サイバーセキュリティにおける オープンソースインテリジェンスに関する考察

A study on Open Source Intelligence in Cyber Security

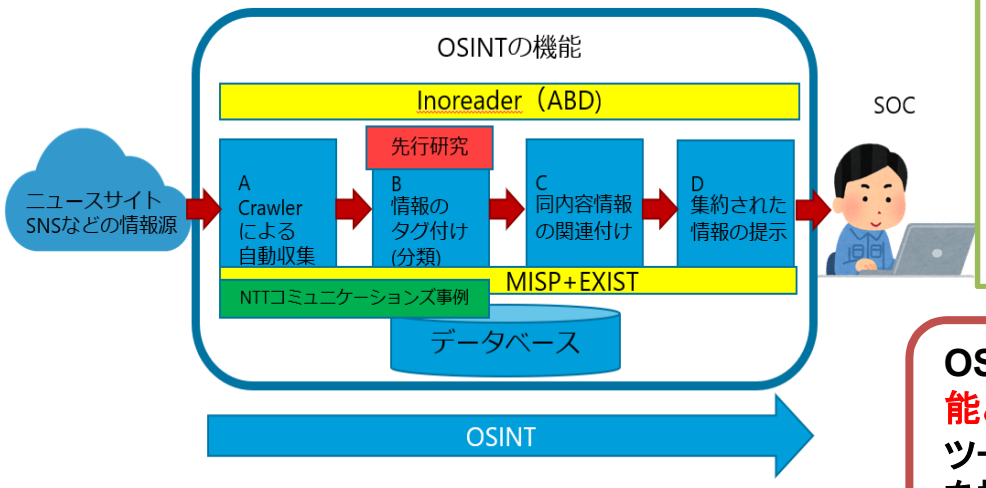
大村 篤生・マネジメント分科会・情報セキュリティ大学院大学

1.研究背景・目的

サイバー攻撃の巧妙化が進む中で、脅威情報や脆弱性情報の素早い収集のために公開情報を活用するOSINT(Open Source Intelligence)が注目されており、組織のセキュリティ防御のためにSOCの支援を目的とした自社でのOSINTが有効と考えられる。本研究では「自組織のセキュリティ対策における脅威・脆弱性情報の早期認識のため、公開情報(主にインターネットのニュースサイトやSNS)から情報収集を行うこと」をOSINTの定義とし、その目的を持ったOSINTにおいて課題があるか確認をすべく先行研究と他社のOSINT機能の構築例を調査した。先行研究の調査を行った結果、情報の自動翻訳や要約化など、収集される情報の高度な分析、情報収集の自動化に必要なクローリング機能におけるセキュリティリスク、収集情報とログ情報との連携が課題点として挙げられる。

2.活動成果・研究計画

(1)OSINT自動化における機能の調査結果(活動成果)



(2)OSINTの課題と今後の予定(研究計画)

1. 情報収集の自動化にセキュリティ脅威がない
2. 収集された情報を分かりやすくするため、収集情報の日本語翻訳が自動的に行われる
3. 収集された情報を分かりやすくするため、収集情報の要約が自動的に行われる
4. SIEMの通信ログと連携させることができ、SOCのインシデント判断に活用される
5. 収集される情報について、信頼性が確保されている

OSINTツール「MISP」,「EXIST」をベースとしてOSINTの機能として導入することを目標とする。また、既存のOSINTツールを比較し評価軸を構築をすることで研究への有効性を持つツール評価を行う。