一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

Telegram 上のサイバー犯罪関連チャンネルの大規模な収集と分析

青砥　陸†　インミンパパ††　吉岡　克成†††,††

† 横浜国立大学大学院環境情報学府
†† 横浜国立大学先端科学高等研究院
††† 横浜国立大学環境情報研究院
E-mail: †aoto-riku-hx@ynu.jp, ††{yinminn-papa-jp,yoshioka}@ynu.ac.jp

あらまし　Telegram は多様なサイバー犯罪活動の主要な基盤となっている．しかし，既存研究の多くは，標本数が限定的であること，観測期間が短期的であること，およびアクセスが制限された商用データベースに依存していることから，網羅性と再現性に課題を抱えている．我々の先行研究では，類似チャンネル推薦機能と大規模言語モデル（LLM）を用いたサイバー犯罪関連チャンネルの収集・分類システムを提案した．本稿では，類似チャンネル推薦機能による探索の深度を先行研究の 2 ホップから 154 ホップまで拡大するとともに，最新の LLM の導入と分類体系の刷新により，悪性判定で加重平均 F1 スコア 0.90，カテゴリ分類で 0.94 を達成した．2025 年 5 月から 12 月にかけて本システムを適用し，41,788 チャンネルと約 7.4 億件のメッセージからなる大規模データセットを構築した．さらに，サイバー犯罪エコシステムの構造分析により，異なる犯罪カテゴリ間の接続性，英語・ペルシャ語を中心とした言語分布とカテゴリごとの言語的特徴，および類似関係ネットワークにおいて多数のチャンネルと隣接するハブチャンネルの存在を明らかにした．また，チャンネル数が最多のカテゴリである「機密性・完全性・可用性（CIA）への侵害」（全体の 52.9%）の時系列分析により，2022 年以降の活動の急増と，窃取された認証情報の取引の活発化を確認した．

キーワード　Telegram，サイバー犯罪，大規模言語モデル，チャンネル分類

Collecting and Categorizing Cybercrime-Related Channels on Telegram at Scale

Riku AOTO†, Yin Minn Pa Pa††, and Katsunari YOSHIOKA†††,††

† Graduate School of Environment and Information Sciences, Yokohama National University
†† Institute of Advanced Sciences, Yokohama National University
††† Faculty of Environment and Information Sciences, Yokohama National University
E-mail: †aoto-riku-hx@ynu.jp, ††{yinminn-papa-jp,yoshioka}@ynu.ac.jp

Abstract　Telegram has become a major platform for diverse cybercrime activities. However, existing studies often rely on limited sample sizes, short observation periods, or restricted commercial databases, which poses challenges in coverage and reproducibility. Our prior work proposed a system for collecting and classifying cybercrime-related channels using the Similar Channels recommendation feature and large language models (LLMs). This paper extends the exploration depth from 2 hops to 154 hops and adopts an advanced LLM along with a refined taxonomy, achieving weighted F1 scores of 0.90 for maliciousness detection and 0.94 for category classification. Applying this system from May to December 2025, we constructed a large-scale dataset of 41,788 channels and approximately 740 million messages. Through structural analysis of the cybercrime ecosystem, we revealed the connectivity across different crime categories, the language distribution centered on English and Persian along with linguistic characteristics by category, and the presence of hub channels with numerous adjacent channels in the similarity network. Additionally, temporal analysis of offenses against confidentiality, integrity, and availability, the largest category accounting for 52.9% of channels, revealed a surge in activity since 2022 and active trading of stolen credentials.

Key words　Telegram, Cybercrime, Large Language Models, Channel Classification

1. はじめに

メッセージングプラットフォームである Telegram [1] は，不正サービスの提供，窃取データやマルウェアの配布，攻撃活動の調整など，サイバー犯罪者にとって主要な通信インフラとなりつつある．このような状況において，サイバー犯罪コミュニティを体系的に発見・分析する手法が求められている．

しかしながら，Telegram は全チャンネルの一覧を取得できる公開 API を提供していない．TGStat [2] や Telemetr.io [3] といった商用データベースもカバレッジが限定的であり，またデータ収集手法が非公開であるため，学術的な再現性の担保が困難である．これらの制約により，既存研究の多くは標本数が限定的であるか観測期間が短期的であり，エコシステム全体の実態解明には至っていない．

この課題に対処するため，我々は先行研究 [4] において Telegram 上のサイバー犯罪関連チャンネルを発見・分類するシステムを提案した．本システムは以下の 3 つのモジュールから構成される．(1) Telegram の類似チャンネル推薦機能（Similar Channels [5]）を用いて，起点となるシードチャンネルから関連チャンネルを探索する **Explore**，(2) 大規模言語モデル（LLM）を用いてサイバー犯罪との関連性を判定する **Filter**，(3) LLM を用いてサイバー犯罪の国際条約であるブダペスト条約に準拠した犯罪類型に分類する **Categorize** である．

本研究では，この手法を拡張し，サイバー犯罪関連チャンネルの大規模な収集と分析を行った．具体的には，探索深度を先行研究の 2 ホップから 154 ホップへ拡大した．また，最新の LLM の導入，分類体系の刷新，およびプロンプトの改良により，分類精度を向上させた．

本稿の主な貢献は以下の通りである．

（1） **大規模データセットの構築：** 2025 年 5 月から 12 月の期間に，120 件のシードチャンネルを起点として，41,788 件のサイバー犯罪関連チャンネルと約 7.4 億件のメッセージを収集した．これは先行研究の約 50 倍のチャンネル数に相当し，本手法のスケーラビリティを実証した．

