ログ調査のためのネットワーク図を用いたイベント出現関係可視化の提案

黒石　花恋[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：デジタルフォレンジックにおけるログ調査では，異常箇所の発見が難しい問題がある．攻撃痕跡のような異常ログは通常のイベントとは異なるイベントの出現順になる場合がある．そこで，イベントの出現順についてノードをイベント，アローの重みを２つのイベントペアの出現頻度とした可視化を提案する．
この場合，出現頻度が低い関係のペアが異常箇所と考えることができるため頻度の低いアローを強調することで，異常なログペアを発見しやすくなると考えられる．本論文では，イベントの出現関係に着目したネットワーク図による可視化について提案し，実際の例を適用した場合の効果について報告する．

キーワード：セキュリティ，フォレンジック，ログ解析

A Proposal of Visualizing Event Sequence Using Network Diagrams for Log Analysis

Karen Kuroishi[1]　Shinta Nakano[2]　Shingo Sekiya[2]　Akira Orita[3]
Yorinori Kishimoto[4]　Atsushi Waseda[4]　Masaki Hanada[4]

Abstract: When investigating logs in digital forensics, it is difficult to detect abnormal logs. An abnormal log such as an attack trace may have an order of occurrence of events that differs from that of normal events. Therefore, we propose a visualization of the event occurrence order, where nodes represent events and the weight of arrows represents the frequency of occurrence of two event pairs.
In this case, pairs with low frequency of occurrence can be considered as abnormal locations, so highlighting the arrows with low frequency can be thought of as making it easier to find abnormal log pairs. In this paper, we propose a visualization method using a network diagram that focuses on the occurrence relationships of events, and report on its effectiveness when applied to an actual example.

Keywords: Security, Forensic, Log analysis

1. 序論

デジタルフォレンジックによるサイバー攻撃の被害調査では，攻撃の痕跡を収集分析し，攻撃の日時や手法について検討する．この際，ログデータから攻撃の痕跡を発見するには，長大なデータの調査になるため時間と労力を要する．これに対して，Autopsy のようなフォレンジック支援システムが提案されている[1]．しかし，これらのシステムでは既知の攻撃痕跡に対応する異常箇所の分析はできるが，未知の攻撃に対する攻撃痕跡の分析については不明な点も多い．特に早期対応の必要性や顧客要求による調査期間の短縮化により初動調査のファストフォレンジックに対応できる支援が求められている．

未知の攻撃に対しても検知が可能な攻撃痕跡可視化手法として，Windows を対象としてイベントの発生順序の頻度を可視化する手法について提案する．標的型攻撃の対象となる業務システムでは，定常業務のように同じ作業が繰り返される場合も多い．また，システムが残す痕跡も時刻に応じて一定のパターンになると考えられる．すなわち，一定のパターン外のイベントは攻撃痕跡の可能性のある異常ログと考えられる．イベントの出現について，その出現順を考慮し，一定の出現順でないイベントの組みは異常ログと考えられる．

そこで，イベントの出現においてその組み合わせに着目する．正常ログを一定のパターンで出現するイベントと考えれば，異常ログは一定パターン外のイベントの組みと考えられる．すなわち，イベントの出現について出現頻度が低いイベントペアを可視化できれば，異常ログ判別の参考

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.
* g25004kk@edu.tuis.ac.jp

になると考えられる．

本論文では，イベントの低頻度出現ペアをネットワーク図で可視化する手法について提案し，実際の例に適用した結果について論じる．

2. 考え方

2.1 異常イベントの考え方

本研究では，イベントの出現順に着目する．OS の動作が原因で出現するイベントなどでは，一定の順序で出現するイベントが多く存在する．例えば，イベント ID4768（Windows の Kerberos 認証チケットの要求）とイベント ID4769（Windows の Kerberos サービスチケットの要求）は通常セットで出現するが，Mimikatz などによる Golden Ticket 攻撃ではイベント ID4769 のみが単独で出現する．このように，攻撃の手法によっては通常のペアとして出現するイベント ID が片方だけ出現する．これを検知する方法としてイベント ID の出現順に着目し，連続する出現頻度の低いペアを検出すれば良いと考える．

2.2 出現頻度の考え方

イベントペアの出現頻度について考える．イベントペアは連続する場合と一定期間の範囲内で出現する場合が考えられる．例えば，イベント ID4768（Windows の Kerberos 認証チケットの要求）とイベント ID4769（Windows の Kerberos サービスチケットの要求）は最大１０時間程度の間隔が発生するが通常のログではペアとして出現する．この対応として一定時間における出現ペアを調査する方法も考えられるが，各イベントペアで出現間隔が異なり，この仕様について明示されていないため正確な対応が難しい．また隣接のみの場合，間に別のイベントが発生する可能性もあり隣接のみでは低頻度のペア検出が難しい．

そこで，出現順として隣接とさらに１つ先の対応を対象として検出する．期間での判別では，アルゴリズムが複雑化するため，ファストフォレンジックで求められるマシンスペックの制約や処理時間の制約に対応できない．そこで，単純に出現順に幅を持たせる．隣接に加えて間に１つ挟んだペアも対象とすることで効果的にペアを確認できると考えられる．

