Vol.2021-IOT-55 No.3
Vol.2021-SPT-44 No.3
2021/9/6

マイクロブログ型SNSにおける スパムボットの検知とスパムの属性判別手法の提案

上野 駿介[1]　今泉 貴史[2]

概要：近年，ソーシャル・ネットワーキング・サービスは急速に普及し単なるコミュニケーションツールに収まらず様々な用途に利用されるようになった．これにより，プログラムによって自動化されたスパムボットと呼ばれるアカウントが出現し，様々な問題を引き起こしている．本研究では，マイクロブログ型の SNS において汎用的に用いることが可能なスパムボットの検知手法と，疑いのあるアカウントに対して注意喚起を行うシステムの設計を提案する．

Detecting spambots and spam attribute classification in microblogging SNS

1. はじめに

近年，スマートフォンやネットワーク網の普及とともに，ネットワーク上を流れる情報量は爆発的に増加している．総務省の試算によると，国内におけるインターネットの総ダウンロードトラフィックは，固定回線，モバイルともに大きく増加しており，今後もさらなる増加が見込まれている [1]．その要因の一つとして，ストリーミング型の動画共有サイトや，SNS（ソーシャル・ネットワーキング・サービス）などに代表される Web サービスの台頭が挙げられる．このトラフィックの増加は，国内のみならず世界規模でも増えており，Cisco の予測によれば、2022 年には年間 4.8 ゼタバイトに達するとされている [2]．

現在，SNS は単なるコミュニケーションツールに収まらず，ファイル共有機能，通話機能，ブログ機能，ソーシャルゲーム機能といった様々な機能に焦点を置いたサービスが展開されるようになり，その利用人口を急激に加速させている．総務省の調査によると，SNS の利用率は，全ての世代で増加し，特に高齢者層で利用人口を拡大している [3]．

SNS には，マイクロブログ型，メッセンジャー型，写真・動画共有型などの種類がある．マイクロブログ型の SNS は，利用者が簡易的なブログのような形式で投稿を行うことができる SNS の形式であり，代表的なサービスの例として，Twitter[4] が挙げられる．マイクロブログ型の SNS は，情報を大規模に広げるための 1 つの手段であり，マーケティング戦略の 1 つとして活用されている．これは，マイクロブログ型の SNS が多くのユーザをもち，特定のユーザに対してアプローチを行うことが容易で，ブログの形式という点から拡散性の高いサービスであることなどが挙げられる [5]．

一方で，マイクロブログ型の SNS は利用者数を拡大し，その影響力を高めた結果，悪質サイトへの誘導やフェイクニュースの拡散，トレンドの操作などを目的としたスパムボットと呼ばれるプログラムによって自動化されたアカウント群が引き起こす様々な悪影響が問題になっている．

2. スパムボット

2.1 スパムボットとは

スパムとは，各種ネットメディアにおいて受信者の意向を無視して大量にばらまかれる迷惑なメッセージのことである．初期のスパムは，電子メールサービスや SMS（Short-MessageService）の開始とともに，電子メールやショートメッセージ形式でのスパムが席巻し，現在でもこちらをス

[1] 千葉大学大学院融合理工学府
Graduate School of Science and Engineering, Chiba University
〒 263–8522, 千葉県千葉市稲毛区弥生町 1–33
E-mail : ueno190@chiba-u.jp
[2] 千葉大学統合情報センター
Institute of Management and Information Technologies Chiba University
〒 263–8522, 千葉県千葉市稲毛区弥生町 1–33
E-mail : imaizumi_takashi@faculty.chiba-u.jp

図 1　SNS に潜むスパムボットの例

パムと定義する場合もある．しかし，近年では SNS の普及により，SNS でもスパムメールと同様の迷惑行為が見られるようになった．これを広義のスパムと呼び，本稿で扱うスパムについては，広義のスパムを指す．

スパムボットとは，これらのスパムを自動的に送信できるようプログラムされたものを指し，多くは SNS 上に出現することから，ソーシャルボットとも呼ばれるスパム行為を行う自動化されたアカウントの総称である．

2.2　スパムボットの目的

スパムボットの目的には，以下のようなものが挙げられる．

- フィッシングやマルウェアへの感染を目的とした悪質サイトへの誘導を目的とするもの．
- フェイクニュースおよび信憑性のない情報の拡散を目的とするもの．
- トレンド機能を活用した SNS 上での意見操作を目的とするもの．
- 短時間で大量の投稿を行うことによる可用性の侵害を目的とするもの．

