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

サイバー犯罪チャンネルに対するTelegramの規制措置のAPIを通じた観測と分析

馬場　大稀† 　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
††† 横浜国立大学大学院環境情報研究院/先端科学高等研究院
E-mail: †{baba-daiki-zj,aoto-riku-hx}@ynu.jp, ††{yinminn-papa-jp,yoshioka}@ynu.ac.jp

あらまし　Telegram はサイバー犯罪の主要な通信基盤となっているが，プラットフォームによる規制措置（モデレーション）がどのように行われているかは明らかでない．本研究では，49,343 件のサイバー犯罪関連公開チャンネルを対象に大規模な調査を実施し，Telegram API を通じて取得可能な「規制理由 **(restriction_reason)**」等の指標を分析した．分析の結果，API を通じて規制措置が執行されたメッセージが 1 件以上確認できたチャンネルはは全体の 7.02% にあたる 3466 チャネルだった．また，規制理由は特定のカテゴリに偏っており，サイバー犯罪関連活動が疑われるチャンネル群であるにもかかわらず，付与された理由の 9 割以上が著作権侵害（copyright）であり，サイバー犯罪（マルウェア，ハッキング，詐欺など）を理由とした規制については確認できなかった．さらに，同一のコンテンツであっても，利用するクライアントプラットフォームの種類（Android や iOS）に応じて，規制情報の表示の有無や提示される理由に差異が見られた．これらの結果を元に，本研究は大規模メッセージングプラットフォームにおけるサイバー犯罪ガバナンスと透明性に関する議論の基盤として貢献することを目指す．
キーワード　Telegram，サイバー犯罪，規制措置，コンテンツ規制措置，プラットフォーム，理由

API-Based Observation and Analysis of Telegram’s Moderation of Cybercrime Channels

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

Abstract　Telegram plays a central role in cybercrime-related communication, yet little is known about what moderation-related information is externally observable for such activity. We conduct a large-scale measurement study of 49,343 public cybercrime-related Telegram channels, focusing on moderation-related indicators returned by the Telegram API. We find that observable moderation signals are rare: only 7.02% of channels expose explicit moderation-related information. When visible, these indicators are highly concentrated in a small number of reason labels, dominated by copyright-related restrictions, and their visibility varies across client platforms. Our results show that only a limited and selective view of Telegram’s moderation is externally observable, highlighting important constraints on API-based measurement and transparency for cybercrime-related content.
Key words　Telegram, Cybercrime, Content Moderation, Moderation Visibility, Client Platform, Restriction Reason

1. はじめに

Telegram は，サイバー犯罪関連活動に関与するコミュニティを含む，さまざまなオンラインコミュニティにおいて広く利用されているメッセージングプラットフォームである．大規模な公開チャンネルの運用が容易であること，アカウント作成時の匿名性が高いこと，および高効率なメッセージ配信機構を備えていることは，オンライン詐欺やマルウェア配布，不正アクセス権の販売といった違法活動の調整・宣伝に有利な環境を提供している．その結果，Telegram は現代のサイバー犯罪エコシステムにおける重要なインフラの一つとなり，研究者，政策立案者，法執行機関からの関心を集めている [1], [2].

Telegram は，有害または違法なコンテンツに対して，ユーザからの通報および自動検出機構を組み合わせた規制措置を実施していると述べており，特に児童性的虐待コンテンツ（CSAM）やテロ関連コンテンツなど，一部のカテゴリについては，その実施状況の統計情報を透明性レポートとして公開している [3]. しかし，サイバー犯罪活動に対しては，どのような規制情報が外部に開示されるのか，また執行結果がチャンネルやメッセージ単位でどのように現れるのかについて，具体的な実態は明らかにされていない．この不透明性により，Telegram 上のサイバー犯罪関連コンテンツに対する規制措置を実証的に分析することが困難となっている．

