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　～グループ発見手法の検討と取得データに基づく考察～

伊藤 純菜 [1]　三田 智之 [2]　趙 智賢 [3]
長田 繁幸 [4]　中川 直樹 [5]　小口 正人 [6]

近年，フィッシング攻撃によるクレジットカード情報の窃取及び不正利用が増加しており，窃取された情報は SNS 上で売買されることも多い．この問題に対処するため，抑止方法として犯罪グループをモニタリングする取り組みが行われている．従来の手法では，既知の犯罪グループの名前や投稿内容を分析し，モニタリングの対象となる新たな犯罪グループの発見に取り組んできた．しかし，その犯罪性の判定には人手による目視が必要であり，評価規模の拡大には限界があった．本研究では機械学習モデルを用いて犯罪グループの自動判定を行うことで，探索およびプロセスの効率化を実現する．また，提案手法を用いた再実行による検証を行う．

1　はじめに

近年のデジタル化によって，SNS（ソーシャル・ネットワーキング・サービス）の普及が進み，我々の生活と密接に結びつくようになった．SNS は情報収集や共有が容易になる一方で，その利便性が詐欺や犯罪に悪用されるケースも見られる．例えば，フィッシング攻撃によるクレジットカード（以下，単にカードと呼ぶ）情報の窃取やカード番号の不正利用被害は年々増加している [1]．フィッシング攻撃とは，金融機関や正規の Web サイトに似せた偽サイトを作り，偽装したメールなどで被害者を誘導し，ID・パスワードやカード番号などの個人情報を盗む手法である．フィッシング対策協議会 [2] によると，2023 年 1 月から 12 月までのフィッシング報告件数は 1,196,390 件で，2022 年と比較して約 1.2 倍となっており，年々右肩上がりで増加している．そこでこれらのサイバー犯罪への対策を講じるために，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．

趙らは，投稿メッセージの収集を行い，それらを分析し，行為別に犯罪者のグループ分けを行った．その結果として，カード情報の窃取と盗用のプロセスについてのモデルが得られた．この犯罪モデルによると，カードの不正利用は，カード情報の窃取から現金化まで大きく 3 つに分業化されており，それぞれの行為は別の人物あるいはグループによって行われている．また，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．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 [3].

筆者らはこれまで，効率的なモニタリングを実現するために，モニタリングの対象となる犯罪グループを効率的に特定する手法を研究してきた．この手法はある程度の有効性が確認されたものの，これによって取得されたグループが真に犯罪グループであるかは，会話履歴などを基に有識者による目視で行われており，評価実験の規模に制約があった．そこで，本稿では犯罪性の判定に先行研究の評価結果を基に機械学習モデルを導入し，探索効率の向上を図るとともに再実行による検証を行う．

本稿の構成は以下の通りである．第 2 章では，先行研究と観察対象に選択されている SNS である Telegram についての概要を紹介する．第 3 章では，先行研究の手法の問題点とそれに対して機械学習を使用した犯罪グループを自動判定する手法を適用することを提案する．第 4 章では，提案手法の有効性を確認するための実験の設計を述べる．第 5 章で実験結果とそれに対しての考察，第 6 章で倫理的考察を行い，第 7 章でまとめる．

2　先行研究

フィッシング攻撃については様々な分析が行われている．一般社団法人日本クレジット協会 [1] によると，クレジットカード不正利用被害額は年々増加しており，2023 年通年の不正利用被害額は 540.9 億円に達したと報告されている．これは統計を取り始めた 1997 年以降，過去最悪の額である．また，図 1 に示すように，クレジットカード不正利用被害額は「偽造カード被害額」「番号盗用被害額」「その他不正利用被害額」の 3 種類に分類される．その中で，番号盗用被害額は 504.7 億円であり，全体の約 93.3% を占めている．このことから，フィッシング攻撃などが原因となる番号盗用被害の割合は増大傾向にあると言える．

趙らは，カード情報の窃取と盗用のプロセスを図 2 のようにモデル化している．この犯罪モデルによると，カードの不正利用は，カード情報の窃取から現金化まで大きく 3 つの段階に分かれ，それぞれの行為は異なる人物またはグループによって行われる．このように，カード番号盗用による不正利用には複雑な犯罪エコシステムが存在している．一般的な商取引では，法律に基づく契約によって取引の確実性が保証されているが，SNS を介したカード番号盗用の取引では，違法性が高いため法的な保証がない．そのため，この犯罪エコシステムは弱い信頼関係の上に成り立っている．この弱い信頼関係を利用したカード番号盗用の抑止方法として，犯罪グループのモニタリングが提案されている．SNS での取引においては，売り手と買い手は互いに身分を隠しているため，信頼関係を築くのが難しい．そのため，売り手は買

[1] 非会員　お茶の水女子大学
g2020507@is.ocha.ac.jp
[2] 非会員　株式会社 日本総合研究所
sanda.tomoyuki@jri.co.jp
[3] 非会員　株式会社 日本総合研究所
zhao.zhixian@jri.co.jp
[4] 非会員　株式会社 日本総合研究所
osada.shigeyuki@jri.co.jp
[5] 非会員　株式会社 日本総合研究所
nakagawa.naoki@jri.co.jp
[6] 正会員　お茶の水女子大学
oguchi@is.ocha.ac.jp

