リスク低減のための偽装検知システム評価

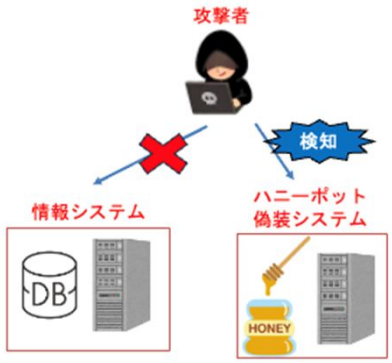
Assessment of a deception detection system for risk reduction

中島明彦・ネットワーク分科会・情報セキュリティ大学院大学

背景

標的型攻撃やゼロデイ攻撃
といった脅威を完全に防ぐこと
は困難
→ネットワークへの侵入を前提
とした偽装防御

ハニーポットや囮ファイル,
偽装ネットワーク
→攻撃者のリソースを消費



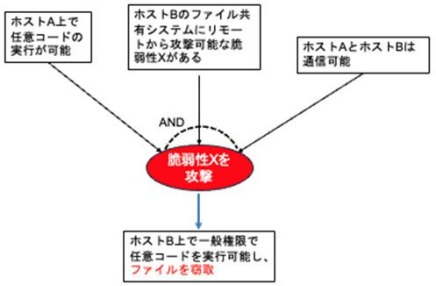
研究目的

2. 研究目的
正規利用者の妨げや予算の限界による
偽装能力の低下の恐れがある

戦略的な偽装システムの配置の評価

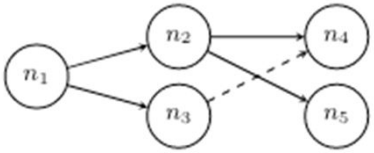
先行研究

攻撃グラフを用いた
セキュリティリスク推定



脆弱性を悪用するための条件をグラフ化
それぞれにCVSSの評価値を元に確立的に選択する

セキュリティリソース
の戦略的割り当て



攻撃者に対する防御側が取る選択をセキュリティゲームとして捉え、偽装技術を加えるゲーム理論の意思決定に関する研究

今後の予定

実システムを想定した環境で偽装技術を実装し、攻撃グラフとセキュリティゲームを用いたセキュリティリソースの戦略的割り当て方法を用いて通常のセキュリティ対策との比較評価を行う.