先行研究では，Telegram 上のサイバー犯罪活動について，詐欺スキーム，Cybercrime-as-a-Service，アクセスブローカー，信頼構築手法などの観点から分析が進められており，Telegram がサイバー犯罪エコシステムの主要な調整・宣伝基盤として機能していることが明らかになっている．[2], [4]〜[6]．これらの研究は主に，コンテンツの発見，エコシステム構造，アクターの行動分析に焦点を当てており，規制措置については，チャンネルの消失やアクセス不能といった結果論的な指標に基づく推測に限定されていた．

このように，Telegram の公開インタフェースを通じて，どのような規制措置の関連情報が観測可能であり，それらがどのような形式で提供されているのかについては，十分な実証的理解が得られていない．このギャップを踏まえ，本研究では次の研究課題を設定する：**サイバー犯罪関連 *Telegram* チャンネルに関して，*Telegram API* を通じて観測可能な規制関連情報は何か．**

本研究では，上記の研究課題に答えるため，先行研究においてサイバー犯罪関連と特定された 49,343 件の公開 Telegram チャンネルを対象とした，大規模なチャンネルレベルの分析を行う [7]．具体的には，Telegram が規制の対象となったメッセージ 1 件ごとに付与する，API を通して取得可能な「規制理由 **(restriction_reason)**」のオブジェクトを分析対象とする．これらは，クライアントアプリケーションに規制情報を伝達するために設計されたものであり，API を通じて外部から直接観測できる．

分析の結果，主に三つの知見が得られた．第一に，規制措置関連の指標が観測されたチャンネルは全体の一部に限られており，49,343 件中 3,466 件（7.02%）のみであった．第二に，検出された規制理由は特定のカテゴリに偏っており，サイバー犯罪関連チャンネルであるにもかかわらず，著作権侵害を理由とする規制が支配的であった．第三に，同一のコンテンツであっても，Android や iOS といったクライアントプラットフォームのメタデータに応じて，規制措置関連の指標が付与されるか否かに明確な差異が存在し，ユーザーがシステムから表示されるメッセージを閲覧する際に，プラットフォームによって見え方に違いがあることが明らかとなった．

本研究は観察的な性質を持つものであり，Telegram における規制措置の判断の正確性や有効性を評価することを目的とするものではない．むしろ，プラットフォーム内部の規制措置全体ではなく，Telegram API を通じて外部から観測可能な規制措置関連の指標に基づき，規制措置の実態を体系的かつ実証的に特徴付けることを目的とする．本研究により，どのような規制関連情報が外部から把握可能であり，どのような情報が把握不可能であるのかを明確化し，将来の研究に向けた測定基準を提供するとともに，大規模メッセージングプラットフォームにおけるサイバー犯罪関連活動のガバナンスおよび透明性に関する議論に貢献する．

2. 関連研究

先行研究では，Telegram 上におけるサイバー犯罪活動について，違法サービスの提供形態，信頼形成メカニズム，およびエコシステム構造を中心に広く分析が行われてきた．これらの研究は，Telegram がサイバー犯罪における主要な調整・宣伝プラットフォームとして機能していることを示している一方で，プラットフォームによる規制がどのように行われ，その執行結果が外部にどのように提示されるかについては扱っていない [2], [4]〜[6].

一方，プラットフォームガバナンスや規制措置の透明性に関する研究では，利用規約や透明性レポートが実際の執行状況を十分に反映していないことが指摘されており，独立した測定の必要性が示されている [8], [9]．Telegram に関しても，公開されている透明性情報は限定的であり，外部からの実証的分析が求められている [3], [10].