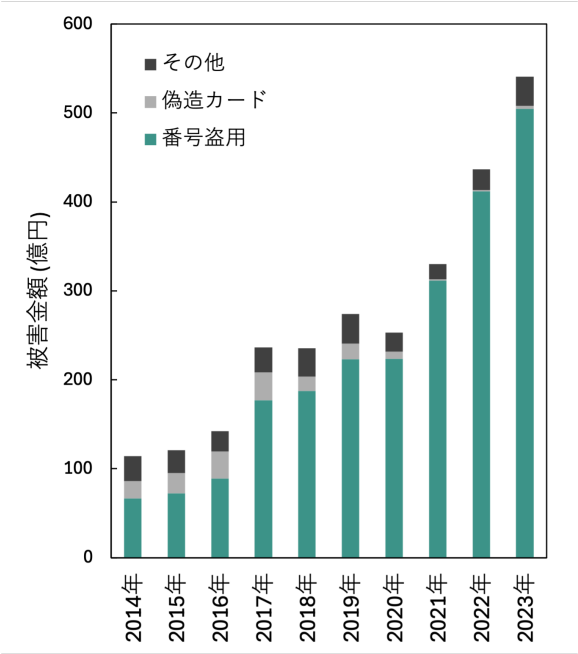

図 1　クレジットカード不正利用被害額の推移

い手の信用を得るためにカード情報の一部をサンプルとして公開する傾向にある．この情報をクレジットカード会社が入手できれば，カードの利用停止などの対応が可能になる．これにより，そのカードの番号盗用を防ぐだけでなく，買い手の売り手への信用度を低下させることができるため，買い手のカード情報入手行動を妨害する効果もある．このように，SNS を介した番号盗用の犯罪エコシステムを弱体化させることができ，結果的にカード番号盗用の抑止に繋がると言える．

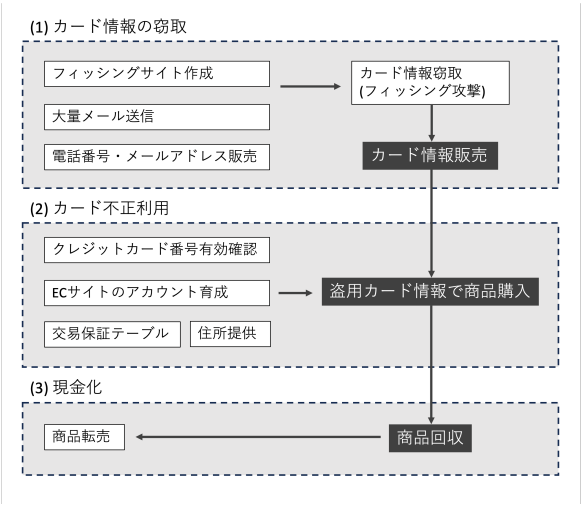

図 2　カード情報の窃取と不正利用の手口のモデル化

上述の抑止方法の有効性を確認するために，実際に犯罪グループのモニタリングを実施している．また，観察対象の SNS としては Telegram（テレグラム）[4] が選択されている．Telegram はテキスト，写真，ビデオの送信や音声電話，ビデオ通話ができるメッセンジャーアプリで，月間アクティブユーザーが 7 億人を超え，世界で最もダウンロードされているアプリの 1 つである [5]．Telegram の特徴は，高度な暗号化機能とメッセージの自動削除機能で，これにより投稿内容が外部に漏れにくく，運営会社にも残らないことが挙げられる．このため，セキュリティ性能が高い一方で，その秘匿性の高さから犯罪に利用されることもある．さらに，最大 20 万人が参加できるチャットルームを作成できる機能があり，この機能を利用したカード情報の売買事例が観察されている．

またモニタリングに使用したツールは図 3 のようなものである．このツールのプロセスは大きく 3 つのステップに分けられる．

1. ステップ 1 では，カード情報の売買を行なっているグループを特定するために情報を収集する．まず，経験的に得られた特徴的な単語を基に検索キーワードリストを作成し，Telegram で使用される API の一つである Telethon [6] を使ってグループを検索する．特定したグループの会話履歴をダウンロードし，そこからカード番号盗用に関連する単語を抽出して，検索キーワードリストを更新する．
2. ステップ 2 では，ダウンロードした会話履歴から得られた画像ファイルの中で，カード番号が含まれる画像を識別する．機械学習を用いて，カード番号を含む画像を判別するモデルを作成し，このモデルを使ってカード番号を含む画像を自動的に判別する．また，カード番号を含まない画像は削除する．
3. ステップ 3 では，カード番号が含まれていると判断された画像ファイルを目視で確認し，関連するカード会社に連絡を行う．

