小口研究室　研究紹介　(2024年度)
(お茶の水女子大学理学部情報科学科)

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
（研究担当:大原　望乃）

研究背景　フィッシング攻撃とTelegram

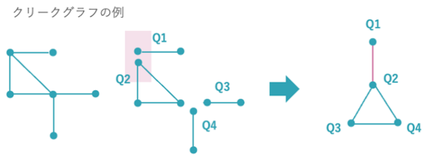
・クレジットカードの不正利用被害は年々増加
・その主な手口はフィッシング攻撃
　→　様々な対策が検討されてきた
・フィッシングサイトで窃取されたカード情報がSNS上で売買されている
　→　特に売買の場にされているのが Telegram（テレグラム）というメッセージアプリケーション

先行研究と提案　モニタリング / 交グラフの活用

・検索APIを使い，カード情報売買に使われる特徴的な文字列を検知可能なモニタリングツールを整備
・結果はカード会社に連携し，利用確認・利用停止などで対応（2022 日本総合研究所）

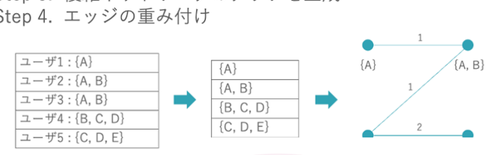
・犯罪に関与するグループをもっと効率よく見つけたい
　→　犯罪コミュニティの中心を特定し、そこから辿る
　→　交グラフを用いた犯罪グループ探索手法を提案

クリークグラフの例



提案手法　交グラフとグラフの彩色

Step 1. データベースからユーザリストをダウンロード
Step 2. ダウンロードしたデータのマイニング
Step 3. 複雑ネットワークのグラフを生成
Step 4. エッジの重み付け



Step 5. 交グラフに変換

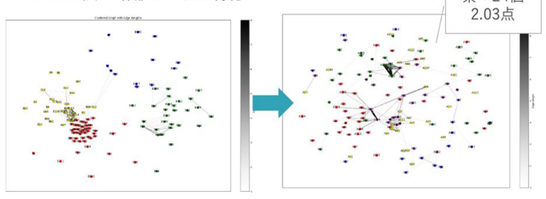
Step 6. 交グラフからコミュニティを抽出
　→　クラスタリングを行い，クラスタごとにノードを彩色
　→　元のグラフに戻した時，複数のクラスタに所属するノード（紫）はコミュニティの中心である可能性が高い

・また，そのままだとデータ数が多すぎるため，重要度の低いと思われるノードとエッジを削減する処理が必要

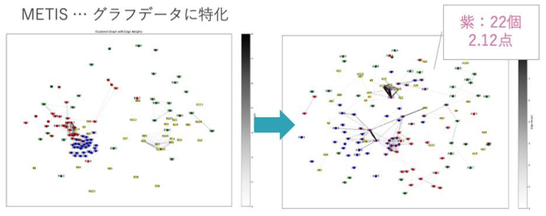
実験　クラスタリング手法の違いによる比較 / ノードの中身の分析

【実験1】クラスタリング手法の違いによる比較

k-means法 … 数値データに特化

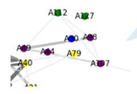


METIS … グラフデータに特化

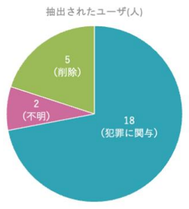


実験1：METISの方が調べるグループを減らし
　かつ調査価値が高いグループを調べられる

【実験2】ノードの中身の分析



A1: {グループ A, B, C},
A2: {グループ B, D, E, F}, …
同じパターンでグループに属するユーザを抽出



① 広報代理業者 (7/18)
・BOTアカウントで代理投稿
・親アカウントのタイムラインからリアルタイム監視が可能

② 店名をブランド化 (4/18)
・信用度を上げるため名前を変更せず長期間販売

広報代理業者またはブランドから辿る方が犯罪者を探索する効率は上がる

実験2：18人中11人がどちらかに該当
　→ 提案法は犯罪の中心の特定に役立つと考えられる

準同型暗号を用いたデータベースシステムの処理性能向上に関する研究
（研究担当:内藤　華）

研究背景

- データ利用が拡大、特に機密性の高いデータを用いてデータ解析を行う際には、**準同型暗号**による暗号化が有用
- 時系列データや画像データに対しては**周波数解析**が用いられるが、周波数成分はノイズが多く準同型暗号演算では特にコスト増大

