2019 年度 委託研究

課題 216

サイバー攻撃ハイブリッド分析実現に向けた セキュリティ情報自動分析基盤技術の研究開発

研究計画書

国立研究開発法人
情報通信研究機構

１．研究開発課題

『サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発』

２．研究開発の目的

マルウェアへの感染は世界的な社会問題となっており、特に政府や重要インフラ事業者などに対する脅威は増加の一途をたどっている状況であるが、感染活動の早期把握やそのマルウェアに関する情報の関連組織間での共有ができていない。そのため、セキュリティインシデント発生後の初動対応が遅れ、機密情報の漏えいなどの重大なインシデントにつながるケースが多く発生している。

この問題の解決には、セキュリティインシデント発生の可能性をより早く検知し、それを分析するための関連情報を自動的に生成し、関連付け、そのインシデントのもととなったマルウェアや脆弱性を分析する必要がある。これらのタスクは大量のデータを分析することが求められるため、人手による分析は非現実的である一方で、コンピュータによる自動処理の効果が大きく期待できる領域である。また、これらの分析は単一の分析にて完結するものではなく、例えばライブネットトラフィック分析やダークネットトラフィック分析、マルウェア分析、脆弱性分析、Web 情報分析など、様々な分析結果を総合的に判断するハイブリッド分析が求められる。そこで本委託研究では、国立研究開発法人情報通信研究機構（以下「機構」という。）が開発中のマルウェア活動発生を自動的に検知する技術と連携し、その検知したイベントに関連するマルウェア・脆弱性・脅威情報などを実時間で精緻に提供することで、より有用性の高いセキュリティ情報自動分析基盤技術の確立を目指す。

本技術の確立により、従来はベンダーや CSIRT、SOC などに在籍するセキュリティアナリストが手動で分析し警告を発していた感染活動を自動的に検知し、マルウェアに関する情報と共に自動的に警告を提供可能となる。それにより、セキュリティ対策を施すべき各組織のセキュリティインシデントへの対応能力の大幅な強化が実現可能となる。本メリットは、日本国民のみならず国際的なサイバー社会全体が享受できるものであり、安心・安全なサイバー社会の構築・運営に大きく貢献するものである。

３．研究開発の内容

本委託研究では、各種の分析により、セキュリティインシデントの発生を自動的にいち早く検知し、そのインシデントに関連する情報を自動的に関連付け、提供できる技術を構築することを目指す。特に、近年発展が目覚ましい（深層学習を含む）機械学習技術を最大限活用することにより、セキュリティビッグデータを実時間かつ精緻に分析する。

