ログ調査のためのイベントログの矩形波表現を用いた可視化の提案

齋藤日華里 [1,*]　中野 心太 [2,] 関谷 信吾 [2,] 折田 彰 [3,] 岸本 頼紀 [4,]
早稲田 篤志 [4,] 花田 真樹 [4,]

概要：ログ調査において,一定パターン出現の把握や異常箇所の視認性向上は重要である.そこで,ログデータを矩形波で表現する手法を提案する.イベントは時系列に並ぶため横軸を時間と設定すれば高さを定義すれば矩形波で表現できる.これにより形状の違いによる異常箇所の表現や,一定パターンの出現について視認性を向上させることができる.本論文では,Windows ログを対象とした矩形波表現のための高さとして出現頻度やイベント ID の固定値などの表現方法について検討し,実際の例に適用した結果とその効果について報告する.

キーワード：デジタルフォレンジック，ログ解析,

A Proposal of Visualization of Event Logs using Square Wave Representation for Log Analysis

Hikari Saitou[1,*]　Shinta Nakano[2,] Shingo Sekiya[2,] Akira Orita[2,] Yorinori Kishimoto[4,]
Atsushi Waseda[4,] Masaki Hanada[4,]

Abstract: In log analysis, improving the visibility of patterns and abnormalities is important. Therefore, we propose a method to represent log data as square waves. Events are arranged in chronological order. If the height can be defined by defining the horizontal axis as time, then they can be represented as square waves. Different shapes can improve the visibility of abnormal log representations and the occurrence of certain patterns. In this paper, we investigate methods for representing Windows logs as square waves, such as frequency of occurrence or fixed values of event IDs, and report the results and effectiveness of applying them to actual examples.

Keywords: Digital Forensics, Log Analysis

1. 序論

デジタルフォレンジックでは,ログ調査により攻撃者の侵入時間や攻撃手法について分析する.この際,ログが長大になると分析が困難になるため,支援システムが求められている.この問題に対して SKYSEA や Autopsy など様々な支援システムが提案されている[1][2].しかし,近年のシステムは SaaS として提供されていたり,リアルタイム監視のために初期から設定登録が必要な場合も多く,攻撃被害を受けた社内システムへの緊急な適用が難しい.また,ログ管理システムを導入していても攻撃被害に合う可能性もあり,この場合,管理システムの支援をすり抜けた攻撃のため,別システムによる調査が求められる.また,早期対応のため初動調査の重要性からファストフォレンジックに対応できるシステムが求められる.

これに対して,Windows のログを対象として Doc2vec で区間の特徴量を計算し,特徴量の違いにより異常箇所を可視化するシステムが提案されている[3].このシステムでは,イベント ID を単語,その並びを文章と考え,8 時間や 1 日といった一定区間のイベント ID の並びの特徴量を Doc2vec で計算し,これを折れ線グラフで可視化することで,他の区間と異なる特徴量の区間を表現できる.本システムは一般的なマルウェアなどの調査結果による特徴に依存せず,未知の攻撃に対しても異常箇所を可視化できることを目的としており,これを用いれば未知の攻撃手法であっても,攻撃が疑われる区間が推定でき,ログ分析の支援となる.

しかし,該当区間のどこが攻撃痕跡か判別するためには,別途ログデータを調査する必要がある.Autopsy のような支援システムではイベントの総数や発生イベント区間を可視化することはできるが,イベントそのものの特徴を時系列に可視化できるものは少ない.そこで,一定区間に対してイベントの特徴を時系列に並べて可視化する手法を提案する.横軸を時間とし,縦軸をイベントの特徴量として棒グラフで可視化する.これにより,OS やシステムの稼働痕跡のような一定パターンを同形として表現でき,出現が稀なイベントは異なる高さとして表現され,イベント発生の集中具合

1 東京情報大学大学院総合情報学研究科
Graduate School of Informatics. Tokyo University of Information Sciences.
2 株式会社日立システムズ セキュリティ技術 R&T センタ
Hitachi Systems, Ltd. Security Technology R&T Center..
3 株式会社日立システムズ セキュリティリスクマネジメント本部
Hitachi Systems, Ltd. Security Risk Management Division.
4 東京情報大学　総合情報学部
Faculty of Informatics, Tokyo University of Information Sciences.
* g25008sh@edu.tuis.ac.jp

も可視化できる.また,可視化結果から目星をつけて調査することで本目的であるファストフォレンジックへの支援となる.

本論文では,Windows のイベントログに対して,1 日程度の短期間のログを棒グラフで可視化する手法について提案し,これを実際の例に適用した効果について論じる.

2. 考え方

イベント出現密度の可視化イベント出現の可視化として,イベントの出現密度と出現頻度に着目する.