分布の偏りが大きく、ピークの情報以外は不要なノイズ

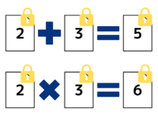
信号対雑音比（SNR）を用いてデータ圧縮
暗号化状態での効率的な周波数解析を目指す

SNRとは

- 信号の強度と雑音の強度の比率（信号の品質）を示す指標
- SNRが大きいほど信号の品質が高い
- 音声、画像、センサのデータ処理などに用いられるx

完全準同型暗号（FHE）

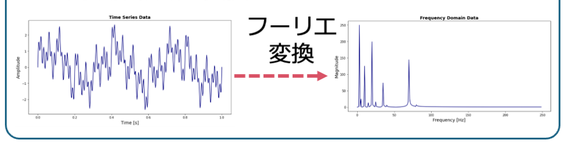
- 暗号化状態で加算・乗算を任意の回数計算可能
- 量子コンピュータに対しても安全
- 高い計算コスト、暗号文のデータサイズが課題
  - OpenFHEのCKKS方式では、平文の100倍以上



実用化に向けてストレージや計算の効率化が必要

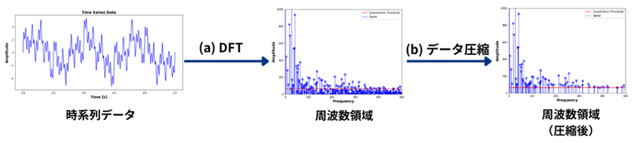
周波数解析

- データを周波数領域に変換することで、周期性や傾向を効果的に抽出
- 一般的にはフーリエ変換やコサイン変換などで周波数領域に変換



SNRを用いたデータ圧縮手法

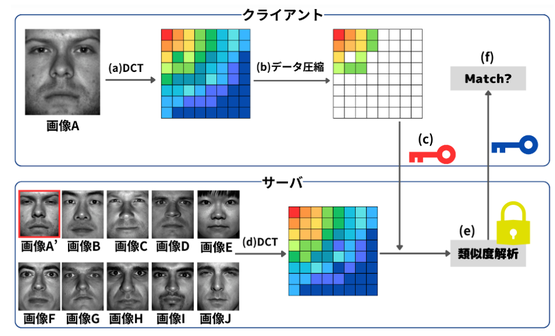
a. 周波数領域に変換
　- 時系列データの場合、DFTで変換
b. データ圧縮
　- T_{SNR}を指定し、βを算出
　- $2^{(\beta-1)}$未満の信号を取り除く



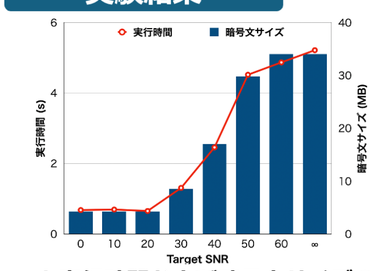
実験 – 顔画像データの類似度解析

実験の流れ
a. クライアントが画像AをDCTで周波数領域に変換
b. T_{SNR}を基にデータ圧縮
c. クライアントが暗号化
d. サーバが画像A'およびB～JをDCTで周波数領域に変換
e. サーバが類似度解析
f. クライアントが結果を復号

実験準備
- データセット：Yale Face Database
- FHEライブラリ：OpenFHE（CKKS方式）

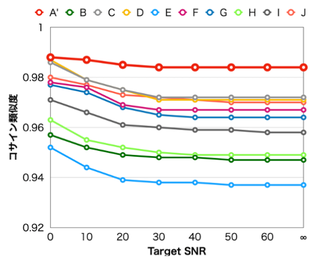


実験結果



T_{SNR}と実行時間および暗号文サイズの関係

- $T_{SNR} \leq 50$で圧縮の効果あり、$T_{SNR} \leq 40$では約50%削減
- T_{SNR}の増加に伴って実行時間・データサイズ増加