2.3　各種 SNS における利用規約

各種 SNS には，利用規約が存在し，いくつかの行為が禁止されている．容認されていない行為について，Twitter のサービス利用規約 [6] では以下の行為が禁止されている．

- 電子メールもしくは投稿での TCP/IP パケットヘッダーまたはヘッダー情報の一部の偽造，または方法の如何を問わず，改ざんされた情報，詐欺的情報もしくは情報源を偽装した情報を送る目的での本サービスの利用．
- いずれかの利用者，ホストもしくはネットワークのアクセスの妨害，または遮断（もしくはその試み）（本サービスへのウィルスの送信，オーバーロード，フラッディング，スパミング，メールの大量送信，あるいは本サービスを妨害したり過度な負荷を与える方法でコンテンツの作成をスクリプトすることを含みますが，これらに限定されません）．

また，Facebook におけるコミュニティ規定 [7] では，スパム行為を禁止としており，具体的な禁止行為として，

- 手動か自動かを問わず，非常に高い頻度で投稿，シェアしたり，コンテンツに対してアクションを実行したり，アカウントやグループ，ページ，イベント，その他のアセットを作成したりすること．
- 虚偽表示を用いてアプリやウェブサイトの「いいね！」，シェア，フォロー，クリックまたは使用を促すこと．

とあり，マイクロブログ型の SNS ではスパム行為が禁止されている．

2.4　スパムボット関連の事件

本節では，スパムボットが関連する被害の例を扱う．

フェイクニュースに関するスパムボットによる被害が確認された例として，2013 年のアメリカで起きたダウ工業株の大きな下落が挙げられる．2013 年，アメリカではダウ工業株の大きな下落が起こった．この急落の要因の一つとして，スパムボットによるテロに関するフェイクニュースの拡散がある．これにより，ダウ工業株平均は 140 ドルほど急落し，大きな経済的損失をもたらした．この例に限らず，実態の不確かな会社の株価を高騰させようとする動きも多く見られている [8]．

トレンド操作に関するスパムボットによる被害が確認された例として，2016 年の米国大統領選挙が挙げられる．この年の大統領選挙では，大量のスパムボットによるトレンドの操作とフェイクニュースの拡散が確認された．これにより，特定の意見を持つ人々の票が操作された可能性があるとされており，民主的な大統領選挙の完全性を危険にさらす行為として問題視されている [9]．そのほかにも，集中的に大量の投稿を行うことで，特定の商品・サービスなどが人気があるように見せることで，規約に反するプロモーションやトレンドの操作が行われている．

悪質サイトへの誘導に関する例としては，実在する企業やサービスになりすまし，その企業の公式サイトに模倣したフィッシングサイトやダイレクトメッセージ機能を利用し，ユーザの ID やパスワード，クレジットカード番号などが盗まれる被害がある [10]，[11]．多くの企業やブランドが公式アカウントのなりすましに関する注意喚起を行っており，Twitter などのサービス提供側も，認証マークの制度を採用し，なりすましを抑制する対策を行っている．

3. 研究の目的

本研究では，様々なマイクロブログ型の SNS に出現するスパムボットの検知を行うと同時に，スパムボットの疑いがあるアカウントに対して，スパムボットの目的とともにユーザに注意喚起を行うことで．スパムボットによる被害を防ぐことを目的とする．また，スパムボットの目的の種類として，悪質サイト誘導型，フェイクニュース拡散型，トレンド操作型の 3 つのタイプを対象とし，それらのどの目的を持つスパムボットかを判別することを目的とする．

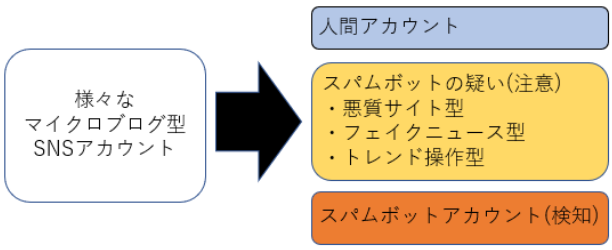

図 2 スパムボットの検知と種類の分別

4. 関連研究

スパムボットに関する研究として，Chao Yang，Robert Harkreader らの Empirical Evaluation and New design for Fighting Evolving Twitter Spammers が挙げられる [12]．彼らは，Twitter 上のスパムボットの集団での活動から，多くのスパムボットが活動することで効果を得るスパムボットの挙動に焦点を置いた検知手法を提案しており，スパムボット間のユーザ間の関係性や投稿内容の類似性を利用して，スパムボット群の検知を行う手法である．