2.1 イベント出現密度の可視化

標的型攻撃では,攻撃者による権限昇格などのイベントが短期間に多く出現すると考えられるため,イベントの出現密度は攻撃痕跡調査の 1 つの指標となると考えられる.そこで,横軸を時間軸として出現イベントをプロットすることで短期間に多くのイベントが出現する場合は密度の高い区間としてこれを表現できる.例えば,通常 1 時間に 2～3 個程度のイベントが発生しているログのうち,ある 1 時間区間に 10 個のイベントが発生すれば,密度の高い区間としてこれを可視化できる.

しかし,DDoS 攻撃のように極めて短い期間に大量のイベントが発生する場合は,同時刻に複数のイベントが発生することが考えられる.この場合は時間軸を拡張し全てのイベントを出現順に可視化する方法を提案する.同時刻に異なるイベントが複数発生する場合,出現タイミングによっては異なる時間になる場合も考えられる.本目的では,一定パターンで出現するログは同様の形状で表現することが望ましいと考える.そのため,同時刻であっても出現順に可視化表現することで同様の形状として表現できる.また,DDoS 攻撃のように同一のイベントが発生する場合は,連続出現自体が特徴となるため全て可視化することで異常箇所を表現できる.

2.2 イベント出現頻度の可視化

サイバー攻撃で発生するイベントには,通常では出現が稀なイベントや,通常ペアで出現するイベントが片方しか出現しない場合も考えられる.そこで,イベントの特徴を高さとして表現することで,同じ高さのイベントは同一,異なるイベントは異なる高さとして表現する.これにより,イベントそのものの特徴を可視化できる.

イベントの高さとして表現する特徴について検討する.サイバー攻撃の特徴として珍しいイベントが出現する場合,出現頻度が低いイベントの値を大きくすることで,より明快に表現できる.しかし,サイバー攻撃の痕跡では,通常のイベントとしてペアで出現するもののうち,片方だけ出現するといった場合も考えられる.この場合,出現頻度が高いものの値を低すると視認性が悪くなる可能性がある.

そこで,本研究では両方の可視化を検討する.出現頻度に応じた値にする場合は,出現頻度の逆数を基準とした値として可視化する.出現頻度を考慮しない場合は Windows のイベント ID の値をそのまま特徴量として採用する.両者による可視化を比較することで,適した表現方法を検討できる.

3. システム概要

本システムはイベントログファイルを読み込み,日ごとのログデータを 2 つのグラフに出力する.1 方は縦軸をイベント ID の値をそのまま使用し,もう一方はイベント ID の頻度を逆数にした値で双方横軸を時間としたグラフに出力する.

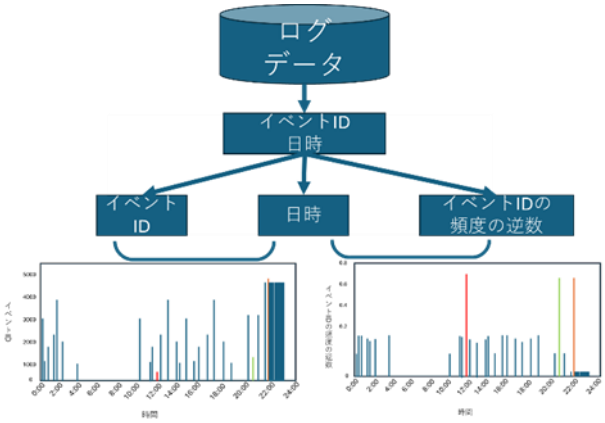

図 1　システム概要

また開発環境は Python　version 3.12.11
Google Colaboratory　である.

4. 適用例

4.1 攻撃ログの作成と環境

攻撃ログについて概要を示す.ログ作成はホスト OS を Windiows11 上の VirtualBox7.2.0 で仮想環境として構築した.

4.2 攻撃の種類

4.2.1 PassTheHash の環境

AD 環境: 構築済みの Active Directory 環境
被攻撃端末:
・ドメインサーバ
OS: Windows Server 2019
・ドメインに所属するクライアント端末（2 台）
OS: Windows 10
攻撃端末:
・OS: Kali Linux
使用ツール: Metasploit, PsExec, Mimikatz

4.2.2 PassTheHash 攻撃の手順

1. ネットワーク内の端末を nmap でスキャンし,ターゲットを探索する（nmblookup を使用して NetBIOS 名やドメイン情報を確認）.
2. Metasploit を使用してターゲット端末 A に接続する.
3. Mimikatz を端末 A に転送し,実行して NTLM ハッシュを取得する.

4. 取得したハッシュを用いて端末 A に再侵入し,PassTheHash 攻撃を実施する.
5. (試行結果) 端末 B へのアクセスは成功しなかった.

作成したログうち,セキュリティログ,システムログの中から攻撃ログの攻撃実行時間のみをトリミングし,長時間起動していた別端末から取得したログを通常時のログとして両者を統合し,攻撃痕跡が含まれているログとして作成した.

5. 結果

本例における可視化結果を示す.図 2,3 は高さをイベント ID の値で表現したものであり,図 4,5 は高さをイベントの出現頻度の逆数で表現したものである.赤枠で囲った部分が攻撃日時に該当する.