より具体的には図 1 に示す通り、ライブネットトラフィック、ダークネットトラフィック、

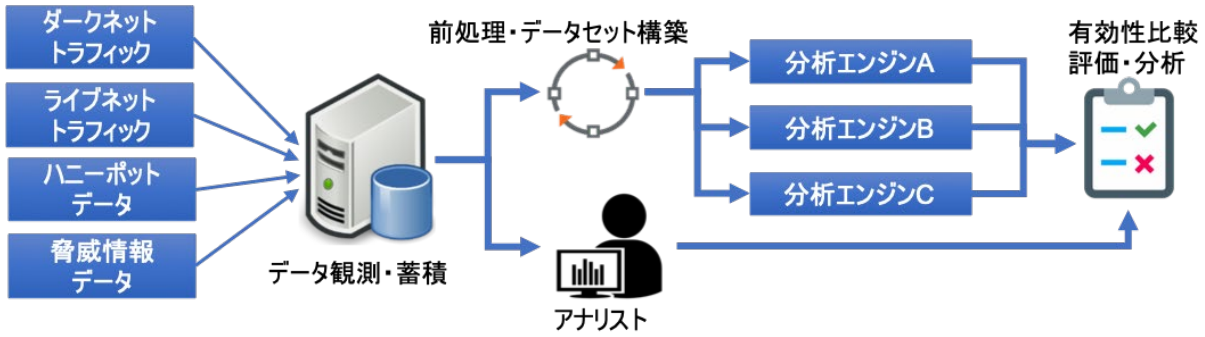

図 1 本委託研究の流れ

ハニーポットデータ、脅威情報を含むセキュリティ関連情報を分析する。そして、マルウェア情報（活動状況やその挙動情報、過去の類似マルウェアの情報など）、脆弱性情報（その脆弱性の深刻度や性質情報など）、脅威情報（Web から抽出した脅威に関する情報、関連するインテリジェンス情報など）を自動的に生成・抽出し、それらの関連性を評価する。

機構では、参考文献[1][2]のとおり、ダークネットトラフィックを分析することによるマルウェア活動の活性化を自動的に検知する技術の検討を進めている。そして、本技術を核に、検知したセキュリティイベントに関連する情報を複数の視点から分析し、アナリストが効率的かつ効果的に判断をすることが可能となる「サイバー攻撃ハイブリッド分析プラットフォーム」技術の実現を目指している。本プラットフォームは、機構の研究成果により新たなマルウェア活動の活性化を自動的に検知し、そのイベントに関する情報を提供するが、本委託研究の研究成果を活用することによりその検知したイベントに関連するマルウェア・脆弱性・脅威情報などを実時間かつ精緻に提供することで、その有用性の大幅な向上を実現する。そのため、本委託研究では、上述の通り機構の成果と連携し、より有用性の高いセキュリティ情報自動分析基盤技術を確立するための研究開発であることが求められる。

上記を踏まえ、本委託研究では、下記のそれぞれの研究項目を実施する。

1）サイバー攻撃インフラ情報の収集と分析

a）マルウェア検体が攻撃インフラに接続する通信の観測・分析

IoT マルウェア検体と攻撃インフラ（主にコマンド＆コントロールサーバ）間の通信が観測可能なハニーポットの研究開発を行う。従来、ハニーポットの研究は多数報告されているものの、攻撃インフラに接続する通信の観測・分析に特化した分析の深化が求められる。特に、近年問題となっている Mirai や Bashlite などの IoT マルウェアが行う通信の観測を実現する。加えて、本観測データを分析することにより、マルウェア通信を擬似的に再現するシステムの研究開発に資する情報（通信先 IP アドレスやマルウェアへの命令とその応答など）を抽出する。

b）検出されたマルウェア活動に関連するハニーポット分析結果を特定する技術の開発

機構が開発している技術がマルウェア活動の発生を検知した際に得られた情報（通信先ポート番号や通信パターンなど）をキーとして、上記項目 a）にて観測したデータから関連するデータをリアルタイムに抽出する技術を構築する。

2）実時間で実現可能な大規模かつ構造的なマルウェア分析

a）マルウェアの機能を精緻に分析し、クラスタリングを行う技術の開発

マルウェアのプログラムコードレベルでの類似性を分析し、マルウェアサンプルを機能面からクラスタリングする技術を構築する。これにより、マルウェア解析者がクラスタ内の数検体のみ解析すれば、当該クラスタ全検体の機能を概観することが可能になる。マルウェアのクラスタリング技術は従来から研究がなされているものの、大規模な分析を実施するには処理速度面で実現可能性に乏しく、そのクラスタリングを高速化するためのアルゴリズムを構築する必要がある。

b）大規模かつリアルタイムに動作するマルウェア解析技術の開発

与えられたマルウェアのクラスタに対してマルウェア解析を自動的に行う技術を研究開発する。同一クラスタには機能的に類似したマルウェアサンプルが存在するが、それらのマルウェア間の細かな差異を自動的に抽出する有力な手法は我々が知る限り存在しない。そこで本マルウェア解析ではプログラムコードレベルの類似性および差異を考慮して、プログラムレベルもしくは関数レベルでどういう差異があるかを自動的に出力する技術を構築する。

