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

信学技報
TECHNICAL REPORT OF IEICE.

複数のSNSを悪用したオンライン詐欺の観測に向けた検討

川口　大翔† 　高田　一樹†† 　インミンパパ† 　田辺　瑠偉††† 吉岡　克成†
松本　勉†

† 横浜国立大学
†† 株式会社セキュアブレイン
E-mail: †kawaguchi-yamato-jc@ynu.jp

あらまし　SNS の利用者数の増加に伴い、SNS を経由したオンライン詐欺が報告されている。本研究では、短文投稿型の SNS を入口としてメッセージ型の SNS のアカウントに誘導し、個別の連絡で不審なサイトや送金処理を促すオンライン詐欺の可能性がある活動を観測するシステムを構築し、誘導メッセージ、入り口となる SNS アカウント、利用された決済代行サービス、背後にある不審サイトの情報を収集した結果を報告する。また、これらの情報から抽出された不審な活動に関わる情報に基づき、当該活動に関係する被害情報を収集した。
キーワード　SNS，オンライン詐欺

Towards observation of online fraud exploiting multiple SNS

Yamato KAWAGUCHI†, Kazuki TAKADA††, Yin MINN PA PA†, Rui TANABE†††, Katsunari YOSHIOKA†, and Tsutomu MATSUMOTO†

† Yokohama National University
†† SecureBrain Corporation
E-mail: †kawaguchi-yamato-jc@ynu.jp

Abstract　SNS (Social Networking Service) fraud has been reported in accordance with the increase in SNS users. In this study, we monitor fraudulent SNS posts that attract the victims contact to attacker’s SNS messaging accounts and finally lead them to scam sites, and fall into money transfer fraud. We will report our findings on fraudulent SNS posts, attacker’s SNS messaging and abused payment services, related scam sites and damage based on our suspicious activity indicators.
Key words　SNS, Online Fraud

1. はじめに

ITC 総研の調査 [1] によると，日本における SNS の利用者数は増加傾向にあり，2022 年度は 8,270 万人に達するとされている．それに伴い SNS を悪用したオンライン詐欺が発生しており，SNS 事業者の対策にも関わらず，被害件数は増加している [2]．本研究では，誰でも閲覧可能な短文投稿型 SNS 上に大量の投稿を行うことで多くの閲覧者の注意を惹き，メッセージ型 SNS の組織用アカウントに誘導することで外部からの監視がされにくい連絡手段を確保し，様々な理由で支払いを要求したり，個人情報を収集する事例について調査を行い，その結果に基づき同様の事例群を効率的に観測，収集する方法を提案する．

提案手法では，短文投稿型 SNS 上で “高額バイト”等のクエリで検索を行い，投稿文の収集を行う．次にマッチした投稿から誘導されるメッセージ型 SNS の組織用アカウントに登録を行うことで当該アカウントからメッセージを受信する．さらに，受信したメッセージのリンクを探索し不審なサイトの情報を取得する．一部のサイトでは電話番号等の情報の入力を促されるため，調査用の番号を入力し，電話や SMS を受信する．このように多段階で行われる誘導を観測することでその実態を明らかにする．

まず事前調査として，“高額バイト”を検索クエリとして短文投稿型 SNS の投稿を収集し，個別連絡への誘導を分析した結果，短文投稿型 SNS のダイレクトメッセージ機能やメッセージ型 SNS に誘導する投稿を多く確認した．そのうち，メッセージ型 SNS への誘導がオンライン詐欺に関連する疑いが確認されたため詳細な調査を行った．次に，短文投稿型 SNS から誘導されたメッセージ型 SNS を名前や内容からいくつかのグループに分けたところ，特徴的なグループがあることを発見した．また，メッセージ型 SNS の組織用アカウントの登録地域，友だ

ち数の推移，短文投稿型 SNS から登録したアカウントを調査したところ，詐欺の疑いのあるサイトへ誘導するアカウントに特徴があることがわかった．最後に，収集した URL の調査を行ったところ，メールサービスを模したサイトの決済方法や被害情報などの実態を明らかにした．