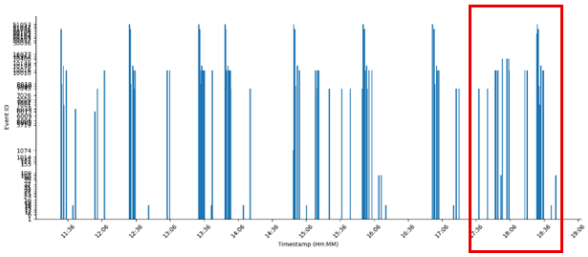

図 2　イベント ID×時間　システムログ

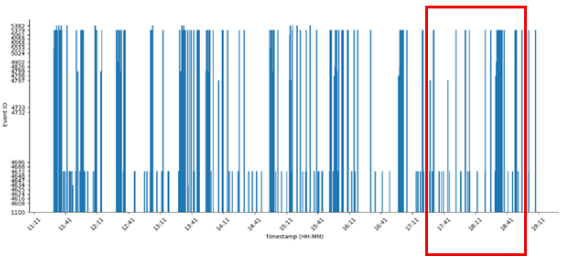

図 3　イベント ID×時間　セキュリティログ

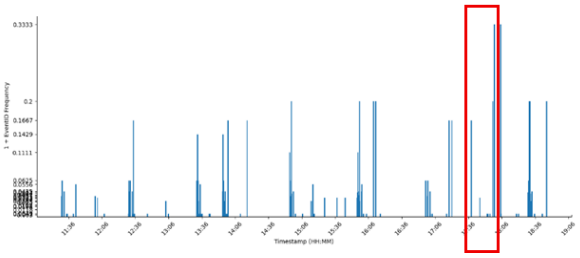

図 4　ID 逆頻度×時間　システムログ

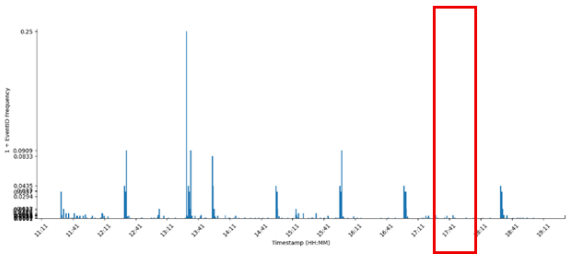

図 5　ID 逆頻度×時間　セキュリティログ

本例では 1 日ごとのイベントログを時系列に可視化を行った.そのため,1 日の起動時間が短い図 2 のグラフでは,1 イベントの幅が大きく出力され,通常ログであっても目立つこととなった,

6. 考察

本例では,図 4,5 よりも図 2,3 の方がイベントの密度がわかりやすく表現された.これは,図 4,5 のように出現頻度の高いイベントが低く表示され,密度が見にくくなることに起因する.本例は pass the hash 攻撃であるため,通常のイベントとして出現するイベントが痕跡として残るため,視認性が悪くなったと考えられる.また,これは DDoS 攻撃のように同じイベントが大量に発生した場合も視認性が悪くなることが予想される.

また,一定のパターンの出現が期待されたが,目立ったパターンは発見できなかった.この原因としては期間が 1 日と短いため,1 日単位で発生するパターンが表現されていないことが原因と考えられる.この問題に対しては期間を延ばす方法も考えられるが,長くなりすぎると視認性が悪くなるため,適切な区間については検討が必要である.

本研究で行った可視化手法のイベント ID の頻度逆数では,イベントログが大量に記録されるブルートフォース攻撃・辞書攻撃・マルウェア感染によるプロセス生成などが可視化できないが,特殊なログを残す攻撃を可視化させることが可能だと考えられる.

だが,全ての攻撃が特殊なログを残すとは限らないため,イベント ID をそのまま使用したグラフの矩形波のパターンを分析することで特殊なログや通常ログに紛れ込んだログの分析がと考えられる.そのため,本研究ではそのままのイベント ID の値を使用することが効果的であるといえる.

7. 結論

本論文では,イベント出現の特徴を矩形波で可視化する手法について提案した.本システムでは矩形波の高さとしてイベント ID の値そのものを使用する場合と,イベントの出現頻度の逆数の場合について検討した.

提案した手法を試作システムとして実現し,pass the hash による攻撃データを入力した結果,出現頻度の逆数では,視認性が悪くなることが確認され,イベント ID そのままの値

の方がわかりやすい結果となった.今後の検討として,イベントID の値以外の高さについても検討する必要がある.

参考文献

[1] “SKYSEA”. https://www.skyseaclientview.net/,(参照 2025-08-22).

[2]“Autopsy - Digital Forensics”. https://www.autopsy.com/, (参照 2025-08-22).

[3]磯野怜, 中野心太, 関谷信吾, 折田彰, 岸本頼紀, 早稲田篤志, 花田真樹. 機械学習を用いた異常ログ可視化のための誤検知された正常ログ対策の検討. コンピュータセキュリティシンポジウム 2024 論文集. p. 1512-1526.