（2） **分類精度の向上：** 最新の LLM の採用，分類体系の刷新，およびプロンプトの改良により，Filter モジュールで加重平均 F1 スコア 0.90，Categorize モジュールで 0.94 を達成した．

（3） **エコシステムの構造的特性の解明：** 類似チャンネル推薦機能によって形成されるネットワーク構造を解析し，犯罪カテゴリ間の接続性，英語・ペルシャ語を中心とした言語分布とカテゴリごとの言語的特徴，および多数のチャンネルと隣接するハブチャンネルの存在を明らかにした．また，チャンネル数が最多のカテゴリである「機密性・完全性・可用性（CIA）への侵害」（全体の 52.9%）について時系列分析を行い，2022 年以降の活動の急増と，窃取された認証情報の取引の活発化を明らかにした．

2. 関連研究

2.1 特定の犯罪類型に関する研究

Telegram 上での特定の犯罪類型を対象とした研究が複数存在する．

児童性的虐待資料（CSAM）に関しては，Packeer ら [9] がキーワード検索とリンクの追跡により 53 チャンネルを特定し，約 1.5 万件のメッセージを分析した．金融詐欺に関しては，Lymishchenko ら [8] がキーワード検索とスノーボールサンプリングにより 40 チャンネルを特定し，ダークウェブとの比較分析を行った．

これらの研究は各犯罪類型の実態解明に貢献しているものの，対象が特定の犯罪類型に限定されており，サイバー犯罪エコシステム全体を捉えるものではない．

2.2 複数の犯罪類型および大規模分析

複数の犯罪類型を横断的に調査した研究もあるが，その数は比較的少ない．

Roy らによる *DarkGram* [6] は，Telegram 上のサイバー犯罪全般を対象とした代表的な研究である．Roy らはカタログサイト（Telemetr.io）と手動レビューにより 339 チャンネルを収集し，認証情報の漏洩やマルウェア配布など 5 カテゴリの活動を分析した．La Morgia ら [7] は，正規チャンネルを模倣した偽チャンネルの検知に焦点を当て，統計サービス（Tgstat）を起点としたスノーボールサンプリングにより 120,979 チャンネルと 2.4 億件のメッセージを収集した．

我々の先行研究 [4] では，類似チャンネル推薦機能と LLM を組み合わせた発見・分類システムを提案し，272 件のシードチャンネルから 791 件のチャンネルと約 130 万件のメッセージを収集した．

2.3 本研究の位置づけ

表 1 に既存研究との比較を示す．既存研究の多くは，特定の犯罪類型に限定されるか，キーワード検索やサードパーティリストに依存しており，推薦機能を用いた大規模な探索は行われていない．

本研究は，先行研究の手法を拡張し，Similar Channels 機能を用いた大規模探索を行った点で独自性を持つ．キーワード検索では事前に定義した用語に合致するチャンネルしか発見できないのに対し，本手法は購読者の重複に基づく推薦機能を活用することで，未知の用語や隠語を用いるチャンネルも発見可能である．ただし，本手法もシードチャンネルの選定に依存するため，シードから推薦機能を通じて到達できないチャンネルは発見できないという制約がある．探索深度を 154 ホップまで拡大し，41,788 件のサイバー犯罪関連チャンネルと約 7.4 億件のメッセージを収集することで，多様な犯罪類型を含むエコシステムの分析を行った．

3. 手　　法

本研究では，先行研究 [4] で提案された発見・分類システムを拡張し，適用する．図 1 に本システムのアーキテクチャを示す．本システムは Explore（探索），Filter（選別），Categorize

表 1: Telegram における不正活動研究の概要（–はデータなし）

研究	焦点	チャンネル数	メッセージ数	発見手法
Roy et al. [6]	サイバー犯罪全般	339	6.4 万	カタログサイトからの抽出と手動選別
La Morgia et al. [7]	偽チャンネル・クローン	120,979	2.4 億	カタログサイト上位を起点としたスノーボール
Lymishchenko et al. [8]	金融詐欺	40	–	キーワード検索とリンク共有関係の追跡
Packeer et al. [9]	CSAM	53	1.5 万	キーワード検索とリンクの追跡
我々の先行研究 [4]	サイバー犯罪全般	791	130 万	類似チャンネル推薦機能と LLM を用いた探索
本研究	**サイバー犯罪全般**	**41,788**	**7.4 億**	**類似チャンネル推薦機能と LLM を用いた大規模探索**

（分類）の 3 つのモジュールから構成され，シードチャンネルを起点として各モジュールを順次実行する．本節では，各モジュールの詳細を述べる．

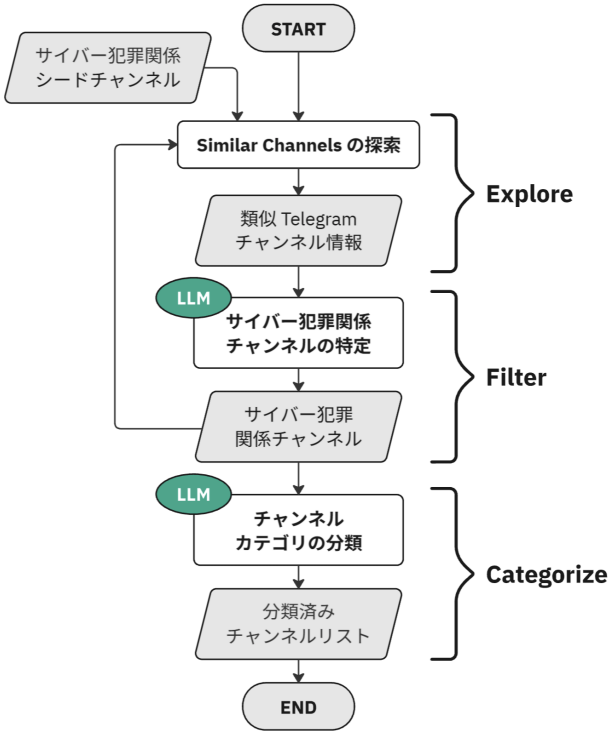

図 1: 本システムのアーキテクチャ概要

3.1 Explore モジュール

Explore モジュールは，類似チャンネル推薦機能によって形成されるチャンネル間のネットワーク（以下，推薦グラフ）を探索し，サイバー犯罪関連チャンネルを発見する．