提案手法により，2022 年 9 月 13 日から 133 日間に渡り情報収集を行った結果，短文投稿型 SNS から登録したメッセージ型 SNS の組織用アカウントと，そのアカウントから紹介された組織用アカウントの中に，通常使用される組織用アカウントと比べて明らかに多くの別アカウントを紹介しているものがあるとわかった．この関係性を観測することによって，詐欺の疑いのあるサイトへ誘導するアカウントを発見できると期待される．

2. 関 連 研 究

SNS のセキュリティに関する研究として，スパムの検知手法やスパムフィルタの構築に関する研究が報告されている．その中には SNS 上のリンクをもとにスパム検知を行う論文がある．論文 [3] では，Twitter に投稿された 2500 万件を検査した結果，そのうちの 8% が既にブラックリストに掲載されていたことを明らかにした．ただし，Twitter 上の URL をブロックリストでフィルタリングしたとしても，リスト登録前に 90% 以上のユーザがアクセスしてしまうと指摘している．論文 [4] では，Twitter を含む短縮 URL について調査を行い，クリックのトラフィック情報に基づいてスパムと非スパムの分類を行った．論文 [5] では，Twitter において悪質な URL のリダイレクトに相関性があると考え，その情報をもとにスパム検知を行っている．本研究では従来と異なり複数の SNS を経由した事例を収集，分析する．

3. 事 前 調 査

本節では，短文投稿型 SNS 上の誰でも閲覧可能な投稿により閲覧者の興味を引き，個別の連絡に誘導する手段について事前調査を行った結果を示す．事前調査では 2022/12/15-2023/1/29 の期間において，ある短文投稿型 SNS 上で “高額バイト”をクエリとして検索した際にヒットした 34,734 件の投稿における個別連絡への誘導の状況を調査した．個別連絡への誘導方法としては，同 SNS のダイレクトメッセージ機能の利用や他の SNS への誘導が考えられる．前者については，34,734 件のうち，誘導を示唆する “DM”という文字列を含む投稿が 13,484 件検出され，その内容をランダムに 100 件確認したところ，そのうち 92 件がダイレクトメッセージによる連絡を指示するものだった．また，3 種類のメッセージ型 SNS(便宜的にサービス A, B と呼ぶ) について各 SNS アカウントへの招待リンクを提示する方法による誘導が，サービス A は 4,246 件，サービス B は 8 件発見された．これらは多くの収入が得られるといった内容の文章や画像と共に提示され，閲覧者の興味を引く工夫が見られた．

次に誘導後の実態を把握するため，2023/2/9 に短文投稿型 SNS で “高額バイト”と検索し，ヒットした投稿からダイレクトメッセージ機能に誘導するものを 10 件ランダムに選び，ダイレクトメッセージ機能で仕事の詳細を尋ねる連絡を行った．そのうち 5 件のアカウントから仕事の詳細について返信が届き，いずれも違法と思われる仕事内容であった．また，8 件からは匿名性の高いメッセージ型 SNS での連絡の指示が届いた．本研究では閲覧者を騙す詐欺行為を調査対象としているため，違法な仕事への勧誘を目的としていることが予想されるダイレクトメッセージによる誘導は調査対象から除外することとした．一方，メッセージ型 SNS であるサービス A へと誘導する投稿について，誘導に従って実際にメッセージ型 SNS の組織用アカウントを登録したところ，最終的に詐欺の疑いのあるサイトへと誘導される事例が多数確認された．以降はこの短文投稿型 SNS からサービス A に誘導するケースを調査対象とし，その詳細を説明する．

4. 詐欺の疑いのあるサイトへの誘導

図 1 に事前調査により明らかになった，詐欺の疑いのあるサイトへの複数の SNS を悪用した誘導の全体像を示す．誘導は，短文投稿型 SNS からメッセージ型 SNS への誘導，メッセージ型 SNS の組織用アカウントを複数登録，メッセージ型 SNS から詐欺の疑いのあるサイトへの誘導の手順で行われる．

