SSVCを活用したLLMによる社内システム脆弱性管理効率化の提案

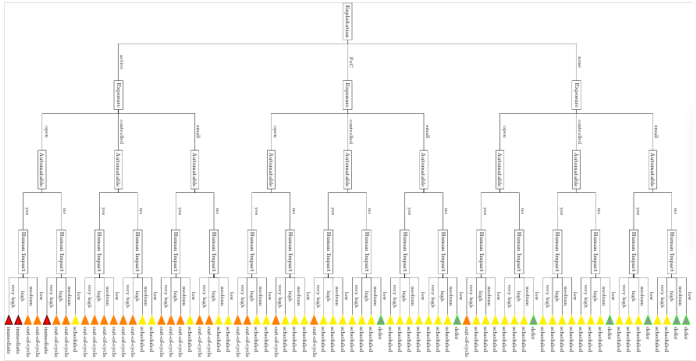
A Proposal for Improving the Efficiency of Corporate System Vulnerability Management Using Large Language Models with SSVC

藤井 舞・マネジメント分科会・情報セキュリティ大学院大学

研究背景・目的

近年，デジタル化の推進や公開CVEの増加により，組織における脆弱性管理の負担は増大している．CVSSスコアが高い脆弱性は緊急対応が望ましいが，実運用ではシステムの設置環境や公開範囲によって実際のリスク評価は異なる．そのため，スコアの高さのみで一律に対応することは現実的ではなく，対応優先度の判断には属人性が入りやすいという課題がある．本研究の特徴は，大規模言語モデルを用いて脆弱性管理の自動化を図るだけでなく，SSVC（Stakeholder-Specific Vulnerability Categorization）を組み合わせることで，脆弱性対応の優先度判断に一貫した基準を与える点にある．さらに，社内環境でLLMを運用することで，実運用において求められる機密性と実用性の両立を目指す．

SSVC



提案手法

（1）脆弱性情報の自動収集・正規化，（2）社内システムDBとの突合，（3）SSVC（Deployer視点）に基づく対応優先度の自動決定の三段階で構成される．NVDから取得した脆弱性情報に対し，LLMを用いて製品名，バージョン，日本語説明，Exploitation情報（CISA， EXPLOITDATABASE ）などを抽出する．次に，抽出した製品情報を用いて社内システムDBを検索し，該当システムを特定する．更にExploitationと社内システムDBに保持されたExposureやHuman Impact等を用いてSSVC判定を行い，システムごとの対応優先度を決定する．最後にユーザにサマリを出力する．

結論

NVDに掲載されている製品名は1040件中1038件完全一致し，LLMが抽出した製品名は808件中453件であった．Expoitationの結果は99.3%一致した．システム検索精度の評価は正解率，適合率，再現率，F値で96%以上となり， SSVCの精度は100%となった．本提案により作業時間が1/3短縮され，日次の脆弱性管理業務における実用性が示された．本研究では，LLMを用いた脆弱性管理自動化手法にSSVCを統合し，社内向けに安全かつ一貫性のある対応優先度決定を実現する手法を提案した．提案手法は，運用負担の軽減と安定した脆弱性対応に寄与するものであり，今後，改良により，実運用でのさらなる有効性が期待される．