして整理し、分類・整理する分析手法)で分析した。

3.3. 本手法の限界

本ホワイトペーパーで紹介する事例や工夫は、16 名の協力者の意見に基づく一例であり、すべての事例を網羅的に取り上げるものではない。また、協力者はインタビュー時に想起できる範囲で回答していることから、過去の事例や実践を一部忘却している可能性も否定できない。したがって、協力者の回答内容が、必ずしもその人物のすべての経験や工夫を反映しているとは限らない。

本ホワイトペーパーでは参考情報として、「回答数」としての数値、すなわち特定の内容に対して回答した協力者の人数（全 16 名）を併記している。ただし、前述のとおり、各協力者が想起できる範囲で回答していることから、この「回答数」は必ずしも正確な実態を示すものではない。また、回答数に基づく単純な比較や議論は適切ではない点に留意する必要がある。

4. マルウェア解析者の業務

インタビューにおいては、協力者に対し、マルウェア解析を実施する業務およびその具体的な事例、各業務の内容・目的、解析のトリガー、ならびに成果・アウトプットについて質問を行った。本章では、そのインタビュー結果をもとに、マルウェア解析に関連する業務を一覧として提示し、各業務の内容、実施の契機となるトリガー、ならびに得られた成果やアウトプットについて順に説明する。

4.1. マルウェア解析者が担う業務

以下に、協力者が担っていた業務の一例を示す（重複を含む）。なお、協力者がすべての業務を単独で担っていたわけではなく、本人が直接担当していた業務に加え、別のメンバーやチームと連携して遂行されていた業務も含まれている。例えば、インシデントレスポンス業務を担う協力者が自らマルウェア解析を実施する事例も存在する一方で、インシデントレスポンスを担当する別のチームからの依頼に基づいてマルウェア解析を行うといった事例も確認された。

以下の表では、協力者本人が直接担っていた業務に焦点を当てて示す。また、4.2 節以降では、これらの業務と他チームとの関係性についても部分的に紹介する。なお、業務の分類として、1〜8 はマルウェア解析の結果を**直接的に活用する業務**であり、9〜14 はマルウェア解析によって得られた**知見や情報を間接的に活用する業務**である。

#	業務	回答数
1	マルウェア解析（他者からの依頼に基づく）	11
2	アラート監視	4
3	インシデントレスポンス	8
4	脅威リサーチ・脅威インテリジェンス作成	14
5	シグネチャ作成	2
6	脅威ハンティング	3
7	セキュリティ教育	5
8	対外活動（情報発信・研究）	13
9	セキュリティポリシー検討	1
10	セキュリティツール検証	1
11	セキュリティ製品・ツール開発	1
12	ソースコード診断	1
13	ペネトレーションテスト	2
14	脆弱性管理	1

4.2. マルウェア解析（他者からの依頼に基づく）

協力者らは、マルウェア解析そのものが業務であり、他者からの依頼に基づいて解析を実施していると述べた。これらの依頼は、依頼元に応じて大きく三つに分類される。すなわち、インシデントレスポンス担当者・チームからの依頼、顧客からの依頼、研究者または研究部門からの依頼である。

インシデントレスポンス担当者・チームからの依頼に関しては、ある協力者が「担当者が手に負えなくなった検体がエスカレーションされてくる」と述べており、他の協力者も「インシデントレスポンス中に解析を完了できないため、役割分担している」と説明していることから、対応困難なケースに対する支援や機能的分業の一環として解析が行われていることがわかる。

また、顧客からの依頼によってマルウェア解析を実施している協力者も多く存在した。これには、セキュリティサービスの一環として契約している顧客からの依頼により、IoC（Indicator of Compromise）やTTPs（Tactics, Techniques, and Procedures）等の情報を抽出する事例が含まれる。さらに、協力者の所属組織内の他部門を経由して解析業務のみを担当するケースも見られた。加えて、外部の研究者や組織内の研究部門と連携を持つ協力者においては、研究支援の一環としてマルウェア解析を実施し、その結果を共有する事例も確認された。これらの依頼に基づくマルウェア解析においては、依頼者に対して所望の情報を提供することが主たる成果であり、その成果物は主にレポートやメモといった文書形式で提供されていた。

4.3. アラート監視

協力者らは、アラート監視業務の一環として、検知アラートがマルウェアによるものであるか否かの判定、アラートの影響調査、アラート自体の分析といった業務を実施していると述べた。これらの業務は、インシデントレスポンスや脅威リサーチと一部重複する側面を持つため、マルウェア解析の技術を有するセキュリティ専門家が関与する業務の多様性、ならびにそれに対する組織ごとの位置づけの違いが示唆される。

検知アラートがマルウェアによるものであるかの判定や、その影響調査に関して、協力者は、アラートを分析する過程で不審なプログラムを発見した場合には、マルウェア解析を通じて正体を特定し、アラート情報のみでは把握できない情報を補完すると述べた。また、マルウェアの挙動、通信先、横展開（ラテラルムーブメント）機能を把握することにより、通信先のブロックによる影響抑制や、横展開の可能性に基づく影響範囲の推定が可能となり、その後のインシデントレスポンスに直結すると説明した。これらの業務におけるアウトプットは多岐にわたり、具体的には、顧客へのレポート、インシデントレスポンスチームへの報告（検体の提供を含む）、他のセキュリティ従事者への IoC 情報や簡易レポートの共有、通信先の遮断処置などが挙げられる。

アラート自体の分析に関連しては、当該アラートから攻撃の傾向を予測し、その予測を裏付ける手段としてマルウェア解析を活用する事例も確認された。協力者の一人は、「アラートの内容が標的型攻撃によるものか、メール配信インフラを経由したものか、あるいはボットネットを介したものか等、攻撃の起点を調査することは重要であり、そのためにマルウェア解析を実施することがある」と述べている。さらに、「通信に含まれるエクスプロイトコードや特徴的な文字列をウェブ上で検索し、それに関連する既知のマルウェアを特定・解析する」との補足もあった。これにより、検知アラートの背後にある攻撃キャンペーンやマルウェアファミリの特定に貢献していることが示唆される。

4.4. インシデントレスポンス

協力者らは、インシデントレスポンス業務の一環として、顧客や社内からのインシデント報告や問い合わせを契機に、マルウェア解析を実施している。不審なファイルが既に特定されている場合には、そのフ

ファイルを直接解析対象とする。一方、ファイルが特定されていない場合には、疑わしい端末群の調査から着手し、不審ファイルを発見・抽出したうえで解析を行うケースも存在する。ある協力者は、「不審なファイルを開封したという問い合わせであれば対応が容易であるが、ゲートウェイのセキュリティ製品（例えば IDS 等）から信頼性の高いアラートがあがった場合には、そのアラートを手がかりに端末を特定し、ヒアリングを通じて該当ファイルを発見し、解析に着手する」と述べている。解析者らは、マルウェアの挙動、通信先、横展開機能、作成ファイルなどを調査し、技術的対処および経営判断に資する情報を収集する。

また、マルウェアの種別によって、特に重視すべき情報が異なる点も指摘されている。たとえば、ランサムウェアの場合には、影響範囲、対象ファイル、攻撃手口、感染経路が重要視される。一方、情報窃取型マルウェアでは、パスワード等の窃取対象が、リモートアクセス型マルウェア（RAT）では、実行可能なコマンドや備えている機能が主たる関心事項となる。

加えて、インシデント対応の初期段階にとどまらず、対応が進んだ復旧段階においても、マルウェア解析が実施されることがある。ある協力者は、「被害者は原因の特定だけでなく、復旧が完了したかどうかの判断にも関心を持っている。その判断支援として、被害組織の端末内にマルウェア関連ファイルが残存していないかといった観点で情報提供を行う」と述べている。