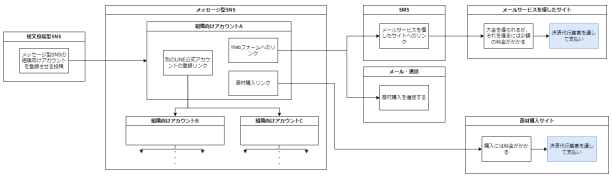

図 1　詐欺の疑いのあるサイトへの誘導の全体像

まず，短文投稿型 SNS のユーザをメッセージ型 SNS に誘導する．ユーザが短文投稿型 SNS で “高額バイト”など特定のクエリで検索すると，詳しい情報を得るためにメッセージ型 SNS の組織用アカウントを登録するように促される．投稿には，多額の金銭が容易に得られるといったように閲覧者の興味を引く内容のメッセージや画像が含まれる場合が多く，メッセージ型 SNS アカウントの招待リンクが含まれる．メッセージ型 SNS の組織用アカウントに登録すると自動でメッセージが届く．メッセージには他の組織用アカウントの登録を促すものがあり前述と同様に閲覧者の興味を引く内容や画像になっていることが多い．このような誘導が繰り返され，閲覧者はメッセージ型 SNS の複数の組織用アカウントに登録することとなる．

登録した組織用アカウントからは，商材購入サイトへ誘導するメッセージ，名前や電話番号などの入力フォームへ誘導するメッセージが届く．これらのサイトでは登録料や手数料等の支払いが要求されるが後述の通り，支払いを行ってもサービスや商材等が提供されないという被害者情報があり，詐欺の疑いがある．なお，入力フォームに名前や電話番号などを入力した場合には，直接電話が掛かったり，SMS による商材購入サイトやメールサービスを模したサイトへの誘導メッセージが届く．

5. 調 査 手 法

3 章で説明した詐欺の疑いのあるサイトへの誘導に関連する，

短文投稿型 SNS，メッセージ型 SNS，Web サイトの URL，通話情報，SMS 情報の 5 項目の情報収集を行う観測システムを構築した．図 2 に全体像を示す．

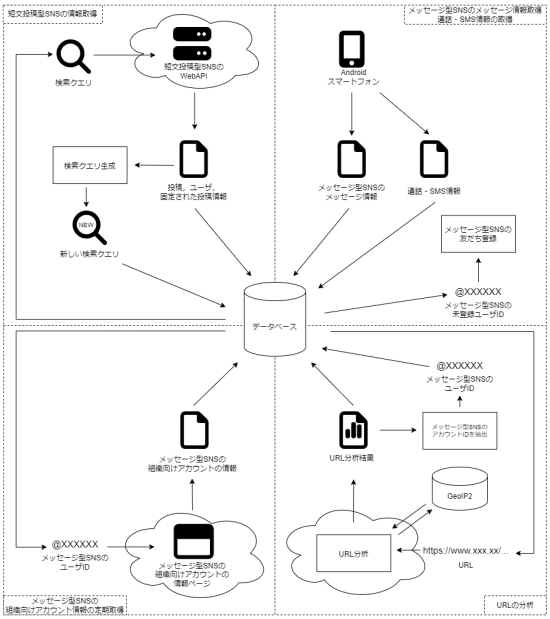

図 2　詐欺の疑いのあるサイトへの誘導の調査手法の全体像

5.1　短文投稿型 SNS の調査

短文投稿型 SNS の情報を自動的に収集するために，同サービスが提供している WebAPI を利用する．この API では “高額バイト”のような検索クエリを使って投稿を検索できる．ヒットした投稿のユーザ情報，プロフィール画面等の情報も併せて取得する．

さらに多くの投稿を収集するために，取得した投稿本文，ユーザのプロフィール，登録したメッセージ型 SNS のアカウント名において出現頻度の高い名詞を抽出し，それらを手動で組み合わせて新しい検索クエリを生成する．生成した検索クエリを使って検索し，メッセージ型 SNS に繋がるリンクの件数が多いものを定期検索クエリとして登録する．

5.2　メッセージ型 SNS の調査

本調査の対象であるメッセージ型 SNS にはメッセージを取得する API がないため，自動的な情報収集が難しい．そこで，Android 実機にこのメッセージ型 SNS のアプリをインストールし，PC から Android 端末を操作するツールである Android Debug Bridge (以下，adb という．) [6] と，Android アプリの UI テストフレームワークである UI Automator [7] を利用してアプリを自動で操作する．