Telegram における規制やガバナンスに言及する研究は存在するものの，多くはチャンネルの消失やアクセス不能といった間接的な指標に基づく推論にとどまっている [11], [12]．そのため，規制措置がどのような形で外部に表出するのか，また，どのような理由が付与されるのかについての体系的な理解は十分に得られていない．

これらの先行研究とは対照的に，本研究は Telegram API を通じて外部から観測可能な規制措置関連の指標を直接分析対象とする．間接的な推論に依存せず，プラットフォームが明示的に露出させている情報に基づいて，サイバー犯罪関連コンテンツに対する規制措置の可視性を大規模に調査し，特徴付ける．

3. 調査手法

本研究は，サイバー犯罪に関連する公開 Telegram チャンネルを対象とし，Telegram API を通じて外部から観測可能な規制措

置関連の指標に着目した分析を行う．本研究は観察的な性質を持つものであり，Telegram における規制措置の判断の正確性，有効性，あるいは公平性を評価することを目的とするものではない．分析はすべて，公開 API を通じて取得可能なデータのみに基づいて実施する．

分析は二つの粒度で行う．まずメッセージ単位において，API から返却される規制措置関連の指標を特定する．次にそれらをチャンネル単位に集約し，各チャンネルにおいて，どのような規制関連情報が API によって表出されているかを分析する．

3.1 データセット

本研究では，青砥らの先行研究において構築された，サイバー犯罪関連の公開 Telegram チャンネルのデータセットを用いる [7]．当該データセットは，手動で検証されたシードチャンネルを起点とし，Telegram の類似チャンネル推薦機能と LLM を用いたフィルタリングを組み合わせることで 50,510 件の公開チャンネルをサイバー犯罪関連として特定したものである．

本データセットに含まれるメッセージは，2015 年 9 月から 2025 年 12 月までの期間に投稿されたものであり，2025 年 5 月から 12 月にかけて Telegram API を通じて収集された．これら 50,510 件の公開チャンネルから取得された公開メッセージの総数は，798,097,185 件に及ぶ．

先行研究におけるデータ収集過程において，Telegram API から取得された各メッセージには，`restriction_reason` フィールドを含む規制措置関連の指標がすでに付与されている．本研究では，これら既存の指標を分析対象とし，新たなチャンネル発見，追加のデータ収集，あるいはコンテンツ分類は行わない．

さらに，テキストメッセージを含まないチャンネルを除外し，最終的に 49,343 件の公開チャンネルに投稿された 794,475,665 件のメッセージを，本研究の分析対象とする．

3.2 規制措置関連の指標

Telegram 上のメッセージが規制措置の対象となった場合，Telegram API は，当該メッセージに関連付けられた `restriction_reason` オブジェクトを返すことがある．本研究では，Telegram API により返却される空でない `restriction_reason` オブジェクトを，メッセージレベルで表出する規制措置関連の指標として扱う．これらは API を通じて外部から直接観測可能な測定対象である．

各 `restriction_reason` オブジェクトには，(i) 制限理由を示すカテゴリラベル，(ii) 制限が適用されるクライアントプラットフォームを示すメタデータ，(iii) ユーザに表示されるシステムが生成した説明文が含まれる．これらの指標は，プラットフォーム内部の判断基準や執行ロジックを明らかにするものではなく，あくまで API を通じてユーザに提示される情報に限定される．

なお，一つのメッセージに複数の `restriction_reason` オブジェクトが付与されている場合には，各オブジェクトを独立した規制措置関連の指標として扱う．また，本研究で観測される規制措置関連の指標は，メッセージの完全な削除やチャンネルの閉鎖を必ずしも意味するものではなく，特定のクライアントプラットフォームにおける閲覧制限など，部分的または表示依存の規制措置を反映している可能性がある．

3.3 チャンネル単位での集約

チャンネル単位の分析では，観測期間中に，当該チャンネル内の少なくとも一つのメッセージに規制措置関連の指標が確認された場合，そのチャンネルは規制措置関連の指標を含むものとみなす．この集約は，未観測の規制措置やプラットフォーム内部の執行を推論することを目的とするものではなく，あくまで API を利用して観測可能な情報に基づき，チャンネル単位での可視性を特付けるための判定方法を定義するものである．

3.4 分析の観点

本研究では，**「サイバー犯罪関連 *Telegram* チャンネルに関して，*Telegram API* を通じてどのような規制関連情報が観測可能であるか」**という研究課題に答えるため，以下の三つの観点から分析を行う．

