金融産業を標的にしたサイバー犯罪抑止のための SNS コミュニケーション分析手法の研究

理学専攻 情報科学コース 大原望乃 (担当教員: 小口正人)

1 はじめに

近年，SNS が犯罪の手段として悪用されるケースが増加しており，その一例として，フィッシング攻撃で窃取されたクレジットカード情報が SNS 上で取引されている問題が挙げられる．我々は，このようなサイバー犯罪の抑止を目的に，SNS 上の犯罪コミュニティのモニタリング [1] やデータ収集を進めてきた．公開グループ内での犯罪者による会話履歴を解析したところ，彼らは SNS を介して「知り合い」や「集団」といった関係性を構築している可能性が示唆された．本研究では，犯罪者間のつながりや中核的なグループを特定することを目的として，交グラフを活用した新たな犯罪者ネットワーク分析手法を提案する．さらに，実際のデータに提案法を適用し，結果を分析する．

2 提案

2.1 先行研究

倉持ら [2] は，様々な複雑ネットワークに対して交グラフとネットワーク上に存在する意味的な情報の解析を利用したグループ発見手法を提案している．この提案手法は，入力されたグラフ $\boldsymbol{G} = (\boldsymbol{V}, \boldsymbol{E})$（$\boldsymbol{V}$ はノードの集合，$\boldsymbol{E}$ はエッジの集合を示す）に対し，1. 密な部分グラフの列挙，2. 交グラフへの変換，3. エッジの重みの算出，4. クラスタリングの 4 つのステップからなる処理フローを行うことでグループを抽出する．

2.2 提案法

提案法は，図 1 に示すように 5 つの処理で構成する．なお，この手法を適用する SNS としては，サイバー犯罪の事例が多く見られる Telegram を対象としている．Step 1 では，犯罪者グループのデータベースから，グループごとに所属するユーザの一覧をダウンロードし，グラフ変換に必要な形になるよう整形する．Step 2 では，整形したデータから，複雑ネットワークのグラフを生成する．Step 3 では，設定した定義に従い重みを計算し，エッジに重みを付ける．Step 4 では，重み付けを完了したグラフを，交グラフに変換する．Step 5 では，交グラフをクラスタリング分析し，クラスタごとにノードを彩色する．さらに，彩色を引き継いで元のグラフに戻したとき，複数のクラスタに属する（複数の色が割り当てられる）ノードを中心と予想されるユーザや集団として抽出する．

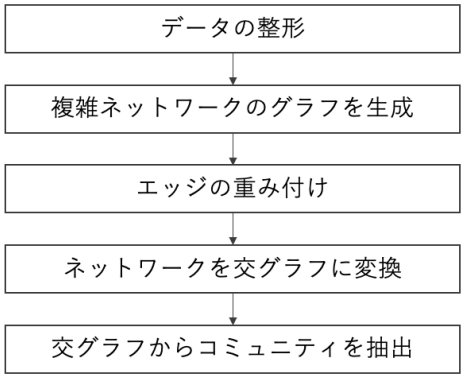

図 1: 提案法の処理フロー

3 実験

提案法を実際の犯罪コミュニティのデータに適用する実験を行った．

3.1 データセット

過去のモニタリングの研究で収集した犯罪に関与するグループをまとめたデータベース（2023 年 8 月時点のもの）内の 50 人以上のユーザを有するグループの中から，100 個のグループを選出し，そのいずれかに所属するユーザの情報を収集した． 結果，収集したデータの内訳は，ユーザ数が 112481，単一のグループだけに所属するユーザ数が 90856，複数のグループに所属するユーザ数が 21625 であった．今回は 2 つ以上のグループに所属するユーザのみ実験対象とし，この 21625 人からなるメンバーリストをデータセットとして実験に適用する．

3.2 実験内容

提案法の処理フローを順に実施する．Step 1〜3 の終了後，重要度の低いデータを減らすためノードとエッジの削減処理を行った．エッジの重みに閾値 n を設け，重みが閾値を下回るエッジと，接続されているエッジが 0 本になったノードを削除する．先行研究 [3] の結果より，今回は $n = 11$ のときのデータを採用した．Step 4〜5 では，グラフ分割ライブラリ METIS を利用し，クラスタ数 $k = 4$ でクラスタリングを実施した．ノードを赤，青，緑，黄色の 4 色に彩色し，元のグラフに戻した際のクラスタ間の重複は紫で彩色した．この 5 色