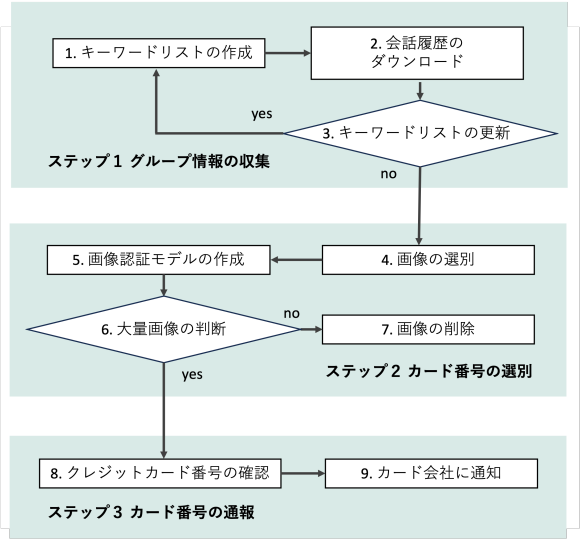

図 3　モニタリングツールの設計

図 4 に示すように，ある監視された Telegram のグループは元々 1 ヶ月間に 2171 件のカード番号が投稿されていたが，4 ヶ

月にわたって対策を継続したところカード番号の投稿がなくなった．他の 2 つのグループに対しても，数ヶ月でカード番号の投稿が 0 件になったことが確認されたことから，モニタリングには抑止方法として一定の効果があることが確認された．

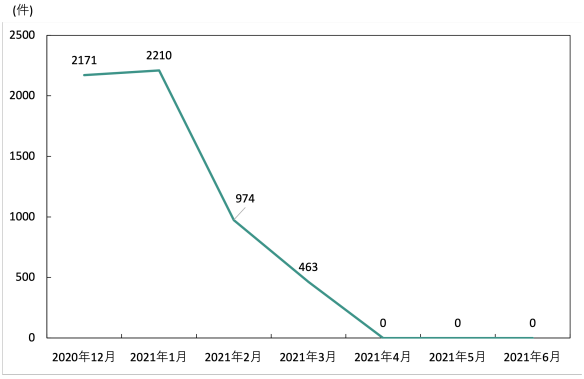

図 4　投稿されたカード番号の数の変化

3　提案

3.1　先行研究の探索手法とその課題

先行研究 [7, 8] では図 5 のようなグループ探索手法を提案している．探索手法は，会話履歴の分析とグループ名の分析を組み合わせた処理フローで構成され，これは大きく分けて 4 つのステップで行われる．

1. ステップ 1 では，初期グループの取得を行う．まず，X のキーワード検索機能を使用して，Telegram グループの URL を含むポストからグループを取得する．並行して，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らも取得する．取得したグループからグループのリストを作成する．このリストにはグループ名，グループ ID，所属人数，グループ作成日，グループの URL（例えば，https://t.me/（グループの ID））などのグループ情報が含まれていることとする．
2. ステップ 2 では，会話履歴の分析による探索を行う．はじめに，既知のグループの会話履歴を取得する．続いて，取得した会話履歴に含まれるテキスト情報から Telegram グループの URL を抽出し，抽出した URL が示すグループの名前や所属人数，作成日などのグループ情報を取得する．
3. ステップ 3 ではグループ名の分析を行う．まず，既知のグループ名に対して形態素解析を行い，辞書を用いてストップワードを除去した後に，キーワードとなり得る単語とその出現回数を取得する．続いて，出現回数があらかじ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．共起頻度があらかじめ定めた閾値を超える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．
4. ステップ 4 では，ステップ 2 の URL を使った検索結果と，ステップ 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，カード情報の売買に関与している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することで判定し，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，リストの更新を行いながら，ステップ 2 からステップ 4 までの流れを 1 周として繰り返す．

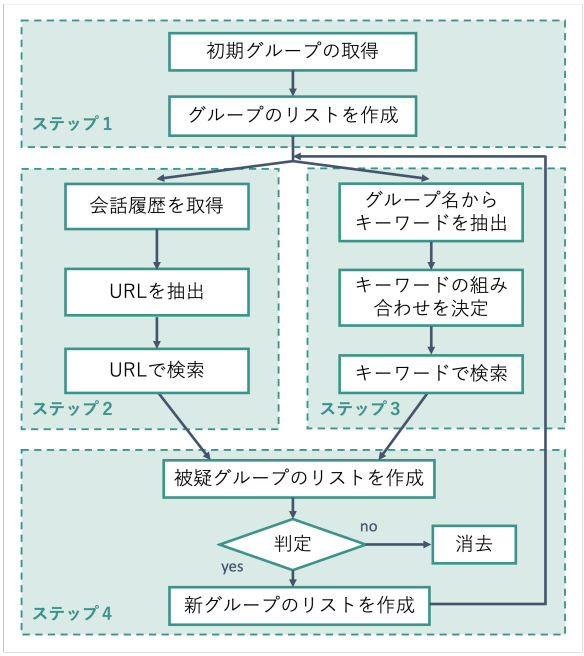

図 5　グループ探索手法の処理フロー．本研究では「判定」工程を機械学習で自動化する．

前述した探索手法は，一定の成果を収めたものの，いくつかの課題が残されている．特に，探索で取得されたグループが実際にカード情報の売買に関与する真の犯罪グループであるかどうかの判定には，有識者による主観的な判断が必要であった．この判定方法には大きく分けて 2 つの問題点がある．

第一の問題点は，判定に要する時間が非常に長くなることである．各グループについて確認作業を行う必要があり，結果としてグループ数が増えれば増えるほど判定作業全体が膨大な時間を要することとなる．このため，迅速に対応が求められる場面においては，手動による判定の遅延が問題となる．実際，取得したグループの中には，1 週間程で設定が非公開に変更されたグループも存在していた．また，人間による判定作業は，時間に追われる状況ではミスが生じるリスクも増大する．