メッセージ型 SNS で受け取るメッセージにはいくつか種類があるため，それぞれ表 1 の内容を取得する．

メッセージが Web サイトへのリンクを有する場合は URL を，メッセージ型 SNS アカウントの登録画面や情報リクエスト画面へのリンクの場合は，アカウント情報をそれぞれ取得する．リンク先の Web サイトが氏名や携帯電話等の入力フォームになっている場合は手動で調査用の電話番号等の情報を入力する．

表 1　メッセージの種類と取得内容

種類	取得内容
通常のメッセージ	本文，送信者，送信日時
リンクを持つ画像	リンク情報，送信日時
リンクを持たない画像	送信日時
画像とリンク	本文，リンク情報，送信日時
選択メッセージ	本文，選択肢，送信日時

次節の URL の情報収集によってメッセージ型 SNS の組織用アカウントの ID を得られた場合，その ID の組織用アカウントをメッセージ型 SNS のアプリ内で登録する．

自動的に公式アカウントの登録ユーザ数の情報を取得するために，トーク情報の取得とは別に，Web 上にあるメッセージ型 SNS の組織用アカウント情報のページから登録ユーザ数を 1 時間ごとに取得する．

5.3　Web サイトの情報収集

5.1 節と 5.2 節で取得した各 SNS の情報から Web サイトの URL を抽出する．抽出した URL に selenium [8] を使ってアクセスし，Web サイトの情報を取得する．

取得する内容を表 2 に示す．まず，メッセージ型 SNS から取得した URL はリダイレクトするものが多いため，リダイレクトの経路とリダイレクト後の URL を取得する．URL が示す Web サイトは時間が経つとアクセスできなくなるものがあるため，HTML もあわせて取得する．また Web サーバの IP アドレスや AS 番号などのホスト情報も取得する．本研究では，ホスト情報の取得に MAXMIND 社の GeoIP2 [9] を用いた．次に，Web サイトが何を目的としているかを判断するために，ページの種類を特定するための特徴情報を HTML から取得する．この情報を使って後述する 9 種類の目的に分類する．最後に，Web サイトがオンライン上で報告されていることがあるので，Google 検索で Web サイトのタイトルを検索し，1 ページ目の検索結果を取得する．Web ページ内の a タグから取得されるリンク先の情報は 1 段階まで取得する．

表 2　URL から収集する情報

収集項目	取得内容
ページ情報	リダイレクト後の URL，ステータスコード リダイレクト経路，HTML
ホスト情報	IP アドレス，AS 番号，管理組織名 登録されている国，緯度経度
ページの種類を特定するための特徴情報	input タグの種類，値段，銀行口座， 電話番号，メールアドレス，リンク先の URL， 電話番号のリンク，メールアドレスのリンク， メッセージ型 SNS のアカウント登録リンク
外部情報	Google 検索結果
リンクの情報	1 段階までのリンク先の情報
その他	収集日時

本調査では Web サイトを 9 種類に区別する．1 つ目はメッセージ型 SNS の招待リンクであり，当該サイトとリンク先のサイト内に，メッセージ型 SNS の登録リンクが含まれているかで

判断する．2 つ目は閲覧者にメールを送信させることを目的とした Web ページであり，サイト内にメールを送信させるリンクがあるかで判断する．3 つ目は閲覧者に電話をかけさせることを目的とした Web ページであり，サイト内に電話をかけさせるリンクがあるかで判断する．4 つ目はフォームを入力させる Web ページであり，サイト内に input タグがあるかどうかで判断する．5 つ目は何かを購入させる Web ページであり，金額に関するテキストがあるかで判断する．6 つ目は銀行振込をさせる Web ページであり，銀行情報の文脈から判断する．7 つ目は詐欺の疑いのあるメールサービスを模してる Web ページであり，Web ページのディレクトリ構成から判断する．8 つ目はアクセスできないサイトであり，最後に 9 つ目は何を目的にしているか判断できないサイトであり，上記のタイプに当てはまらない場合になる．