4.5. 脅威リサーチ・脅威インテリジェンス作成

協力者らは、脅威リサーチおよび脅威インテリジェンス作成業務の一環として、主に 3 つの観点からマルウェア解析を実施していると述べた。

第一の観点は、話題性や流行性のある脅威が自組織に与える影響、ならびに現行の対策が有効かどうかを確認するために、最新のマルウェアを解析するというものである。ある協力者は、「自組織を狙う可能性のある話題のマルウェアの挙動を把握し、それがどのようにログ上に痕跡を残すかを確認することで、脅威をどのように検知可能かを検討できる」と述べた。また別の協力者は、「VirusTotal などから最新の検体を取得し、自組織の現行の対策が有効かを確認する。IoC 情報はあるものの、通信先は頻繁に変化するため、検体の持つテクニックや手口が変化していないか、またそれに対応可能かといった観点でも注視している」と述べている。

第二の観点は、攻撃者の視点を調査するために、特定の攻撃者が使用するマルウェアを解析するというものである。ある協力者は、「マルウェアは攻撃者によって作成されたものであるため、その解析を通じて攻撃者の視点や目的を推察することができる。防御側としては、攻撃者の思考や戦略を理解することが極めて重要である」と述べている。

第三の観点は、自組織を標的とする攻撃の傾向を把握するためである。例えば、組織に届いたメールに添付されたマルウェアを解析し、それが属するマルウェアファミリや背後に存在する攻撃者の傾向を明らかにすることにより、自組織の戦略に資する情報を得ることができる。

4.6. シグネチャ作成

協力者らは、シグネチャ作成業務の一環として、定期的に、あるいは最新の脅威情報を入手した際にマルウェア解析を実施していると述べた。シグネチャ作成は、アラート監視サービスにおける付加価値として提供するほか、自組織の防御体制を強化する目的でも実施されている。ある解析者は、「近年では、

SIEM に取り込める Sigma 形式でルールを作成することが多い」と述べている。その上で、「すべての検知項目をルール化するわけではなく、ルール化に値するかどうかを評価したうえで作成する。ばらまき型のマルウェアについては、比較的ルール化しやすく、実際に多くのケースでルール作成が行われている」と補足している。

4.7. 脅威ハンティング

協力者らは、脅威ハンティング業務の一環として、定期的にマルウェア解析を実施していると述べた。具体的には、セキュリティベンダのブログ等に掲載されている攻撃情報やマルウェアの特徴を参照し、それらの情報を基にハンティングを行っている。また、既存の情報に不足がある場合には、マルウェア解析を通じて詳細な挙動や追加の IoC などを補完し、より実効性の高い脅威ハンティングを実施していると説明された。

4.8. セキュリティ教育

協力者らは、セキュリティに関する教育業務の一環として、講義教材の充実およびチーム内の人材育成を目的にマルウェア解析を実施していると述べた。講義教材の充実に関しては、協力者の一部がセキュリティ業務、特にマルウェア解析に関する講義を担当しており、その際に用いるハンズオン教材や紹介用マルウェアの選定を目的として解析を行っている。ある協力者は、「せっかくなら新しく興味深い検体を講義で取り上げたい。そのため資料の更新を目的として解析を実施し、受講者にとって適切なレベルの検体を選定する。しかし、マルウェアの解析阻害機能が原因で、選定は非常に難しい」と述べた。

チーム内の人材育成の一環として、初学者とともにマルウェア解析に取り組む協力者も存在する。マルウェア解析とセキュリティ人材育成の関係について、ある協力者は「セキュリティ人材には、攻撃と防御の両方の視点が求められる。実際の業務においてマルウェア解析を行う人は限られているが、マルウェア解析を通じて両視点を学ぶことができる点で有用である。例えば、マルウェアの解析を通じて攻撃者の挙動や目的を理解し、さらにログを読むことでどこに痕跡が残るのか、なぜ検出されるのかといった実践的な理解を深めることができる」と説明している。

4.9. 対外活動（情報発信・研究）

協力者らは、対外活動業務の一環としてマルウェア解析を実施していると述べた。解析結果をカンファレンスやブログ等で公開することにより、自身や所属組織の技術力をアピールし、社会貢献を通じたプレゼンス向上につなげていると説明した。ある協力者は、「積極的に発信することで、企業に対する関心を高めてもらうことができる」と述べている。また、マルウェア解析者個人の観点からも、対外活動への参加が有益であるとの意見が挙げられた。別の協力者は、「個人の性格にもよるが、対外活動への積極的な関与は、セキュリティコミュニティ内でのつながりを形成し、マルウェア解析者としての成長にも寄与する」と述べている。

4.10. セキュリティポリシー検討

協力者は、マルウェア解析を通じて得られる攻撃者の手口に関する知見が、セキュリティポリシーの検

討業務に活用されていると述べた。具体的には、マルウェアが用いる攻撃手法が既存のセキュリティポリシーに適切に反映されているかどうかの観点から、改善や見直しに関するアドバイスを提供していると説明された。

4.11. セキュリティツール検証

協力者は、マルウェア解析で得られた最新の攻撃手法や傾向に関する知識を活用し、セキュリティツールの検証業務を実施していると述べた。たとえば、EDR（Endpoint Detection and Response）製品などのセキュリティツールを導入する際には、導入前に実際の攻撃手法に即した検証を行うことがあり、その際に流行中のマルウェアや攻撃テクニックに関する知見を検証方法の設計や評価に活用していると説明した。

4.12. セキュリティ製品・ツール開発

協力者は、マルウェア解析によって得られた知見を活用し、OSS（オープンソースソフトウェア）のツールや自社セキュリティ製品の開発業務に従事していると述べた。ある解析者は、自身の所属組織におけるセキュリティ製品の開発チームに参加し、また、セキュリティ専門家向けの OSS ツール開発に貢献していると説明した。加えて、一部の協力者は開発部門に正式に所属しているわけではないものの、製品の開発方針や要件設計に関する意見を求められ、開発チームと連携して活動する機会が多いと述べている。このように、マルウェア解析の知見は、製品開発現場における実用的なフィードバックとして活用されている。

4.13. ソースコード診断

協力者は、マルウェア解析、特に静的解析、とソースコード診断には共通してリバースエンジニアリングの技術が活用されると述べた。その上で、こうした技術を活かしてソースコード診断業務を実施していると説明した。

4.14. ペネトレーションテスト

協力者らは、マルウェア解析を通じて得られる攻撃者の手口や戦略に関する知識を活用し、ペネトレーションテスト業務を実施していると述べた。ペネトレーションテストやレッドチームによるサービスには、現実的かつ実践的な攻撃シナリオや妥当なスコープ設定が求められる。そのため、実際の攻撃事例をマルウェア解析により観測・理解している協力者が、これらの業務に従事するケースも存在する。
また、一部の協力者は、ペネトレーションテストやレッドチームの部署に正式に所属していないものの、当該部署から技術的なアドバイスやコメントを求められることがあり、日常的に連携して業務を行っていると説明した。このように、マルウェア解析の知見は、攻撃者視点を取り入れたリアルな攻撃手法の模倣やシナリオ設計に資する知見として活用されている。

4.15. 脆弱性管理

協力者は、マルウェア解析やアラート監視業務を通じてエクスプロイトコードに関する知見が蓄積されることから、これらの知識が脆弱性管理業務に活用されていると述べた。

5. 業務での主な解析フロー

協力者が業務において実施しているマルウェア解析の主なタスク、およびそれらを組み合わせた解析フローについて、以下の表に示す。本表では、マルウェア解析の実施目的に応じて、大きく二つのカテゴリに分類して説明する。一方は、マルウェア解析（他者からの依頼に基づく）・アラート監視・インシデントレスポンスなど、特定の事象に対して可能な限り迅速な対応が求められる解析である。もう一方は、脅威リサーチ・脅威インテリジェンス作成・シグネチャ作成といった情報収集・分析を目的とした解析である。