第二の問題点は，判定基準が明確化されていない点である．先行研究においては，有識者がグループ名や説明文，ユーザーネーム，参加者数，会話履歴などの情報をもとに，経験則的な基準に従って判定を行っていた．しかし，主観的な判断に依存するこの手法では，異なる有識者が同じグループを判定した場合に，判定結果が一貫しない可能性もある．

以上のように，目視による判定方法には時間効率と基準の一貫

性という 2 つの課題が存在しており，これらの問題を解決するためには，自動化された客観的な手法の導入が必要であると考えられる．

3.2 判定モデルを用いた自動化手法の提案

本研究では，図 5 に示した先行研究の探索フローにおける「判定」工程を機械学習モデルで置き換えることにより，自動化・反復可能な探索手法を提案する．具体的には，先行研究で人手によって行われていた関連グループの判定を，後述する TF-IDF と LightGBM を組み合わせたモデルにより自動化する．

この置き換えにより，以下の利点が得られる：

- 大量のグループへの適用が可能
- 判定基準が明示的なモデルとして定義されるため再現性が高い
- 反復探索が現実的な労力で実施可能

この自動化により，本研究では実際に 3 周の反復探索を実施し，その有効性を検証した．

3.3 判定モデルの構築と選定

本節では，前節で提案した自動化手法に使用する判定モデルについて述べる．判定モデルの構築と比較は筆者らの先行発表 [9] で実施しており，本研究ではその結果を踏まえて最適なモデルを選定し，実際の探索に適用した．

3.3.1 モデルの構築と比較

Telegram から収集した 1498 グループに対して，有識者がラベル付けをしたデータセットを用いて, TF-IDF, Doc2Vec, Sentence-BERT の 3 種類のベクトル化手法と，SVM, LogisticRegression, LightGBM の 3 種類の分類手法を組み合わせた合計 9 種類のモデルを構築・評価した．評価指標として Accuracy, Recall, Precision, F1 スコアを用い，テストデータ 450 グループで性能を測定した．表 1 に各モデルの評価結果を示す．

表 1 判定モデルの性能比較

ベクトル化手法	分類手法	Accuracy	Recall	Precision	F1
TF-IDF	SVM	0.822	0.837	0.850	0.843
TF-IDF	Logistic Regression	0.831	0.841	0.861	0.850
TF-IDF	LightGBM	**0.868**	**0.872**	**0.896**	**0.884**
Doc2Vec	SVM	0.682	0.655	0.908	0.761
Doc2Vec	Logistic Regression	0.697	0.662	0.932	0.774
Doc2Vec	LightGBM	0.677	0.680	0.796	0.733
Sentence-BERT	SVM	0.797	0.862	0.809	0.835
Sentence-BERT	Logistic Regression	0.797	0.862	0.809	0.835
Sentence-BERT	LightGBM	0.789	0.813	0.830	0.822

3.3.2 考察とモデル選定

TF-IDF をベクトル化手法，LightGBM を分類手法とする組み合わせが最も高い精度を得ることができ，正解率，再現率，適合率，F1 スコアのどの指標に対しても 85% 以上の精度が得られた．この理由として，第一に，クレジットカード情報の売買を関与するグループでは特定のキーワードの出現が判定の重要な手がかりとなり，TF-IDF がこれらの単語の出現パターンを効果的に捉えられることが挙げられる．Doc2Vec や Sentence-BERT は文脈理解には優れるが，本タスクでは単純な単語の有無がより重要であったと考えられる．第二に，LightGBM は不均衡データに対する頑健性が高く，関連グループと非関連グループで若干の偏りがあるデータセットでも安定した性能を発揮する．

以上の結果から，本研究では TF-IDF と LightGBM を最終的な判定モデルとして採用し，3.2 節で提案した自動化探索手法に組み込んだ．

4 実験

4.1 実験内容

本研究では，提案手法の有効性を検証するため，従来のグループ探索手法に機械学習モデルを統合し，2 周目以降も探索を実施してその結果を分析する．特に，1 周のみの探索で確認された特徴は 2 周目以降でも見られるのかを確認する．以下に使用データと実装環境，探索条件を説明する．

4.2 使用データと実装

初期グループとして，X のキーワード検索で取得した 6 個のグループと Telegram のキーワード検索機能で取得した 101 個のグループの計 107 個のグループを使用した．実装には Python を利用し，検索には Python の Telegram の API である Telethon を使用した．Telegram は公開グループにおいて，API を通じて参加メンバーや投稿メッセージを取得できる仕様となっており，本研究ではこの機能を活用してデータを収集した．形態素解析には，グループ名の多くは中国語であるため，中国語の形態素解析エンジンである jieba を使用した．探索フローでは，グループ名から単語を抽出するときの出現回数の閾値は，出現回数が多い方から 30 番目の単語の出現回数とした．また，1 周目の探索の時に共起頻度の閾値が 0 の場合と 1 の場合で精度に大きく差が出ていたため共起頻度の閾値は常に 1 とした．さらに，会話履歴の分析による探索の時，取得する会話履歴の期間の上限は 3 ヶ月とし，件数の上限は 10000 件とした．すなわち，3 ヶ月分の会話履歴が 10000 件を超えない場合は 3 ヶ月分全てを取得し，10000 件を超える場合は最新の方から 10000 件取得することとする．