また、Twitter におけるスパムボットを判別するシステムとして，Clayton A Devis，Onur Varol，Kaicheng Yang らの「Botometer」が挙げられる [13]．このシステムは，Twitter 上のスパムボットを検知するシステムであり，対象アカウントのユーザ情報や投稿情報を，様々なスパムボットと人間のアカウントによってトレーニングされた教師データをもとに学習させ，スパムボットかどうかを判別するシステムである．このシステムでは，英語におけるスパムワードのフィルターや，自然言語処理による意味解析を行うことで，対象言語が英語の場合に高い判別精度を持つ．

5. 提案手法

5.1 マイクロブログ型 SNS の共通要素

マイクロブログ型の SNS は，メッセンジャー型 SNS に比べて，1 つの投稿が多くのユーザの目に触れるというシステムから拡散性が非常に強く，電話番号を必要とせず登録可能なサービスも多く，登録が簡単であるということからも悪意をもったアカウントがもたらす影響が大きい．

本稿では，これらのマイクロブログ型の SNS に共通に適用可能なシステムを考えるうえで，多くのマイクロブログ型 SNS において，共通に扱える要素を抽出する必要がある．そのため，スパムボットの報告が多くあげられるマイクロブログ型 SNS である Facebook[14]，Weibo（微博）[15]，Twitter[4]，VK[16] の各サービスで共通に取得できる要素を使用し，その要素を**表 1**，**表 2** に示す．

表 1 マイクロブログ型 SNS のユーザ要素

変数名	ユーザ要素
name	ユーザ名
follow_count	フォロー数
follower_count	フォロワー数
profile	プロフィール文
profile_url	プロフィール文に含まれる url
post_count	総投稿数
share_count	他ユーザ投稿の共有数
certification	認証・検証済みマーク

表 2 マイクロブログ型 SNS の投稿要素

変数名	投稿要素（1 件ごと）
post	投稿文
post_time	投稿時間
reaction_count	共有・いいねなどの合計数
tag	トレンドタグ内容
tag_count	トレンドタグの個数
picture	画像，動画コンテンツの有無
url	url データ
url_count	url の個数

5.2 スパムボットの検知と属性判別

本稿では，スパムボットの検知のほかに，スパムボットの疑いのあるアカウントに対して，その可能性を提示することが目的である．そのため，スパムボットの目的によってその種類を分け，以下のどの目的を持つスパムボットであるかを分類する．

- 悪質サイト誘導型．
- フェイクニュース型．
- トレンド操作型．

5.3 ユーザスコア

ユーザスコアは，そのユーザが持つ影響力を判別する目的で作成する．これは，多くのスパムボットはフォロー数に対してフォロワー数が少ない傾向であること，いいねや共有の数が他のユーザに対して少ないことが挙げられる．この特性から，ユーザスコアはスパムボットが一般の人間アカウントに比べて外部に対する影響力が少なく，そのユーザの影響力を示す特徴量を用いる．

表 3　ユーザスコア要素

特徴量	
follow_rate	フォロー比率
avg_reaction	平均リアクション数
max_reaction	最大リアクション数
name_len	ユーザ名の長さ
profile_len	プロフィール文の長さ

5.4　投稿時間スコア

投稿時間スコアは，そのユーザの投稿の周期性を判別する目的で作成する．図 3 はスパムボットアカウントと人間アカウントの投稿分布を示したもので，スパムボットアカウントは人間アカウントに比べて，均一的な投稿分布となる．これは，スパムボットが周期的な投稿を行うことによるもので，岡本らの研究 [17] によると，ボットの投稿には周期的な特性が確認されている．

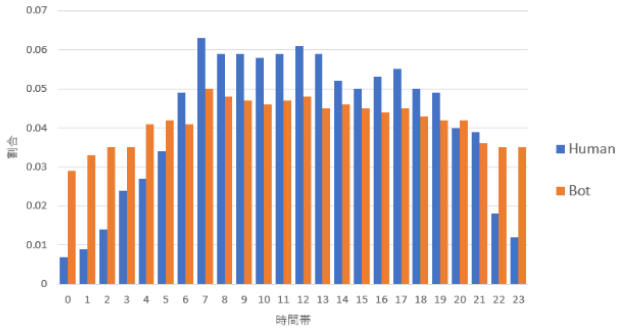

図 3　スパムボットの投稿分布

これらの特性から，投稿時間スコアはスパムボットが人間アカウントに比べて投稿に規則性があることから，投稿の規則性を示す特徴量を用いてスパムボットの判定を行う．

表 4　投稿時間スコア要素

特徴量	
post_var	投稿間隔の分散
posttime_same	同一時刻投稿割合
posttime_day	曜日別投稿割合
posttime_zone	時間帯別投稿割合

