家庭でのIDSの誤検知削減手法の提案

4EP4-46 平井 聖人

進捗

- 論文調査(わからない+途中)

論文

- IDSアラートに対する誤検知削除方法の提案とその評価(2019)

情報学広場：情報処理学会電子図書館 (nii.ac.jp)

- この削除手法はフィルタを用いてアラートの削除を行う。フィルタは 3 つのコンポーネント(NRA、HAF、UFP)で構成されている。

論文

- NRA : 実際の攻撃により、送信元 /送信先 IP アドレスに類似度を持つひとまとまりのアラート群が生成される

- HAF :実際の攻撃により，同一のシグネチャにより生成されたアラートが異常な分布を生じる

- UFP : 誤検知はシグネチャが誤検知を引き起こす頻度で識別できる
- この3つの評価値を最大値、最小値、平均値の 3 つのうちいずれかと設定した閾値 th を比べることで行う

論文

- そしてDBSCANを用いてクラスタリング(データ間の類似度に基づいてデータをグループ分けしていく手法)し、精度を向上させる。

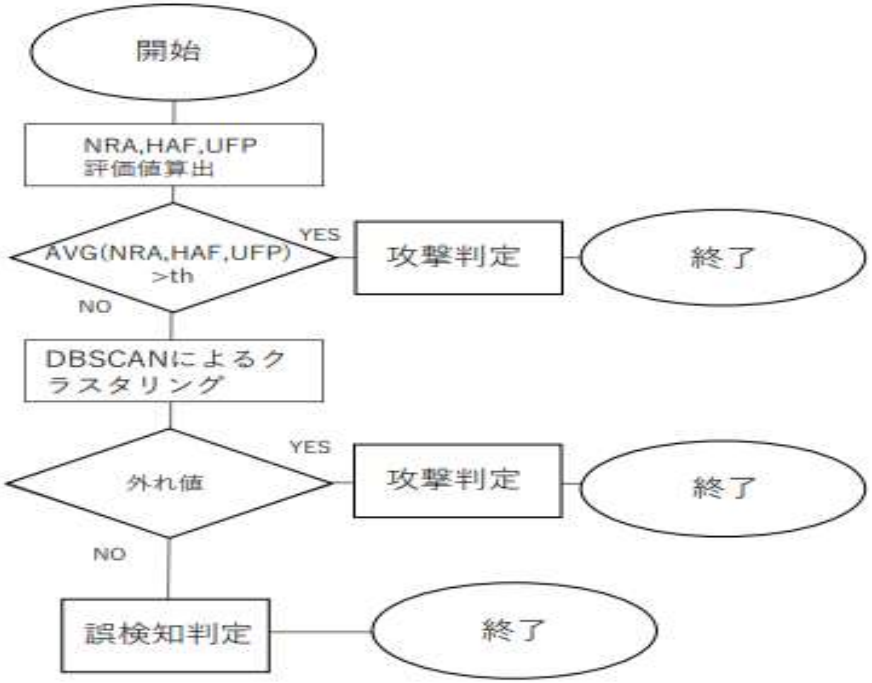

図 2　DBSCAN を用いた削除法

論文

- 途中まで読んでみたが、よく分からなかった
- なぜシグネチャ型で誤検知が発生するのかも書いていなかった。

今後

- 中間発表の資料作り
- シグネチャ型で誤検知が出る理由を調べる
- 論文の続き

- どのような攻撃があるか
- どのような通信内容なのか
- 推測か文献
- 現状のセキュリティがどのくらいか。それだけで足りるのか。足りない場合は何が起こるのか