解析の目的	解析フロー	回答数
マルウェア解析（他者からの依頼に基づく）・アラート監視・インシデントレスポンス	**検体入手**→検知情報の整理→動的解析(サンドボックス製品)→公開情報調査→動的解析(構築環境)→静的解析・デバッグ	1
	検体入手→検知情報の整理→表層解析→公開情報調査→動的解析(サンドボックス製品・構築環境)→静的解析・デバッグ	1
	検知情報の整理→メモリ解析→**検体入手**→アンチウイルスソフトでのスキャン→静的解析→公開情報調査→動的解析(サンドボックス製品･構築環境)→静的解析・デバッグ	1
	検体入手→表層解析→公開情報調査→動的解析(サンドボックス製品・構築環境)→静的解析・デバッグ	5
	検体入手→検知情報の整理→公開情報調査→動的解析(サンドボックス製品・構築環境)	2
脅威リサーチ・脅威インテリジェンス作成・シグネチャ作成などの情報収集での解析	公開情報調査→**検体選定**→動的解析(サンドボックス製品・構築環境)	1
	公開情報調査→**検体選定**→動的解析(サンドボックス製品･構築環境)→静的解析・デバッグ	5
	検体入手→表層解析→公開情報調査→動的解析(サンドボックス製品・構築環境)→公開情報調査→静的解析・デバッグ	2
	検体入手→表層解析→公開情報調査→動的解析(サンドボックス製品・構築環境)→静的解析・デバッグ	1
	検体入手→動的解析(サンドボックス製品)→公開情報調査→動的解析(構築環境)→公開情報調査→静的解析・デバッグ	3
情報収集での解析(IoT マルウェア)	公開情報調査→**検体選定**→表層解析→静的解析→動的解析	1

協力者が実施したマルウェア解析タスクには、検知情報の整理、公開情報調査、アンチウイルスソフトウェアでのスキャン、メモリ解析、表層解析、動的解析(サンドボックス製品・構築環境)、静的解析・デバッグが含まれていた。これらに加えて、解析の出発点となる検体選定および検体入手といったタスクも存在していた。これらのうち、公開情報調査、アンチウイルスソフトウェアでのスキャン、メモリ解析、表層解析、動的解析(サンドボックス製品・構築環境）、静的解析・デバッグは、複数の協力

者により共通して実施されていた解析タスクであり、これらの詳細な実施方法については第 7 章で具体例を紹介する。

マルウェア解析（他者からの依頼に基づく）、アラート監視、インシデントレスポンスにおける解析に関しては、以下のような解析フローが例として挙げられた：

- **検体入手**→検知情報の整理→動的解析(サンドボックス製品)→公開情報調査→動的解析(構築環境)→静的解析・デバッグ
- **検体入手**→検知情報の整理→表層解析→公開情報調査→動的解析(サンドボックス製品・構築環境)→静的解析・デバッグ
- **検体入手**→検知情報の整理→公開情報調査→動的解析(サンドボックス製品・構築環境)

これらのフローは、セキュリティ製品のアラートやエンドユーザからの報告を契機とする解析プロセスに該当する。協力者によれば、こうした事例では解析対象となる検体は既に特定されており、検知情報や報告内容を整理し、それを手がかりに公開情報調査を実施、続けて動的解析および必要に応じた静的解析・デバッグを行うという流れになる。

なお、セキュリティ製品やユーザからの情報整理段階で、検索キーとなるハッシュ値やファミリ名が得られない場合もあるため、公開情報調査に先立って表層解析や動的解析（特にサンドボックス製品）を用いて情報を取得する必要があるとされた。ある協力者は、「サンドボックスを用いた動的解析は自動化されており比較的低コストで実施できるため、解析初期段階で用いることが多い。ただし、オンラインサンドボックスは外部に検体を送信するため、組織や顧客の取り決め次第では使用できない場合もある」と述べた。

また、**マルウェアが入手できていない場合のインシデントレスポンスにおける解析フロー**の一例として、次の手順が示された：

- 検知情報の整理→メモリ解析→**検体入手**→アンチウイルスソフトでのスキャン→静的解析→公開情報調査→動的解析(サンドボックス製品・構築環境)→静的解析・デバッグ

ここでは、メモリ解析によって検体を抽出する工程が含まれており、いずれのフローにおいても、最終的には検体を入手することが解析の出発点となる。加えて、解析タスクにおける工夫として、複数のアンチウイルスソフトウェアを用い、出力された検知名からマルウェアファミリを推定する手法が紹介された。VirusTotal でも同様の手法が可能であるが、VirusTotal にアップロードすること自体が情報漏洩リスクを伴うため、外部通信を行わないローカル環境で動作するアンチウイルスソフトを使用することにより、リスクを回避することが可能であるとされた。

一方で、**脅威リサーチやインテリジェンス作成など、情報収集を目的とした解析**では以下のような解析フローが紹介された：

- 公開情報調査 → **検体選定** → 動的解析（サンドボックス・構築環境）
- 公開情報調査 → **検体選定** → 動的解析（サンドボックス・構築環境）→ 静的解析・デバッグ

これらは、特定のマルウェアを前提とせず、最新の流行や話題に応じて幅広く情報収集を行う場合に採用される。最初に公開情報を調査し、有用と思われる検体を選定したうえで、動的および静的解析を実施する形式である。

他方で、**すでに検体を入手している状況下での情報収集**においては、以下のようなフローが採られる：

- **検体入手** → 表層解析 → 公開情報調査 → 動的解析（サンドボックス・構築環境） → 公開情報調査 → 静的解析・デバッグ
- **検体入手** → 表層解析 → 公開情報調査 → 動的解析（サンドボックス・構築環境） → 静的解析・デバッグ
- **検体入手** → 動的解析（サンドボックス） → 公開情報調査 → 動的解析（構築環境） → 公開情報調査 → 静的解析・デバッグ

また、**IoT マルウェアの解析においては、動的解析環境の構築が困難であることから、静的解析を優先して実施する**事例も紹介された。ある協力者は、「IoT マルウェアでは x86 や x64 と異なる CPU アーキテクチャが対象となることが多く、そのたびに解析環境を構築するのは困難であるため、まずは静的解析を実施することが多い」と述べた。

このように、解析の目的にかかわらず、「情報収集 → 動的解析 → 静的解析・デバッグ」といった一連の解析プロセスは、協力者間で共通する基本的な流れであるといえる。ただし、解析手順が大きく変化するポイントや、フローの途中で解析を終了する判断がなされる場面も少なくないと協力者らは述べていた。
本章の以降では、そうした**解析手順の違いや、解析の終了条件**について、事例をもとに整理・考察する。

5.1 手順の違い

マルウェア解析においては、目的や状況に応じて解析手順が変化する。協力者の発言をもとに、手順が変化する主な要因として、以下の 4 点を分析した。

(1) 検体を入手しているか否か

すでに解析対象の検体を入手しているかどうかは、手順に大きな影響を与える。検体が入手済みの場合には、検知情報の整理、表層解析、動的解析（サンドボックス製品）、アンチウイルススキャンなどを通じて、ハッシュ値、ファミリ名、接続先等の属性情報を取得し、それらを検索キーとして公開情報調査を行う。一方で、解析対象の検体が未定である場合には、公開情報調査を先行させ、その中で有用と判断される検体を選定する手順が取られる。この検体の選定に関して、ある協力者は次のように述べている。「公開情報調査の中で、業務で割ける時間と検体から得られそうな情報量を天秤にかけて判断している」。

(2) 解析開始時に入手している情報 と (3) 利用可能な解析環境・ツール

解析初期段階で保有している情報の種類や、利用可能な解析ツール・環境も、実施されるタスクや手順に影響を与える。例えば、検知情報にハッシュ値が含まれていれば、当該ハッシュ値をもとに VirusTotal 等で公開情報を検索することで、表層解析と同等の知見を取得することが可能である。一

方、ハッシュ値を含む検知情報が存在しない場合には、表層解析を先行的に実施し、得られた情報をもとに公開情報調査に進むといったフローが取られる。

加えて、動的解析に使用するサンドボックス製品や、アンチウイルスソフトウェアの有無、さらには外部へのアップロード（例：オンラインサンドボックス）の可否といった条件も、組織のセキュリティポリシーや運用ルールに依存し、解析手順の設計に影響を及ぼす。

(4) 解析対象の検体（特に IoT マルウェアか否か）

解析対象が IoT マルウェアであるか否かも、手順選定における重要な変数である。Windows マルウェアの場合、一般的には動的解析 → 静的解析・デバッグという順序が取られるが、IoT マルウェアではこれが逆転するケースがある。