Telegram は Similar Channels と呼ばれる推薦機能を提供しており，購読者の重複に基づいて類似チャンネルを推薦する．本モジュールでは，既知のサイバー犯罪関連シードチャンネルを起点として Similar Channels 機能による探索を開始し，取得された類似チャンネルに対して再帰的に探索を行う．既に処理済みのチャンネルは除外することで，重複なく探索を進める．

ただし，この機能は購読者の重複のみに基づくため，サイバー犯罪と無関係なチャンネルも含まれる可能性がある．このノイズは Filter モジュールで除外する．

3.2 Filter モジュール

Filter モジュールは，Explore モジュールで発見されたチャンネルからサイバー犯罪に関連しないものを除外する．推薦グラフにはニュースメディアや技術議論チャンネルなどの良性チャンネルも含まれるため，本モジュールでこれらを除外する．

各チャンネルについて，メタデータ（タイトル，説明文）と最新メッセージからコンテキストを抽出し，LLM を用いてサイバー犯罪との関連性を判定する．先行研究では 3 段階分類（Benign，Suspicious，Malicious）を採用していたが，Suspicious の定義が曖昧であったため，本研究では以下の 2 段階分類を採用する．

- **Benign**：サイバー犯罪との関連が認められないチャンネル．
- **Malicious**：サイバー攻撃の調整，窃取データの取引，不正サービスの提供など，サイバー犯罪に関連する活動が認められるチャンネル．

Benign と分類されたチャンネルは除外し，Malicious チャンネルのみを Categorize モジュールへ送る．また，Malicious チャンネルは次ホップの探索における Similar Channels の入力としても利用し，悪性チャンネルの発見効率を高める．

3.3 Categorize モジュール

Categorize モジュールは，悪性チャンネルをブダペスト条約 [10] および Tsakalidis ら [11] によるサイバー犯罪分類のフレームワークに基づくカテゴリに分類する．先行研究では 22 種類のサブカテゴリを用いたが，分類精度向上のため本研究では 5 つの主要カテゴリに簡略化した．各チャンネルについて，Filter モジュールと同様にコンテキストを抽出し，LLM を用いて以下のカテゴリへ分類する．

- **カテゴリ A：コンピュータデータおよびシステムの機密性，完全性，可用性に対する脅威：**システムへの不正アクセス，機密データの窃取，通信の不正傍受，データの改ざん・破壊，システム機能の妨害，およびサイバー犯罪ツールの作成・配布に関与する行為を含む．
- **カテゴリ B：コンピュータを介した犯罪：**デジタル記録の偽造，金銭的利益を目的とした詐欺行為，および ID の窃取・不正使用を含む．
- **カテゴリ C：コンテンツに関連する違法行為：**露骨な違法コンテンツの配布，児童搾取素材，宗教的信念を標的とす

る行為，サイバーいじめ，違法ギャンブル，スパム，および差別的・憎悪的コンテンツの拡散を含む．

- **カテゴリ D：知的財産権の侵害：**著作権で保護された素材の不正使用・配布，および商標の不正使用を含む．
- **カテゴリ E：複合的な違法行為：**フィッシング，不正収益処理のためのデジタルツール使用，国家安全保障や重要インフラを標的とするサイバー戦争，およびデジタルプラットフォームを通じたテロリズムの促進を含む．

4. 実　　装

4.1 インフラストラクチャ

再現性の確保とデータの機密性保護のため，すべての処理はローカル環境で実施した．LLM には 2,350 億パラメータの Qwen3-235B [12] を採用し，量子化（モデルの軽量化手法）なしで展開した．推論基盤として，4 基の NVIDIA RTX 6000 Ada GPU を搭載したサーバ上で Ollama [13] を使用した．Telegram API との通信には Telethon [14] を，データ永続化には Elasticsearch [15] を使用した．

4.2 Explore モジュールの実装

4.2.1 シード選定

著者らがサイバー犯罪関連用語や既知の脅威アクター名で Telegram を検索し，120 件のシードチャンネルを選定した．シード選定時に Filter および Categorize モジュールで判定した結果，カテゴリ A：96 件，B：5 件，C：0 件，D：4 件，E：1 件，良性：14 件であった．良性と判定されたチャンネルも探索の多様性確保のためシードに含めた．

4.2.2 探索の実行

2025 年 5 月 19 日から 12 月 8 日までの約 7 か月間，154 ホップまで探索を実施した．探索は以下の 3 つの期間に分けて実施した．

- **P1（ホップ 0–54）**：試験的探索．入力チャンネル数などのパラメータを検証した．
- **P2（ホップ 55–133）**：本格的な探索．各ホップで 50 件のチャンネルを入力として使用した．
- **P3（ホップ 134–154）**：探索の拡大．入力チャンネル数を 100 件に増加した．

各ホップでは，Similar Channels の入力として未使用の Malicious チャンネルからランダムに選定し，特定のチャンネル群への探索の集中を防いだ．