5.5　投稿内容スコア

投稿内容スコアは，そのユーザの投稿の内容の中身を判別する目的で作成する．スパムボットは，人間アカウントが様々な内容について投稿するのに対して，スパムとして似た内容の投稿を繰り返すものがある．

この特性から，投稿内容スコアはスパムボットが人間アカウントに比べて投稿内容の変化が薄いことから，投稿の内容の変化を示す特徴量を用いる．

表 5　投稿内容スコア要素

特徴量	
post_leve	前 2 投稿との平均類似度
post_share_rate	共有した投稿の割合
post_reply_rate	返信の割合
media_rate	メディアコンテンツ含有率
avg_tags	平均タグ数
tags_inheritance	継承タグ率

5.6　URL スコア

URL スコアは，投稿内に含まれる URL を判断する目的で作成する．スパムボットは，マルウェアやフィッシングサイトなど悪質なサイトへの誘導を目的としており，それらのサイトの URL は，ランダムな文字列のドメインが使われたり，同じドメインでも，アクセス元を特定するための固有 ID と呼ばれる文字列が付加される場合がある．URL スコアでは，悪質サイトの URL の特徴を用いてスパムボットの判定を行う．

表 6　URL スコア要素

特徴量	
url_rate	URL を含む投稿の割合
avg_url_count	平均 URL 個数
short_url_rate	短縮 URL 割合
avg_redirect	平均リダイレクト回数
same_domain	同一ドメイン割合
url_ent	平均 URL エントロピー

5.7　判別結果

それぞれのスコアの判別は，教師データとして，人間アカウントおよびスパムボットアカウント各 1000 アカウントを教師データとして学習を行い，アカウント 1 個に対する投稿データ数は，最大 200 件である．データセットには，S Cresci らによってフラグ付けされたアカウントを用いる [18]．分類モデルの構築には scikit-learn を利用し，機械学習のアルゴリズムはランダムフォレストを採用する．これは，Varol O らの研究 [19] においてランダムフォレストを利用した場合の精度が最も高いためである．

スパムボットの検知は，2 つ以上の項目において，スパムボットと判別されたものをスパムボットと判別する．1 つの項目にのみスパムボットと判別されたアカウントについては，スパムボットの疑いとし，それらの中でも URL スコアのみがスパムボットと判別されたものを，悪質サイト誘導型，投稿内容スコアの項目のみがスパムボットと判別されたもののうち，タグに関する項目においてスパムボットと判別されたものを，トレンド操作型，残りをフェイクニュース型と，投稿時間スコアの項目のみがスパムボットと判別されたものを，サーバ負荷型と判別する．ただし，認証済みアカウントに対してはスパムボットの判別は行わ

ない．

以下では，スパムボットのアカウントをスパムボットのアカウントとして判別することを TP(True Positive)，スパムボットのアカウントを人間のアカウントとして判別することを FN(False Negative)，人間のアカウントをスパムボットのアカウントとして判別することを FP(False Positive)，人間のアカウントを人間のアカウントとして判別することを TN(True Negative) とする．また，正解率 (Acc) は以下の式で求められる．

$$Acc = (TP + TN)/(TP + FN + FP + TN)$$

Twitter を対象とした英語アカウントにおけるスパムボットの判別結果を**表 7** に示す．

表 7 スパムボット検知結果（Twitter-英語）

手法	TP	TN	Acc
先行研究 [13]	0.930	0.996	0.963
提案手法	0.758	0.982	0.870

Twitter を対象とした多言語アカウントにおけるスパムボットの判別結果を**表 8** に示す．

表 8 スパムボット検知結果 （Twitter-多言語）

手法	TP	TN	Acc
先行研究 [13]	0.856	0.988	0.922
提案手法	0.747	0.977	0.862

他のマイクロブログ型 SNS を対象としたスパムボットの判別結果を**表 9** に示す．

表 9 スパムボット検知結果 （Facebook，Weibo）

対象 SNS	TP	TN	Acc
Facebook	0.72	0.96	0.84
Weibo	0.71	0.93	0.82

また，Twitter におけるスパムボットの属性の判別として，悪質サイト誘導型，フェイクニュース型，トレンド操作型とフラグ付けされたアカウントそれぞれ 100 件と人間アカウント 100 件に対してスパムボットの判別を行った結果を**表 10** に示す．