ある協力者は、「IoT マルウェアは x86 や x64 とは異なる CPU アーキテクチャで動作することが多く、対応する動的解析環境の構築が困難であるため、まず静的解析を優先的に実施する」と述べており、動的解析の前段階として静的解析からアプローチする手法が現場で用いられている実態が示された。

5.2. 終了条件

マルウェア解析における終了条件として、協力者らの発言から主に以下の二点が共通して挙げられた。

(1) 解析目的（取得が必要な情報の収集）を達成したかどうか

多数の協力者が、「解析終了の判断は、必要な情報が収集できたかどうかに基づく」と述べている。情報収集や解析レポートの作成を主目的とする業務に従事する解析者は、**静的解析まで丁寧に実施する傾向**が見られた。ある協力者は、「レポート作成に必要な情報や、興味深い挙動の多くは静的解析で得られることが多い」と述べている。一方で、アラート監視やインシデントレスポンスを主業務とする協力者は、「緊急対応に必要な情報は動的解析で把握できるため、静的解析はほとんど実施しない（実施できない）」と述べており、**業務上の緊急度や時間制約が終了条件に大きく影響する**ことが示唆される。

(2) 解析を継続して情報が得られそうかどうか

業務においては、解析にかけられる時間に制約がある。そのため、解析を継続した場合に得られる情報と、それに要するコスト（時間・労力）を比較し、**コストが上回ると判断された場合には解析を終了する**という判断がなされることが多い。

インシデントレスポンスに従事する協力者の一人は、「標的型攻撃やエンドポイントへの侵入が示唆される検体は優先度が高く、緊急対応のために動的解析で必要情報を収集したのち、必要に応じて静的解析まで実施することもある」と述べた。一方で、情報収集を目的とした解析者は、「必ずしもレポートが必要な検体でない場合や、通信が発生せず動作しないなど、解析継続が困難と判断されるケースでは解析を中止することもある」と述べており、**解析可能性や意義の見極めが重要な判断基準**となっている。

また、解析を個人で終了させるのではなく、**役割分担によって解析を引き継ぐ体制**も存在していた。あるインシデントレスポンス担当者は、「動的解析を行いながら対応を進める前線の解析担当と、静的解析

などを担う後方支援の解析担当が分担してインシデントに対応する」と述べており、組織的な分業による効率的な運用も実践されている。

6. 解析環境

解析者らが利用している解析環境の種類について、説明する。

オンラインサンドボックスサービスは、手軽に利用できるという利点がある一方で、マルウェアに関する情報や検体自体を外部にアップロードする必要があるという点で、情報漏洩のリスクが伴う。そのため、使用に際しては組織のセキュリティポリシーや顧客との取り決めを踏まえた判断が求められる。

ローカルのサンドボックス環境としては、商用製品のほか、CAPE v2 をはじめとするオープンソースソフトウェア（OSS）を活用している事例が挙げられた。また、多くの協力者は、物理 PC や仮想マシン上に自前で構築した解析用の環境を利用しており、必要に応じて環境の設定を柔軟に変更できる構成を取っていた。

さらに、一部の協力者は、単体の解析用マシンにとどまらず、**複数の端末、プロキシ、DNS サーバ等を組み合わせて構成した、組織ネットワークに近い高度な解析環境**を用意していた。これにより、マルウェアの横展開や通信挙動の再現・観察が可能となり、より現実的かつ精密な解析が実施できると述べた。

最後に、ある解析者は、**インシデントレスポンスの支援等で関与した顧客の担当者が使用している解析環境**をあえて用いて解析を行うことで、顧客側の担当者に実践的な解析技術や知見を伝える機会を作っていると述べており、解析を通じた教育的側面にも言及があった。

本章では、物理 PC や仮想マシン上に構築する自前の解析環境を対象として説明する。インタビューでは、仮想マシンと物理マシン、OS、インストールするソフトウェア、監視ツール、ネットワークの観点で質問した。本章ではマルウェア解析環境（主に動的解析）についてその環境と工夫点について説明する。

6.1. 仮想マシンと物理マシン

解析環境には、大別して**物理マシン**と**仮想マシン**が存在するが、多くの協力者は仮想マシン上での解析を主に実施していると述べている。

物理マシンにおける解析環境の構築について、ある協力者は「物理マシンでは、解析環境を巻き戻す（復旧する）作業が困難であり、仮想マシンに比べて容易に復旧できない。巻き戻し可能な製品も存在するが、復旧に時間を要する」と述べており、環境の復旧の観点から物理環境の利用は優先度が下がると指摘した。一方で、IoT マルウェアの解析においては、物理デバイスを用いた解析も実施されている。別の協力者は、「IoT 系マルウェアの解析時には、Raspberry Pi（ラズパイ）などの物理デバイスを利用することがある」と述べており、特定のマルウェアに対しては物理環境の必要性があることが示唆される。

仮想マシンの解析環境構築に関しては、性能面への配慮が求められている。ある協力者は、「仮想環境においては、ディスク容量やメモリ容量など、ノート PC 相当以上のスペックを確保するようにしている」と述べており、解析作業に必要なリソースを考慮した構成が重要であると述べた。また、別の協力者は、「スペックの低い環境で実行された際に解析用の仮想環境であることを見破って、動作を停止するマルウェアも存在するため、解析環境のスペックには特に注意を払う必要がある」と述べており、解析対象によっては仮想環境のスペックが解析成否に直結することを指摘している。

6.2. OS

解析者がマルウェア解析において利用しているオペレーティングシステム（OS）は以下のとおりである。

利用されている OS 一覧

- Windows 10
- Windows 7
- Ubuntu
- Tiny Core Linux
- macOS（Mac OS X）
- Android

協力者らは、**組織内で従業員が最も多く利用している PC の OS が Windows 10 であったことから、解析環境にも Windows 10 を採用している**と述べた。一方で、Windows 7 は Windows 10 に比べて、マルウェア以外のバックグラウンド通信などの“ノイズ”が少ないという理由から、解析精度の向上を目的に利用されるケースもあると補足された。また、解析対象となるマルウェアが macOS や Android 端末を標的としている場合には、対象 OS に応じた解析環境を構築し、macOS や Android を使用する事例も確認された。加えて、IoT マルウェアの解析においては Linux 系 OS が活用されており、Ubuntu や Tiny Core Linux を用いた環境構築が行われている。とくに Tiny Core Linux は、「軽量であること」「必要最小限の構成で容易にカスタマイズできること」といった利点があり、IoT 系マルウェアの検体実行や挙動の観測に適していると説明された。

このように、解析対象のマルウェアの特性や標的環境に応じて、適切な OS を選定し解析環境を構築することが、実務上の重要な判断要素となっている。

6.3. インストールするソフトウェア

解析環境においては、マルウェアの挙動を引き出すため、あるいは情報窃取などの目的を成立させるために、**マルウェア実行に必要な前提条件や実行対象となるアプリケーションを事前にインストールしておく必要がある。**以下は、協力者らが実際に解析環境内へ導入している代表的なソフトウェアの一覧である。

解析環境にインストールされるソフトウェアの一例：

- Visual C++ Redistributable
- Microsoft Office
- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Java
- .NET Framework

協力者らは、これらのソフトウェアをマルウェアの正常な実行や挙動の再現、または窃取対象となる情報を達成させる目的で活用していると述べた。特に Microsoft Office については、特定の脆弱性を悪用するマルウェアが多く存在するため、特定のバージョンよりも古い Office をインストールした環境を用意することで、解析が円滑に進む場合があると説明された。

また、言語環境についても考慮されており、日本語環境および英語環境の両方を準備することで、特定言語圏を標的としたマルウェアへの対応が可能となる。これにより、マルウェアが環境変数やロケールに応じて異なる挙動を示すケースにも対応できる柔軟な解析環境が構築されている。

このように、解析対象のマルウェアの特性や依存条件を踏まえ、適切なソフトウェアを事前に導入した環境を構築することが、効果的なマルウェア解析を行ううえで極めて重要である。

