様式 1-4-2 (2020-1)

令和元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

多様なセキュリティインシデント関連情報を解析しインシデントへの対策を講じることを目標に、人工知能に基づく基盤技術に関する研究開発を実施する。

（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（令和元年度 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
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）
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
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）
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
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）
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）
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	0	0
	その他研究発表	5	5
	標準化提案	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

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

マルウェア検体が接続する攻撃インフラを観測し、攻撃者の挙動やその変化等、攻撃の実態を把握する技術に関する基本方式の設計と試作を行った。

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

研究開発項目１－１で収集したマルウェア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ための基本方式の設計と試作を行った。

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

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

系統樹を用いたクラスタリング手法の設計と試作を行い、4000 検体のデータに対して速度と精度の評価を行った。結果、精度 90%以上を保持しつつ、20 倍程度の高速化を達成した。

2-2 マルウェア機能推定技術の開発

検体を逆アセンブルし関数呼び出しシークエンスから機能を推定する手法について、基本方式の設計と試作を行った。

研究開発項目３： インテリジェンス情報の生成と分析

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

脆弱性情報を記述したデータから脆弱性の種類を自動で付与する手法の設計と試作を行い、CVE データを対象に CWE 頻出ラベルの判別精度を評価した。既存研究に比べて多数のラベル(31 種)の判別に対して 80%以上の精度を達成した。

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

Web 上にあるセキュリティレポートから脅威に関連するキーワードを抽出をするクラスタリングに基づく手法の基本設計と試作を行った。

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

脆弱性情報・脅威情報からの特徴的な単語の抽出手法、およびセキュリティインシデントとの関連付け手法の設計のための調査を行った。