SecHack365

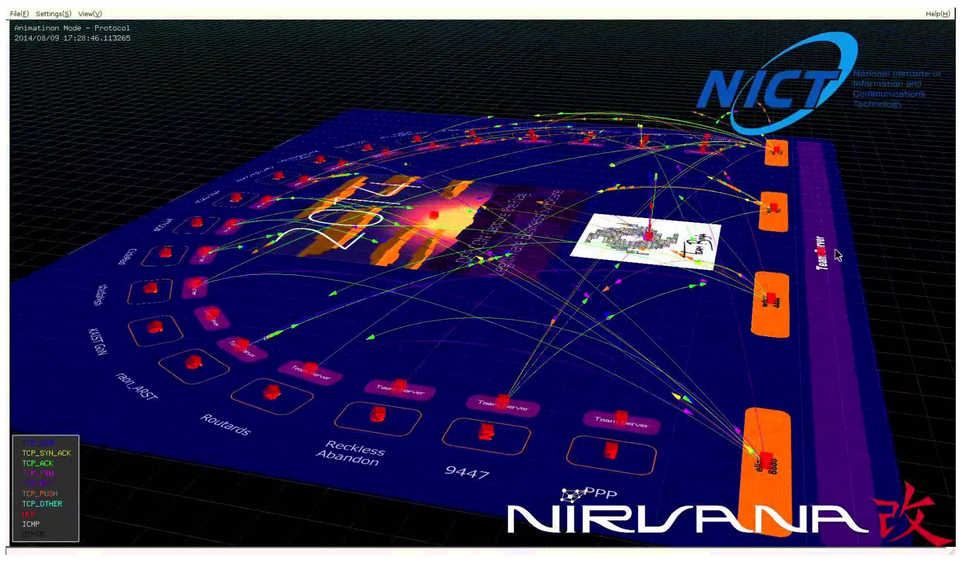
LOG VISUALIZATION

金沢工業大学 竹村太一
NTT-ME Cyber Security Center 藤井翼

1.課題 | 可視化システムとは

可視化システムのメリット

・内在するリスクや状況の認識共有
・ネットワーク全体の可視化



https://www.youtube.com/watch?v=1FO19NpSSBs

可視化システムの課題

・可視化をしても、使いこなすには専門的な知識と技術が必要

・画面を眺めているだけで本質が見えにくい

2.提案 | 新しい可視化手法の提案

可視化される情報

・攻撃元のIPアドレス
・攻撃の種類
・攻撃の脅威度
・ポート番号などの付加情報

脅威度をモンスターで表現

深刻な攻撃をどの程度受けているのか視覚的かつ直感的に把握

インターネットからの攻撃を受けやすいWebに着目

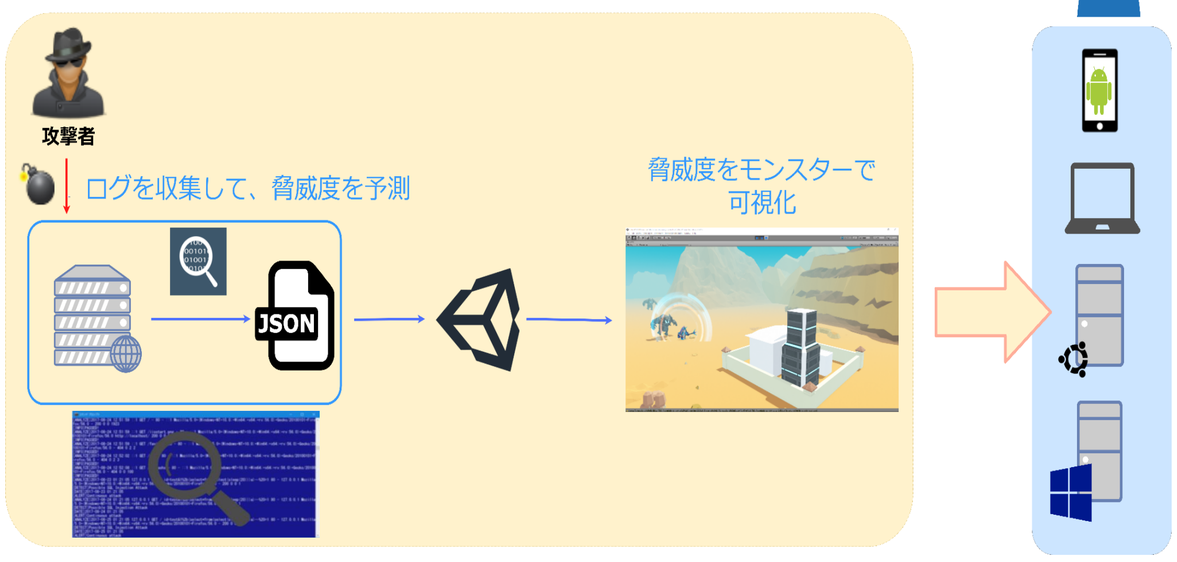
3.概要 | 可視化システムの概要

ログ収集・解析処理

1. Webサーバのログを収集し解析
2. 解析結果を出力(JSON形式)

主な解析対象

・Tor Exit Nodesからのアクセス
・インジェクション攻撃の特徴的な文字
・急激なアクセスの増加
・継続的に攻撃が続いている傾向



可視化処理

3. 結果を可視化システム(Unity)へ取り込み
4. 脅威度に基づいてモンスターを生成

LOG Visualization