6.4. 監視・ロギングツール

マルウェアの挙動を監視し、各種ログを取得するために、解析者らは目的や好みに応じて複数のツールを選定・導入している。こうしたツールの導入は個別に行うこともあるが、多くのツールを一括でセットアップできるディストリビューション「FLARE-VM」が活用されるケースも多い。FLARE-VM を利用することで、解析ツール群を効率的に環境へ導入することが可能であると、協力者らは述べている。

また、自組織で導入している EDR 製品を解析環境に組み込むことで、マルウェアが実際にどのように検知・対応されるかを確認する取り組みも一部で行われている。ただし、こうした製品の導入にあたっては、本番環境に悪影響を与えるリスクや、ライセンス・ポリシー上の制約が存在する場合があるため、十分な注意が必要であると補足された。

さらに、ある協力者は、「解析回避の手法として、マルウェアが監視ツールのプロセス名を検知し、それに応じて挙動を変える場合があるため、解析用ツールのプロセス名を変更して運用している」と述べ、ツールの導入・運用時の工夫についても言及した。

解析環境で利用される主な監視ツール

以下は、協力者らが実際に活用している主な監視・ロギングツールである：

- Process Monitor
- Process Hacker
- Process Explorer
- Noriben
- API Monitor
- Task Manager（タスクマネージャ）
- Autoruns
- Regshot
- Sysmon
- Wireshark
- TCPView
- FakeNet-NG

- 自組織導入の EDR 製品

これらのツールは、プロセスの生成や終了、レジストリ変更、ファイル操作、ネットワーク通信など、マルウェアの多岐にわたる挙動を詳細に記録・観察することに寄与する。適切な組み合わせによる導入と設定により、マルウェア解析の網羅性および効率性を大きく向上することが可能となる。

6.5. 通信の模倣・監視

協力者らは、マルウェアの通信を模倣・監視することを目的として、専用のツールや解析環境を構築することがあると述べた。マルウェアは、攻撃者が管理する C2 (Command and Control) サーバと通信し、レスポンスに応じて挙動を変更するほか、別のマルウェアをダウンロードしたり、追加機能をアップデートしたりすることがある。

そのため、解析環境から実際の攻撃者サーバへ通信が発生した場合、情報漏洩や攻撃者側に解析情報を与えるリスクが存在する。このようなリスクを回避するため、解析環境の外部通信を完全に遮断する運用を行うこともある。一方で、通信後のマルウェア挙動を観察する必要があるケースにおいては、攻撃者との通信を模倣する環境を構築することがある。

このような通信模倣の手法としては、以下のような構成が確認された：

- 解析環境内で稼働する **FakeNet-NG** などのローカルでのツール活用
- **FakeDNS** や **INetSim** 等のツールを利用し、解析環境と同一ネットワーク内に設置した模擬サーバと通信させる構成
- **Apache 等で自作した模擬（HTTP）サーバ**を用い、より柔軟なレスポンス設計を可能とする構成

ある協力者は、自作サーバを用いた通信の模倣について、「公開情報を収集して特定した実際の攻撃者サーバからのレスポンスを再現し、それを自作サーバに設定する。さらに、同一ネットワーク内に構築した DNS サーバにおいて、当該攻撃者サーバのドメインに対する名前解決先を自作サーバに変更することで、通信を模倣している」と説明した。

このような構成により、**マルウェアが実環境と同様に通信先へ接続しようとした場合でも、リスクを回避しつつ挙動の再現と解析が可能となる。**

7. 解析方法

本章では、協力者が説明した表層解析、公開情報調査、動的解析、静的解析・デバッグの主な解析方法について概説する。

7.1. 表層解析

5 章で述べたとおり、検体の入手状況によっては、表層解析を実施しない解析者も一定数存在した。一方で、不審ファイルを入手しているもののハッシュ値などの属性情報が不明である場合には、表層解析を通じて必要な情報を取得する手順が一般的に採用されている。特に、ファイルのハッシュ値を取得し、それを用いて公開情報調査へと進む流れが確認された。

表層解析で取得可能な主な情報

以下は、協力者らがインタビューにおいて言及した、表層解析により取得可能な主な情報である。特に文字列抽出に重きを置く解析者が多く、通信先が平文で記述されているケースでは、得られた文字列を用いた公開情報調査が有効であるとされた。加えて、協力者らはオンラインサンドボックスや VirusTotal 等のサービスが提供する情報の中に、表層解析で得られる情報が含まれていると指摘しており、これら外部サービスの活用によって作業を効率化できる場合もあると述べている。

- **ファイル名**
  ファイルに付されている名称。
- **ファイルタイプ**
  実行ファイル（PE、ELF など）、スクリプト（VBS、JS など）といった形式の識別
- **ハッシュ値（MD5、SHA-1、SHA-256 など）**
  一意な識別子として、VirusTotal 等のサービスを用いた既知マルウェアとの照合に利用
- **文字列（およびその特徴）**
  ファイルに含まれる文字列であり、通信先 URL、コマンド、内部識別子、ソースコードの一部などが含まれる可能性がある。
- **アイコン**
  リソースに埋め込まれている画像データ
- **Import するファイル・API**
  実行時に呼び出される外部ライブラリや API 関数の一覧
- **証明書**
  デジタル署名の有無や署名者情報
- **ファイルの作成時間**
  ファイル作成のタイムスタンプ
- **パッカー（Packers）**
  マルウェアが使用しているとみられるパッカーの種類

表層解析に用いられる代表的ツール

以下は、協力者らが表層解析において使用している代表的なツール群である。協力者らはファイルタイプや解析対象に応じて適切なツールを選定することが重要であると言及した。例えば、PeStudio は PE ファイル、Viper Monkey は VBA、Detect It Easy は PE や ELF といった実行形式のファイル全般を確認し、ファイルのヘッダ情報といったメタ情報を解析することができる。

- **PeStudio**
  PE ファイルの構造を視覚的に把握できる解析ツール
- **Strings**
  バイナリファイルからプレーンテキスト文字列を抽出するコマンドラインツール
- **PE-bear**
  PE ファイル内部構造の詳細な可視化・編集を可能とするツール
- **Stirling**
  バイナリエディタ
- **ImHex**
  バイナリエディタであり、データ構造テンプレートを用いた解析が可能
- **CFF Explorer**
  PE ファイルの詳細な解析・編集に特化したツール
- **Resource Hacker**
  PE ファイルに埋め込まれたリソース（アイコン、ダイアログ、文字列など）の抽出・変更が可能なツール
- **FileInsight**
  Hex 表示と構造解析機能を備えたセキュリティ向けバイナリエディタ
- **Viper Monkey**
  VBA マクロの解析に特化した静的解析ツール
- **Detect It Easy（DIE）**
  バイナリファイルの種類判別およびパッカー検出を行うためのツール

7.2. 公開情報調査

公開情報調査とは、マルウェアに関する既存の解析情報やレポートを外部から収集する手法であり、他の解析者や組織が公開している知見を活用することで、解析業務の効率化を図るものである。協力者らは、必要な情報を公開情報調査によって得られた場合、自身での動的解析や静的解析を省略でき、業務上の効率性向上に大きく寄与すると述べている。

公開情報で収集する主な情報

協力者らが公開情報調査を通じて特に頻繁に収集すると述べた情報は以下のとおりである：

- 投稿日時
- ファイル名

- ハッシュ値
- 特徴的な文字列
- 通信先サーバのバージョン
- 通信先サーバの OS
- 通信先サーバのソフトウェア
- 通信先サーバのポート
- マルウェアファミリ名
- Config（構成ファイル）情報
- 通信先のドメイン・IP アドレス・ポート番号
- パッカー
- 挙動（ファイル操作・レジストリ操作等）
- キャンペーン情報（攻撃活動全体の特徴）
- HTML や Web 通信の構造
- 通信の特徴（プロトコル等）

検索方法と情報収集先

協力者らが活用している情報源および検索対象カテゴリを以下に示す：

カテゴリ	サイト名（情報源）
マルウェアに関するサービス	Malware Bazzar
	Any.run
	Tria.ge
	VirusTotal
	Joesandbox
	Hybrid Analysis
通信に関するサービス	shodan
	Censys
	urlscan.io
	PassiveTotal
	VirusTotal
検索エンジン	Google
	Duckduckgo
その他	X・Twitter
	github
	セキュリティベンダのブログ
	公開レポート

