令和元年度研究開発成果概要図 （目標・成果と今後の研究計画）

採択番号:21601

1．研究課題・受託者・研究開発期間・研究開発予算

◆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
◆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
◆研究開発期間：令和元年度～令和2年度（2年間）
◆研究開発予算：総額60百万円（令和元年度30百万円）

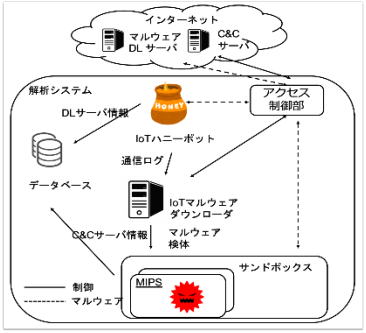
2．研究開発の目標

・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。

3．研究開発の成果

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

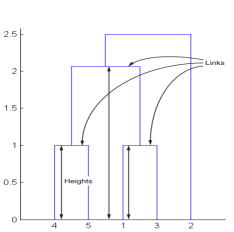
1-1 マルウェア検体が攻撃インフラに接続する通信の観測・分析
マルウェア検体が接続する攻撃インフラを観測し、攻撃者の挙動やその変化等、攻撃の実態を把握する技術に関する基本方式の設計と試作
1-2 検出されたマルウェア活動に関連するハニーポット分析結果を特定する技術の開発
研究開発項目１－１で収集したマルウェア解析結果をデータベース化し、様々な観点から検索が出来るようにするための基本方式の設計と試作を行った。



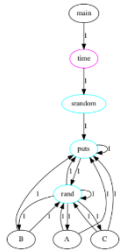
ハニーポットとサンドボックスによる攻撃インフラ観測機構

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。



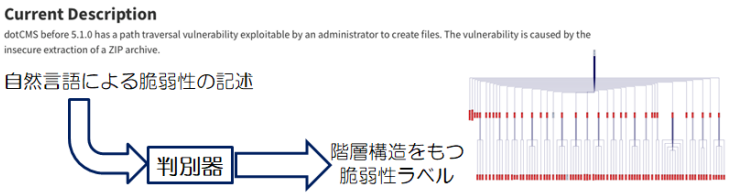
系統樹によるクラスタリング



関数呼び出しシーケンスグラフ

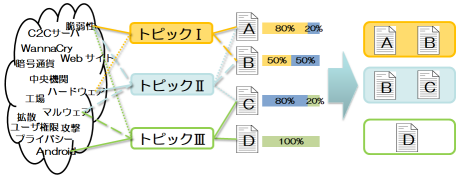
研究開発項目3：インテリジェンス情報の生成と分析

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。



AI技術による脆弱性分類

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。



キーワードに基づくクラスタリング手法

4. 特許出願、論文発表等、及びトピックス

国内出願	外国出願	研究論文	その他研究発表	標準化提案	プレスリリース 報道	展示会	受賞・表彰
0 (0)	0 (0)	0 (0)	5 (5)	0 (0)	0 (0)	0 (0)	0 (0)

※成果数は累計件数、( )内は当該年度の件数です。

令和2年1月から3月の期間に下記5件の学会発表を行った。

1. 川添玲雄, 韓燦洙(NICT), 伊沢亮一(NICT), 高橋健志(NICT), 竹内純一, “関数呼び出しシーケンスに着目したIoTマルウェアの機能推定に関する考察, ” 2020暗号と情報セキュリティシンポジウム予稿集
2. 長田侑樹, 瀧田愼, 古本啓祐(NICT), 白石善明, 高橋健志(NICT), 毛利公美, 高野泰洋, 森井昌克, “トピックモデルとクラスタリングによるセキュリティレポートのマルチラベル分類, ” 信学技報, Vol.119, No.437, pp.283-288
3. 杉本健太, 長田侑樹, 瀧田愼, 古本啓祐(NICT), 白石善明, 高橋健志(NICT), 毛利公美, 高野泰洋, 森井昌克, “半教師ありトピックモデルによるセキュリティレポートの分類の評価方法について, ” 情処研報, Vol.2020-SPT-36, No.44, pp.269-272
4. 長澤龍成, 古本啓祐(NICT), 瀧田愼, 白石善明, 高橋健志(NICT), 毛利公美, 高野泰洋, 森井昌克, “セキュリティレポートの時系列トピックモデルを用いた分析, ” 情処研報, Vol.2020-SPT-36, No.45, pp.273-277
5. 後藤圭太, 毛利公美, 白石善明, “ティッカー表示による組織に即した脅威情報の閲覧, ” 情報処理学会全国大会論文集第3巻, pp.501-502

5. 今後の研究開発計画

令和2年度には, 各課題においてこれまでに開発した手法の精度評価やフィージビリティスタディを行う. また, それに基づいて精度とスケーラビリティの向上を行う. 研究開発項目1については, ケーススタディとして分析結果レポートを作成する.