SNS コミュニケーション分析手法を用いた 金融犯罪情報の早期検出に関する研究

大原望乃 (指導教員：小口 正人)

1 はじめに

近年，クレジットカード（以下，単にカードと呼ぶ.）の不正利用による被害は年々増大している．中でも番号の盗用による被害は多く発生しており，主な手口となるフィッシング攻撃について効果的な対策の検討がなされてきた．

趙ら [1] の研究では，番号盗用の全体の流れのモデル化を行い，窃取されたカード情報が SNS 上で売買されているということを明らかにした．また，このときカード情報の売り手が信頼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に着目し，番号盗用を抑止する手法として定期的なモニタリングを提案した．実験によりこの手法に一定の抑止効果があることが示唆されている．しかし，この提案手法にはセキュリティ面での問題が確認された．本研究ではこの問題点に対する提案と実装を目的とする．

2 先行研究

2.1 Telegram

カード情報の売買が行われている SNS として Telegram(テレグラム) が観察対象となった．Telegram はテキスト，写真など様々なタイプのメッセージの送信や，音声電話などを行うことができるメッセンジャーアプリである．

趙らの観察によると，Telegram はカード情報の売買をはじめとした犯罪に利用される事例が多く見られる SNS である．その理由に，まず暗号化方式が独特で管理しにくいことが考えられる．Telegram は 2 つのチャットモードを有しており，それぞれで異なった暗号化を採用している．次に，グループという独自の機能が存在することが挙げられる．グループは複数人でチャットルームを作る機能だが，このときグループ内で投稿されたチャットはそのグループに参加していなくても誰でも閲覧が可能である．すなわち，閲覧の痕跡が残らないため，犯罪に関与する人間を特定しにくい．カード情報の売買も，このグループ機能を利用して行われているケースが多く見られている．

2.2 モニタリングツールと問題点

先行研究では図 1 のようなシステムのモニタリングツールが用いられた．まず，ステップ 1 では，カード情報売買を行っているグループを検出するために，検索用のキーワードリストを作成する．次に，作成したリストを用いて API でグループの検索を行い，検出したグループの会話履歴をダウンロードする．ここで得られたテキストの内容より，さらにキーワードリストを更新する．

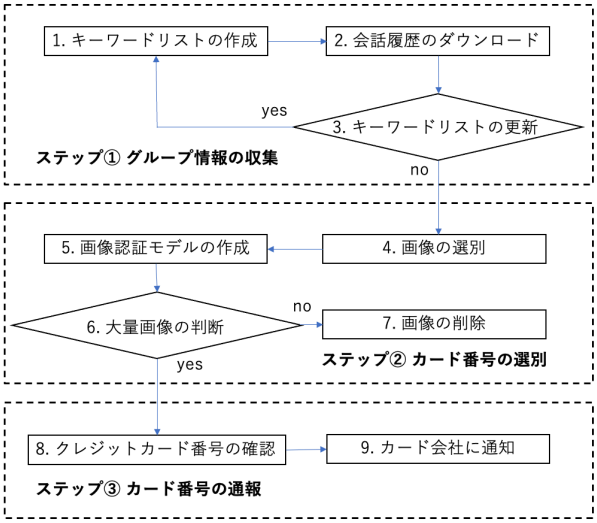

図 1: モニタリングツールの設計

ステップ 2 では，収集した画像ファイルにカード情報が含まれるか否かを選別する．カード情報が含まれる画像に現れる一定の特徴を機械学習によって判別するようなモデルを作成し，これを用いて収集した画像すべてを選別する．カード情報が含まれないと判断された画像は破棄され，含むと判断された画像は次のステップで処理する．

ステップ 3 では，得られた画像ファイルを目視で確認して，関係するカード会社へ連絡を行う．

このツールによるモニタリングは一定の成果を収めたが，実験に使用していた Telegram アカウントについて，登録していた電話番号の漏洩が起き，DOS 攻撃を受けた．すなわち，モニタリングを安全に継続するにあたって，監視者の電話番号を含む個人情報を秘匿できるような方法と，それを保証するための手段の検討が必要である．

3 提案

2 つの課題に対し，まず 1 つ目の秘匿化には Telethon という Telegram が提供する API によるユーザ設定の強制変更を提案する．漏洩が問題となった電話番号は公開範囲を 3 段階に変更可能で，全員に公開する Everybody，連絡先ユーザのみに公開する My Contacts，非公開にする Nobody のいずれかを選択する．我々は今回，この公開範囲のパラメータを API から変更できることを発見した．これにより公開範囲の変更をアプリ外から強制変更することが可能であり，個人情報の秘匿化が期待できる．

