4ZD-08

Telegramにおけるグループ名と投稿メッセージの分析によるグループ発見手法の検討

伊藤　純菜†　趙　智賢††　長田　繁幸††　中川　直樹††　小口　正人†

† お茶の水女子大学
†† 株式会社 日本総合研究所

1 はじめに

近年，サイバー空間上での犯罪が増加している．例えば，クレジットカード（以下，単にカードと呼ぶ.）の不正利用被害は年々増加しており，中でも番号盗用による被害は最大を占める．

番号盗用の主な手口であるフィッシング攻撃に対しては様々な対策が検討されてきた．趙ら [1] は，フィッシング攻撃を含む番号盗用全体の流れのモデル化をしている．この犯罪モデルでは，窃取されたカード情報は SNS 上で売買されており，その際カード情報の売り手は買い手からの信用度を上げるために，カード情報の一部をサンプルとして投稿する傾向にあることを明らかにしている．また，趙らは，この点に着目し番号盗用の抑止方法として投稿メッセージのモニタリングを提案し，その有効性を確認している．しかし，このモニタリングツールには改良の余地がある．例えば，モニタリングの対象となるグループをより効率的に発見できるようになれば，モニタリング自体もより効率的に行うことができ，結果として犯罪抑止に繋がる．そこで，本稿ではグループ名と投稿メッセージを分析することによるグループ発見手法を提案する．

2 先行研究

2.1 Telegram

趙らの研究では，カード情報の売買が行われている SNS として Telegram が観察対象に選択されている．Telegram はテキスト，写真，ビデオなどのメッセージの送信や，音声電話，ビデオ電話などができるメッセンジャーアプリである．また Telegram は，高度な暗号化機能を持ち，セキュリティ性能が高い反面，その秘匿性の高さから犯罪に利用されやすいという一面もある．加えて Telegram には，複数人でチャットを行うことができる機能が存在し，これを使用したカード情報の売買事例が観察されている．

2.2 モニタリングツール

趙らは，経験的に得た検索キーワードを用いて，Telegram の API を使用して，カード情報の売買を行なっているグループを特定するモニタリングツールを実装している．また，特定したグループの投稿メッセージをダウンロードする．ここで，グループとは，Telegram のチャット機能を使用してやりとりする集団のこととする．次に，投稿メッセージから得た画像ファイルにカード情報が含まれるかどうかを判別し，含まれていた場合は関係するカード会社へ連絡を行う．

2.3 投稿メッセージによるグループ発見

Kloo ら [2] は，2022 年のロシア・ウクライナ情勢の悪化の中で，Telegram 上で行われた情報活動を分析している．分析にあたっては，Kloo らは，Telegram でグループ検索する前に，X（旧 Twitter）に投稿されたメッセージの中で，Telegram に関係する URL を含むものを検索する．この検索結果を起点に，Telegram でスノーボールサンプリングを行う．ここで，スノーボールサンプリングとは，ある既知の要素から始め，その要素と直接繋がっている新たな要素を収集する方法のことであり，このグループ探索においては，既知のグループから言及のあったグループを新規のグループとして収集している．このようにして，既知のグループから未知のグループを発見する．

3 提案

3.1 方針

前節で述べた投稿メッセージを監視する方法の有効性を向上させるには，監視対象となるカード情報の売買に関係のあるグループを効率的に発見する手法が必要である．そこで，Kloo らの投稿メッセージを分析することでグループを発見する手法とグループ名を分析することでグループを発見する手法を組み合わせる．

3.2 処理フロー

図 1 に示すように，提案手法は，投稿メッセージの分析によるグループ探索とグループ名の分析によるグループ探索との 2 つを組み合わせた処理フローで構成する．

図中のステップ①では，初期グループの取得を行う．初期グループは，Kloo らの手法と同様に，X のキーワード検索機能を使用して，Telegram のグループの URL を含むポストから取得する．並行して，趙らが行なっている，Telegram のキーワード検索機能を使用して，既知の単語を指定した検索結果か

：Group Discovery Methods by Analyzing Group Names and Posted Messages in Telegram
：†Junna Ito　††Zhixian Zhao　††Shigeyuki Osada
：††Naoki Nakagawa　†Masato Oguchi
：†Ochanomizu University
：††The Japan Research Institute, Limited

らも取得する．

ステップ②では，投稿メッセージの分析による探索を行う．初めに，既知のグループの投稿メッセージを取得する．続いて，取得した投稿メッセージから Telegram のグループの URL（例えば，https://t.me/GroupName）を抽出し，抽出した URL が示すグループの名前や所属人数などのグループ情報を取得する．