以下では，スパムボットのアカウントをスパムボットまたは正しいスパムボットの種類の疑いとして判別することを TP'(True Positive)，スパムボットのアカウントを人間アカウントまたは誤ったスパムボットの種類の疑いとして判別することとして判別することを FN'(False Negative)，人間のアカウントをスパムボットまたはスパムボットの疑いとして判別することを FP'(False Positive)，人間のアカウントを人間のアカウントとして判別することを TN(True Negative) とする．

表 10 スパムボット属性判別結果（Twitter）

対象データ	TP'	FN'	TN	FP'	Acc
悪質サイト	0.83	0.17	0.87	0.13	0.85
フェイクニュース	0.69	0.31	0.85	0.15	0.77
トレンド操作	0.87	0.13	0.87	0.13	0.87

6. 考察

6.1 スパムボットの検知精度

表 7，表 8 より，Twitter 上のスパムボットを対象とした結果においては，先行研究の方が TP，TN，Acc ともに高い精度が得られた．この 1 つの要因として，投稿元端末情報の有無が挙げられる．この特徴量は， H Wang らの研究 [20] によると，人間ユーザとボットユーザの判別において，投稿元端末情報 (API) は大きな判別能を持つとされている．しかし，投稿元端末情報は，全てのマイクロブログ型の SNS において取得できるわけではないため，提案手法においては，様々なマイクロブログ型 SNS での利用を想定したため，利用しなかった．

6.2 様々な言語への対応

表 7，表 8 より，対象言語が英語の場合と，それ以外の多言語の場合において，先行研究では精度の低下がみられたが，提案手法においては，わずかに精度は落ちたものの大きな変化は見られなかった．このことから，異なる言語においてもスパムボットに共通的な特性を抽出できたと考える．この要因として，先行研究の特徴量に含まれる英語におけるスパムワードフィルタの有無が挙げられる．スパムワードフィルタは，判別対象の言語におけるスパムボットのデータや知識が十分に得られる時有効であるが，マイナーな言語においては，適用することが難しい．他にも，利用地域の違いによる文化的な影響などが考えられる．

6.3 様々なマイクロブログ型 SNS への対応

Facebook や Weibo を対象としたスパムボットの検知結果 (表 9) においては，わずかに検知精度は落ちたものの，大きな判別精度の低下は見られなかったことから，他のマイクロブログ型においても，提案手法はマイクロブログ型 SNS におけるスパムボットの共通的な特性をある程度抽出できたと考える．精度が落ちた原因については，教師データとして Twitter のデータを利用したことによる，それぞれの SNS において利用形態の違いなどが考えられる．

6.4 スパムボットの属性判別

また，スパムボットの属性判別結果 (表 10) については，

スパムボットの中でも，フェイクニュース拡散型のスパムボット判別精度が最も低かった．フェイクニュース拡散型のスパムボットの検知の精度が低かった理由として，

フェイクニュースにも需要があることが挙げられる．フェイクニュース拡散型のスパムボットの多くは，選挙などの政治的な意思決定に関連したものが多く，それらは，一部の人にとっては都合の良いニュースとして受け入れられる場合がある．これにより，他のスパムボットの種類に比べて，ユーザスコアによる判別ができなかったことが原因の一つとして考えられる．フェイクニュース型のスパムボットは，誤った疑いについても，他のスパムボットに比べて多かったことからフェイクニュース型のスパムボットの特性を十分に捉え切れてないと考えられ，これは大きな改善の余地があると考えられる．

7. おわりに

7.1 まとめ

本稿では，様々なマイクロブログ型の SNS において適用可能なマイクロブログ型の SNS のモデルを設計し，多種類，多言語のマイクロブログ型の SNS の環境において，適用することができるスパムボットの検知手法と，その疑いのあるアカウントに対して注意喚起を行うシステムの設計を提案した．また，投稿時間や投稿内容，ユーザ情報，URL といった情報からそれぞれスコアを算出し，それらをもとにスパムボットの種類の判別を行った．

