表層解析の効率化に向けた情報提示方式の提案

Proposal of Information Presentation Method
for Improvement of Surface Analysis Efficiency

本部 建大[1] 竹原 一駿[1] 檜垣 龍徳[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. Motobu[1] I. Takehara[1] T. Higaki[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

日々高度化するサイバー攻撃に対応する，サイバーセキュリティ人材が不足している．組織のサイバーセキュリティ人材(セキュリティ管理者)は，サイバー攻撃のリスク評価，戦略策定のために調査として“表層解析作業”を行う．表層解析作業では，大量のセキュリティ情報を閲覧し，精査しなければならず，大きな負荷となっている．我々はこの負荷軽減を目指したシステムを試作して評価した[1]．本システムの UI を実装するために，記事解析部とともに開発している．記事解析部は，自組織に関係するトピックの抽出，分類，時間情報の抽出をテキスト解析によって行う．UI は，実際のセキュリティ管理者の評価を受けながら開発している．そこで，試作システムのレイアウトに関して改善の余地があるとの評価を受けた．本稿では，その評価を踏まえて，表層解析作業の難しさを解消するための新たな UI を提案する．

2. 表層解析作業の現状

組織は，調査したいセキュリティに関する用件(トピック)を大量に持っており，これを毎日セキュリティ管理者が精査する(表層解析作業)．この作業の難しさを，以下に示す．

①: 情報が更新される時期がわからない．このため，毎日，セキュリティ情報の更新をチェックする．株式会社 STNet では，40 以上のセキュリティ情報サイトと，10 以上の SNS アカウントをチェックしている．

②: 公開された情報が最新であるかわからない．あるトピックについて，複数のセキュリティ情報サイトや SNS で情報が発信されている．それらを比較することで情報の鮮度を把握する．

③: 段階的に情報が詳細化される．一般的に，まず被害の状況が発信される．その後，原因の仮説と，その対策に関する情報が公開される．仮説が検証されていくことで，より確かな原因と対策の情報が発信される．

④: 情報に誤りがあることが後日発覚する．被害の原因と対策はあくまでその時点の仮説であり，後に正しい情報が流れることがある．特に，誤った情報はインターネットから消えることはないので，過去の経緯を遡り，何が正しいかを判断する必要がある．

つまり表層解析作業では，継続的に大量のトピックの調査が必要である．

3. 課題

現状，一般的には 1 トピックの情報を比較するために，ブラウザのタブを大量に開いている．図 1 は，あるトピックを精査している画面例であり，間違った情報や古い情報を抽出して判断した結果である．その結果を導くために，複数の記事を開き比較するため，大量のタブが開かれている．このとき，タブを見ただけでは記事の内容がわからず，何度もタブの内容を確認する手間が発生している．さらに，共同研究先の評価から，閲覧したい記事や比較したい記事の概要を一度に画面に表示すると，表示領域が狭く確認しにくいという問題が発覚した．本研究では，これらの問題を解決できる新たな UI を提案する．

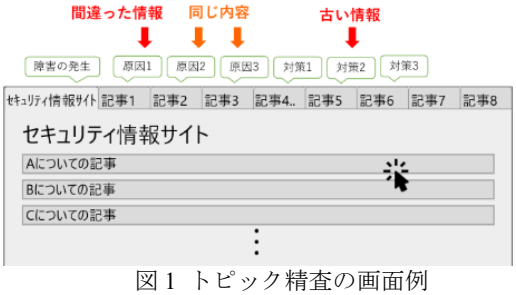

図 1 トピック精査の画面例

4. 提案する UI

(UI) 起動すると，自組織に関係するトピックのサマリの一覧が表示される(図 2)．前回起動したときと比べ，そのトピックの更新状況をバッジで表示する．トピックを選択すると，記事閲覧画面に遷移し，この画面は関連記事表示部(画面左部)と Web ページ表示部(画面右部)から構成される．遷移直後は，そのトピックの最も重要な記事を，Web ページ表示部に表示する．関連記事表示部では，このトピックに関連する記事のサマリを，最新の記事から降順に表示し，不必要な場合は隠すことができる．サマリを選択すると，Web ページ表示部にその記事の内容を表示する．既に読んだ記事のサマリは，薄い灰色で表示する．

(典型的な利用の流れ) トピック選択画面のバッジを確認し，情報が更新されているかを確認する．更新されているトピックを選択し，記事閲覧画面に遷移する．そのトピックの最も重要な記事を読み，トピックの内容を把握する．その後，最新の記事を読み，更新内容を閲覧する．記事の内容が，その 1 記事では判断できない場合は，過去に遡って Web ページを閲覧する．

(課題解決の検証) この UI で課題が解決する理由は，まずトピックに関連する記事を時間順に並べているためである．これによりトピックの最新記事がわかり(難しさ②)，情報が段階的に詳細化する流れが追え(難しさ③)，情報を比較することで誤った情報かを判定できる(難しさ④)．難しさ①に関しては，記事解析部で解決する．表示領域が狭い問題は，領域のサイズを可変にすることで解決する．

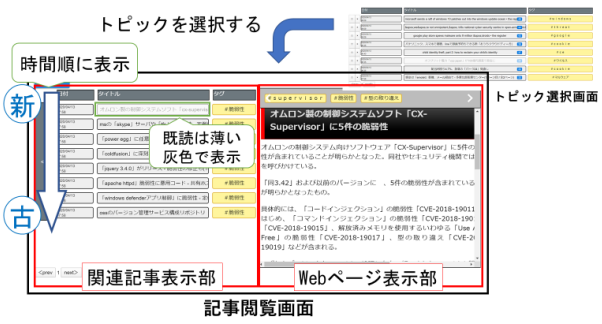

図 2 提案 UI

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).