4.3 Filter および Categorize モジュールの実装

Filter および Categorize モジュールは共に Qwen3-235B を使用する．各チャンネルについて，メタデータ（タイトル，説明文）と最新メッセージを最大 8,000 文字のコンテキストとして集約する．この上限は，コンテキストが長すぎると分類精度が低下するためである．

4.3.1 Filter モジュールのプロンプト設計

Filter モジュールでは，LLM にサイバーセキュリティアナリストとしての役割を与え，チャンネルの悪性度を二値分類させる．先行研究からの主な改良点として，悪性チャンネルが正当なサービスに偽装するパターン（欺瞞パターン）への対処と分析フレームワークの明確化が挙げられる．プロンプトには以下の要素を含めた．

- **分類基準**：Benign と Malicious の明確な定義．Benign は正当な目的（教育，研究，合法サービス）を持つチャンネル，Malicious はサイバー犯罪の実行・促進・利益獲得を意図するチャンネルと定義した．
- **分析フレームワーク**：表面的な自己記述に惑わされず実際のコンテンツを評価する指針を提示した．具体的には，チャンネルの意図分析，ビジネスモデルの検証，およびコンテンツ分析の手順を含む．
- **欺瞞パターンの警告**：悪性活動が正当なサービスに偽装されるパターン（教育コンテンツを装った詐欺など）を具体例とともに提示した．

4.3.2 Categorize モジュールのプロンプト設計

Categorize モジュールでは，悪性と判定されたチャンネルを 5 つのカテゴリに分類させる．先行研究では 22 種類のサブカテゴリへの分類を試みたが，本研究では 5 つの主要カテゴリに簡略化した．これに伴い，プロンプトも刷新し，カテゴリ間の境界が曖昧なケースに対する判断基準を明確化した．プロンプトには以下の要素を含めた．

- **カテゴリ定義**：第 3. 節で定義した 5 つのサイバー犯罪カテゴリ（A–E）の詳細な説明．
- **分類ルール**：曖昧なケースに対する優先順位付きの判断基準．例えば，スポーツの八百長情報を扱う「固定試合（Fixed Match）」チャンネルについては，情報を販売する場合はカテゴリ B（詐欺），賭博を促進する場合はカテゴリ C（違法ギャンブル）と区別する指針を提示した．

両モジュールとも，出力形式として JSON 形式を指定し，分類結果と理由の要約（著者らの確認のため日本語で出力）を含めることで，結果の解釈と後続の分析を容易にした．

5. 評　　価

5.1 正解データセットの構築

分類精度を評価するため，正解データセットを構築した．収集データはカテゴリ A に偏っているため，少数カテゴリ（C, E など）のサンプルを確保する必要があった．そこで，Llama 3.3 による事前分類に基づく層化サンプリングを採用し，Malicious と Benign からそれぞれ 150 件，カテゴリ A–E から各 30 件をランダムに選出した．ただし，事前分類と人間のアノテーション結果には差異が生じたため，最終的なカテゴリ分布は当初の設計とは異なるものとなった．

表 2: Filter モジュールの分類性能（$N = 299$）

分類	Precision	Recall	F1	Support
Benign	0.87	0.87	0.87	118
Malicious	0.92	0.92	0.92	181
Weighted Avg	0.90	0.90	0.90	299

表 3: Categorize モジュールの分類性能（$N = 181$）

カテゴリ	Precision	Recall	F1	Support
カテゴリ A	0.96	0.92	0.94	60
カテゴリ B	0.98	0.94	0.96	53
カテゴリ C	0.80	0.92	0.86	13
カテゴリ D	0.92	0.97	0.94	35
カテゴリ E	0.90	0.95	0.93	20
Weighted Avg	0.94	0.94	0.94	181

2 名のセキュリティ研究者が独立してアノテーションを実施し，各チャンネルのタイトルと最新 50 件のメッセージを確認して悪性度およびカテゴリを判定した．アノテータ間一致度は Cohen の κ 係数 [16] で悪性度 $\kappa = 0.85$，カテゴリ分類 $\kappa = 0.84$ であり，不一致は議論により解決した．最終的な正解データセットは，Benign 118 件，Malicious 181 件（A：60，B：53，C：13，D：35，E：20），判定不能 1 件の計 300 件となった．

5.2 Filter モジュールの評価

判定不能の 1 件を除いた正解データセット（$N = 299$）を用いて Filter モジュールを評価した．表 2 に結果を示す．

加重平均 F1 スコア 0.90 を達成し，Malicious クラスに対する F1 スコアは 0.92 であった．Malicious クラス（F1=0.92）と比較して Benign クラス（F1=0.87）の精度が低い．誤分類の分析から，主に 2 種類のパターンが観察された．第一に，倫理的ハッキングに関するチャンネルやセキュリティニュースチャンネルなど，本来 Benign であるチャンネルが Malicious と誤判定されるケースである．これらのチャンネルはサイバー攻撃手法や脆弱性に関する用語を多く含むため，悪性チャンネルとの区別が困難であった．第二に，著作物の不正配布チャンネルなど，本来 Malicious であるチャンネルが Benign と誤判定されるケースである．これらのチャンネルは明示的に違法性を示す表現を避け，一般的なコンテンツ共有チャンネルと類似した記述を用いる傾向があるため，悪性と判定されにくかったと考えられる．