検索手法の例

協力者らが実施していた公開情報調査に関して、その検索手法を「検索キー」と「検索先」に着目して分類し、5 つの代表的な例としてまとめた。これにより、実務においてどのような観点から情報収集が行われているかを明示する。

- **(a) ハッシュ値をキーとした調査**

  協力者らは、表層解析などで得られたハッシュ値をキーに、VirusTotal、Tria.ge、Any.run などのサービスで検体を検索していた。**一つのサービスに依存せず、複数のサービスを併用することで情報の網羅性を高める**といった方針を取る傾向にあった。

- **(b) マルウェアファミリ名をキーとした調査**

  不審ファイルの検知名や各種解析サービス（VirusTotal の Community のコメント、JoeSandbox 等）からファミリ名を特定する。その名称を用いて検索エンジンで検索し、セキュリティベンダの技術ブログ等を確認することで、挙動や特徴の調査を行うという手法がとられていた。

- **(c) 通信先をキーとした調査**

  C2 サーバなどの通信先情報をもとに、Shodan や urlscan.io などでサーバの OS やポート、証明書、ソフトウェア構成を調査する例があった。ある協力者は「特定のマルウェアファミリが利用する C2 サーバの OS、バージョン、開放しているポート番号、証明書がといった情報がわかると、shodan などから類似したサーバを探すことが可能で、これらの情報で類似しているかどうかを判断できる。攻撃者もサーバのデプロイはビルダーで行っているのでサーバの構成は類似すると推察していると述べた。加えて、「あるファミリの検体を発見したいときに、既知の検体の C2 サーバと類似する C2 サーバを発見することで、VirusTotal で当該類似サーバへ接続する検体を調査すると同じファミリの検体だということもある」と補足した。

- **(d) 特徴的な文字列をキーとした調査**

  strings 等を用いて抽出された文字列のうち、特徴的なものを Google や GitHub で検索する手法が紹介された。ある協力者は「特徴的な文字列を Google で検索すると情報が得られる」と述べ、別の協力者は「マルウェアが github 上の OSS を活用して作成されている場合があるので、特徴的な文字列を GitHub で調べると活用した OSS が見つかることもある。README を読むと機能が書いてあり、解析のコストを下げることにつながることもある」と説明した。

- **(e) SNS や検索エンジンでの広範な調査**

  SNS や検索エンジンでハッシュ値、通信先、特徴的な文字列、ファミリ名などをキーに幅広く検索すると協力者らは説明した。ある協力者は「X(旧 Twitter)でハッシュ値や特徴的な文字列、通信先で検索すると、類似した事例についての投稿が見つかるときがある」と述べ、別の協力者は「Google 検索をするが、他の検索エンジンと併用することも有用だと思う。duckduckgo とかだとロシア圏の情報が出てきやすいと聞いたことがある」と述べた。

7.3. 動的解析

動的解析で収集する情報

動的解析では、**マルウェアを実行させることで得られる挙動に基づき、通信先やファイル操作、レジストリ変更、プロセス生成等の情報を観察・収集する**。協力者らは、特に**通信先に着目することが多く、初期対応の判断材料や防御策の立案において重要な手がかりとなる**と述べた。

以下は、動的解析で収集される主な情報である：

- 通信先（IP アドレス、ドメイン名）
- 通信プロトコル
- 通信先のポート番号
- 通信内容（送信データ、コマンド等）
- 通信先の属性
- 通信先の使い回し（既知の攻撃、キャンペーンとの重複性）
- ドロップするファイル
- ダウンロードするファイル
- 操作するファイル（作成、削除、編集など）
- 操作するレジストリ
- 関連プロセスの生成・終了
- C2 サーバからの RAT コマンド（実行指示内容）
- ランサムウェアが付与する拡張子および脅迫文の内容

協力者の多くは、通信先の特定とプロキシ等でのブロックを、特にインシデントレスポンスやアラート監視業務における優先度の高いタスクと位置付けていた。また、協力者らは動的解析において、マルウェアによる検知回避（anti-analysis）の兆候がないかも確認すると述べている。ある協力者は「サンドボックスの結果で ATT&CK でいう Defense Evasion の機能がないかは確認する。特定のプロセスを確認して検知しているといったログがあったら、うまく動作していない可能性があるので方針を考え直す必要がある。また、ログを見てマルウェアが動作していない場合、プロセスインジェクションや dll サイドローディングされる可能性がある。そのため、例えば、dll を操作してないか、操作しようとしてないかといった点を確認する」と説明した。

安全な動的解析実施の注意点

動的解析ではマルウェアを実際に実行するため、誤って感染を拡大させてしまうリスクが存在する。そのため、協力者らは以下のような安全対策を講じて解析を実施している。

タイミング	安全性の注意点
解析前	仮想環境上での構築
	ファイル共有をホストからゲストに制限
	解析マシンと通信するマシンはマルウェアの対象とは異なる OS を利用
	ホストとゲストを区別しやすい壁紙に設定
解析中	マルウェアであることが分かるファイル名に設定
	実行時以外はマルウェアを暗号化 Zip として管理
解析後	C2 サーバへの通信の制限・ネットワークの切断
	ホストマシンとのファイル共有の停止
	ホストマシンとゲストマシンのコピーアンドペーストを制限

7.4. デバッグ

デバッグは動的解析の一手法であるが、協力者らはその実施タイミングとして静的解析と併用するケースが多いと述べている。特に、逆アセンブルやデコンパイルされたコードと併せて、処理の流れや実行時の変化を追跡する目的で用いられる。本節では、デバッガの種類とデバッグの目的について概説する。

デバッガの種類

協力者らは、代表的な静的解析ツールである IDA Pro や Ghidra に付属するデバッガ機能を活用すると述べており、特にコードの解析とデバッグを連携させることで効率を高めている。さらに、解析対象の形式や環境に応じて、以下のような多様なデバッガを使い分けていると補足された。

- **x64dbg**
  Windows 環境で広く用いられる 64bit 対応の高機能デバッガ
- **OllyDbg**
  軽量で逆アセンブル表示に優れる 32bit 専用の Windows 用デバッガ
- **BlobRunner**
  マルウェア分析中に抽出したシェルコードなどを動的に実行することに特化したツール
- **LoadDll**
  DLL ファイルの解析に特化したツール
- **Immunity Debugger**
  セキュリティの専門家向けにスクリプトによる自動化や拡張性を高めたデバッガ
- **strace**
  Linux 環境において、システムコールのトレースするツール

デバッグの目的

協力者らは、デバッグの目的として以下の 4 点を主に挙げていた：

1. **難読化の解析**
   マルウェアに施された難読化を解除し、実際の処理内容を把握する。特に動的な API 解決等に対応するために、デバッガによる追跡が有効である。
2. **挙動の詳細把握**
   静的解析では容易に判別できない挙動、分岐条件やメモリ上の変化の確認に活用される。
3. **暗号化・復号処理の解析**
   C2 サーバと通信する際に暗号化されるパラメータや、マルウェアが内部で扱う構成ファイルなど、復号処理の中間値を取得するためにブレークポイントを設定して観察する手法が用いられる。
4. **解析回避機能への対応**
   マルウェアがデバッガやサンドボックスを検知して挙動を変化させるケースに対し、検知条件を特定し、パッチを当てることで解析回避機能へ対応し、解析の継続を実現する。

7.5. 静的解析

マルウェアが動的解析環境で正常に動作しない場合や、より詳細な内部構造や処理内容を把握したい場合に静的解析が実施される。協力者らは、静的解析が脅威リサーチなどの情報収集系業務において特に重要であると強調していた。一方で、インシデントレスポンスやアラート監視を主業務とする解析者においては、対応時間の制約等から静的解析を実施しないことも多く、業務の性質により静的解析の位置付けが異なることが示唆された。