第一に，規制措置関連の指標が観測されるチャンネルの割合を算出し，規制措置がどの程度執行されているのか，API で取得できる情報からを定量的に把握する．第二に，観測された規制措置関連の指標に付与された理由ラベルの分布を分析し，どのような規制理由が外部から確認可能であるかを明らかにする．第三に，`restriction_reason` オブジェクトに含まれるクライアントプラットフォームのメタデータを用い，規制措置の表示の有無や提示される理由がクライアントプラットフォーム間でどのように異なるかを分析する．

4. 分析結果

本節では，第 3. 節で示した三つの分析観点に基づき，本研究の分析結果を報告する．以下の結果はすべて，Telegram API を通じて外部から観測可能な規制措置関連の指標のみに基づき，結果の信頼性は API から得られるデータの信頼性に依存するものである．

4.1 規制措置関連の指標が存在する割合

まず，規制措置関連の指標が，チャンネル単位およびメッセージ単位でどの程度外部から観測可能であるかを定量的に評価する．第 3. 節で定義した通り，Telegram API から取得されたメッセージのうち，少なくとも一つのメッセージに空でない `restriction_reason` フィールドが含まれる場合，当該チャンネルを「規制措置関連の指標が観測されるチャンネル」とみなす．

分析対象とした 49,343 件のサイバー犯罪関連公開 Telegram チャンネルのうち，3,466 件（**7.02%**）のチャンネルで，少なくとも一つの規制措置関連の指標が観測された．一方で，残りの **92.98%** のチャンネルでは，観測期間中に API を通じて規制措置は確認されなかった．この結果は，サイバー犯罪関連チャンネルのうち，外部から観測可能な形で規制措置が表出しているのは一部に限られることを示している．

メッセージ単位で見ると，本データセットには合計 794,475,665 件のメッセージが含まれており，そのうち 1,650,738 件に規制措置関連の指標が付与されていた．すなわち，規制措置関連の指標は一定数のチャンネルで観測されるものの，全体のメッセージに占める割合は極めて小さいことが分かる．

さらに，規制措置関連の指標が観測されたチャンネルにおいて，その出現数の分布を分析した．表 1 は，チャンネル単位で観測された規制措置関連の指標の出現数分布を示している．

表 1　表出した規制措置関連の指標の分布（チャンネル単位）

規制措置関連の指標数	チャンネルの割合
1 件	31.00%
2–5 件	29.62%
6–10 件	10.82%
10 件超	28.56%

約 **31%** のチャンネルでは指標の出現が 1 件のみにとどまる一方で，**28.56%** のチャンネルでは 10 件を超える指標が観測された．この偏った分布は，API を通じて観測される規制措置関連の指標が，サイバー犯罪関連 Telegram エコシステム全体に一様に分布しているのではなく，特定のチャンネル群に集中して表出していることを示唆している．

4.2　規制措置関連の指標に付与される理由ラベルの分布

次に，観測された規制措置関連の指標に付与された理由ラベルの分布を分析する．各指標について，対応する `restriction_reason` オブジェクトから，プラットフォームにより割り当てられた理由ラベルを抽出した．

