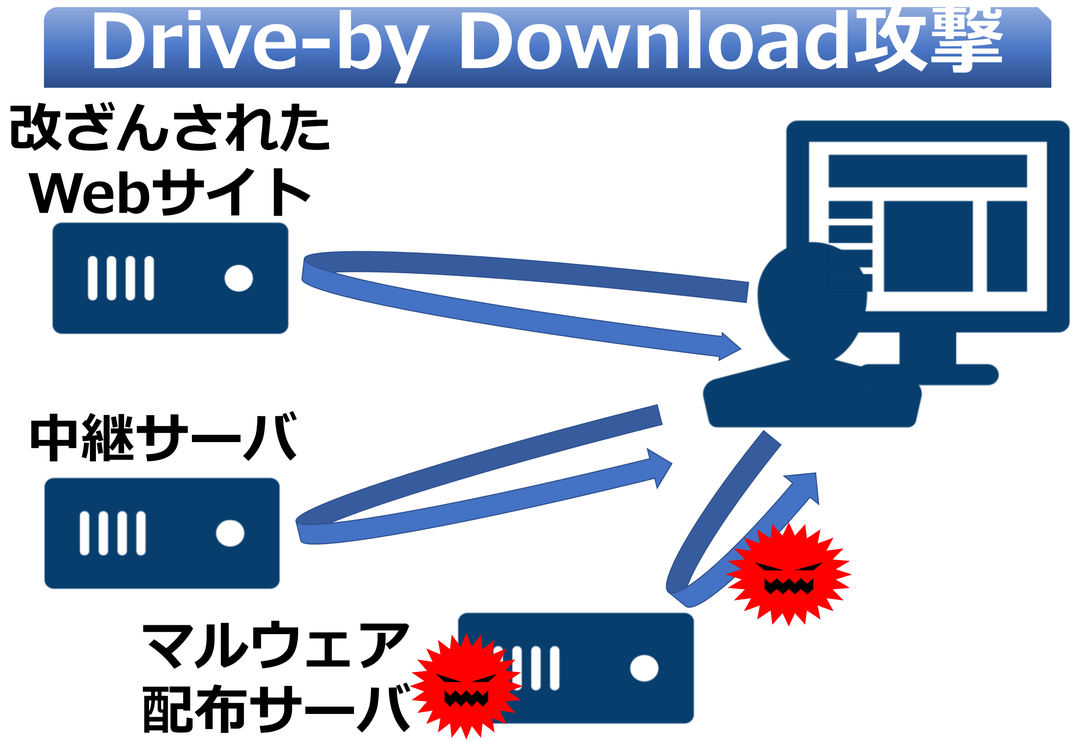
# 決定木を用いた Drive-by Download攻撃解析支援手法の提案

尾崎 幸也-関西大学総合情報学部 小林研究室

## 1. はじめに

Drive-by Download攻撃の被害は依然としてとどまらない．この攻撃は，リダイレクトに用いるスクリプトタグ等を難読化することで解析の妨害を行う．その為，攻撃の解析が非常に困難である．

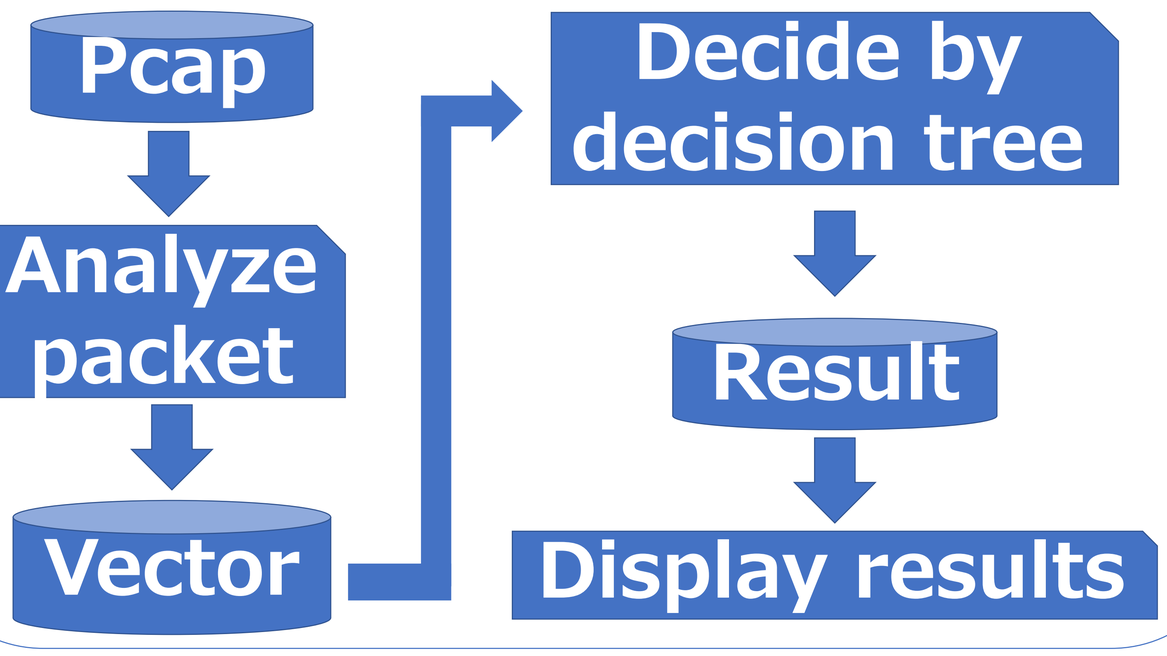
そこで本研究では，Drive-by Download攻撃の解析を支援するアプリケーションを開発することで，解析作業の効率化を目指す．




## 2. 提案手法

本アプリケーションは，webサイトへ接続したパケットが記録されたファイル(pcapファイル)を解析し，その中からHTTPセッションを抽出する．また，各パケットの宛先アドレスやHTTPリファラを元に抽出したセッションを木構造化する．その後，抽出したURLの文字列及びリクエストパケットの特徴量を抽出し，決定木によってそれらの良悪判定を行う．悪性だと判定されたURLは危険度によって段階的に色付けする．これにより攻撃の発生箇所の特定，及びリダイレクトに用いられたサーバの特定，解析の優先順位の決定が容易になると考えられる．

### 本システムの流れ




### 結果画面のイメージ


## 3. 今後の展望

本提案ではHTTPセッションを木構造化し，悪性だと推定されるURLを段階的に色付けすることで，Drive-by Download攻撃の解析を支援するアプリケーションを開発した．しかし，現在は決定木によってどのように良悪判定が行われたのかを視覚化できていない状態である．そのため，今後視覚化する必要がある．

また，本アプリケーションはHTTPSなどの暗号化を用いた通信を解析することができないため，改良しなければならない．