この手法について効果の確認が必要と考え，隣接のみの場合と，１つ挟んだペアまでを対象とする両方の効果について調査する必要がある．

2.3 可視化の考え方

低頻度イベントペアの可視化について検討する．この可視化手法としては，出現頻度の低い順に列挙する方法が考えられる．しかし，本目的のログ解析ではイベント ID をキーとしてその隣接を確認する．このため，イベント ID に対して関連するイベントを調査する可視化が望ましい．

そこで，ネットワーク図による可視化を行う．ネットワーク図ではイベントをノード，出現ペアをアローとして表現でき，アローの出現頻度を線の色として可視化できる．この際，ネットワーク図のレイアウトについて検討が必要と考える．ネットワーク図のレイアウトによっては視認性が悪くなることが考えられる．そこで，Python の networkx におけるネットワーク図のレイアウト設定に着目する．これらのネットワーク図の表現方法について，本目的に適した設定が確認できれば，適切な可視化方法の検討ができると考えられる．

3. システム概要

本システムは Windows ログのイベントの低頻度出現ペアをネットワーク図で可視化するシステムである．本システムの構成を図 1 に示す．

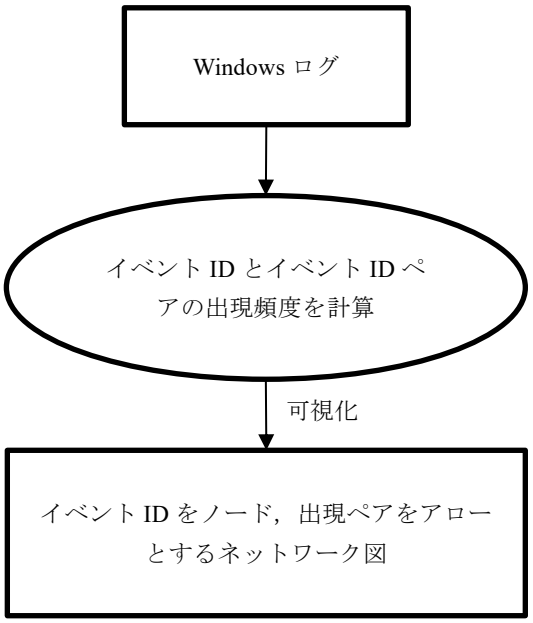

図 1 システム構成

また，本システムの開発環境は以下の通りである．

開発環境：Google Colaboratory

開発言語：Python 3.12.11

ライブラリ：pandas 2.2.2，networkx 3.5，matplotlib 3.10.0

4. 適用データ

本システムに適用した windows ログの概要を表 1 に示す．このログは Pass-the-Ticket 攻撃を受けたマシンのログである．

表 1 実験に用いた windows ログの概要

ログのタイプ	ログ数	ログ記録期間
Application	15967	170日間
セキュリティ	22799	15日間
システム	46123	28日間

5. 適用例

本システムの適用例 3 種を表 2 に示す.

表 2 システム適用例

適用例	可視化範囲	アローの色	ログタイプ
1	全ての出現ペア	珍しい出現ペアを赤く表示	3種類
2	出現頻度下位30位の出現ペア	全て灰色	セキュリティのみ
3	出現頻度下位30位の出現ペア	全て灰色	セキュリティのみ

適用例 3 種に共通して，ノードはイベント ID を，アローは出現ペアを表し，出現が珍しいイベント ID のノードは大きく表示している．適用例 1 においては，すべてのイベントペアを可視化範囲とし，出現が珍しいペアは赤く，そうでないペアは灰色で表示することで各ペアの出現頻度の差を表している．適用例 2，3 においては，可視化範囲を限定しており，アローを色分けする必要性がないため全て灰色となっている．また，適用例 1，2 では隣接するイベントペアのみをネットワーク図に用いたが，適用例 3 では隣接ペアに加えて間に 1 つ挟んだイベントペアもネットワーク図に用いた．適用ログデータのタイプについては，適用例 1 は Application，セキュリティ，システムの 3 種類を，適用例 2，3 はセキュリティのみを対象とした．

6. 結果

適用例 1 のネットワーク図を図 2，図 3，図 4 に示す.

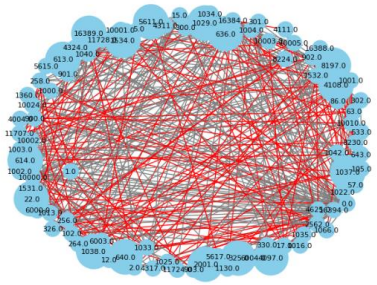

図 2 適用例 1 のネットワーク図（Application）

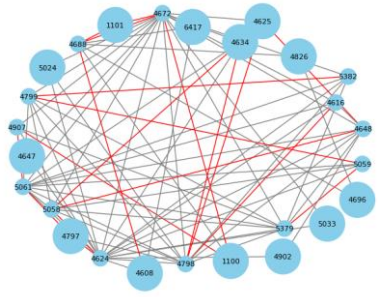

図 3 適用例 1 のネットワーク図（セキュリティ）

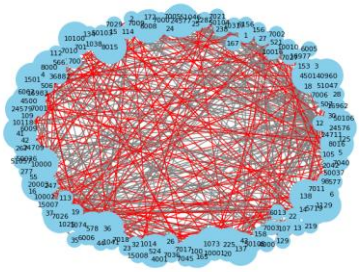

図 4 適用例 1 のネットワーク図（システム）

図 2，図 4 より，Application ログとシステムログにおいてはイベント ID とイベントペアの種類が多く，視認性に難があることが分かる.