5 結果と考察

提案手法を用いて探索を 3 周実施した結果を図 6 に示す．横軸は何周目の探索であるかを示し，縦軸は発見グループ数である．ただし，ここでの発見グループ数とは，取得したグループのうち，番号盗用に関係があると判定されたグループの総数を指し，前の周で取得したグループとの重複は考慮していないものとする．まず，初期グループとして 107 個のグループを用いて，1 周目の探索を実施した．その結果，グループ名の分析による探索で 415 個，会話履歴の分析による探索で 18 個，合計 433 個の犯罪グループを取得した．次に，1 周目で新たに取得したグループを基に 2 周目の探索を実施したところ，グループ名の分析による探索で 644 個，会話履歴の分析による探索で 482 個，合計 1123 個の犯罪グループを取得した．さらに，2 周目で取得したグループを基に 3 周目の探索を実施したところ，グループ名の分析による探索で 423 個，会話履歴の分析による探索で 1142 個，合計 1565 個の犯罪グループを取得できた．なお，各周のグループ名の分析による探索と会話履歴の分析による探索で取得したグループの合

計数は，これら 2 つの探索間の重複を取り除いたものである．

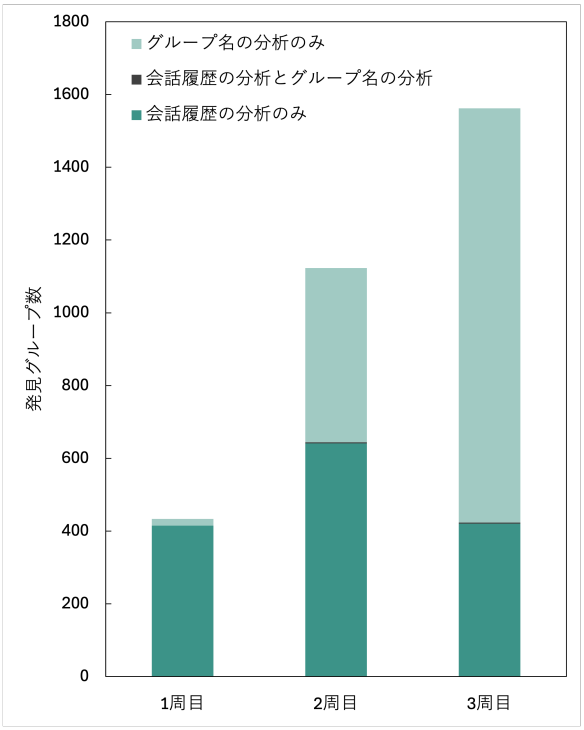

図 6　各周における発見グループ数

次に，探索で得られたグループ間の重複を調べた．1 周目で取得したグループと 2 周目で取得したグループの間には，全体で 114 個の重複が確認された．このうち，グループ名の分析による探索同士の重複が 96 個，会話履歴の分析による探索同士の重複が 10 個であった．一方で，異なる探索手法間の重複は非常に少なく，1 周目のグループ名の分析による探索と 2 周目の会話履歴の分析による探索の重複は 9 個，1 周目の会話履歴の分析による探索と 2 周目のグループ名の分析による探索の重複は 0 個に留まった．また，1 周目で取得したグループと 3 周目で取得したグループの間では，全体として 46 個の重複が確認された．その内訳として，グループ名の分析による探索同士の重複が 41 個，会話履歴の分析による探索同士の重複が 3 個であった．さらに，1 周目のグループ名の分析による探索と 3 周目の会話履歴の分析による探索の重複は 3 個，1 周目の会話履歴の分析による探索と 3 周目のグループ名の分析による探索の重複は 0 個であった．加えて，2 周目で取得したグループと 3 周目で取得したグループの間には，全体で 289 個の重複が確認された．そのうち，グループ名の分析による探索同士の重複が 105 個，会話履歴の分析による探索同士の重複が 160 個であった．一方で，2 周目のグループ名の分析による探索と 3 周目の会話履歴の分析による探索の重複は 23 個，2 周目の会話履歴の分析による探索と 3 周目のグループ名の分析による探索の重複は 2 個であった．さらに，各周におけるグループ名の分析による探索と会話履歴の分析による探索の間の重複についても，1 周目では 0 個，2 周目，3 周目ではそれぞれ 3 個と，いずれの周でも極めて少ないことが確認された．この結果から，グループ名の分析と会話履歴の分析の 2 つの探索手法は異なる特徴を捉えており，それぞれが異なるグループを取得できていることがわかる．したがって，両手法は補完的に機能し，並列して実行することは幅広いグループを効率的に取得する上で有効であると考えられる．また，以上の結果を踏まえ，各周の探索によって取得されたグループのうち，既知のグループがどの程度含まれているかを可視化した結果を図 7 に示す．横軸に探索の周数，縦軸に取得されたグループの総数をとり，取得グループの内訳として，新規グループ，初期グループで取得済みのグループ，1 周目で取得済みのグループ，2 周目で取得済みのグループを示している．本図から，1 周目の探索で取得したグループのうち，初期グループと重複していないものは 427 個であった．さらに，2 周目の探索では，初期グループおよび 1 周目で取得したグループとの重複を除外した結果，1008 個の新規グループを取得できていた．同様に，3 周目の探索では，初期グループ，1 周目，および 2 周目で取得したグループとの重複を取り除くと，1244 個の新規グループを取得していた．これらの結果から，取得グループにおける既知のグループの割合は周を重ねるごとに増加しているものの，新規グループ数自体は増加していることが確認できる．このことから，初期グループを起点とした探索だけでなく，新たに取得したグループを活用して探索を繰り返すことで，提案手法が探索範囲を段階的かつ効果的に拡大しているといえる．