URL 先がメールサービスを模したサイトである場合は，メールサービスを模したサイトには決済代行業者を通してポイントを購入する仕組みがあるため，追加で決済方法の情報を取得する．メールサービスを模したサイトは HTML やページ構成がどれも同じなので，そのページ構成に従って支払い方法やポイントのレート，決済代行業者の情報を自動取得する．また，サイトについて Web 上に口コミ情報があるため，それらの情報を手動で収集した．

5.4 通話情報・SMS 情報の収集

メッセージ型 SNS でフォームに電話番号を入力すると，相手から電話がかかってくることや SMS が届くことがある．通話がかかってきた場合は手動で応答する．通話履歴と SMS の情報は観測用の Android スマートフォンから抽出する．

6. 調 査 結 果

本節では提案手法により情報収集を行った結果を示す．なお，以下では短文投稿型 SNS から直接誘導されるメッセージ型 SNS の組織用アカウントを “1 次アカウント” と呼ぶ．また観測したアカウントの中には他のアカウントへ更なる誘導を行うものがある．他のアカウントから誘導されるアカウントを “2 次アカウント”と呼ぶ．

6.1 短文投稿型 SNS の調査結果

短文投稿型 SNS に 2022/12/15-2023/1/29 に投稿され，“高額バイト”という検索クエリに一致した投稿と投稿アカウント，固定された投稿を取得した．取得した投稿数の推移と，投稿アカウント数の推移を図 3 に示す．

期間内で “高額バイト”で検索したときの投稿数は合計 34,734 件であり，投稿アカウント数は合計 4,025 人であった．そのうちメッセージ型 SNS に誘導する投稿数は 4,246 件 (12%), 投稿アカウント数は 353 人 (8.77%) だった．いずれも年末に一旦急増し，減少した後は微増を続けていた．なお，後述の通り，これらの投稿が誘導する先はごく少数のメッセージ型 SNS の一次アカウントであることから，実際は少数のグループにより行われた投稿であると推測される．

“高額バイト”とは別の検索クエリをシードとして収集できる情報を調査するために，投稿により誘導されるメッセージ型

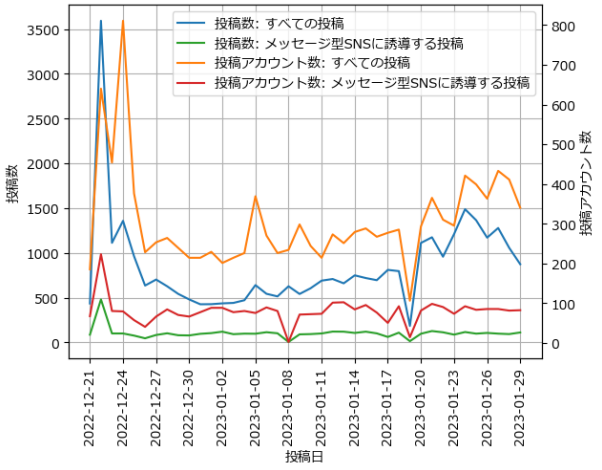

図 3 “高額バイト”に一致する投稿数と投稿アカウント数の推移

SNS のアカウント名を参考に検索クエリを作成した．検索クエリが特定のメッセージ型 SNS のアカウント名の場合は英単語を含むことが多いので，日本語の投稿のみに絞っている．作成した検索クエリを 2023/1/29-2023/1/31 の 3 日間で用いた結果を表 3 に示す．金銭に関係する名詞と “副業”を組み合わせた検索クエリはヒットする投稿数も多く，メッセージ型 SNS のアカウントへの誘導も確認できる．特に “FX 副業”といった検索クエリは多数のアカウントに誘導されており新たな誘導の構造が発見できる可能性がある．このように収集した情報を基にフィードバックを掛けることでさらに多くの情報を収集できる．

表 3 検索クエリごとの結果

検索クエリ	投稿数	メッセージ型 SNS に繋がる投稿数	メッセージ型 SNS のアカウント数
“FX 副業”	14694	4140	205
アカウント名 A	2683	0	0
“プレゼント 副業”	2251	520	113
“宝くじ 副業”	467	44	14
“競馬 副業”	402	94	13
“競艇 副業”	220	72	2