5.3 Categorize モジュールの評価

正解データセットのうち悪性と確定した 181 件を用いてカテゴリ分類を評価した．表 3 に結果を示す．

加重平均 F1 スコア 0.94 を達成した．カテゴリ C は Precision 0.80 と他のカテゴリと比較して低い．しかし，本来カテゴリ C であるチャンネルを他のカテゴリに誤分類したのは 1 件のみ（カテゴリ B に誤分類）であり，他のカテゴリのチャンネルをカテゴリ C に誤分類したのも 3 件にとどまる．したがって，この精度の低さはカテゴリ C の特性が判別困難であることを示すものではなく，サンプル数の少なさ（$n = 13$）による影響が大きいと考えられる．

表 4: カテゴリ別のチャンネル数およびメッセージ数

カテゴリ	チャンネル数	メッセージ数
A（CIA への侵害）	22,101	463,263,786
B（詐欺・偽造）	12,370	176,311,637
C（コンテンツ犯罪）	876	17,768,516
D（知財侵害）	6,326	79,010,180
E（複合的犯罪）	115	3,770,595
合計	**41,788**	**740,124,714**

6. 収集データセットの概要

6.1 探索過程

図 2 に，ホップ数に対するチャンネル発見数の推移を示す．上部は各ホップでの新規発見数（棒グラフ）と累積発見数（折れ線）を，下部は発見されたチャンネルのカテゴリ割合を示す．図中の区間は，P1 期間（ホップ 0–54），P2 期間（ホップ 55–133），P3 期間（ホップ 134–154）に対応する．

P1 期間（試験的探索）は発見数にばらつきが見られるが，P2 および P3 期間では安定した発見が継続している．154 ホップ時点でも新規発見が継続しており，エコシステムの規模が本研究の探索範囲を超えている可能性が示唆される．カテゴリ別の割合を見ると，全期間を通じてカテゴリ A が最も高い割合を維持している一方，良性チャンネルも一定割合存在しており，購読者の重複のみに基づく推薦機能の限界を示している．

図 3 に，Similar Channels の入力として使用したチャンネル（行）と，それにより発見されたチャンネル（列）のカテゴリ間関係を示す．同一カテゴリ内での発見（対角線上の値）が多い傾向にある一方，カテゴリ間の接続も多数存在する．特にカテゴリ A とカテゴリ B の間には強い相互接続が見られ，機密性・完全性・可用性への侵害に関するチャンネルと詐欺チャンネルの購読者層が重複していることを示している．

6.2 データセット規模

探索により 87,111 件のチャンネルを発見し，50,510 件が Malicious と判定された．最終的なデータセットは，収集期間中に最低 1 件のメッセージ投稿があった 41,788 件のチャンネルと約 7.4 億件のメッセージで構成される．

表 4 にカテゴリ別内訳を示す．カテゴリ A（機密性・完全性・可用性への侵害）が 52.9% と最多であり，不正アクセスや認証情報の窃取・売買に関連するチャンネルが大半を占める．次いでカテゴリ B（詐欺・偽造）が 29.6%，カテゴリ D（知財侵害）が 15.1% を占め，カテゴリ C（コンテンツ犯罪）およびカテゴリ E（複合的犯罪）は相対的に少数である．

