攻撃パターンによるアタックツリーの再利用性向上

Improving Reusability of Attack Trees by Attack Patterns

大矢政基　マネジメント分科会　情報セキュリティ大学院大学

Abstract — The attack tree is an effective method for analyzing threat occurrence scenarios, but there are many issues regarding its practicality, so various researches have been conducted to streamline the task. In this study, we propose a framework for generating "reusable attack trees" using CAPEC, aiming to improve efficiency by utilizing past analysis results.

はじめに

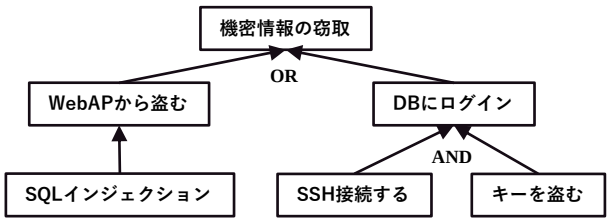
情報セキュリティ対策の費用対効果を最大にするためには、システム開発の初期段階で脅威分析を行うことが重要である。アタックツリーは脅威の生起シナリオを分析するのに効果的な手法であるが、高度な専門性や実施コストが課題である。本研究ではそのような**実用性に関する課題解決のためのフレームワークの開発を目指す。**

アプローチ：アタックツリーの再利用性向上

- **分析結果の再利用により作業負担を軽減**
- **CAPEC活用により再利用可能なツリーの作成**

アタックツリー / CAPEC

- **アタックツリー**：脅威（攻撃者のゴール）をルートノードとし、それを実現する手段をブレイクダウンしていく手法
- **CAPEC**：米MITRE社が管理する攻撃パターンデータベース。各パターンには攻撃概要や成立条件、影響等の情報が付与



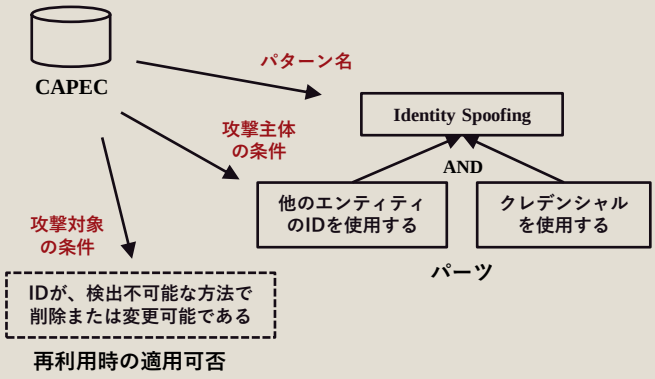
アタックツリーの例

先行研究

アタックツリーの実用性向上に向けた先行研究として、CAPECを活用した自動化や効率化は行われているものの、**「再利用」に焦点を当てたものは無いため、本研究の独自性となっている。**

CAPECを活用した再利用可能なアタックツリー

- **作成時の流れ**：CAPECからアタックツリーのパーツを作り、それらを組み合わせることでアタックツリーを完成させる。
  ① 攻撃成立条件を「**攻撃主体の条件**」と「**攻撃対象の条件**」に分類する。
  ② 攻撃パターン名をトップノード、「**攻撃主体の条件**」をその子ノードに配置することでパーツを作る。
- **再利用時の流れ**：完成しているアタックツリーからパーツを抽出し、再利用する。
  ① CAPECを参照し、「攻撃対象の条件」を抽出する。
  ② 分析対象のシステムが「**攻撃対象の条件**」を満たすかどうかでパーツの再利用の可否を判断する。



今後の研究方針 / 期待される効果

今後はフレームワークを具体化した後、ケーススタディにより効果を検証する予定である。本フレームワークに期待される効果として、**作業負担や結果の属人性の課題が改善される**ことに加え、過去の分析結果を正しく評価できるようになることで、**組織の脅威分析の精度を高めていく**ことにも寄与できると考えている。