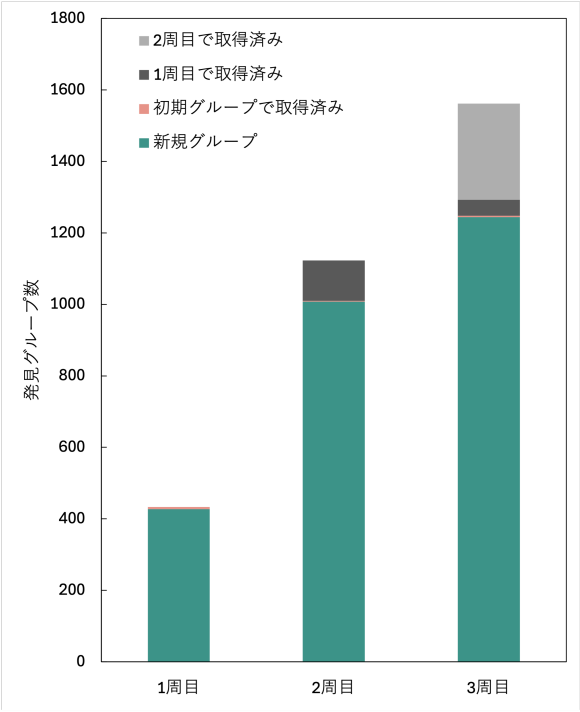

図 7　各周における重複と新規グループ数

続いて，各探索手法で取得したグループの作成年の分布を調べた結果を図 8 に示す．横軸はグループが作成された年，縦軸は取得されたグループのうちその年に作成されたグループ数を示している．探索結果から，いずれの探索においても取得されたグループの作成年は比較的新しいものが多く，全体の約 80% が 2022 年

以降に作成されたグループであり，特に 2023 年以降に作成されたグループが半数以上を占めていた．この結果は，犯罪グループが頻繁に削除され，新たなグループを立ち上げられる性質に起因していると考えられる．加えて，探索手法により取得されたグループの作成年に違いも見られ，特に会話履歴の分析による探索では，グループ名の分析による探索と比較して，より新しいグループが多く取得されていた．具体的には，グループ名の分析による探索では 2023 年に作成されたグループが最も多く取得できているのに対し，会話履歴の分析による探索では，2024 年に作成されたグループが最も多く取得されており，さらに 1 周目，2 周目，3 周目のいずれにおいても，作成から 1〜2 ヶ月程度の 2025 年に作成されたグループも取得できていた．この傾向は，犯罪グループが活動拠点を別のグループへ移動する際に，過去のグループの会話履歴内で新たな移動先を共有・宣伝することが多くあるためだと考えられる．この結果から，会話履歴の分析による探索では，作成されてから日が浅い最新のグループをより効率的に探索できる可能性が示唆された．また，グループ名の分析による探索では，特定の単語を手掛かりに検索を行うために，時間の経過と共にグループ名に含まれる特徴的な単語が変化すると，探索に適した単語の発見が困難になる可能性がある．この問題に対し，会話履歴の分析による探索を組み合わせることで，新しく作成されたグループを継続的に取得できるだけでなく，それらのグループのグループ名を基に新たな検索ワードを抽出し，適応的に探索を継続できると考えられる．このように，会話履歴の分析による探索を活用することで，最新の犯罪グループをより迅速に取得し，グループ名の変化にも対応しながら，効果的な探索を実施できるといえる．