7. サイバー犯罪エコシステムの分析

7.1 時系列的特性

図 4 に，カテゴリ別の月間メッセージ数の時系列推移を示す．全カテゴリにおいて 2022 年以降に活動が急増しており，

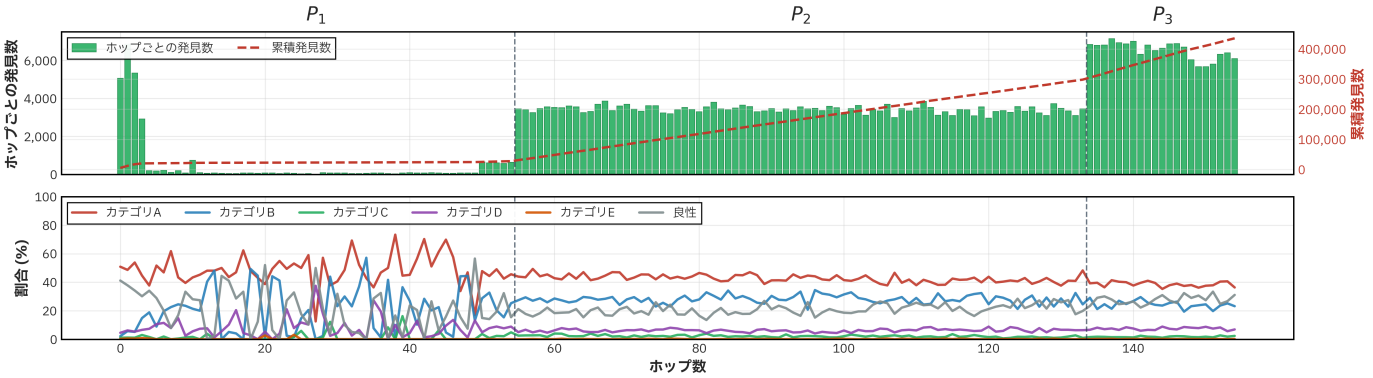

図 2: ホップごとのチャンネル発見数の推移．上部：各ホップでの発見数と累積発見数．下部：発見されたチャンネルのカテゴリ割合．

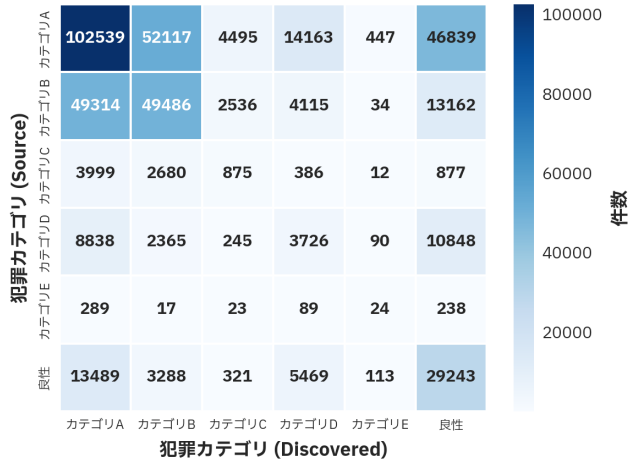

図 3: カテゴリ間の発見関係．行は入力チャンネル，列は発見チャンネルのカテゴリ．

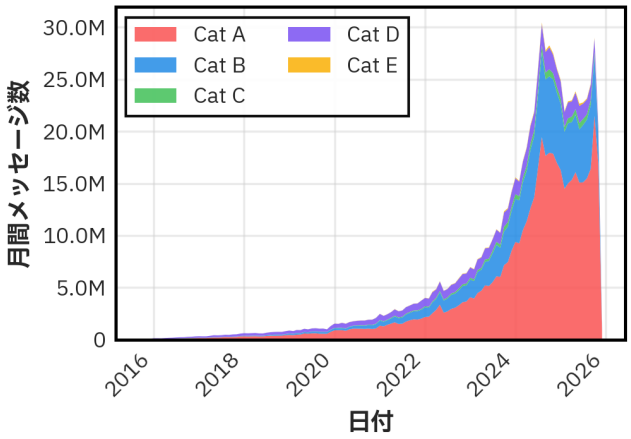

図 4: カテゴリ別の月間メッセージ数の時系列推移

特にカテゴリ A（CIA への侵害）の増加が顕著である．なお，本データセットは 2025 年 5 月以降に収集を開始したため，それ以前に過去に削除されたチャンネルのメッセージは含まれていない．この生存者バイアスにより，特に古い期間のメッセージ数は過小評価されている可能性がある．しかしながら，このバイアスを考慮しても 2022 年以降の増加傾向は明確であり，Telegram 上でのサイバー犯罪活動が急速に拡大していることを示している．

7.2 言語的特性

langdetect [17] を用いてメッセージの言語分布を分析した（表 5）．なお，複数の言語が混在するメッセージや，URL や絵文字のみで構成されるメッセージは言語判定が困難であるため，「不明（unknown）」が 10.4% を占めている．英語（29.0%）が最多であるが，ペルシャ語（22.4%）も高い割合を示しており，イラン地域における Telegram の普及率の高さを反映している．また，ポルトガル語，ドイツ語，アラビア語，ロシア語など 50 以上の言語が検出され，エコシステムの多言語性が確認された．図 5 にカテゴリ別の言語分布を示す．カテゴリ D（知的財産権の侵害）ではペルシャ語の割合が特に高く，イラン地域における海賊版コンテンツの流通が活発であることを示している．

表 5: メッセージの言語分布（上位 10 言語）

言語	コード	メッセージ数	割合 (%)
英語	en	214,279,432	29.0
ペルシャ語	fa	165,651,568	22.4
不明	unknown	77,081,143	10.4
ポルトガル語	pt	30,660,990	4.1
ドイツ語	de	30,378,779	4.1
アラビア語	ar	26,472,372	3.6
ロシア語	ru	20,538,763	2.8
ソマリ語	so	15,995,455	2.2
ベトナム語	vi	14,310,881	1.9
フランス語	fr	5,917,038	0.8

7.3 ネットワーク構造

ネットワーク構造の観点から，チャンネル間の接続数分布を分析した．大多数のチャンネルは接続数 100 件以下であるが，一部のチャンネルは 700 件以上の接続を持ち，ネットワーク内で「ハブ」として機能している．表 6 に接続数上位のチャンネルを示す．ハブチャンネルの多くは暗号資産コミュニティやプロキシサービスであり，特定の犯罪活動に特化するというよりも，多様なユーザー層を引きつけることで異なるカテゴリのチャンネル間をつなぐブリッジとして機能していると考えられる．

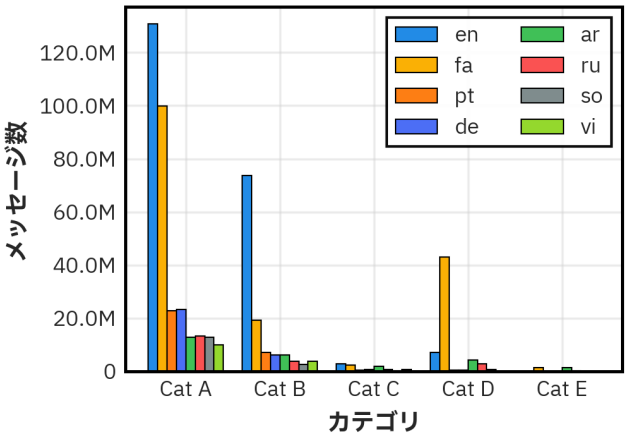

図 5: カテゴリ別の言語分布（上位言語）

表 6: 接続数上位のチャンネル

チャンネル名	カテゴリ	接続数	メッセージ数
DOGS Community	A	729	561
Whale Chanel	B	587	16,784
Proxy MTProto (2)	A	471	39,338
Blum: All Crypto	A	458	1,135
Yescoin	B	451	561
Notcoin Community	A	415	1,142

8. ケーススタディ：カテゴリ A の詳細分析

チャンネル数が最多のカテゴリ A（機密性・完全性・可用性への侵害）について，キーワード検索に基づくサブカテゴリ別分析を行った．カテゴリ A は全体の 52.9% を占め，サイバー犯罪エコシステムの中核をなすため，詳細な分析の対象とした．