静的解析で使用されるツール

協力者らが静的解析で使用している代表的ツールは以下のとおりである。IDA Pro および Ghidra が最も多く利用されていたが、対象検体の形式に応じて.NET 系のツールを使い分けていると補足された。

- **IDA Pro**
- **Ghidra**
- **Hex-Rays Decompiler**
  IDA Pro に付属する C 言語へのデコンパイル機能を提供するプラグイン
- **dnSpyEx**
  . NET マルウェアの解析に特化したデコンパイラ
- **dotPeek**
  .NET アセンブリの解析ツール
- **ILSpy**
  オープンソースの.NET デコンパイラ

静的解析の起点とアプローチ

静的解析におけるアプローチは、対象の目的や前段階の解析状況に応じて複数のパターンに分かれる。協力者らが活用していた主な起点は以下のとおりである：

- **気になる機能から**
  明確な目的を持って、通信、暗号化手法など気になる処理と関連する Windows API を呼び出している箇所から分析する。
- **特定の文字列から**
  通信先ドメインやファイルパスなど、strings 等で抽出された文字列を起点に追跡する。ファミリの特定や通信処理の解明につながりやすい利点を有する。
- **前段階（動的解析等）で不明だった点の補完**
  動的解析で挙動の一部が判明している場合、動的解析で不明だった点の関連処理に絞って静的解析を実施する。特にインシデントレスポンスに従事する協力者がこのアプローチをとる傾向にあった。
- **メイン関数から順に解析**
  実行フローの全体像を把握するために、エントリーポイントから順に辿る。

ある協力者は「動的解析で通信先がわかった場合、その文字列を参照している処理や、通信を行う API 呼び出し付近を中心に調査する」と述べた。別の協力者は「構造が複雑な場合、通信処理や特徴的な文字列を先に確認する」と述べつつ「**柔軟な視点の切り替えが静的解析を進める上で重要である**」と説明した。

静的解析の着目点

静的解析では、以下のような機能や処理を重点的に確認することで、マルウェアの機能特性や攻撃ベクトル、解析回避機構の有無を明らかにする。

- レジストリ操作の有無と内容
- 攻撃機能の存在と攻撃ベクトルの特定
- 通信処理（ドメイン解決、プロトコル、暗号処理等）
- 解析検知・回避機能の有無と手法
- マルウェアファミリの特定に資する構造・文字列
- 難読化の有無とその方式
- RAT におけるコマンド処理
- 特定の Windows API の呼び出し状況
- Config の内容と構造体定義
- 使用するモジュールやライブラリ（Import 情報）
- 悪用される脆弱性（CVE 情報など）
- 情報窃取処理の対象（ブラウザ、証明書、キーストローク等）
- ランサムウェアの暗号方式・鍵の取扱・対象ファイルの特定方法・拡散手法・拡張子・脅迫文など

ある解析者は、通信処理に着目することについて、「インシデントが発生した場合、窃取された情報などを明らかにするため通信をすべて復号する必要がある。その際に、マルウェアの通信の復号処理を中心に見ることになる」と述べた。別の協力者は「Config 情報や文字列が構造体になっているので、それを特定して IDA Pro でエクスポートして残す。マルウェアがバージョンアップしても構造体は変化してないことも多く、構造体を共有している」と説明した。

8. おわりに

本資料は、マルウェア解析に従事する専門家へのインタビューを基に、実務におけるマルウェア解析の実態および現場での工夫を整理・共有することを目的とし、国内におけるセキュリティ対策の強化に資する知見を提供するものである。

前半では、マルウェア解析業務の実務的側面に焦点を当て、解析によって取得される情報の種類とその意義を明確化したうえで、具体的な活用事例を整理した。アラート監視、インシデントレスポンス、脅威リサーチ、ならびに解析知見の他業務への応用といった観点から、マルウェア解析の多様なユースケースを提示するとともに、典型的な業務フローとその分岐条件についても体系的に記述した。

後半では、マルウェア解析技術そのものに焦点を移し、解析環境の構築方法や使用ツールの構成要素について解説した。さらに、表層解析、公開情報調査、動的解析、静的解析、デバッグといった各種解析手法について、実務での具体的な活用例や着目すべき視点を踏まえて概説を行った。

本資料が、マルウェア解析を担う実務者にとって、既存知見の整理や業務改善の一助となり、ひいては組織全体のインシデント対応力および脅威分析力の向上に資することを期待する。加えて、本資料に示した解析者の業務実態や直面する課題が、マルウェア解析者のマネジメント層における組織運営の改善にも資するものと考える。今後も、現場に根ざした知見の継続的な蓄積と共有を通じて、より高度で効果的なセキュリティ運用体制の構築が進展することを望む。

謝辞

本調査プロジェクトでは、マルウェア解析チームの役割と連携強化に向けたコミュニケーション課題の調査を実施しました。その調査結果は、下記論文として投稿公開しています。本ホワイトペーパーならびに下記論文の作成にあたりインタビューにご協力いただいた専門家の方々、コメント・議論いただいた方々に深く感謝致します。

Title: Collaborative Work in Malware Analysis: Understanding the Roles and Challenges of Malware Analysts

Authors: Rei Yamagishi, Shota Fujii, Shingo Yasuda, Takayuki Sato, Ayako A. Hasegawa

URL：https://dl.acm.org/doi/full/10.1145/3706598.3713652

付録. 解析遂行上の課題

インタビューにおいて協力者らは、マルウェア解析の遂行に際して直面する課題について言及した。これらの課題は、今後の研究や実務的改善において解決が期待される重要な論点であることから、本資料の付録に一覧として記載した。各課題は内容に応じてカテゴリおよびサブカテゴリの二階層に分類した：

カテゴリ	サブカテゴリ	課題
解析継続の困難性	C2 サーバへのコネクションの成功	C2 サーバがすぐに閉じてしまうので接続するタイミングを見つけるのが難しい
	追加ファイル等のダウンロード	二次以降の検体がダウンロードできないと解析が進まない
		DLL がないと解析が進まない
	挙動を観測できる解析環境	脆弱性のあるバージョンのソフトウェアがないと解析ができない
	解析環境の検知	同一の環境から C2 サーバに接続するのでフィルタされる懸念がある
		解析検知機能で解析が進まない
	クローズドなコミュニティへの潜入が困難	discord などクローズドなサービスとの通信
検体入手の困難性	脅威リサーチ・脅威インテリジェンス作成	外部レポートで話題になっていても VirusTotal などで発見できないことがある
		特定組織を対象とする検体が入手できない
	インシデントレスポンス	メモリの中が消えていると解析できない
解析環境の高度化が抱えるトレードオフ	解析効率化とのトレードオフ	解析環境のノイズ抑制などをやりすぎると解析環境だと気づかれるリスクがある
	解析環境の安全性とのトレードオフ	安全性の観点から通信を外に出せないので解析でできることが限られる
解析環境準備・管理の困難性	解析環境を充実させる予算不足	導入できるツールは予算次第になってしまう
	会社・業務の方針での解析リソース不足	情報漏洩の懸念でオンラインサンドボックスが利用できない
		業務で利用できる解析のリソースが限られる
	解析環境構築のコスト	環境の定常通信など解析のノイズになる通信を減らすことが大変
	複数解析環境の準備と管理	Linux マルウェアは動作するアーキテクチャを用意する必要があり大変
		解析検知回避のために複数環境やリージョンを用意しているが準備や管理が困難
解析の自動化・効率化不足	自動化するための時間確保不足	時間がなく自動化できてない部分がある（静的解析のスクリプト）
		時間がなく自動化できてない部分がある（動的解析）

