# 小口研究室　研究紹介　(2023年度)
## (お茶の水女子大学理学部情報科学科)

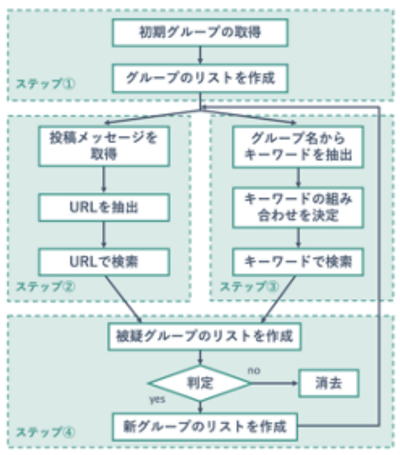
## Telegramによるグループ名と投稿メッセージの分析によるグループ探索
## （研究担当:伊藤　純菜）

### 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及び不正利用被害は年々拡大
先行研究から窃取されたカード情報は，Telegramのような秘匿性の高いSNS上で売買されていることが判明
抑止方法として，SNSに投稿されたメッセージのモニタリングが有効であることが確認された

モニタリングの効率化を進めるために監視対象となる犯罪グループを効率的に発見する手法を提案

### 提案手法




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

**ステップ①　初期グループの取得**
X(旧Twitter)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する

**ステップ②　投稿メッセージの分析による探索**
既知のグループの投稿メッセージを取得し，そこに含まれるテキスト情報からTelegramのグループのURLを抽出し，URLが示すグループの情報を取得する

**ステップ③　グループ名の分析による探索**
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する
予め定めた閾値を超えた単語間の共起頻度を計測し，共起頻度の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

**ステップ④　被疑グループの判定**
ステップ②とステップ③で得られた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し，有識者によって関係性の有無を目視で確認し判定する

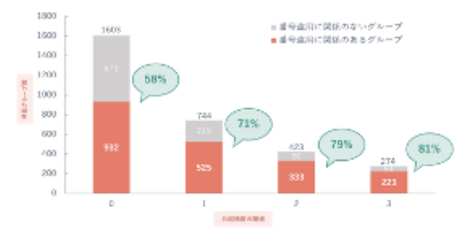
ステップ④終了後，ステップ②～ステップ④を繰り返す

### 実験結果

- 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
- 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

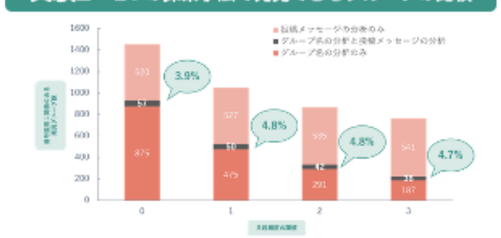
合計95個のグループに対して提案手法を実行

**実験1　共起頻度の閾値ごとの比較**




共起頻度の閾値を上げるにつれ有識者対応の効率性を左右する精度が向上している

**実験2　2つの探索手法で発見できるグループの比較**




閾値がいずれの場合でも共通しているグループの割合は5%以下であり2つの探索手法で発見できるグループには違いがあると言える

**実験3　グループ名から抽出したキーワードの比較**


どちらの場合でもある程度の重みを持つエッジが存在している
→初期のグループ名から取得したキーワードとは別のキーワードが得られている

### 今後の課題

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りたい

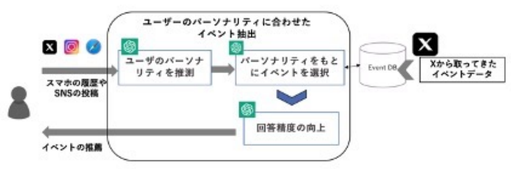
## マルチモーダルSNSデータを用いたイベント情報推薦システムにおけるGPT活用
## （研究担当:大本　詩織）

### 研究背景

・SNS には固定的なメディアに掲載されていないような大小様々な規模のイベントに関する情報が存在
・ユーザについての情報をSNSの投稿から取得可能
・LLMの急速な発展

LLMを利用した、SNS上のデータを用いた推薦システムの構築
ユーザのパーソナリティを利用した推薦精度の向上


### システム概要




**ChatGPTを用いたシステムの概要**

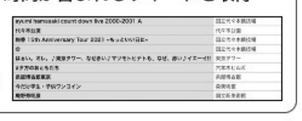
① ユーザのパーソナリティの推測
② パーソナリティに基づいたイベントの選択
③ 回答精度の向上
の３パートに分けて、それぞれで、chatGPTを用いて検証

