平成 30 年度プロジェクト研究実績報告書

【研究課題名】	セキュリティインシデント解析技術に関する研究
【研究代表者】	布広　永示（東京情報大学・教授）
【研究分担者】	花田　真樹（東京情報大学・准教授） 村上　洋一（東京情報大学・助教） 中野　心太（東京情報大学・総合情報学部 4 年） 佐野　涼太（東京情報大学・総合情報学部 4 年）

【研究の目的】

セキュリティインシデント解析に関連する次の 2 つのテーマについて研究する。

a)　セキュリティインシデント解析システムの研究・開発

本研究では、ニュース記事などの Web 情報を調べて、セキュリティインシデントの発生状況を抽出し、インシデントの発生パターンや件数などの推移や発生動向を解析すると共に、過去に発生したサイバーセキュリティインシデントと株価などの経済状況の変動などとの関係性を解析するセキュリティインシデント解析システム SIAS（Security Incident Analysis System）の研究・開発を進める。

b)　悪性 Web サイト検知手法に関する研究

近年、ドライブバイダウンロード攻撃やフィッシング攻撃など、悪性 Web サイトを経由した Web 媒介型攻撃による被害が増加している。これらの被害を防止するために、従来より、悪性 Web サイトの JavaScript の調査が行われ JavaScript 関数の種類や関数の実行回数などに関する特徴が明らかになっている。本研究では、このような JavaScript の動的な振る舞いの特徴量に加えて、ソースコードに着目した特徴量を用いた悪性 Web サイト検知手法を提案し、評価する。

【研究報告】

a) セキュリティインシデント解析システムの研究・開発

SIAS の機能として、Web サイトの情報からセキュリティインシデントに関連する企業名やインシデント情報を抽出する固有表現抽出機能、セキュリティインシデント発生前後のネガティブ文章の増減の傾向を分析するための極性分析機能の開発を進めている。本研究では、固有表現抽出機能の中核であるパターンマッチングによる固有表現抽出と係り受け解析による固有表現抽出、感情極性分析機能を開発した。感情極性分析では、世評の感情極性値がネガティブかポジティブかを自動的に判定することを目的としているが、今回の結果では、正常に判断した割合は 60%程度であり、精度を向上するための改良として、不要単語の除去等の辞書の改良、係り受けを考慮した文脈解析などの研究を進めていく予定である。

b) 悪性 Web サイト検知手法に関する研究

本研究では，悪性 Web サイトを経由した Web 媒介型攻撃による被害を防止することを目的とし，Web ページに埋め込まれた JavaScript の抽象構文木における出現キーワード（出現文字列）とその属性，階層数（入れ子の深さ）に関する特徴を利用した悪性の JavaScript の検知手法を提案した．評価実験では，3 種類（ナイーブベイズ，ランダムフォレスト，サポートベクターマシン）の機械学習アルゴリズムに対し，出現キーワード（特徴 1），出現キーワードとその属性（特徴 2），出現キーワードとその属性と階層数（入れ子の深さ）（特徴 3）の 3 つの特徴を用いた場合の悪性の JavaScript の検出率に関する評価を行った．結果として，ランダムフォレストの機械学習アルゴリズムに対し，特徴 3 を用いた検出率が 93.4%と高い値を示した．今後は，更なる検出率向上に向け，悪性の JavaScript の特徴に関する再検討を進めていく予定である．

【成果の公表】

[1] 中野心太，宇都太祐，黒澤祐一郎，花田真樹， 村上洋一，布広永示,”セキュリティインシデントに関する固有表現抽出及び極性分析機能の開発”、電子情報通信学会，情報セキュリティ研究会(ISEC)（九州大学）、2018 年 11 月

[2] 佐野涼太，佐藤順子，村上洋一，花田真樹，布広永示，”抽象構文木に基づく情報を用いた悪性 JavaScript 検知手法，” 電子情報通信学会 情報セキュリティ研究会(ISEC)（九州大学），2018 年 11 月