表層解析の効率化に向けた情報鮮度判別方式の提案

Proposal of Information Freshness Discrimination Method for Improvement of Surface Analysis Efficiency

檜垣 龍徳[1] 竹原 一駿[1] 本部 建大[1] 楠目 幹[1] 西岡 大助[1] 西山 賢[2] 合田 翔[2] 最所 圭三[1] 喜田 弘司[1]
T. Higaki[1] I. Takehara[1] T. Motobu[1] M. Kusume[1] D. Nishioka[1] M. Nishiyama[2] S. Gouda[2] K. Saisho[1] K. Kida[1]
(香川大学[1]，株式会社 STNet[2])

1. はじめに

大学や企業などの組織では，サイバー攻撃のリスク評価，戦略策定のために行う“表層解析作業”が，大きな負荷となっている．表層解析作業では，脆弱性やマルウェアなどの情報(以下セキュリティ情報)とそれに対する注意喚起や被害報告などの情報(以下意見情報)を用いて，最新の状況を把握する．セキュリティ情報は，主に Web ページから集められ，意見情報は，SNS やブログなどから集められる．

我々は表層解析作業の負荷軽減を目指したシステムを試作して評価した[1]．その評価の中で，“記事は新しい順に表示されて欲しい．”といった意見を得た．このことから，セキュリティ管理者は，セキュリティ情報の情報鮮度を重要視していることがわかった．そこで本稿では，意見情報を用いたセキュリティ情報の情報鮮度判別方式を提案する．

2. 課題

セキュリティ情報は日々更新される．例えば“EMOTET”[2]の場合，この攻撃で使われる標的型攻撃メールの本文は，日々巧妙になっており，対策するためには最新のセキュリティ情報に追随する必要がある．しかし，時間情報が複数あり公開日時が特定できないこと(課題 1)や公開日時を明示していないこと(課題 2)もあり，どれが最新であるかわからない．そのため，情報鮮度を判別する一要素としてすべてのセキュリティ情報の公開日時を推定することが求められる．本稿では，課題 1 に対応する方式を提案し，課題 2 に関しては 5 章にて考察する．

3. 提案方式

公開日時の推定には，セキュリティ情報内の時間情報(①)と，意見情報の時間情報(②)を利用することが考えられる．本研究では，公開日時を推定するには，セキュリティ情報の公開後すぐに意見が集まることが重要であると考えられるため，意見情報に，更新の速い Twitter の投稿を用いる．

公開日時の推定が困難である要因として，①のみを用いる場合は，公開日時が明示されていない，1 つのセキュリティ情報の中に時間情報が複数ある，ということが挙げられる．②のみを用いる場合は，過去のセキュリティ情報を参照している，同一のセキュリティ情報を参照している投稿が複数ある，ということが挙げられる．これらに対して，①と②を対応付けることで，公開日時を推定することにした．

提案方式を，例を使って説明する(図 1)．ここで用いるセキュリティ情報と意見情報は事前に収集されているものとする．この例は，セキュリティ情報をテキスト解析した結果，時間情報を 3 つ見つけた(Step1)．しかし，見つけたすべての時間情報の前後に，更新日時といった表記がなく，公開日時を一意に特定できない状況である．この時，見つけたそれぞれの時間情報を下端とした一定の時間区間(この例では 3 日間)を設定する(Step2)．当該セキュリティ情報に対する意見情報を抽出し(Step3)，抽出した意見情報から Step2 で設定した時間区間中に投稿されたものを探す(Step4)．区間内に投稿された意見情報が最多の時間区間の意見情報を確認し(Step5)，その中で最古の意見情報が投稿された時間を，セキュリティ情報の公開時間とする(Step6)．この例では“1/25 6:00”が公開日となる．Step2 で設定する間隔は，実際に EMOTET に関するセキュリティ情報[2]について Twitter で調査したところ，セキュリティ情報の公開から数日間の投稿が多く確認できたため数日の幅であればよいと考える．

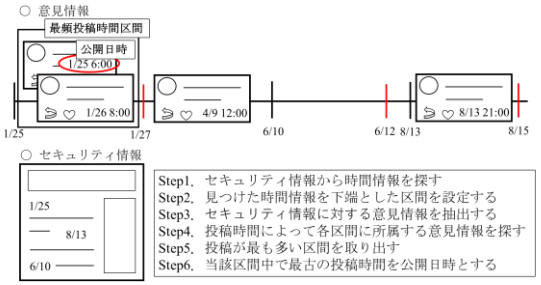

図 1 提案方式のイメージ

4. システム構成

テキスト解析部，日時抽出部，リンク情報検索部，時間情報照合部，公開日時推定部から構成される(図 2)．テキスト解析部では，セキュリティ情報の形態素解析を行う．日時抽出部では，テキスト解析部の結果から時間情報を抽出する．リンク情報検索部では，Twitter を利用してセキュリティ情報に対する意見情報を検索する．時間情報照合部では，日時抽出部にて抽出した時間情報と，リンク情報検索部にて発見した意見情報の投稿時間を照合する．公開日時推定部では，時間情報照合部の結果に基づいて，セキュリティ情報の公開日時を推定する．

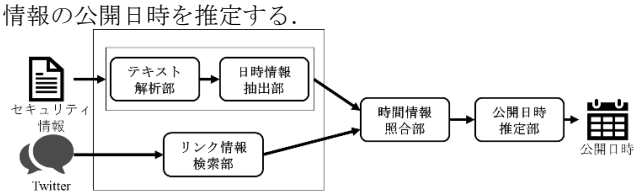

図 2 システム構成図

5. 課題 2 の考察

この課題に対して，意見情報の分布から推定する方式(案 1)と，内容が似ているセキュリティ情報の公開日時から推定する方式(案 2)が考えられる．案 1 に関しては，意見情報が少ないか，投稿時間の分布にばらつきがある場合には効果が期待できない．そのため，まずは課題 2 に該当するセキュリティ情報に対する意見情報が，どれほどあるか検証する必要がある．案 2 に関しては，予備実験として Word2Vec による内容分析を行ったが，現状では内容の似た情報を得るに至っていない．

参考文献

[1] 竹原一駿ほか：“AI によるセキュリティ情報解析支援システムの提案”，マルチメディア，分散，協調とモバイルシンポジウム 2020 論文集，Vol. 2020, pp. 1606-1615 (2020).
[2] IPA セキュリティセンター：“「Emotet」と呼ばれるウイルスへの感染を狙うメールについて：IPA 独立行政法人 情報処理推進機構”，入手先(https://www.ipa.go.jp/security/announce/20191202.html) (参照 2020/07/23).