3）インテリジェンス情報の生成と分析

a）脆弱性の種類や深刻度を AI 技術により自動的に推定する技術の開発

脆弱性の種類を自動で分析・付与する技術の研究開発を実施する。脆弱性の種類はセキュリティ解析者にとって脅威情報分析の重要な手がかりとなっているが、現時点では手動で分析・ラベリングされており、日々生成される大量の新たな脆弱性情報のラベリングに対応しきれない。本項目では、共通脆弱性タイプのツリー構造に着目し、従来着目されてこなかったより深い階層まで脆弱性情報を分類する技術を構築する。

b）Web 情報を分析することによりインテリジェンス情報を生成する技術の開発

本課題では SNS やセキュリティレポート等の Web 上に存在する情報を入力として、トレンドとなっている脅威（Mirai や Cobalt などのキーワード）を特定し、インテリジェンス情報を生成する技術を構築する。同時に、各脅威に関連するキーワード（Web camera や Financial Institution など）を自動抽出してから、抽出された各脅威とその関連キーワードを軸にこれらの情報のクラスタリングを実現する。OSINT など、公開情報から優位な秘密情報を抽出する研究も報告されているが、本研究ではインテリジェンス情報になりうる情報の抽出を検討する点に焦点がある。本技術により、セキュリティオペレータが必要な情報を効率的に取得できるのと同時に、インターネット上の脅威の状況を概観することが可能となる。

c）インテリジェンス情報とセキュリティインシデントを関連付ける技術の開発

機構が開発している技術がマルウェア活動の発生を検知した際に、関連する上記項目 a）b）にて生成した情報を含む各種インテリジェンス情報をリアルタイムに抽出する技術を構築する。

4．研究開発の到達目標と、委託研究後のマイルストーン

到達目標

以下の３つの課題のすべてを研究開発対象とし、セキュリティ情報自動分析基盤技術の確立を目標とする。

1）サイバー攻撃インフラ情報の収集と分析

a）マルウェア検体が攻撃インフラに接続する通信の観測・分析

マルウェア経由で行われる攻撃者の悪意ある挙動やその挙動の時間的な変化、マルウェア活性化のタイミング、攻撃インフラの転移など、攻撃の実態を把握する技術を構築する。ケーススタディとして、2019・2020 年度に猛威を振るっている３個以上のマルウェアについて、分析結果レポートを作成する。

b）検出されたマルウェア活動に関連するハニーポット分析結果を特定する技術の開発

機構の技術にて発生を検知したマルウェアについて、マルウェアの種類やマルウェアへの命令とその応答など、サイバー攻撃分析に役立つ付加情報をリアルタイムに提供可能であることをフィージビリティスタディにより検証する。また、項目１について、国内外の学術研究会にて１件以上成果発表を実施する。

２）実時間で実現可能な大規模かつ構造的なマルウェア分析

a）マルウェアの機能を精緻に分析し、クラスタリングを行う技術の開発

従来では３千検体をクラスタリングするのに１年～3 年程度を要するものを、１ヶ月以内に実現する。同時に、従来と同程度のクラスタリング精度（精度 90%程度）を維持する。また、本項目について、国内外の学術研究会にて１件以上成果発表を実施する。

b）大規模かつリアルタイムに動作するマルウェア解析技術の開発

クラスタ内のマルウェアサンプル間の差異の自動分析アルゴリズムを構築し、そのフィージビリティを検証する。同時に、その解析を、数千検体規模の検体間に対してリアルタイム（遅延は数分～数十分程度に抑制）で実現可能にする。また、本項目について、国内外の学術研究会にて１件以上成果発表を実施する。