趣味趣向
性格特性
感情

**イベントデータの取得**

X(旧Twitter)のAPIのキーワード検索機能を使用して、場所・日付・時間が含まれるツイートを取得し、正規表現を用いてイベント名を抽出

イベントリストの一部



### 関連研究

**CoT**
LLMに段階的に推論を行わせることで、高度な推論タスクを可能にするプロンプトエンジニアリング手法

**PsyCoT**
・心理学的なアンケートを基にした性格特性の評価方法をCoTとして利用することで、テキスト入力からの性格特性を診断
・**ビッグファイブ性格特性**(協調性、外向性、開放性、神経症的傾向、誠実性) に基づいて、人間の性格を記述することで、性格検出性能と堅牢性を大幅に向上することが可能

**Chain of Empathy**
ChatGPTを心理療法にもとづいて実行し、高い共感力と思いやりある会話をさせる共感の連鎖プロンプト手法。
CBT・DBT・PCT・RTなどの心理療法をを用いることでLLMはユーザーの感情的な状態をより深く理解し、具体的で共感的な対応を提供可能

**ハルシネーション**
LLMの出力が現実の事実やユーザ入力と矛盾する現象
→ ハルシネーションを減らす工夫として、
**前処理、後処理** (テキスト生成後、生成したテキストをレビューし、ハルシネーションを識別して修正するためのステップを導入する)**の活用など**がある

例：「上記で生成したテキストはすべて事実に基づいていますか？」といった質問を行う

### 実験結果

ユーザの<u>パーソナリティ</u>の推測

**趣味趣向の場合**

**Xから:**
ツイートで少し触れただけの内容も趣味趣向に挙げられてしまう
**Instagramから:**
投稿の内容が偏っていることが多く、得られる趣味趣向に偏りが生じる
**検索履歴から：**
趣味趣向に関係のない履歴を与えると不適切な回答が得られる場合がある

共通している趣味趣向はより適切であるとして優先して回答させることでより信憑性が高い趣味趣向を推測可能

**性格特性の場合**

PsyCoTを用いたプロンプトを与える

テキストを分析し、書き手の性格特性を評価してください。
**協調性（Agreeableness）**
著者は他人の欠点に気づくことがありますか？（スコア: 1-5）
著者は自己中心的ですか？（スコア: 1-5）
~~略~~
各項目から得られたスコアを集計し、最終的に性格特性を導いてください。

スコアづけが行われ、それに基づいた性格特性の推測が可能

**感情の場合**

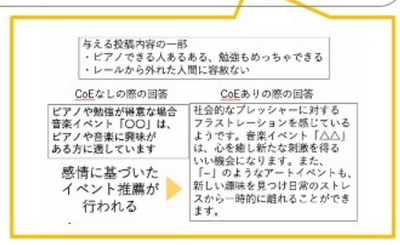
CoEを用いたプロンプトを与える

ユーザー（私）が話すことに対して、以下の枠組みで対応してください：
感情の識別：ユーザーが示している感情は何ですか？
感情の原因：その感情はどのような状況や考えから生じていますか？
共感と理解：ユーザーが感じている感情に共感し、理解を示してください。
具体的なアドバイスと解決策：ユーザーが抱える問題に対して、具体的なアドバイスや解決策を提案してください。

感情の推測が可能

以上のようなやり方で推測したパーソナリティを用いることで、
より精度の高いイベント推薦を行うことができる

感情に基づいてイベント推薦を行った結果の例 ▶




イベント推薦を行う中で、イベント内容をでっちあげて推薦するといったハルシネーションが発生することがある
→ webブラウジング機能(ChatGPTがリアルタイムでウェブ検索を行い、最新の情報や特定のトピックに関するデータを取得できる機能)を用いて、実際にイベントが存在するか調べるよう後処理を導入することで回答精度の向上が可能

### 今後の課題

・ChatGPTによるパーソナリティの分析、イベント推薦の精度改善
・推測されたパーソナリティや推薦されたイベントの評価手法の検討
・一連の流れのシステム化

## 分散台帳を利用したデータ検証可能な分散データベースの性能に関する検討
## （研究担当:坂本　明穂）

### 研究背景

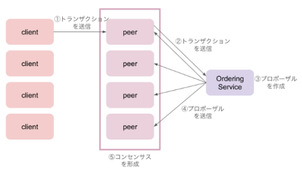
分散データベースを用いたデータ管理により，複数ユーザ間でのデータ共有が容易となる．しかしデータベース上のデータを有効に活用するためには，データの健全性の保証が必要である．