のノードの内容を分析し，比較と考察を行う．

4　結果と考察

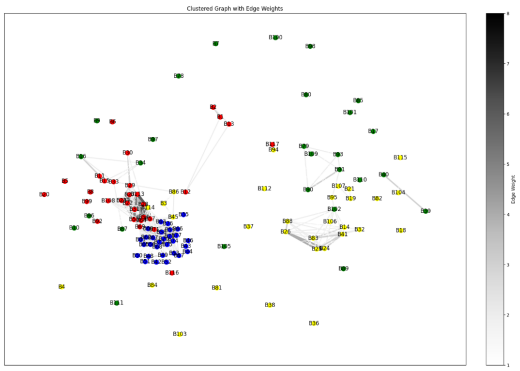

図 2: 彩色した交グラフ

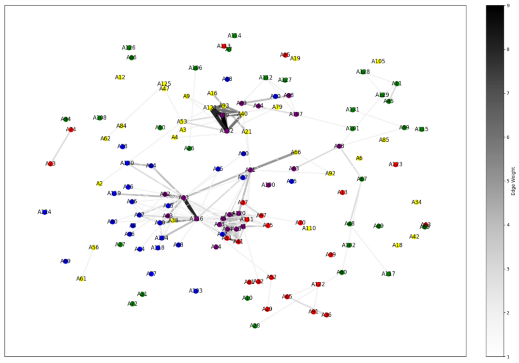

図 3: 元に戻したグラフ

図 2 と図 3 は，それぞれ，変換した交グラフを彩色したグラフ，それを変換前の元に戻したグラフである．まず，ノードの個数は紫が 22 個，赤が 23 個，青が 27 個，緑が 31 個，黄色が 29 個であった．ノードの中身は，A1: { グループ A, B, C}，A2: { グループ B, D, E, F}，… のように，グループの集合体である．そこで，まずノードの中身から各グループが何回現れたかをカウントした．現れたグループの総数は，全ての色を合わせると 64 個，色別に見ると紫が 55 個，赤が 50 個，青が 46 個，緑が 49 個，黄色が 54 個となり，紫が一番多いという結果になった．これらの結果より，提案法によって抽出された紫のノードは，ノード数は一番少ないが含まれるグループの種類は一番多く，紫のノードに絞って調査を行うことで調査コストを減らすことが期待できる．

また，各色内で各グループの登場回数がその色の中で占める割合を算出し結果をまとめたものが図 4 である．横軸はグループ，縦軸は割合で，グループ名は G1, G2,... とラベリングされ，5 色の平均割合でソートされている．例えば，最も平均割合が高い G1 は 70%であり，各色では紫が 77.3%，赤が 60.9%，青が 66.7%，緑

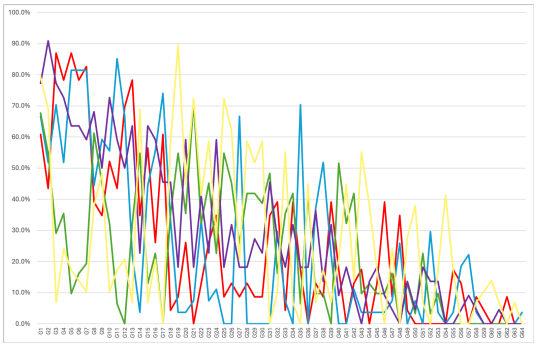

図 4: 各色における各グループの占める割合

が 67.7%，黄色が 79.3%である．さらに詳しく分析すると，合計 64 グループのうち，現在もアクティブなものは 19 個で，特に平均割合が高いグループの多くは既に削除されていた．また，これらのグループは人数が多く，頻繁に名前を変更している特徴があった．これは犯罪者コミュニティ間の情報流通を目的としたグループで，監視を避けるため定期的に削除されていると考えられる．さらに，削除されたグループは名前を少しだけ変更して新たなグループとして再出現することが多く，この特徴は新しいグループを発見する手法として応用の余地がある．

5　おわりに

SNS を利用したサイバー犯罪抑止を目的に，交グラフを用いた新たなネットワーク分析手法を提案した．提案法を実際の犯罪コミュニティのデータに適用したところ，抽出されたノードに絞って調査を行うことで調査コストを減らすことが期待できることがわかった．また，今後削除されたグループから新たなグループを辿る応用も考えられる．

参考文献

[1] 趙 智賢, 長田 繁幸, SNS を経由するクレジットカード不正利用のモデル化と抑止方法の検討, 研究報告セキュリティ心理学とトラスト（SPT）, 2022-SPT-48, No.25, pp.1-7, 2022.

[2] 倉持俊也，岡田直樹，谷川恭平，土方嘉徳，西田正吾，複雑ネットワークにおける交グラフと意味的解析を用いたグループ発見手法, 日本知能情報ファジィ学会誌，情報と知能，Vol.25，No.1，pp.540-555, 2023.

[3] 大原望乃，伊藤純菜，趙智賢，長田繁幸，中川直樹，小口正人，交グラフを利用した SNS における犯罪グループ探索アルゴリズムの提案，DICOMO2024，2024 年 7 月