様式 1-4-2 (2020-2)

令和２年度研究開発成果概要書

採 択 番 号　　21601
研究開発課題名　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
副　　題　　機械学習に基づくサイバー攻撃情報分析基盤技術の研究開発

（１）研究開発の目的

ライブネットトラフィック、ダークネットトラフィック、マルウェアデータベース、脆弱性情報、Web 情報などの多様なデータを分析する技術と、それら分析結果を総合し、インシデント対策のための意思決定を自動的に行うセキュリティ情報自動分析基盤技術を確立することが目的である。研究開発にあたっては、国立研究開発法人情報通信研究機構（以下、NICT。）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することで、より効果的に成果を追求する。NICT では、「サイバー攻撃ハイブリッド分析プラットフォーム」技術の実現に向け、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研究開発を行っている。この技術を用いると、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ことができる。本研究では、この成果を活用して、マルウェア・脆弱性・脅威情報などの、さらに有用なインシデント関連情報を生成する技術の研究開発を行う。

（２）研究開発期間

令和元年度から令和２年度（２年間）

（３）実施機関

国立大学法人九州大学 ＜代表研究者＞
学校法人早稲田大学
国立大学法人横浜国立大学
国立大学法人神戸大学

（４）研究開発予算（契約額）

総額 60 百万円（令和２年度 30 百万円）
※百万円未満切り上げ

（５）研究開発項目と担当

研究開発項目１　サイバー攻撃インフラ情報の収集と分析
研究開発項目 1-1　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（横浜国立大学）
研究開発項目 1-2　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（横浜国立大学）

研究開発項目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
研究開発項目 2-1　大規模系統樹によるマルウェアクラスタリング技術の開発（九州大学）
研究開発項目 2-2　マルウェア機能推定技術の開発（九州大学）

研究開発項目３　インテリジェンス情報の生成と分析
研究開発項目 3-1　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 （早稲田大学）
研究開発項目 3-2　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 （神戸大学）

研究開発項目 3-3　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　（神戸大学）

（6）特許出願、外部発表等

		累計（件）	当該年度（件）
特許出願	国内出願	0	0
	外国出願	0	0
外部発表等	研究論文	1	1
	その他研究発表	20	15
	標準化提案・採択	0	0
	プレスリリース・報道	0	0
	展示会	0	0
	受賞・表彰	0	0

（7）具体的な実施内容と成果

研究開発項目１：サイバー攻撃インフラ情報の収集と分析

研究開発項目 1-1　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

【目標】IoT ボットネット検体を解析環境内で動作させ、攻撃者サーバとの通信を観測し、攻撃者サーバの分析を行うことで、攻撃の実態を把握する。ケーススタディとして、現在活発に活動している３個以上の IoT ボットネットに対し、これらの分析結果レポートを作成する。

【実施内容・成果】短期動的解析と長期動的解析により、マルウェア検体が攻撃インフラに接続する通信を観測した。また、動的解析により得られたマルウェア通信データを入力として、マルウェア検体が攻撃インフラに接続する通信を分析する技術を構築し、サイバー攻撃インフラの特徴を把握した。そして、合計３種類のボットネットについて分析結果レポートを作成した。

研究開発項目 1-2　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

【目標】研究開発項目 1-1 による解析結果をデータベース化し、様々な観点から検索が出来るようにする。NICT の技術にて発生を検知したマルウェアについて、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検証する。

【実施内容・成果】マルウェア解析結果を ElasticSearch を用いてデータベース化した。攻撃元 IP アドレス、宛先ポート番号など NICT のダークネットで観測される情報に基づき様々な観点から検索を行い、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とした。

研究開発項目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

研究開発項目 2-1. 大規模系統樹によるマルウェアクラスタリング技術の開発

【目標】従来技術で 3 千検体をクラスタリングするのに 1 年以上要するものを、1 ヶ月以内に短縮する。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。

【実施内容・成果】6.5 万検体を対象に、クラスタリングの実証実験を行った。従来手法と同等以上のマルウェアファミリーの分類正解率（90%）を保ったまま、30 倍の高速化を実現した。すなわち、従来と同じ計算機環境であれば、３年かかる計算を１か月以内で完了できる。

研究開発項目2-2. マルウェア機能推定技術の開発

【目標】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。

【実施内容・成果】関数呼び出し列グラフ（FCSG）を用いたマルウェア解析手法を設計した上で実装し、2 万検体以上を対象に遅延時間を数分に抑えられることを確認した。また、クラスタリング結果に対し適用し、有効な解析が可能であることを確認した。

研究開発項目３：インテリジェンス情報の生成と分析

研究開発項目３-１. 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

【目標】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。頻出カテゴリ（トップ 30）において、分類精度 90%以上を達成する。

【実施内容・成果】上位層 19 ラベルでは 90%以上の精度（F1micro 96.9%, F1macro 92.9%）を達成するものの、頻出 31 ラベルでは 80%台（F1micro 88.2%, F1macro 82.8%）に留まる。ただし、少数サンプルのラベルを含む 44 ラベルの一部の精度（F1micro 94.8%、F1macro 58.5%）では 90%を達成した。

研究開発項目３-２. 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

【目標】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。最近のトレンドに対する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。

【実施内容・成果】セキュリティレポートを入力としてトレンドとなっている脅威に関するインテリジェンス情報を生成するためのラベル付け手法と、インテリジェンス情報の出力品質が向上するラベル付け手法を構築した。二つの手法を統合して生成したラベルを用いることで、注目するトレンドに対してインテリジェンス情報を 100 件以上自動生成することが可能となった。

研究開発項目３-３. 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

【目標】NICT の技術にて発生を検知したマルウェアについて、研究開発項目 3-1、3-2 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。

【実施内容・成果】研究開発項目 3-1、3-2 にて生成される情報を含めてインテリジェンス情報をリアルタイムに提供可能な検索エンジンを構築した。その検索エンジンを用いることで NICT の技術にて発生を検知したマルウェアに関する情報を取得できることを確認した。

（8）研究開発成果の展開・普及等に向けた計画・展望

計画：本研究は NICT が推進するセキュリティ情報自動分析基盤技術研究の一環であり、中でも機械学習技術に基づいて要素技術を確立することを目的としている。最終的には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いるが、これら基盤技術の研究は本研究期間内で完結するものではなく、NICT 及び受託者を含むより大きな研究組織によるプロジェクトとして、開始した総務省委託研究「電波の有効利用のための IoT マルウェア無害化/無機能化技術等に関する研究開発」（令和 2 年度～令和 4 年度）で継続して行われる。この研究計画では、本研究の成果をさらに発展させ、他の技術と総合的に組み合わせることで、電波資源有効利用の観点で社会貢献につなげていく計画である。

展望：総務省委託研究「電波の有効利用のための IoT マルウェア無害化/無機能化技術等に関する研究開発」にて、令和 3 年度まで基盤技術の研究を行い、令和 4 年度には、社会実装を想定した実証実験を実施する。