	一部作業の効率化ができてない	統計的な分析の効率化ができない
	ツールの開発とツールが必要な時期のズレ	ツール開発は必要になって行われるため、ツールが必要な時期とツールが利用可能になる時期にずれが生じる
	大規模言語モデルの活用	LLM を活用して作業を効率化したいが現状ではできてない
解析中の判断の困難性	不審・悪性の判断	何をもって不審とするかの判断（特に情報窃取型）
	コストを鑑みての解析継続の判断	難読化解除のコストを考えて落としどこを見つけるのが大変
		工数と興味の妥協点を見つけるのが難しい
解析方法・手順のノウハウ共有・体系化不足	解析者教育の困難性	解析のスキルは一般化しづらく教育が困難
		静的解析までできるようになるには時間がかかる
	解析手順の体系化	解析手順が体系化できてないので、実施忘れがある可能性がある
		解析のスキルは一般化しづらい
	解析方法の統一	コメントの仕方など解析方法が人によって異なる
	利用ツールでの互換性・ツールの違いによるノウハウ共有	IDA Pro ユーザと Ghidra ユーザでのノウハウ共有が難しい
	結果の MITRE ATT&CK へマッピング方法	解析結果を MITRE ATT&CK へマッピングする際、人によって結果が異なる
	解析のメモや結果の書き方	読みやすいフォーマットのベストプラクティスが見つかってない
		解析メモや結果の検索性が低い
攻撃や環境の変化への対応の困難性	マルウェアの変化	解析すべきアーキテクチャが多様化
		マルウェアの難読化技術の多様化・進化
	マルウェア解析だけでは不十分	攻撃がマルウェアだけでない

以下では、表の内容それぞれの内容をカテゴリごとに補足する。

(1) 解析継続の困難性

マルウェアの挙動を継続的に観測・分析する過程で発生する困難が示されている。C2 サーバへのコネクションの成功に関しては、C2 サーバが短期間で停止するため、C2 サーバとコネクションが成立するタイミングを見極めて解析し、通信に成功することが困難であると協力者は言及した。関連して、追加ファイル等のダウンロードに関する課題も挙げられた。解析を進めるうえで必要となる二次以降の検体や依存 DLL の取得ができず、解析が継続できない問題がある。挙動を観測できる解析環境では、攻撃対象の特定バージョンのソフトウェアが入手困難であり、観測に適した環境が整備できないことが障壁となっている。解析環境の検知では、同一環境からのアクセスがフィルタ対象となる懸念や、マルウェアに実装された環境検知機能により挙動が抑制されることがある。最後に、クローズドなコミュニティへの潜入が困難な点が課題として挙げられる。一部攻撃の分析に過程で、Discord のクローズドなサーバー等の

非公開のコミュニティに行きつくこともあるが、コミュニティの内部は把握が困難なため、解析の継続が困難となる。

(2) 検体入手の困難性

解析の出発点となる検体の入手が困難である課題も、多くの協力者が直面していた。脅威リサーチ・脅威インテリジェンス作成において、協力者は VirusTotal 等からマルウェアを入手する。しかし、外部の技術記事で報告された脅威が VirusTotal 等に公開されておらず取得できない場合があり、同様の脅威を再現・分析できないことがある。また、特定組織を標的とした検体は、解析対象として関心を持つ協力者が多い一方で、公開されておらず入手することが難しいことも指摘された。インシデントレスポンスに関連する検体では、メモリ上の痕跡が揮発してしまっており、解析に必要な情報が失われていることがある。

(3) 解析環境の高度化が抱えるトレードオフ

解析環境を高機能化する一方で、他の要件との間にトレードオフが発生する。解析効率化とのトレードオフで、協力者はノイズ除去等の対策が過度になると、マルウェアに環境と認識され、挙動を抑制される懸念があることを指摘した。一方でノイズ除去を実施しない状態での解析は負担が増加するため、トレードオフの解消に苦心している。解析環境の安全性とのトレードオフ においては、安全性確保のためにインターネットへの通信を遮断する必要があり、マルウェアの通信型挙動が観測できなくなるなどの制約が生じる。

(4) 解析環境準備・管理の困難性

解析環境の整備と維持に係る負担も課題として挙げられている。解析環境やツールを充実させると解析が効率化・高度化されるが、必要なツールの導入可否が財政的制約に左右される。また、会社・業務の方針での解析リソース不足も指摘された。情報漏洩リスクへの配慮からオンラインサンドボックスの使用が制限され、業務で利用できるリソースが限られている事例も存在した。解析環境構築のコストにおいて、定常的な通信や余計なログを削減するための作業等に工数がかかることも指摘された。最後に、複数解析環境の準備と管理が困難であると説明された。例えば、Linux マルウェア等に対応するための特定アーキテクチャの準備が必要であるが、準備や管理コストが必要となる。加えて、解析検知回避のために複数の環境を整備する必要がある（通信元、言語の異なる環境など）が、その管理は煩雑である。

(5) 解析の自動化・効率化不足

効率的な解析を実現するための自動化が不十分である点も課題である。自動化するための時間確保不足により、静的・動的解析に必要なスクリプトの整備が後回しになることが多い。一部作業の効率化ができていない事例としては、統計的な分析作業の自動化・省力化が進んでいないことが挙げられる。また、ツールの開発とツールが必要な時期のズレも指摘された。攻撃が観測され、必要になった時点でツール開発が始まるため、ツールが開発されたタイミングではツールが間に合わないことが多い。大規模言語モデルの活用に関しては、LLM を活用した作業効率化の期待がある一方で、インタビューの 2024 年時点では十分に活用できていないことが指摘された。

(6) 解析中の判断の困難性

マルウェア解析においては、分析者の判断を要する場面で多くの困難が報告されている。不審または悪性と評価すべき挙動の判別基準が曖昧である点が顕著である。例えば、業務利用が想定される正規のアプリケーションであっても、一部の情報を外部サーバに送信する機能を有している場合がある。このような通信挙動について、協力者は観測された情報の送信がマルウェアに特有の悪意あるものか否かを判断することは容易ではないことを指摘した。解析作業の継続可否に関しても、コストとのバランスを考慮した判断が求められるが、その基準設定の困難性が指摘されている。特に、難読化が高度かつ煩雑なマルウェアに対しては、解除に要する労力が非常に大きくなる一方で、その労力に見合う成果が得られるか否かを評価することは困難である。このような状況において、解析の打ち切りを判断する明確な基準が存在しないことが、実務上の課題となっている。

(7) 解析方法・手順のノウハウ共有・体系化不足

解析の実施・教育・共有に関する体系化の欠如も顕著な課題である。解析者教育の困難性では、解析スキルが属人的であり、一般化が困難なため教育に時間と労力を要することが指摘された。同様に、解析手順の体系化の不備により、標準手順がなく、実施漏れのリスクが存在することを懸念する協力者も存在した。また、解析方法の統一では、コメントの付け方や作業手順が解析者ごとに異なり、情報共有に支障をきたすと多くの協力者が述べた。利用ツール間の互換性・ノウハウ共有に関しては、IDA Pro と Ghidra など、ツール間でのノウハウ移転が難しいことも指摘された。また、解析結果を MITRE ATT&CK へマッピングして報告する協力者も存在した。その一方で、MITRE ATT&CK へのマッピングも属人的で、同一の結果を見ても解析者間でマッピングが異なることも指摘された。解析結果・メモの記録や共有方法においてもフォーマットが確立されておらず、結果の共有性や検索性に課題が残る。

(8) 攻撃や環境の変化への対応の困難性

攻撃手法および解析対象が急速に変化する中で、従来の解析手法では対応が困難となるケースが増加している。特にマルウェアのアーキテクチャや難読化技術の多様化が進み、これに対応するためには解析者の専門的スキルの向上に加え、解析支援ツールの拡充が不可欠である。解析者への負担も増加するため、課題として挙げられた。加えて、近年の攻撃はマルウェア単体にとどまらず、複数の手段や段階的な攻撃が組み合わされることが一般的となっていることが指摘された。

更新履歴

2026 年 2 月 13 日 1.0 版

セキュリティ業務におけるマルウェア解析の調査 1.0 版

2026 年 2 月発行

企画・製作

国立研究開発法人情報通信研究機構 / 株式会社日立製作所

著者

佐藤 隆行（株式会社日立製作所） 安田 真悟（国立研究開発法人情報通信研究機構）

お問合せ

国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所 サイバーセキュリティネクサス

CYNEX アライアンス事務局

〒184-8795 東京都小金井市貫井北町 4 – 2 – 1

URL https://cynex.nict.go.jp

Mail cynex@ml.nict.go.jp