6.2 メッセージ型 SNS の調査結果

5.2 節の手法により，短文投稿型 SNS から誘導されるメッセージ型 SNS のアカウントに関する調査結果を述べる．4,246 件の短文投稿の誘導先は，メッセージ型 SNS の 1 次アカウント 15 個であった．これらすべてに登録を行い，2022/11/28-2023/1/29 の期間でアカウントから届くメッセージを観測した．なお，これら 15 のアカウントのうち，7 つはアカウント名が完全に一致しており，同一の管理者に管理されていることが予想される．アカウント名や届くメッセージの内容から，これらは副業の紹介に関するアカウント群であることがわかるため，以降では「副業系 1」グループと呼称することとする．副業系 1 に属するアカウントは登録者へのメッセージ送付により他のアカウント (2 次アカウント) への誘導も行う．観測期間中に副業系 1

によって誘導された 2 次アカウント数は 59 であった．副業系 1 以外のアカウントは他のアカウントへの誘導は行わず，アカウント名も独立しているため，ここでは独立したグループとして扱い，同様にアカウント名等に基づき命名する．副業系以外には，投資系，アフィリエイト，打ち子募集といった内容が見られた．表 4 に観測されたグループの一覧を示す．副業系 1 グループは登録者数最大の 1,486 人を有し，他のアカウントの紹介も頻繁に行う活発なグループといえる．なお，メッセージ型 SNS のアカウントには作成時に接続していた IP アドレスに基づき国情報が付与されている．75% のアカウントは日本で作成したものであるが，副業系グループの 1 次アカウントはすべて地域がタイである．したがって，この運営者はタイを拠点とするか，プロキシなどでタイを経由していると考えられる．

表 4　メッセージ型 SNS におけるアカウントグループ

グループ名	誘導する投稿数	1 次アカウント数	登録者数の合計	関連 2 次アカウント数
副業系 1	4068	7	1486	59
副業系 2	2	1	4	0
副業系 3	1	1	322	0
副業系 4	1	1	56	0
打ち子募集	168	1	81	0
投資系 1	1	1	511	0
投資系 2	1	1	110	0
アフィリエイト 1	1	1	133	0
アフィリエイト 2	3	1	15	0

副業系 1 グループに誘導した短文投稿型 SNS の投稿の掲載期間とメッセージ型 SNS の各 1 次アカウントの登録数の増加期間，2023/01/29 時点の各 1 次アカウントの登録者数を表 5 に示す．各アカウントは数日から 1 週間程度短文投稿型 SNS の投稿による誘導を受けた閲覧者を受け付け，その期間は登録者が増加する．登録数が数百名に達したころ，短文投稿型 SNS での投稿は新たなアカウントへの誘導をはじめ，旧アカウントへの流入は停止するため，登録者数は頭打ちになる．これを何度も繰り返していることでメッセージ型 SNS の運営者によるアカウント停止を回避している可能性がある．

表 5　短文投稿型 SNS からメッセージ型 SNS への登録者流入

短文投稿型 SNS の掲載期間	登録者数の増加期間	登録者数
- 2022/12/24	- 2022/12/23	236
2022/12/25 - 2022/12/29	2022/12/24 - 2022/12/28	141
2022/12/30 - 2023/01/05	2022/12/29 - 2023/01/04	231
2023/01/06 - 2023/01/07	2023/01/05 - 2023/01/06	79
2023/01/09 - 2023/01/16	2023/01/08 - 2023/01/17	236
2023/01/19 - 2023/01/29	2023/01/19 - 2023/01/29	377

6.3　Web サイトの情報収集

5.3 節の手法による調査結果を述べる．メッセージ型 SNS と SMS で送られてきたメッセージから合計 551 個の URL を収集し，それらにアクセスしてサイト情報を 2023/01/24 に取得した．取得した 551 ページの種類とその件数，URL を得た場所を表 6 に示す．不明とアクセス不可を除くと，フォームやメール，電話という情報を送信させるページが全体の 57% を占める．メッセージ型 SNS の招待リンクの件数も多く，全体の 27% を占める．残りはメールサービスを模したサイトが 15%，商材を購入させるサイトであり，全体の 1% 程度である．SMS に貼られていた URL はすべてメールサービスを模したサイトへのリンクであった．