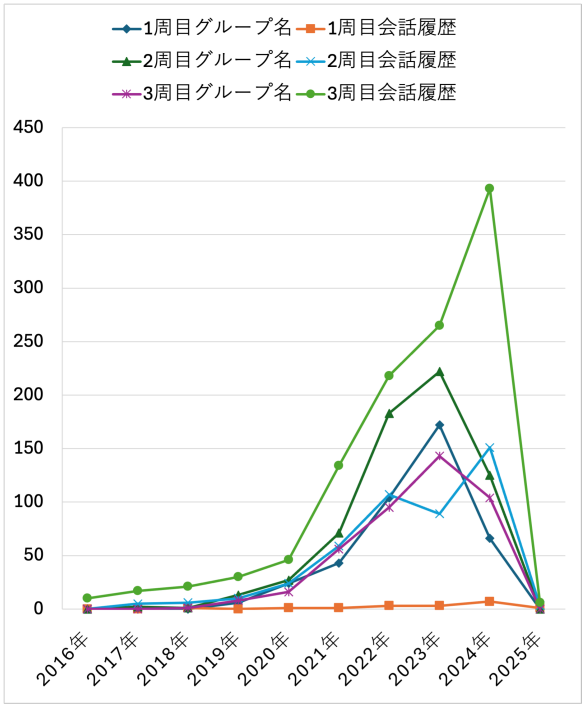

図 8　取得グループの作成年の分布

また，各探索手法で取得したグループにおける最終発言の時期の分布を調べた結果を図 9 に示す．横軸はグループ内で最後に発言があった時期を半年ごとに区切ったものであり，縦軸はその期間内に最終発言が確認された取得グループ数である．図 9 から，グループ名の分析および会話履歴の分析の両手法において，最新の発言が 2024 年後半から 2025 年に集中していることが確認された．特に，最終発言が 2025 年であるグループ数が各周の全ての取得方法で急増している．さらに，最終発言が 2025 年に確認されたグループ数の割合を各周ごとに見ると，1 周目では約 53.7%，2 周目では約 60.2%，3 周目では約 71.2% と増加傾向にあり，探索を繰り返すことでより新しいグループが取得されやすくなっていることがわかる．一般に，最終発言が直近であるほど，グループが現在も活発に活動している可能性が高い．そのため，最新の発言を持つグループほど，新規の情報を含む可能性があり，モニタリングの対象として有効であると考えられる．この点から，本手法が時間の経過に伴い適応的に探索を行い，活動中の犯罪グループを優先的に取得できていることが示唆される．

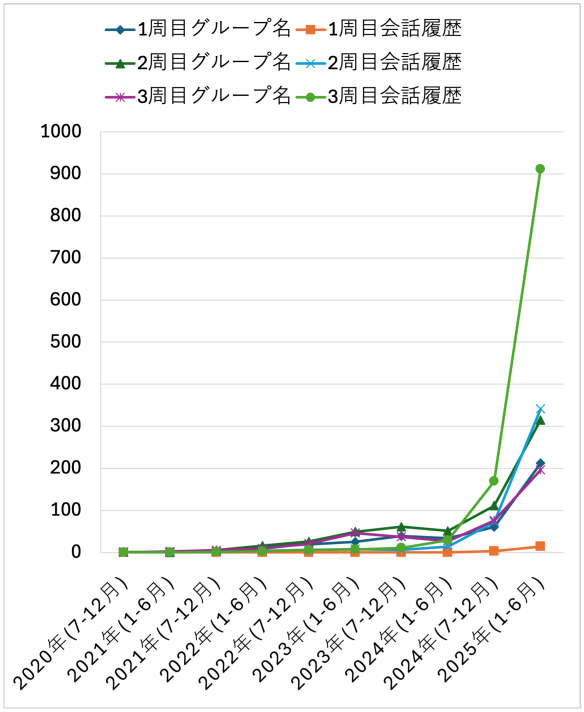

図 9　取得グループの最終発言の時期の分布

さらに，各グループの活動期間を調べた結果を図 10，図 11 に示す．図 10 はグループ名の分析による探索で取得したグループの活動期間，図 11 は会話履歴の分析による探索で取得したグループの活動期間をそれぞれ示している．横軸は活動期間（日数）を 90 日ごとに区切ったものであり，縦軸はその範囲に該当するグループ数を示している．また，活動期間は，グループの作成日から最終発言日までの期間として定義した．図 10 より，グループ名の分析による探索で取得したグループは，0〜90 日の短期間で活動を終えるものが最も多く，全体的に短命なグループが多い傾向が確認された．一方，図 11 に示す会話履歴の分析によ

る探索では，活動期間が 180〜270 日のグループが最も多く，より幅広い活動期間のグループが取得されていることがわかる．さらに，会話履歴の分析では 3000 日以上活動しているグループも一定数含まれており，これらのグループを詳細に確認したところ，直近まで活動を継続していることが確認された．このことから，提案手法が過去から継続的に活動を続ける犯罪グループの追跡にも有効であることが分かる．グループ名の分析による探索では，カード情報の売買を試みる犯罪グループが特有の単語を含める傾向にあることを利用しており，これは新規の買い手にも発見されやすくするためである．言い換えれば，検索に引っかかるような単語を含める必要があるのは，まだ十分なネットワークを持たず，比較的一時的なグループであるからだともいえる．また，Telegram のキーワード検索アルゴリズムの影響により，0〜90 日程度の活動期間を持つグループが優先的に検索結果に表示されている可能性も考えられる．一方，会話履歴の分析による探索では，既存のグループ内で言及された新たなグループが取得対象となるため，新しく作成した移動先のグループを共有・宣伝する目的以外では，既に一定のネットワークを持つグループが多く含まれると考えられる．その結果，グループ名の分析による探索よりも長期間活動するグループが多く検出されたと推測される．特に，直近まで長期間活動しているグループは，参加者数も多く大規模なグループであることが多いため，今後も継続的な情報源となる重要なグループだといえる．

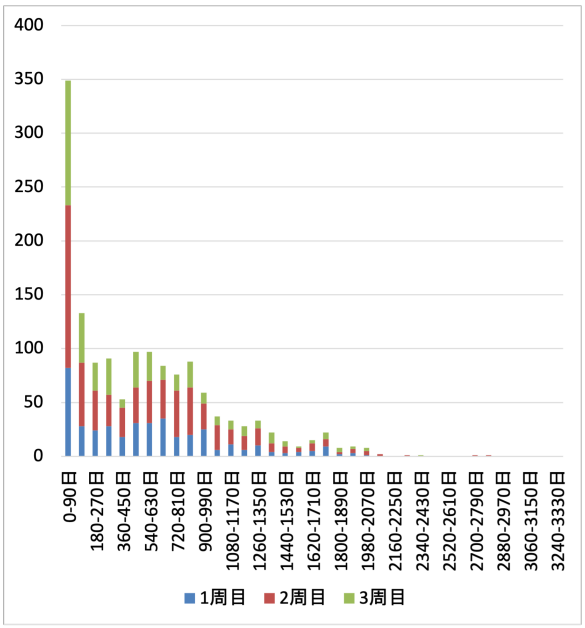

図 10　グループ名の分析による探索で取得したグループの活動期間

6　倫理的考察

本研究では，Telegram 上の犯罪グループを効率的に探索する手法を提案した．しかし，この手法は犯罪グループの特定を目的とする一方で，同様の技術が犯罪を試みる者によって悪用される可能性も考慮する必要があり，本研究においても倫理的観点から

