脆弱性DBを用いた脅威分析手法へのトピックモデル解析ツールの活用

Utilization of topic model analysis tool for threat analysis method using vulnerability database

梅澤 克之[1] 三科 雄介[2] 寶木 和夫[2] Sven Wohlgemuth[3]
Katsuyuki Umezawa Yusuke Mishina Kazuo Takaragi

湘南工科大学 情報工学科[1]
Shonan Institute of Technology, Department of Information Science
国立研究開発法人産業技術総合研究所 情報技術研究部門[2]
Advanced Industrial Science and Technology (AIST), Information Technology Research Institute (ITRI)
(株) 日立製作所 研究開発グループ[3]
Hitachi Ltd. Research & Development Group

1 まえがき

我々は脆弱性事例データベースとシステム設計情報を活用した脅威分析方法を提案してきた [1]. この提案アルゴリズムの中で, 自然言語処理と AI 処理を用いて突合評価を行う処理が記述されているが, 未解決である. 本論文では, トピックモデル解析ツールを用いて突合処理の実現性を評価する.

2 従来技術

2.1 脅威分析アルゴリズム

文献 [1] で示した脅威分析アルゴリズムでは, 評価対象システムに関するアタックツリー (*AT* と呼ぶ) の各ノードと, 既存の脆弱性毎に作成された *AT* の各ノード (それぞれ自然言語で記述されている) を突合評価し, 新たな *AT* を構築する. これにより起きては困る事象の発生確率の計算や今後の分析における活用が可能になる.

2.2 トピックモデル解析

文書には潜在的なトピックがあり, 各キーワードはそのトピックから生成されているという考え方をトピックモデルという. トピックモデル解析では, キーワードから潜在的なトピックを推定する. 国立研究開発法人産業技術総合研究所では, トピックモデル解析技術を用いたセキュリティ要件分析支援ツールを開発している [2].

3 脅威分析手法へのトピックモデル解析ツールの活用

3.1 脆弱性事例データベース CVE の体系化

本節ではまず, 発見順にリスト化されている膨大な数の脆弱性事例データベース CVE をトピックモデル解析で階層構造に体系化可能か否かを検証する. 日本語用のトピックモデル解析ツールを使うため Google 翻訳を活用した. Google 翻訳を活用する利点としては, 用語の表記ゆれを防ぐ効果もあると考えられる. 図 1 に示した通り, 似たような脆弱性が階層構造の近くに分類されていることがわかる.

3.2 既知の攻撃手法との突合

2.1 節で示した突合処理にトピックモデル解析ツールが活用できるかを検証する. 今回既知の攻撃手法としてテスラ社の自動車への攻撃を例にする. 発表された論文を節ごとに Google 翻訳にかけて日本語訳したものと CVE

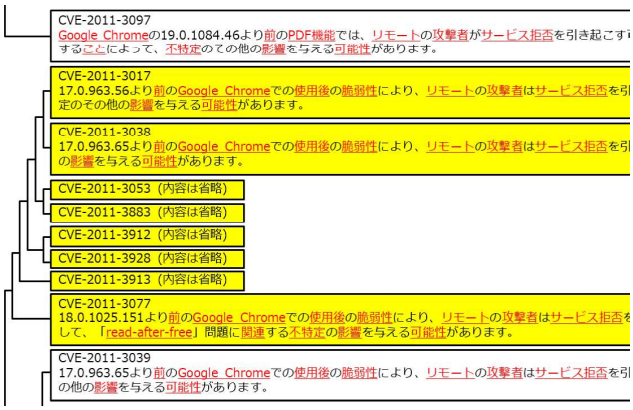

図 1 脆弱性事例データベース CVE の体系化 (抜粋)

の日本語訳をツールに入力として与え比較分析を行った. その結果, 攻撃手法を紹介した論文の指定した章に類似した既存の脆弱性を抽出する可能性を確認できた.

4 まとめと今後の課題

トピックモデル解析ツールを用いて, 脆弱性事例データベースの体系化および既知の攻撃手法との自然言語処理と AI 処理を用いた突合の実現可能性を確認できた. 今後は, 脆弱性事例データベースとシステム設計情報を活用した脅威分析方法 [1] に適用して実事例で評価を行う必要があると考える.

謝辞

本研究 (の一部) は, 総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム (SIP)「重要インフラ等におけるサイバーセキュリティの確保」(管理法人 : NEDO) によって実施されました.

参考文献

[1] 梅澤克之, 三科雄介, 田口研治, 寶木和夫, “脆弱性データベースを使用した脅威分析方法の提案, ” 暗号と情報セキュリティシンポジウム (SCIS2018) 予稿集, 1C2-6, Jan. 2018.

[2] 半田剣一, 大崎人士, 竹内泉, “セキュリティ要件分析支援ツール TACT, ” 情報処理学会ソフトウェア工学研究会 ウィンターワークショップ 2017・イン・飛騨高山予稿集, 2017.