表 6　ページの種類ごとの URL 数

ページの種類	URL 数	URL を得た場所
不明	173	メッセージ型 SNS
フォームを入力させるサイト	150	メッセージ型 SNS
メッセージ型 SNS の招待リンク	96	メッセージ型 SNS
メールサービスを模したサイト	52	SMS
メールを送らせるサイト	42	メッセージ型 SNS
アクセスできないサイト	24	メッセージ型 SNS
電話をかけさせるサイト	9	メッセージ型 SNS
なにか購入をさせるサイト	5	メッセージ型 SNS
銀行振込をさせるサイト	0	メッセージ型 SNS
合計	551	

メールサービスを模したサイトは，メッセージ型 SNS のメッセージに URL が貼られている場合と SMS の本文に URL が貼られている場合があるが，メッセージ型 SNS のメッセージに貼られていたものはサイト内では決済が行われないため，SMS の本文に貼られているものに絞って調査する．5 件のメールサービスを模したサイトの決済方法を調査した．その結果，合わせて 3 つの決済代行業者と 4 種類の電子マネーが利用可能だった．このように，多くの決済方法を用意することで幅広い年代の人が利用できるようにしている．

詐欺の疑いのあるサイトでどのような被害が出ているのかを調べるため，詐欺の疑いのあるサイト名に関連する口コミ情報を Web 上で収集した．口コミの件数を表 7 に，口コミに書かれている詐取された金額を表 8 に示す．詐欺の疑いのあるサイトには当該サイトが不審であるという口コミが一定数存在していることが分かる．

表 7　詐欺の疑いのあるサイトの口コミ数

名前	詐欺に関係するという口コミ数	金銭を詐取されたという口コミ数
メールサービスを模したサイト A	55 件	15 件
メールサービスを模したサイト B	14 件	3 件
副業商材 A	16 件	4 件

6.4　通話履歴と SMS 情報の収集結果

5.4 節の手法による調査結果を述べる．2022/09/15-2023/01/15 に受信した通話履歴と，2022/12/01-2023/01/22 に受信した SMS 情報を収集した．通話履歴が 24 件あり，そのうちの 1 件が着信，2 件が発信，21 件が不在着信となっている．なお，年末年始の時期は通話がかかってきていない．

SMS は 2022/12/01-2023/01/22 の期間に 55 件受信している．

表 8　詐欺の疑いのあるサイトで詐取された金額

名前	詐取された金額 (万円)				
	100 ~	10 ~ 100	1 ~ 10	~ 1	不明
メールサービスを模したサイト A	1	3	2	1	8
メールサービスを模したサイト B	0	2	1	0	8
副業商材 A	0	0	0	3	0

だが，2022/12/22-2023/01/08 までの年末年始の期間では 1 件しか受信していない．受信した 55 件のうち，52 件がメールサービスを模したサイトへ誘導していて，8 件の送信者が送信している．送信者名は誘導するメールサービスを模したサイトの略称になっている．残りの 3 件のうち 1 件はリンクが無効なスミッシング，2 件は正規の SMS であった．

6.5　メッセージ型 SNS におけるアカウント間の関係の分析

SNS のアカウントが別のアカウントに誘導するという関係を有効グラフで可視化した結果を図 4 に示す．グラフのノードはメッセージ型 SNS のアカウント ID，エッジはアカウント間の関連を表しており，誘導元から誘導先へ伸びている．青色のノードと青色のエッジは短文投稿型 SNS からの誘導，緑色のエッジはメッセージ型 SNS の組織用アカウントからの誘導を表す．なお，アカウント登録と当該アカウントの活動時期がずれると誘導が観測できないため，実際に発生していた全ての誘導が可視化されているわけではない点に注意が必要である．この図から，短文投稿型 SNS からの誘導はいくつかのメッセージ型 SNS の 1 次アカウントに誘導を行い，さらに多数の 2 次アカウントへ誘導が広がり相互誘導のネットワークを形成していることがわかる．