Tsakalidis ら [11] のフレームワークに基づき，カテゴリ A は以下の 6 つのサブカテゴリを含む．違法アクセス（*A1*）：システムへの不正アクセスに関与する行為．違法データ取得（*A2*）：機密データの窃取を対象とする行為．違法傍受（*A3*）：通信の不正傍受を指す行為．データ妨害（*A4*）：データの改ざんまたは破壊に関与する行為．システム妨害（*A5*）：システムの機能を妨害する行為．デバイスの不正使用（*A6*）：サイバー犯罪のためのツールの作成，所持，または配布を指す行為．

各サブカテゴリを特徴付けるキーワード（サブカテゴリごとに約 50 語）を設計し，Elasticsearch で検索を行った．キーワードにはサイバー犯罪コミュニティで使用される用語や隠語（例：「fullz」「logs」「stealer」）を含め，キーワード間に最大 2 語が挟まるケースに対応するため slop パラメータを 2 に設定した．

図 6 に，サブカテゴリ別メッセージ数の時系列推移を示す．上部は月次推移，下部は 2022 年以降の週次推移である．

時系列分析から以下の知見が得られた．第一に，2022 年以降，全サブカテゴリで活動が急増しており，近年 Telegram がサイバー犯罪基盤として急速に浸透していることがうかがえる．第二に，違法データ取得（A2）が全期間を通じて他のサブカテゴリを大きく上回っている．これは，違法に収集された認証情報やクレジットカード情報の流通が Telegram 上で活発に行われていることを示している．第三に，週次データでは急激な増減が複数回発生しており，特に 2024 年後半に違法データ取得（A2）で顕著なスパイクが観測された．これは，大規模データリークの公開や無料サンプルの配布がトリガーとなるイベント駆動型の市場特性を示している．第四に，違法傍受（A3），データ妨害（A4），システム妨害（A5）は全期間を通じて相対的に低い水準にある．DDoS 攻撃の調整やランサムウェアの身代金交渉といった高リスク活動は，公開チャンネルでは観測されにくく，非公開グループで行われている可能性がある．

9. 考　　察

9.1 主要な知見の解釈

本研究の結果から，Telegram 上のサイバー犯罪エコシステムに関するいくつかの重要な知見が得られた．

第一に，全体の 52.9% を占めるカテゴリ A（機密性・完全性・可用性への侵害）では，窃取された認証情報の取引が最も活発であり，Telegram がその流通基盤として機能している実態が確認された．

第二に，言語分布の分析から，エコシステムが特定の地域に偏らず多言語・多地域にわたることが確認された．特にペルシャ語の高い割合（22.4%）は，イラン地域における Telegram の普及と，同地域でのサイバー犯罪活動の活発さを示唆している．カテゴリごとの言語的特徴の違いは，各犯罪類型が異なる地域コミュニティと結びついていることを示している．

第三に，ハブチャンネルの存在は，エコシステムが単なるチャンネルの集合ではなく，構造化されたネットワークとして機能していることを示している．これらのハブは，異なる犯罪カテゴリ間の情報流通を促進し，新規参入者がエコシステムにアクセスするための入口として機能している可能性がある．

9.2 制 限 事 項

本研究にはいくつかの制限が存在する．第一に，データ収集は 2025 年時点のスナップショットに基づいており，収集時点まで存続していたチャンネルに限定されるため，削除されたチャンネルは含まれない．第二に，発見メカニズムが Telegram の Similar Channels 機能に依存しており，シードセットから到達できない孤立したクラスタが存在する可能性がある．第三に，メディアファイルを除外したため，画像ベースの通信は分析対象外である．第四に，カテゴリ A のサブカテゴリ別分析は研究者が設計したキーワードに基づいており，隠語や新語を完全には捕捉できていない可能性がある．第五に，公開チャンネルに限定しているため，非公開グループで行われる実際の取引や機微な作戦調整は捉えられていない．

