令和2年度研究開発成果概要図 （目標・成果と今後の成果展開）

採択番号:21601

1. 研究開発課題・実施機関・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、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 ： 平成元年度から平成2年度（2年間）
◆研究開発予算 ： 総額60百万円（令和2年度30百万円）

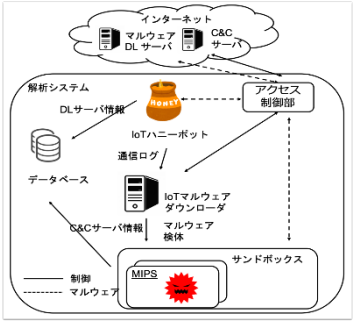
2. 研究開発の目標

・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

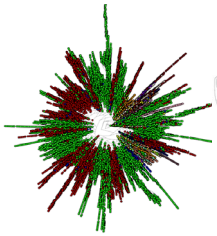
1-1 マルウェア検体が攻撃インフラに接続する通信の観測・分析
動的解析によりマルウェア検体が攻撃インフラに接続する通信を分析する技術を構築し、サイバー攻撃インフラのネットワーク情報、寿命、頑強性、特徴を把握。3種類のマルウェアについて分析結果レポートを作成
1-2 検出されたマルウェア活動に関連するハニーポット分析結果を特定する技術の開発
ElasticSearchを用いてデータベース構築。
NICTダークネットの情報に基づく検索で、攻撃分析に役立つ付加情報をリアルタイムに提供



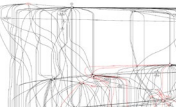
ハニーポットとサンドボックスによる攻撃インフラ観測機構

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を実装。65000検体のデータに対して速度と精度を評価。精度90%以上を保持しつつ、30倍程度の高速化を達成。
2-2 マルウェア機能推定技術の開発
FCSGを用いたマルウェア解析手法を実装。2万検体を対象に遅延時間を数分に抑えられることを確認。クラスタリング結果に対し適用し、有効性を確認。



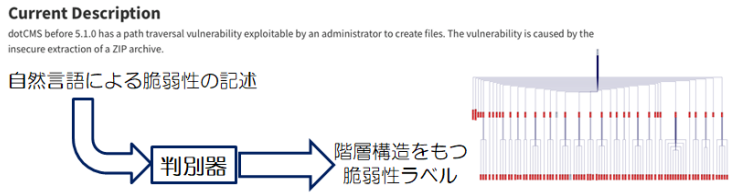
生成した系統樹



関数呼び出しシーケンスグラフ(FCSG)

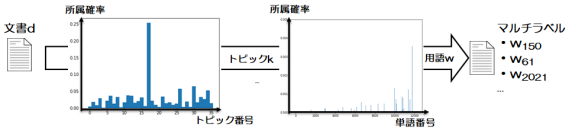
研究開発項目3:インテリジェンス情報の生成と分析

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実装を行い、CVEデータを対象にCWE頻出ラベルの判別精度を評価。多数のラベル(31種)の判別に対してほおむね90%以上の精度を達成。



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インテリジェントレポートを生成するシステムを実装。最新のセキュリティレポートから100件の情報を自動生成。
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
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実用性を実証。



LDAによる文書のラベル付け技術

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 ）	1 （ 1 ）	20 （ 15 ）	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。

1. Rui Tanabe, Tatsuya Tamai, Akira Fujita(NICT), Ryoichi Isawa(NICT), Katsunari Yoshioka, Tsutomu Matsumoto, Carlos Ganan and Michel Van Eeten, “Disposable Botnets: Examining the Anatomy of IoT Botnet Infrastructure” , Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES `20), ACM ICPS, Aug. 2020
2. 吉岡　克成，“IoTにおけるサイバーセキュリティの現在とこれから”，Aruba ATM Digital Japan，Sep. 2020
3. Thin Tharaphe Thein, Yuki Ezawa, Shunta Nakagawa, Keisuke Furumoto(NICT), Yoshiaki Shiraishi, Masami Mohri, Yasuhiro Takano, Masakatu Morii, “Paragraph-based Estimation of Cyber Kill Chain Phase from Threat Intelligence Reports”, Journal of Information Processing, Vol.28, pp.1025-1029, Dec. 2020
4. 古川凌也，白石善明，森井昌克，“SoK：データ駆動型社会に向けたセキュリティ分野へのオントロジの活用に関する一考察”，情報処理学会論文誌，Vol.61，No.12，pp.1802-1813, Dec. 2020
5. 吉岡　克成，“IoTセキュリティ対策の今とこれから～新たな脅威への準備～”，基調講演，ET&IoT Digital 2020，Dec. 2020
6. 吉岡　克成，“脆弱なIoT機器を守るための総合的サイバーセキュリティ研究 ～攻撃観測・脆弱機器探索から注意喚起、マルウェア駆除、防御まで～”，IoT Security Forum 2020，Dec. 2020
7. 何 天祥（九大），韓 燦洙，伊沢 亮一，高橋 健志（NICT），来嶋 秀治，竹内 純一（九大），“高速な系統樹構成アルゴリズムにおけるスケーラブルなクラスタリング評価”，情報通信システムセキュリティ研究会 (ICSS)，Mar. 2021
8. 石橋亮典，後藤大輝（九大），韓　燦洙・班　涛，高橋健志（NICT），竹内純一（九大），“NIDSアラートに対する原因通信の抽出手法の提案及び考察”，情報通信システムセキュリティ研究会 (ICSS)，Mar. 2021
9. Reo Kawasoe, Chansu Han (NICT/Kyushu University), Ryoichi Isawa (NICT), Takeshi Takahashi (NICT), Jun‘ichi Takeuchi, “Investigating Behavioral Differences between IoT Malware via Function Call Sequence Graphs”, The 36th ACM/SIGAPP Symposium On Applied Computing (SAC 2021), Mar. 2021

5. 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、情報通信研究機構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。