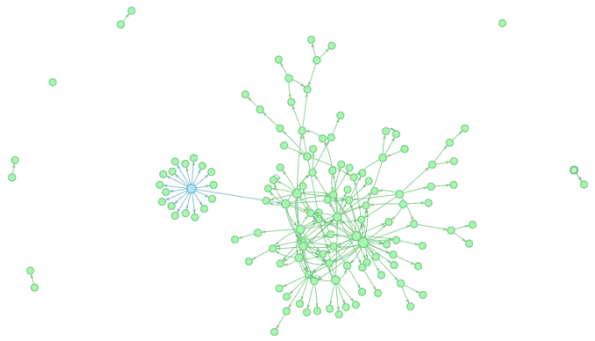

図 4　メッセージ型 SNS のアカウント間の関係

一般にメッセージ型 SNS の組織用アカウントは自社商品の宣伝や通知に使うことが多く，他のアカウントに誘導することは少ない．したがって，他の多くのアカウントに招待リンクを張っているアカウントと，そのアカウントに誘導されているアカウント，それらの相互誘導により構成されるネットワークはある種の異常性を有しており，これを基に同様の異常なアカウント集合を認識できる可能性がある．このような誘導の実態を正確に把握するためには，アカウント登録や登録後に受信されるメッセージ，そしてメッセージからさらに誘導されるアカウントの登録など，誘導の関係を追跡しリアルタイム性のあるデータ取得を行う必要がある．

7.　まとめと今後の課題

本研究では複数の SNS を悪用したオンライン詐欺の疑いがある事例について，短文投稿型 SNS の WebAPI，Android 実機からのメッセージ型 SNS や通話記録，受信した SMS の収集，得られた URL の Web ページの調査，メッセージ型 SNS の組織用アカウントの定期的な情報収集を行った．さらに得られた情報から，メッセージ型 SNS のアカウント間の関係を調査した．その結果，アカウントの登録地域や登録数の推移，登録数の増加期間に特徴のあるアカウント群を発見した．また，詐欺の疑いのあるサイトへ誘導するメッセージ型 SNS のアカウントの関係性を調査したところ，それらのアカウントの多くが相互に誘導を行う 1 つのネットワークを形成していることがわかった．また，詐欺の疑いのあるサイトは多くの決済方法に対応していて，それらのサイトの被害が Web 上で発見された．今後は情報収集の頻度とリアルタイム性を向上し，さらなる誘導の関係を調査すると共に短文投稿型 SNS でダイレクトメッセージ機能に誘導している事例も今後調査を行いたい．

謝辞　本研究の一部は JSPS 科研費 JP21H03444 の助成を受けて行われた．

文　　献

[1] 株式会社ＩＣＴ総研. 2022 年度 sns 利用動向に関する調査 | ict 総研. https://ictr.co.jp/report/20220517-2.html. (Accessed on 01/03/2022).
[2] 消費者庁. 令和 4 年版消費者白書目次 第 1 部 第 1 章 第 4 節 (3)sns に関連する消費生活相談 — 消費者庁. https://www.caa.go.jp/policies/policy/consumer_research//white_paper/2022/white_paper_113.html. (Accessed on 02/08/2022).
[3] Chris Grier, Kurt Thomas, Vern Paxson, and Michael Zhang. @spam: the underground on 140 characters or less. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pp. 27–37, New York, NY, USA, October 2010. Association for Computing Machinery.
[4] De Wang, Shamkant B Navathe, Ling Liu, Danesh Irani, Acar Tamersoy, and Calton Pu. Click traffic analysis of short URL spam on twitter. In *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pp. 250–259, October 2013.
[5] Sangho Lee and Jong Kim. WarningBird: A near Real-Time detection system for suspicious URLs in twitter stream. *IEEE Trans. Dependable Secure Comput.*, Vol. 10, No. 3, pp. 183–195, May 2013.
[6] Android Developers. Android debug bridge（adb） — android デベロッパー — android developers. https://developer.android.com/studio//command-line/adb?hl=ja. (Accessed on 01/03/2022).
[7] Android Developers. Ui automator — android デベロッパー — android developers. https://developer.android.com/training/testing/ui-automator?hl=ja. (Accessed on 01/03/2022).
[8] Selenium. https://www.selenium.dev/ja/. (Accessed on 02/09/2022).
[9] MaxMind. Geolite2 free geolocation data — maxmind developer portal. https://dev.maxmind.com/geoip/geolite2-free-geolocation-data?lang=en. (Accessed on 01/03/2022).