その結果，観測されたすべての規制措置関連の指標において，合計 9 種類の異なる理由ラベルが確認された．図 1 は，これらの理由ラベルの分布を示している．

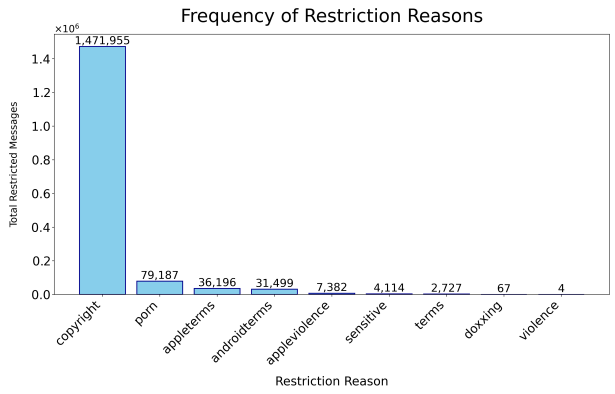

図 1　Telegram API を通じて観測された規制措置関連の指標に付与された理由ラベルの分布

分析の結果，理由ラベルは少数のカテゴリに強く集中していることが明らかとなった．特に，`copyright` は全体の **90.13%** を占めており，最も頻繁に観測される理由ラベルであった．次いで，`porn`（**4.85%**），`appleterms`（**2.22%**），`androidterms`（**1.93%**）が続き，それ以外の理由ラベルはいずれも個別には **0.5%** 未満であった．このようにサイバー犯罪関連チャンネルを分析対象としているにも関わらず，サイバー犯罪に関わる理由での規制措置は確認できなかった．

ここで強調すべき点として，本結果はあくまで Telegram API を通じて外部から観測可能な理由ラベルの分布を示すものである．これは，Telegram プラットフォーム内部で実際に行われている規制措置全体を反映するものではなく，特定のコンテンツカテゴリが一般的により頻繁に規制されていることを意味するものでもない．本分析は，API を通じて規制措置が観測される場合に，どのような理由がユーザや外部観測者に提示されるのかを特徴付けるものである．

4.3　クライアントプラットフォーム別の規制措置関連の指標の可視性

最後に，規制措置関連の指標の可視性が，クライアントプラットフォーム間でどのように異なるかを分析する．本研究の測定は Telegram API のみを用いて実施しているが，各 `restriction_reason` オブジェクトには，当該制限が適用されるクライアントプラットフォームを示す `platform` フィールドが含まれている．したがって，本分析は，測定手法やアクセス経路の違いではなく，API を通じて明示的に露出される「プラットフォーム別の可視性」の差異を捉えるものである．

観測された規制措置関連の指標の大半は，全クライアントプラットフォーム共通して観測されるものであった．具体的には，全指標のうち 1,439,446 件（**88.1%**）が，`all` として，全プラットフォームに適用されるものとして記録されていた．一方で，iOS 向けとして適用される指標は 131,857 件（**8.1%**），Android のみに適用される指標は 61,825 件（**3.8%**）であった．その他のプラットフォームに関連付けられた指標は，ごく少数にとどまった．

さらに，一部の理由ラベルは特定のプラットフォームにのみ対応していることが確認された．例えば，`appleterms` は iOS 向けの制限にのみ現れ，`androidterms` は Android 向けの制限にのみ観測された．この結果は，規制措置関連の指標の外部可視性が，クライアントプラットフォーム固有のメタデータに依存して変化し得ることを示している．

重要な点として，本分析が明らかにするのは，規制措置判断そのものの違いではなく，**規制措置結果がどのように *API* を通じて観測されるか**という点である．観測された差異は，Telegram 内部の執行方針や判断基準の違いを直接示すものではなく，異なるクライアントプラットフォームを通じて，どのような情報がユーザに提示されるかの違いを反映したものである．

5.　考　　察

本研究は，Telegram API を通じて，サイバー犯罪関連 Telegram チャンネルに対する規制措置の分析を行った．

5.1　API により観測できる規制措置の限界

分析対象となったサイバー犯罪関連チャンネルのうち，規制措置関連の指標が確認されたのは 7.02% にとどまり，残りの 92.98% のチャンネルでは，観測期間中に API を通じた規制関連情報は確認されなかった．

ただし，これは Telegram における規制措置が限定的であることを意味するものではない．本研究で観測できるのは，API を通じて明示的に表出する規制措置結果に限られており，メッセージの完全削除，チャンネルの閉鎖，あるいは内部的な制限措置など，Telegram の API による観測では認識できない規制措置が行われている可能性がある．