これらの制限への対処は今後の課題である．

10. 結　　論

本研究では，Telegram の類似チャンネル推薦機能と LLM を組み合わせたサイバー犯罪関連チャンネルの発見・分類シス

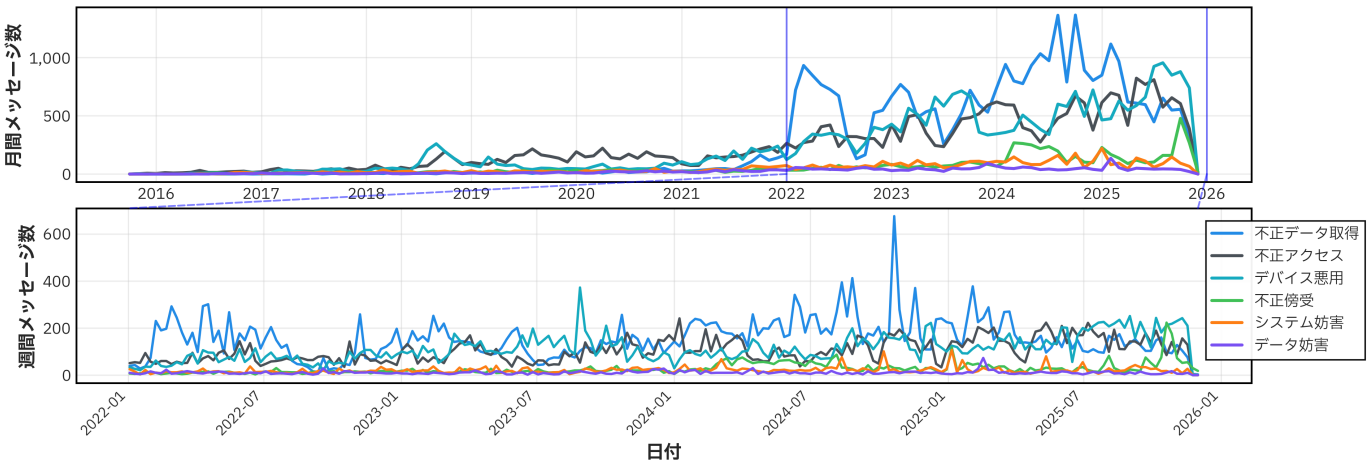

図 6: カテゴリ A のサブカテゴリ別メッセージ数の時系列推移．上部：月次，下部：週次（2022 年以降）．

テムを拡張し，大規模なデータセットの構築とエコシステムの構造分析を行った．

先行研究からの主な改善として，探索深度の大幅な拡大，最新 LLM の導入，および分類体系の刷新を行った．これにより，先行研究の約 50 倍に相当する 4 万件以上のサイバー犯罪関連チャンネルを収集し，本手法のスケーラビリティを実証した．また，悪性判定および犯罪カテゴリ分類において高い精度を達成した．

エコシステムの構造分析からは，機密性・完全性・可用性への侵害が最大のカテゴリであること，2022 年以降に活動が急増していること，および窃取された認証情報の取引が最も活発であることが明らかになった．また，異なる犯罪カテゴリ間の接続性，英語・ペルシャ語を中心とした多言語性，およびネットワーク内でブリッジとして機能するハブチャンネルの存在を解明した．これらの結果は，Telegram がサイバー犯罪の主要なインフラとして機能している実態を示している．

11. 倫理的考察

本研究は人間を対象とした調査や実験を伴わないが，収集データには個人識別情報や違法コンテンツが含まれる可能性がある．そのため，危害の最小化とプライバシー保護を優先し，以下の 3 つの点に配慮した方法論を採用した．

第一に，データ収集は公開チャンネルに限定した．これは当該チャンネルの情報が一般にアクセス可能であり，合理的なプライバシー期待が限定的であるためである．非公開の招待制グループへの参加や，偽の身分を用いた閉鎖的コミュニティへの潜入は行わなかった．

第二に，収集されたメッセージには機微情報が含まれる可能性があるため，すべての推論はローカル環境で実行し，サードパーティへのデータ送信を防いだ．また，収集したデータは多要素認証などの適切なセキュリティ対策を施した環境に保管している．

第三に，Telegram のサイバー犯罪エコシステムでは，マルウェアや児童性的虐待資料（CSAM）を含む違法コンテンツが流通している．研究者の安全を確保し，違法コンテンツの意図せぬ取得を防ぐため，メディアファイルおよびバイナリ添付ファイルは収集せず，テキストとメタデータのみを収集した．

謝辞：この成果の一部は，ＮＥＤＯ (国立研究開発法人新エネルギー・産業技術総合開発機構) の委託業務「経済安全保障重要技術育成プログラム／先進的サイバー防御機能・分析能力強化」（JPNP24003）の結果得られたものです．

文　献

[1] Telegram. Telegram messenger. https://telegram.org/.
[2] TGStat. TGStat. https://tgstat.com/.
[3] Telemetrio. Telemetrio. https://telemetr.io/.
[4] 青砥陸, インミンパパ, 吉岡克成. 類似チャンネル提示機能を活用した telegram におけるサイバー犯罪関連チャンネルの発見と分析. 電子情報通信学会技術研究報告, Vol. 124, No. 422, pp. 399–406, mar 2025.
[5] Telegram. Similar channels. https://core.telegram.org/api/recommend.
[6] Sayak Saha Roy, Elham Pourabbas Vafa, Kobra Khanmohammadi, and Shirin Nilizadeh. Darkgram: A large-scale analysis of cybercriminal activity channels on telegram, 2025.
[7] Massimo La Morgia, Alessandro Mei, Alberto Maria Mongardini, and Jie Wu. Pretending to be a vip! characterization and detection of fake and clone channels on telegram. *ACM Trans. Web*, Vol. 19, No. 2, 2025.
[8] Valeriia Lymishchenko, Eden Kamar, Ekaterina V. Botchkovar, and David Maimon. Comparative analysis of cyber fraud ecosystems: Telegram and dark web platforms in digital criminal landscapes, 2025. Available at SSRN: https://ssrn.com/abstract=5722747.
[9] Shafran Packeer and D.T.V Kannangara. Detection of pedophilia content online: A case study using telegram. *Iraqi Journal for Computer Science and Mathematics*, Vol. 3, No. 2, p. Article 7, 2022.
[10] Council of Europe, Budapest. *Convention on Cybercrime*, November 2001. European Treaty Series - No. 185.
[11] George Tsakalidis and Kostas Vergidis. A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 49, No. 4, pp. 710–729, 2019.
[12] An Yang and others (Qwen Team). Qwen3 technical report. Technical Report arXiv:2505.09388, Alibaba Cloud, 2025.
[13] Ollama. Ollama, 2023. https://ollama.com/.
[14] LonamiWebs. Telethon: Pure Python 3 MTProto API Telegram client library, 2016. https://github.com/LonamiWebs/Telethon.
[15] Elastic. Elasticsearch, 2010. https://www.elastic.co/elasticsearch.
[16] Jacob Cohen. A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, Vol. 20, pp. 37 – 46, 1960.
[17] Mimino666. langdetect. https://github.com/Mimino666/langdetect.