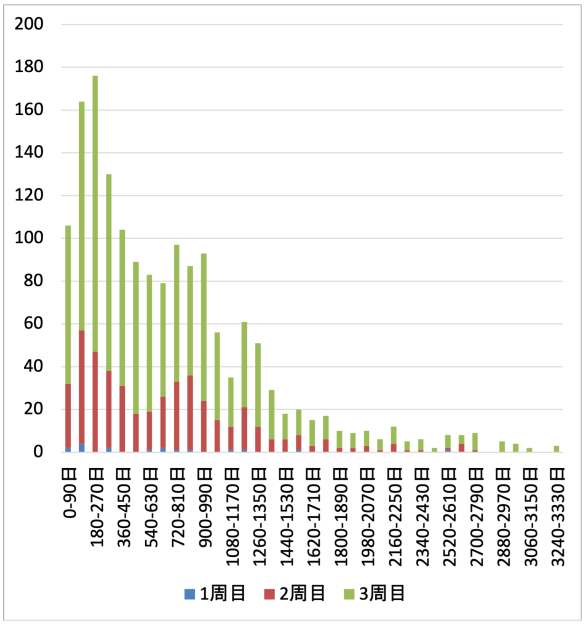

図 11　会話履歴の分析による探索で取得したグループの活動期間

慎重に検討を行った．まず，本研究は情報処理学会倫理綱領 [10] に基づいて実施され，適切な倫理的点検を経た上で進められている．また，研究の遂行にあたっては，研究者間で相互チェックを行うことで，一個人の判断に依存した研究の暴走を防止している．次に，本研究で提案した手法は，クエリエクスパンションの一般的に考えられる応用の範囲である．本手法自体は新たな攻撃手法の開発を目的とするものではなく，サイバーセキュリティ領域における防御的な活用を意図していることを明確にしておきたい．さらに，本手法を悪用するためには，データ収集や機械学習モデルの構築，実装に関する一定の知識が必要である．そのため，本研究が攻撃や悪用の障壁を下げるものではない．以上の点を踏まえ，本研究が犯罪行為の助長に繋がらないよう慎重に取り扱うとともに，今後の研究においても倫理的な側面を十分に考慮しながら進めていく．

7　おわりに

本研究では，クレジットカード情報の売買に関与する Telegram グループを効率的に特定するため，探索手法に機械学習モデルを導入し，その有効性を評価した．提案手法では，機械学習モデルを判定部分に導入することで，探索手法を複数回繰り返し実行可能となり，従来の 1 周目のみの探索に比べて取得できるグループ数が増加することが確認できた．特に，2 周目以降においてもグループ名の分析による探索と会話履歴の分析による探索は取得できるグループの傾向が異なることがわかり，補完的に機能していることが確認された．また，取得したグループの作成年や最終発言日の分析により，比較的新しく作成されたグループが多く取得できており，現在まで活動しているグループが多数を占めていることが確認された．加えて，過去に作成されたグループであっても現在もアクティブなものが取得されていることが確認された．

今後は，探索の繰り返しによる取得グループ数の収束性を検証するとともに，Telegram 以外の SNS への適用可能性についても検討していく予定である．

参考文献

[1] 一般社団法人日本クレジット協会. クレジットカード不正利用被害の発生状況. オンライン. アクセス日: 2025-01.
[2] フィッシング対策協議会. フィッシング報告状況（月次報告書）. オンライン. アクセス日: 2025-01.
[3] 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. SITE2022-26 123, 信学技報, 7 2022.
[4] Telegram. Telegram 公式サイト. オンライン. アクセス日: 2025-01.
[5] Telegram. What is Telegram? What do I do here? オンライン. アクセス日: 2025-01.
[6] Telethon. Telethon API. オンライン. アクセス日: 2025-01.
[7] 伊藤純菜, 趙智賢, 長田繁幸, 中川直樹, 小口正人. 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. **第 *86* 回全国大会講演論文集**, 2024(1):579–580, 3 2024.
[8] 伊藤純菜, 趙智賢, 長田繁幸, 中川直樹, 小口正人. SNS におけるサイバー犯罪抑止のためのグループ探索手法. **マルチメディア，分散，協調とモバイル *DICOMO 2024* シンポジウム**, 2024.
[9] 伊藤純菜, 趙智賢, 長田繁幸, 三田智之, 中川直樹, 小口正人. 機械学習による Telegram グループの犯罪性判定の自動化. **コンピュータセキュリティシンポジウム *2024* 論文集**, pages 1088–1094, 10 2024.
[10] 一般社団法人情報処理学会. 情報処理学会倫理綱領. オンライン. アクセス日: 2025-01.