2 つ目の秘匿の保証に関しては，プライバシサンドボックスを用いたユーザのプライバシのモニタを提案する．Luo ら [2] によると，プライバシサンドボックスはユーザのプライバシプランを管理するものと定義されており，ユーザが他者から見られると想定している個人情報の範囲と実際の範囲のギャップを管理するシステムのことを指す．すなわち，我々が期待する「電話番号が非公開である」状態と実際の状態の違いを管理するシステムを作成し，そのモニタを行うことで，意図せぬ電話番号の公開状態を防ぐことが可能だと考える．

4 実験

4.1 実験概要

まず，新たに 3 つの Telegram アカウント A，B，C を用意し，それぞれ表 1 で示すような役割を与えた．これらの動作は毎時 5〜20 分ごとの決められた時刻に繰り返し行われる．

表 1: 実験環境におく各アカウントの役割

アカウント	実験におく役割
A	グループ A’ で定期的に発言
B	グループ A’ の会話履歴をダウンロード グループ検索を定期的に行う
C	アカウント B のユーザ情報を監視 グループ A’ の情報を監視

アカウント A は仮想の犯罪コミュニティ，B は犯罪コミュニティの監視者，C は監視者のプライバシの観察者の役割を担う．さらに，プライバシサンドボックスとして，取得したユーザデータを比較し結果をログファイルに記録した．このとき，データに特に違いがなければ “No change.”，違いがあれば異なる箇所のみ抽出しログに出力する．

さらに，個人情報が漏洩している状態を検知できるかテストする目的で，定期的に API により監視者の電話番号の公開範囲設定を Everybody，Nobody に変更する動作を行い，前後のログを観察した．

4.2 実験結果

まず，個人情報の漏洩が発生していない状態のログは図 2，図 3 のようになった．ログは，データに変更があった場合，冒頭にマイナス記号がある行が以前のデータ，プラス記号がある行が最新のデータを示す．

図 2 のアカウント B の観察については，B は会話履歴のダウンロードと検索のみ行っているため，ユーザ情報に変化なしの “No change.” が繰り返し記録されている．一方，図 3 のグループ A ’ については定期的に投稿を行っている状態であるため，おそらく投稿数のパラメータだと推測される “pts ” の数字が 4 ずつ増加していた．

続いて，個人情報の漏洩が発生した状態，すなわち

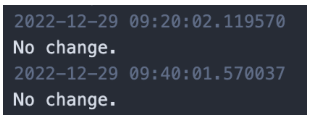

図 2: アカウント B ログ

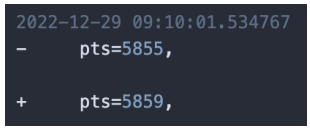

図 3: グループ A’ ログ

公開範囲が Everybody に変更される前後のログは図 4 のようになった．グループ A ’ については，図 3 と同じ結果となったため省略する．

このときログには “add_contact” のパラメータが False から True に，“phone ” のパラメータが None から登録していた電話番号に変化したことが記録された．電話番号の漏洩と，電話番号が公開されたことによる連絡先への追加許可を検知している．

最後に，再び公開範囲が Nobody に変更される前後のログが図 5 のようになった．ここでは各パラメータが図 4 と逆の変化を起こしており，再び電話番号が保護されたのが読み取れる．これは提案手法によって個人情報の秘匿化が成功しているといえる．

図 4: Everybody に変更

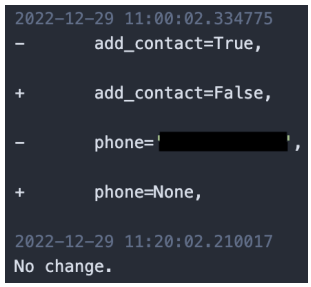

図 5: Nobody に変更

5 まとめと今後の展望

先行研究で発生したモニタリング時に監視者の個人情報が漏洩する可能性がある問題について，API による強制的な設定方法と，プライバシサンドボックスを用いたプライバシのモニタを提案した．実験結果から，提案手法によって個人情報の秘匿とその保証が可能になることを示した．

今後は，他の SNS への一般化や，犯罪コミュニティの危険度指数に合わせたモニタリングの改良を目指す．

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] Bo Luo, Dongwon Lee, On Protecting Private Information in Social Networks: A Proposal, 2009 IEEE 25th International Conference on Data Engineering, pp.1603-1606, 2009