画像Aとのコサイン類似度

- すべてのT_{SNR}で画像A'を正しく認識
- が小さいほどコサイン類似度が大きい
　→ 大まかな特徴のみ保存され、人間の顔として類似

暗号化状態で**ストレージと周波数解析の効率化＋高い解析精度**を達成

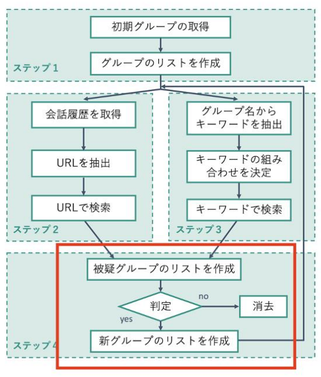
SNSコミュニケーション分析手法を用いた金融犯罪情報の早期検出に関する研究～グループ発見手法の検討と取得データに基づく考察～
（研究担当:伊藤　純菜）

背景・目的

- フィッシング攻撃によるクレジットカード情報の窃取・不正利用被害は年々拡大しており，窃取されたカード情報は主にSNSで売買されている
- 匿名での取引では信頼関係が築きにくく，売り手は買い手から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
- 先行研究ではこの点に着目した犯罪グループのモニタリングが抑止方法として有効であることを確認された

モニタリングの効率化を進めるため**監視対象となる犯罪グループを効果的に発見する手法が必要**

提案



ステップ①
Xのキーワード検索機能とTelegramのキーワード検索機能を使用して初期グループを取得
ステップ②
既知のグループの会話履歴からTelegramのグループのURLを抽出
ステップ③
既知のグループ名に対して形態素解析を行い単語を抽出
単語間の共起頻度を計測し閾値を超えた場合検索ワードとし検索
ステップ④
有識者による目視で関係性の有無を判定

前回　判定に要する時間長くなる
　　判定基準が明確化されていない

今回　機械学習による自動判定モデルを作成し置き換える

TF-IDF
Doc2Vec
Sentence-BERT
×
SVM
Logistic Regression
LightGBM

9種類のモデルを作成し精度を比較

TF-IDF+LightGBMが最も精度が高かった

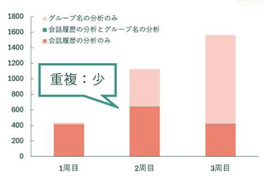
▽各指標に対する精度評価値

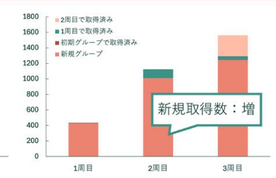
Accuracy	Recall	Precision	F1-Score
0.868	0.872	0.896	0.884

実験

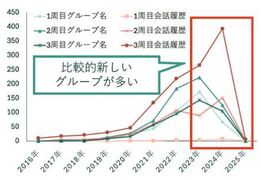
取得グループ間の重複

2つの探索手法は異なる特徴を捉えている
⇨両手法は補完的に機能している
探索を繰り返すことで探索範囲を拡大





取得グループの作成時期の分布



特に会話履歴の分析による探索ではより新しいグループを取得
⇨活動拠点を別グループへ移動する際に，過去グループの会話履歴内で移動先を共有・宣伝
より新しいグループを基にキーワードを抽出することでグループ名の変化にも適応

取得グループの最終発言時期の分布

最終発言が2025年に確認されたグループ数の割合を見ると，周を重ねるごとに増加傾向
⇨探索を繰り返すことでより新しいグループを取得できる
最終発言が直近であるほど現在も活発に活動しているグループである可能性が高い

取得グループの活動期間

犯罪グループがグループ名に特有の単語を含める傾向にあることを利用しているが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
⇨十分なネットワークを持たない一時的なグループ

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
⇨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

使用データと条件

初期グループ：107個
　Xのキーワード検索で取得したグループ：6個
　Telegramのキーワード検索で取得したグループ：101個
グループ名の分析による探索
　出現回数の閾値：多い方から30番目の出現回数
　共起頻度の閾値：常に1
会話履歴の分析による探索
　取得する会話履歴の期間の上限：3ヶ月
　取得する会話履歴の件数の上限：10000件

https://www.is.ocha.ac.jp/~oguchi_lab/　　oguchi@is.ocha.ac.jp