3）インテリジェンス情報の生成と分析

a）脆弱性の種類や深刻度を AI 技術により自動的に推定する技術の開発

共通脆弱性タイプのツリー構造は、階層が深くなると、脆弱性情報の分類が細分化され、カテゴリ数が急増するが、現在利用されている最深層のカテゴリにおいても、分類精度 90%以上を達成する。また、項目３について、国内外の学術研究会にて１件以上成果発表を実施する。

b）Web 情報を分析することによりインテリジェンス情報を生成する技術の開発

提案技術により、最近のトレンド別にインテリジェンス情報を 100 件以上自動生成し、その精度を評価することで、本技術のフィージビリティを検証する。

c）インテリジェンス情報とセキュリティインシデントを関連付ける技術の開発

機構の技術にて発生を検知したマルウェアについて、上記項目 a）b）にて生成した情報を含む各種インテリジェンス情報から、サイバー攻撃分析に役立つものをリアルタイムに提供可能であることをフィージビリティスタディにより検証する。

委託研究後のマイルストーン

2021 年度以降に３つの課題において開発した技術を組み合わせて、早期検知によるインシデントの被害縮小、組織間の脅威情報の共有化の社会実装、及び収集・解析データの公開を開始することを想定して、各技術の設計・実装・評価を行うこと。

2021 年　本委託研究で確立したセキュリティ情報自動分析基盤技術を基にサイバー攻撃ハイブリッド分析プラットフォームシステムの PoC（Proof Of Concept）実装

2022 年　サイバー攻撃ハイブリッド分析プラットフォームシステムの評価
2023 年　サイバー攻撃ハイブリッド分析プラットフォームシステムの実証実験実施

5．採択件数、研究開発期間及び研究開発予算等

採択件数　　：1 件
研究開発期間：2019 年度（契約締結日）から 2020 年度
研究開発予算：各年度、総額 30 百万円（税込）を上限とする。
（提案の予算額の調整を行った上で採択する提案を決定する場合がある。）
研究開発体制：単独の提案も可能であるが、ハニーポットやライブネットの分析など、異なる技術に精通している複数の実施主体からなる体制とすることを推奨する。

6．提案に当たっての留意点

- 具体的目標に関しては、定量的に提案書に記載すること。特に、第 4 章に記載の到達目標を踏まえ、期間内に実現可能な目標を記載すること。
- 研究開発成果の情報発信を積極的に行うこと。
- 本委託研究の遂行過程で得られる科学的なデータがあれば、広くオープンにするのが望ましい。公開できると想定する科学的なデータの有無と、有る場合には公開計画（例：公開するデータの種類、公開先、公開方法）を提案書に記載すること。

7．運営管理

- 機構と受託者の連携を図るため、代表提案者は、プロジェクトオフィサーの指示に基づき定期的に連絡調整会議を開催すること。
- 複数の機関が共同で受託する場合には、代表提案者が受託者間の連携等の運営管理を行い、受託者間調整会議を定期的に開催すること。
- 社会情勢や研究環境の変化等、必要に応じて、プロジェクトオフィサーが研究計画書を変更する場合があるので、留意すること。

8．評価

- 機構は、2020 年度に終了評価を実施する。また、本委託研究終了後に成果展開等状況調査を行い、追跡評価を行う場合がある。
- 機構は、上記以外にも本委託研究の進捗状況等を踏まえて、臨時にヒアリングを実施することがある。

9．成果の社会実装等に向けた取組

- 本委託研究の成果を活用し、機構がサイバー攻撃ハイブリッド分析プラットフォームシステムの実現に向けた研究開発を計画しているため、代表提案者は機構との連絡調整を密に行うこと。

１０．プロジェクトオフィサー

サイバーセキュリティ研究所サイバーセキュリティ研究室 高橋健志

参考

[1] C. Han, J. Shimamura, T. Takahashi, D. Inoue, M. Kawakita, J. Takeuchi, and K. Nakao. Real-Time Detection of Malware Activities by Analyzing Darknet Traffic Using Graphical Lasso. IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom): Security Track, 2019.

[2] H.Kanehara, Y.Murakami, J.Shimamura, T.Takahashi, D.Inoue, N.Murata, ″Real-Time Botnet Detection Using Nonnegative Tucker Decomposition,″ ACM Symposium On Applied Computing, ACM, April, 2019.