5.2 API を通じて観測された規制措置の集中と偏り

規制措置関連の指標が観測されたチャンネルに限定して見ると，その出現分布は一様ではなく，大きく偏っていることが分かる．約 3 分の 1 のチャンネルでは，観測された指標は 1 件のみであった一方，10 件を超える指標が確認されたチャンネルも同程度の割合で存在していた．

この結果は，API を通じて観測される規制措置が，サイバー犯罪関連チャンネル全体に均等に分布しているのではなく，特定のチャンネル群に集中していることを示唆している．ただし，前述の通り本研究は API 上に表出する情報のみを対象としているため，この偏りを執行強度や優先順位の違いとして解釈することはできない．

5.3 API を通じて観測される規制理由の特徴

観測された規制措置関連の指標に付与された理由ラベルの分布を見ると，`copyright` が全体の 90% 以上を占めており，API を通じて観測される規制理由が少数のカテゴリに強く集中していることが明らかとなった．一方で，その他の理由ラベルは相対的にごく少数であった．

この分布は，Telegram における規制措置全体の優先順位や執行方針を反映したものではなく，あくまで，どのような規制理由が API を通じてユーザや外部の観察者に提示されやすいかを示しているに過ぎない．特に，著作権関連の規制は理由ラベルの標準化やユーザ向け表示が進んでいる可能性があり，その結果として API 上でも表出しやすいと考えられる．一方で，詐欺やマルウェアなどのサイバー犯罪関連行為に対する執行は，異なる形態で実施され，必ずしも API 上に理由として表出しない可能性がある．

この点は，API 上の理由ラベルを用いてプラットフォームの規制措置方針や重点分野を推定することの限界を示している．

5.4 プラットフォームに依存した可視性の差異

本研究では，`restriction_reason` オブジェクトに含まれるプラットフォームメタデータを分析することで，規制措置関連の指標の出現頻度がクライアントプラットフォーム間でどのように異なるかを検討した．測定自体は Telegram API を通じて一貫して実施されているが，当該メタデータは，どのクライアント環境に対して規制情報が提示されることを想定しているかを示すものである．

その結果，大半の規制措置関連の指標は全プラットフォーム共通として表出している一方で，iOS または Android に限定して観測される指標も一定数存在することが確認された．また，`appleterms` や `androidterms` といった理由ラベルが，特定のプラットフォームにのみ関連付けられていることから，API を通じた規制関連情報の外部への表出がプラットフォーム固有の仕様に依存していることが示された．

これらの差異が規制措置判断そのものの違いを意味するものではない点である．本研究が捉えているのは，同一の執行結果がユーザにどのように提示されるかという**プラットフォームごと見え方の違い**であり，Telegram 内部で実行されている規制措置全体を反映するものではない．

5.5 測定研究および透明性に対する示唆

本研究の結果は，Telegram API を通じて観測可能な規制措置関連の指標が，プラットフォームガバナンスの一側面のみを部分的に表していることを示している．これらの指標は，特定の規制措置結果がどのように外部に提示されているかを理解する上では有用であるが，サイバー犯罪関連コンテンツに対する執行全体を網羅的に把握することはできない．

研究者にとっては，API に基づく測定結果を解釈する際に，観測可能な信号と観測不可能な執行の存在を明確に区別する必要があることを示唆している．また，プラットフォームの透明性やガバナンスを議論する観点からも，API レベルで露出する情報のみでは，規制措置の全体像を評価するには不十分である可能性がある．

本研究は，Telegram における規制措置の妥当性や有効性を評価するものではない．その代わりに，外部から観測可能な規制関連情報の範囲と構造を明確化することで，将来の測定研究における前提条件と制約を整理し，大規模メッセージングプラットフォームにおけるサイバー犯罪ガバナンスと透明性に関する議論の基盤を提供するものである．