ステップ③では，グループ名の分析による探索を行う．まず，既知のグループ名に対して形態素解析を行う．次に，辞書を用いてストップワードを除去し，キーワードとなり得る単語とその出現回数を取得する．出現回数が予め定めた閾値を超えた単語について，グループ名に対する共起頻度を計算する．ここで，グループ名に対する共起頻度とは，グループ名の中で 2 つの単語が同時に出現する回数を計測したものとする．共起頻度が予め定めた閾値を超えた単語の組を検索キーワードとして，Telegram のキーワード検索機能に指定し，検索を行う．Telegram では単語間の空白の有無で検索結果が異なるため，同じ組み合わせでも空白の有無を考慮する．

ステップ④では，ステップ②の URL を使った検索結果と，③のキーワードを使った検索結果で得られた両方のグループを，番号盗用の疑いがある被疑グループとしてリスト化する．その後，有識者によって関係性の有無を目視で確認し，番号盗用に関係のあるグループをリストに追加する．

ステップ④終了後，得られたリストを用いて，ステップ②〜④を繰り返す．

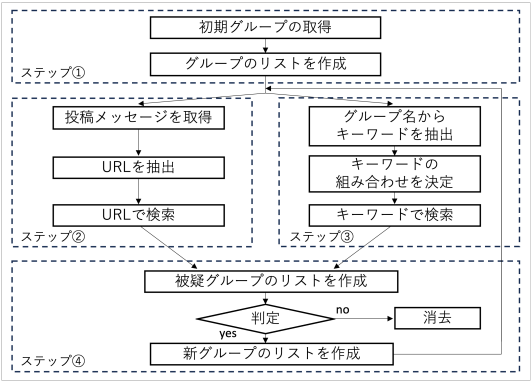

図 1　処理フローの概要

4　実 行 結 果

X のキーワード検索機能を使用して取得したグループ 6 個と Telegram のキーワード検索機能を使用して取得したグループ 89 個の計 95 個のグループに対して提案手法を実行した結果を示す．ただし，この 95 個のグループは有識者によって番号盗用に関係のあるグループだと予め判定されたものである．

まず，投稿メッセージの分析による探索法では，95 個のグループの投稿メッセージから 2830 個のグループを発見できた．そのうち番号盗用に関係のあるグループは 577 個であった．

次に，グループ名の分析による探索法では，キーワード検索の際に指定する単語の組み合わせを共起頻度によって決定することの有効性を確認するために，共起頻度の閾値を変え，図 2 の通り 4 種類の検索を行った．ただし，グループ名からキーワードを抽出する際，出現回数が 3 以上の単語 35 個をキーワードとし共起頻度を計測した．図 2 の横軸は指定する単語の組み合わせの条件であり，縦軸は発見グループ数である．また，発見グループを番号盗用に関係のあるグループと，番号盗用に関係のないグループの 2 つに分けた．発見グループ数に対する番号盗用に関係のあるグループ数の割合をみると，共起頻度 0 以上の場合，すなわち，共起頻度に関係なく全ての組み合わせで検索を行った場合は 58%であるのに対し，共起頻度 3 以上の場合は 81%であった．このことから，共起頻度の閾値を上げるにつれて，有識者対応の効率性を左右する精度が向上していると言える．

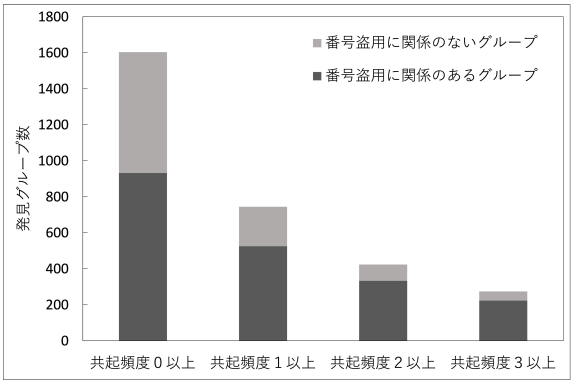

図 2　共起頻度ごとの検索結果

また，投稿メッセージの分析によって取得したグループ 577 個とグループ名の分析によって取得したグループ 932 個で共通しているグループ数を計測すると，57 個であった．共起頻度の閾値を変えた場合にも同様に共通しているグループ数は少なく，取得できるグループには違いがあることがわかる．したがって，2 種類の探索を並列して実行することで，より多くのグループを発見することができると期待できる．

5　お わ り に

Telegram のグループを効率的に発見する手法について，投稿メッセージの分析による手法とグループ名の分析による手法を組み合わせた手法を提案し，その有効性を確認した．今後の課題は，現在では取得したグループが番号盗用に関係のあるグループであるかを有識者に判定してもらっているため，自動で判定するプログラムを実装し，判定部分での効率化を図る必要がある．

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] Ian Kloo, kathleen M.Carley, “Social Cybersecurity Analysis of the Telegram Information Environment During the 2022 Invasion of Ukraine,” Social, Cultural, and Behavioral Modeling. SBP-BRiMS 2023. Lecture Notes in Computer Science, vol 14161. Springer, Cham, 2023.