ブロックチェーンの検証メカニズムを応用して，データ保存時にデータ検証を実行

- **ブロックチェーンのパフォーマンス評価**

### Hyperledger Iroha

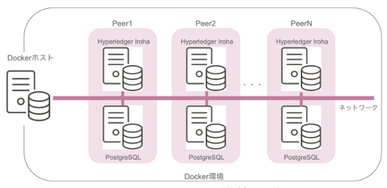
- 事前に承認されたユーザしか参加できないプライベートブロックチェーン
- コンセンサス形成にピア間での合意が必要
- コンセンサスアルゴリズムにYAC方式を採用
- 一般的なデータベースと比較し，トランザクション処理に時間がかかる




トランザクション処理プロセス

### 実験概要

**実験環境**




Hyperledger Iroha構築環境

| | |
|---|---|
| OS | Ubuntu20.04LTS |
| CPU | Intel(R) Xeon(R) Silver 4314 CPU @ 2.40GHz |
| コア数 | 32 |
| スレッド数 | 64 |
| メモリ | 192GB |

実験に使用したサーバ環境

**実験1**

Hyperledger Irohaの各ピアはデータの格納先としてPostgreSQLを使用している．
そこで，PostgreSQLでのクエリ1件の処理時間とHyperledger Irohaの1件あたりのトランザクション処理時間の比較を行う．
両者の実行時間の差はHyperledger Irohaにおけるコンセンサス形成にかかる時間とすることができる．
またHyperledger Irohaを構成するピア数を5, 10, 20, 30と変化させ，スケーラビリティの評価も行う．

**実験2**

トランザクション送信レートとネットワークサイズを以下の表のように変化させたときの，平均レイテンシとスループットの評価を行う．
測定にはブロックチェーン基盤の測定ツールであるHyperledger Caliperを用いる．

| | |
|---|---|
| トランザクション送信レート(tps) | 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 150, 200 |
| ネットワークサイズ | 5, 10, 20, 30 |

### 実験結果

**実験1**

| 測定対象 | 測定結果 (ms) |
|---|---|
| PostgreSQL | 10.3 |
| Hyperledger Iroha 5ピア | 5696.27 |
| Hyperledger Iroha 10ピア | 5641.27 |
| Hyperledger Iroha 20ピア | 5777.56 |
| Hyperledger Iroha 30ピア | 5804.01 |

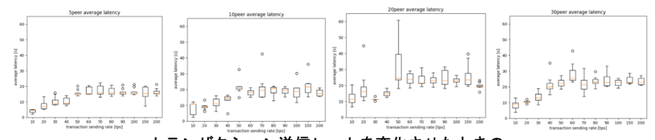

Hyperledger Iroha実行時ログ

PostgreSQLの実行時間はHyperledger Irohaの実行時間の約0.2%であり，Hyperledger Irohaのトランザクション処理時間の大部分をコンセンサス形成が占めていることがわかった．
また実行時ログより，オーダリングサービスがクライアントからトランザクションを収集してから，ピアがプロポーザルを受信するまでにかかる時間が長いことがわかった．

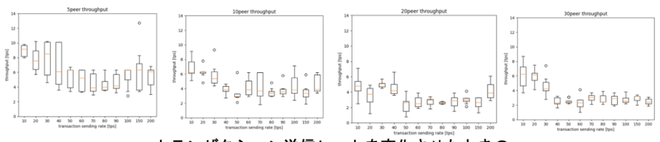
**実験2**

- トランザクション送信レートを変化させたとき
  トランザクション送信レートが小さいとき→増加させるほど性能が低下
  トランザクション送信レートが大きいとき→性能に変化が見られない
- ネットワークサイズを変化させたとき
  ネットワークサイズが大きくなるほど性能が低下した．

ある程度トランザクション送信レートが大きいとき，性能に変化がなかった理由としてオーダリングサービスからピアに送信されるプロポーザル数に上限が設定されていることが考えられる．
ネットワークサイズを大きくすると，コンセンサス形成時にやり取りされるメッセージ数が増加するため性能が低下したと考えられる．




トランザクション送信レートを変化させたときの
各ピア数での平均レイテンシの変化




トランザクション送信レートを変化させたときの
各ピア数でのスループットの変化

### まとめ

分散データベースにおけるデータ検証機能としてのブロックチェーンの活用を目指し．Hyperledger Irohaの性能評価を行った．
Hyperledger Irohaのコンセンサス形成にはかなりの時間がかかることがわかった．またHyperledger Irohaネットワークが1秒あたりに受け取るトランザクション数が増加すると性能が低下し，ネットワークサイズが大きくなると性能が低下することがわかった．
現在はノード間を仮想ネットワークで接続しているが，今後は実ネットワークで接続しパフォーマンスの評価を行う．

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