6. 結　　論

本研究では，サイバー犯罪関連 Telegram チャンネルを対象として，Telegram API を通じて外部から観測可能な規制措置関連の指標を体系的に分析した．その結果，規制関連情報が API によって観測されるのは，チャンネルおよびメッセージ全体の中でも限定的であり，観測される規制理由には大きな偏りが存在すること，確認できた少数の規制理由の中にサイバー犯罪関連（マルウェア，詐欺など）の理由が含まれていないことを明らかにした．また，クライアントプラットフォームに依存して，規制措置関連の指標の見え方が異なることを実証的に示した．

7. 倫理的配慮

本研究は，公開されている Telegram チャンネルからの公開アクセス可能なデータのみを分析対象としており，ユーザーとの接触，コンテンツの注入，欺瞞行為，あるいはアカウントの新規作成などは一切行っていない．プライベートメッセージ，非公開グループ，または個人を特定できる情報（PII）の収集および分析も含まれていない．すべての分析結果は統計的に集計された形で報告され，個別のユーザーやチャンネルが特定されることはない．

本研究は，チャンネル運営者や参加者の意図や責任を判断するものではない．本研究の分析は，客観的に観察可能な規制信号およびプラットフォームレベルの挙動に限定されている．

なお，本調査で使用したデータセットの収集および API の利用については，先行研究 [7] および Telegram API の利用規約 [13] に準拠して実施した．

謝辞：本発表は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）の委託事業「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）

によるものである．

文　　献

[1] Europol. Internet organised crime threat assessment (iocta) 2024. Technical report, European Union Agency for Law Enforcement Cooperation, 2024.

[2] Anupam Roy, Paulo Shakarian, and Jana Shakarian. Darkgram: A large-scale analysis of cybercriminal activity channels on telegram. In *Proceedings of the USENIX Security Symposium*, 2025. To appear, https://www.usenix.org/conference/usenixsecurity25/presentation/roy.

[3] Telegram. Telegram transparency reports. https://telegram.org/moderation, 2024.

[4] 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. *SSRN Electronic Journal*, 2025. doi: 10.2139/ssrn.5722747.

[5] Roy Ricaldi, Tina Marjanov, Alice Hutchings, and Luca Allodi. Uncovering the trust signals supporting telegram's cybercrime economy. In *Proceedings of the APWG Symposium on Electronic Crime Research (eCrime)*, 2025.

[6] Adriana Radu. From trust to trade: Analyzing how telegram facilitates cybercriminal activities. Master's thesis, Eindhoven University of Technology, 2024.

[7] 青砥陸, インミンパパ, 吉岡克成. 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. CSS2026 予稿集 (ICSS 研究会), 2026.

[8] Gintarė Gulevičiūtė, Monika Mačiulienė, Aelita Skaržauskienė, Asta Zelenkauskaitė, and Aistė Diržytė. A comparative analysis of content moderation guidelines. *Journal of Digital Media & Policy*, 2024. Mykolas Romeris University, Lithuania.

[9] A. Trujillo, T Fagni, and S Cresci. The dsa transparency database: Auditing self-reported moderation actions by social media. *Proceedings of the ACM on Human-Computer Interaction*, Vol. 9, No. CSCW1, pp. 1–28, 2025.

[10] Gautam Kishore Shahi, Benedetta Tessa, Amaury Trujillo, and Stefano Cresci. A year of the dsa transparency database: What it (does not) reveal about platform moderation. *arXiv preprint arXiv:2504.06976*, 2025. Analyzing the limitations of the DSA Statement of Reasons (SoR) database.

[11] Anh V. Vu, Daniel R. Thomas, Ben Collier, Alice Hutchings, Richard Clayton, and Ross Anderson. Getting bored of cyberwar: Exploring the role of low-level cybercrime actors in the russia-ukraine conflict. In *Proceedings of the ACM Web Conference 2024 (WWW '24)*, 2024.

[12] Tom Willaert, Stijn Peeters, Jasmin Seijbel, and Nathalie Van Raemdonck. Disinformation networks: A quali-quantitative investigation of antagonistic dutch-speaking telegram channels. *First Monday*, Vol. 27, No. 9, 2022.

[13] Telegram. Telegram api development. https://core.telegram.org/, 2025.