7.2 今後の課題

今後の課題としては，以下のことが挙げられる．

7.2.1 判別精度の向上

本稿では，スパムボットの検知を行ったが，検知精度において従来手法に大きく劣る結果となった．この判別精度を向上させるために，さらなる投稿間隔や URL の分析を行う必要があると考える．祝日や長期休暇および年末年始による投稿分布は，他の時期と異なった特性を持つ可能性が大きく，URL についても，有名ブランドに見た目や音を似せたものが悪質サイトに使われるといったこと [21] を考慮することで，判別精度を向上させる可能性が挙げられる．また，検知精度の低かったフェイクニュース型のスパムボットの特性のさらなる分析を行い，判別精度の向上を目指すことが挙げられる．

7.2.2 さらなる種類の SNS への適用

本稿では適用可能なマイクロブログ型の SNS として，Facebook，Weibo（微博），Twitter を挙げたが，それ以外にも Tiktok や Instagram といったサービスがある．これらは，画像や動画の共有が主目的となっており，マイクロブログ型の SNS として分類されないことが多いが，そのサービスの形態には共通点が多い．また，LINE のタイムライン機能のようにメッセンジャー型 SNS の一部の機能として，マイクロブログ型 SNS の機能が埋め込まれる場合もある．これらの SNS でも，スパムボットの存在が報告されていることから，今後は適用できる SNS の範囲を広げることで，スパムボット検知の範囲を増やしていくことも重要だと考える．

参考文献

[1] 総務省 総合通信基盤局，
”我が国のインターネットにおけるトラヒックの集計結果”，
https://www.soumu.go.jp/main_content/000761096.pdf.

[2] Cisco，
”Cisco VNI global IP traffic Forecast 2017–2022”，
https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1955935.

[3] 総務省，　”令和 2 年版 情報通信白書”，
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd252120.html.

[4] Twitter.
https://twitter.com.

[5] 伊藤嘉浩，高橋優音，
”日本企業における SNS を用いたマーケティング戦略：有効な活用とマネジメント”，
http://www2.lib.yamagata-u.ac.jp/kiyou/kiyous/kiyous-45-1/image/kiyous-45-1-091to127.pdf.

[6] Twitter.　”Twitter サービス利用規約”，
https://twitter.com/ja/tos.

[7] Facebook.　”Facebook コミュニティ規定”，
https://ja-jp.facebook.com/communitystandards/spam.

[8] Ferrara E，Varol O，Davis C A，Menczer F and Flammini A.
”The Rise of Social Bots”，
Communications of the ACM 59 (7)，96-104.

[9] Bessi A and Ferrara E.
”Social bots distort the U.S. Presidential election online discussion”，
First Monday　Volume 21，Number 11-7.

[10] is702.　”公安調査庁のなりすましアカウントが出現，SNS 上の偽者に注意”，
https://www.is702.jp/news/3872/.

[11] Yahoo!ニュース.　”Instagram のなりすましアカウントが急増中．資生堂，コクヨ等有名企業 70 社以上が被害に．”，
https://news.yahoo.co.jp/byline/ohmototakashi/20201229-00215064.

[12] Chao Yang，Bobert Harkreader and Guofei Gu.
”Empirical Evaluation and New design for Fighting Evolving Twitter Spammersn”，IEEE Transactionson Information Forensics and Security8 (8)，1280-1293.

[13] OSoMe project.　”Botometer”，
https://botometer.osome.iu.edu/.

[14] Facebook.
https://facebook.com.

[15] Weibo（微博）.
https://weibo.com.

[16] VK（VKontakte）.
https://vk.com/.

[17] 岡本大輝，宮崎太郎，後藤淳.
”統計的手法に基づいたウェブサービスにおけるボット検出．”，
情報処理学会第 81 回全国大会.

[18] S Cresci, R Di Pietro, M Petrocchi, A Spognardi and M Tesconi.
”The Paradigm-Shift of Social Spambots: Evidence, Theories, and Tools for the Arms Race”, Proceedings of the 26th International Conference on World Wide Web Companion.

[19] Varol O, Ferrara E, Davis C, A Menczer, F and Flammini A.
"Online Human-Bot Interactions : Detection, Estimation, and Characterization", Proceedings of the Eleventh International AAAI Conference on Web and Social Media.

[20] Haining Wang , Zi Chu and S Gianvecchio.
"Who is Tweeting on Twitter: Human, Bot, or Cyborg?", Twenty-Sixth Annual Computer Security Applications Conference 6-10 December 2010.

[21] BIGLOBE セキュリティ.
ネットの詐欺に要注意！巧妙化するフィッシング詐欺の手口 (2/3). ",
https://security.biglobe.ne.jp/column/001/02.html.