サーバのログ解析によるサイバー攻撃検出

教授 ・ 武藏　泰雄

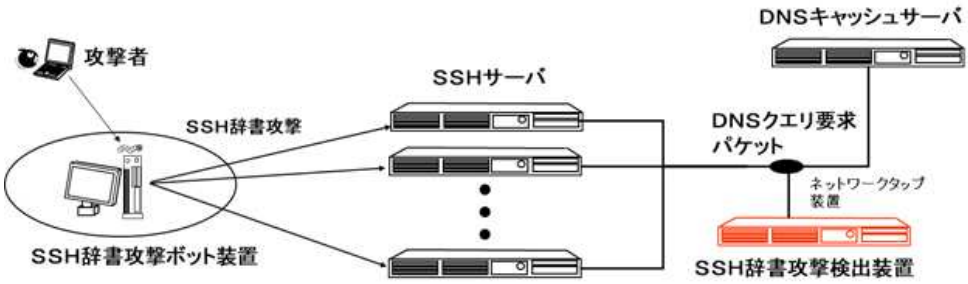
半導体・デジタル研究教育機構 コンピュータサイエンス分野

研究内容

将来起こりえるネットワークに対してのサイバー攻撃に対応するため、ドメインネームシステム (DNS) サーバや E-mail サーバ、または Web サーバ等、様々なネットワークサーバのログの解析を行っています。

従来の攻撃に対する対策として、不正な通信を検知・防御するシステム 不正侵入検知システム等 を導入するという方法があります。しかし、システムの導入はコストがかかるため、容易ではありませんでした。そのため、ログを監視しパケットを捕獲して、攻撃ホスト名やIPアドレスを精査するにことにより、攻撃を検知する手法を提案しています。そして、小さい処理負荷、かつ短時間での攻撃検知・対策を実現しています。

また現在、量子機械学習モデルを中心とした攻撃の検知や、サイバー攻撃に関する様々な情報を収集分析し知見として蓄積する「脅威インテリジェンス」にも取り組んでいます。



提供できる技術

サーバ等が書き出すログ解析によるSSH辞書攻撃の検出
DNSベースによるスパムボット、ホスト検索活動の検出

特許

特開2011-097468 監視装置、監視システム、監視方法及び監視プログラム

キーワード

ネットワークセキュリティ　異常検知　ログ解析　DNSベース検出　ホスト検索