適用例 2 のネットワーク図を図 5 に示す.

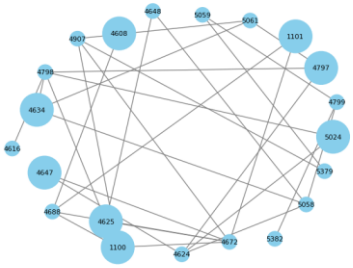

図 5 適用例 2 のネットワーク図

図 5 より，出現頻度下位 30 位のイベントペアを示す 30 個のエッジと，それを構成する 21 種類のイベント ID を示す 21 個のノードが表示されていることが分かる.

適用例 3 のネットワーク図を図 6 に示す.

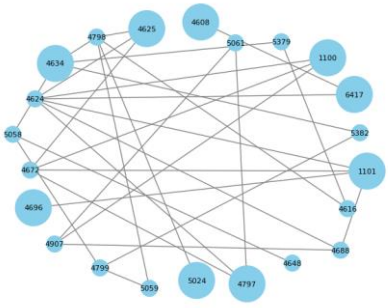

図 6 適用例 3 のネットワーク図

図 6 より，出現頻度下位 30 位のイベントペアを示す 30 個のエッジと，それを構成する 22 種類のイベント ID を示す 22 個のノードが表示されていることが分かる.

7. 考察

適用例 1 に関して図 2，図 4 より，すべての出現ペアを表示し珍しい出現ペアのみ色付けする可視化手法は，

Application やシステムなどの出現ペアのパターンが多いログデータには適さないことが分かった．

適用例 2 に関して，図 5 で可視化した出現ペア 30 種が，異常ログが残っている可能性の高い，攻撃開始時刻から攻撃終了時刻の約 20 分後までの区間に出現しているかを調査したところ，いずれも出現を確認できなかった．したがって，この方法では攻撃による異常なイベントペアの出現を可視化できないことが分かった．

表 3 調査区間における図 5 の出現ペア 30 種の出現

イベントidペア	出現
1100-4672	×
1100-4907	×
1101-4672	×（攻撃時刻の数分前）
1101-4688	×（攻撃時刻の数分前）
4608-4688	×（攻撃時刻の数分前）
4616-4798	×
4625-4798	×
4624-4797	×
4624-5058	×
4625-4648	×（攻撃時刻の数分前）
4634-5058	×
4797-5061	×
4648-5058	×
4672-4688	×
4634-4798	×
4799-5059	×（攻撃時刻の数分前）
5059-5379	×
4907-5061	×
4799-5382	×（攻撃時刻の数分前）
4625-4672	×（攻撃時刻の数分前）
4647-4672	×
4797-4798	×
4634-5061	×（攻撃時刻の5時間後）
4624-5024	×（攻撃時刻の数分前）
4624-4647	×
1100-4688	×
4799-5058	×
4907-5379	×
4798-5024	×
4672-4907	×

この結果を踏まえ適用例 3 では，隣接するペアだけでなく，間に 1 つ挟んだペアも含めたネットワーク図を作成し，出現ペアではなくイベント ID が先ほどの調査区間に出現しているかを確認した．結果，ネットワーク図の 22 種類のイベント ID のうち 7 種類の出現を確認できた．

表 4 調査区間における図 6 のイベント ID22 種の出現

イベントID	出現
1100	×
4624	○
4672	○
1101	×
4688	×
4696	×
4616	×
5379	○
4625	×
4798	○
4648	×
5058	×
4634	×
5382	○
4907	×
4797	×
5024	×
4799	○
5059	×
5061	○
4608	×
6417	×

ネットワーク図のアローではなくノードに着目することで，攻撃の痕跡の可能性のあるイベント ID を検出できることが分かった．

8. 結論

本論文では攻撃痕跡の可能性のある異常ログ判別方法として，イベントの低頻度出現ペアをネットワーク図で可視化する手法を提案し，実際の例に適用した結果について論じた．

本例においては，低頻度の出現ペアをアローの色によって区別する手法では視認性に難があるため，低頻度な出現ペアに限定したネットワーク図が適していること，出現頻度下位 30 位の出現ペアのネットワーク図から，攻撃期間に出現しているイベント ID を検出できることが分かった．

参考文献

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

[2] IIJ. “IIJ Technical WEEK2017 Mimikatz 実行痕跡の発見手法”. https://www.iij.ad.jp/dev/tech/techweek/pdf/171108_02.pdf, (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.