DEIM Forum 2013 F5-2

Account Reachability Checker:
アカウント到達可能性に着目した SNS における個人情報検出システムの開発

吉國　綺乃† 　石澤　恵†† 　渡辺知恵美††

† お茶の水女子大学理学部情報科学科　〒 112-0012 東京都文京区大塚 2 丁目 1-1
†† お茶の水女子大学大学院人間文化創成科学研究科理学専攻情報科学コース　〒 112-0012 東京都文京区大塚 2 丁目 1-1
E-mail: †{g0920541,ishizawa.megumi,chiemi}@is.ocha.ac.jp

あらまし　近年ソーシャルネットワーキングサービス（以下 SNS）が普及し，それに伴い利用者も増加している．SNS の利用による個人情報の流出は深刻な問題であり，サイバーストーキングによる個人の特定などの問題が多く起こっている．サイバーストーカーは複数の SNS の組合せから多くの個人情報を得ることで，個人を特定していく．しかしながら利用者はどれだけの情報が SNS の組合せで洩れてしまうのか認識しておらず，自身を被害から守るにはきちんと情報の漏れを認識する必要がある．我々は SNS の組合せによってどれだけの個人情報が流出してしまうのか算出する指標である「アカウント到達可能性」（Account Reachability）を定義し，これを用いてシステムを開発した．本システムを繰り返し利用していくことで，自身が公開している情報の制御をしていくことができる．
キーワード　ソーシャルネットワーキングサービス，プライバシ

Account Reachability Checker:
Development of individual information detection system in Social Networking Service

Ayano YOSHIKUNI†, Megumi ISHIZAWA††, and Chiemi WATANABE††

† Department of Information Sciences, Ochanomizu University　2-1-1 Otsuka, Bunkyo-ku, Tokyo 112-8610 Japan
†† Ochanomizu University Graduate School of Humanities and Sciences　2-1-1 Otsuka, Bunkyo-ku, Tokyo 112-8610 Japan
E-mail: †{g0920541,ishizawa.megumi,chiemi}@is.ocha.ac.jp

1. はじめに

近年ソーシャルネットワーキングサービス（以下 SNS とする）が普及し，それに伴い利用者も増加している．現在，主流 SNS である Facebook(注1) の登録者数は 10 億人を超え，Twitter(注2) の登録者数は 5 億人を超えたといわれている． SNS は日記やタイムラインへの投稿，コミュニティへの参加などを通して，他者とのコミュニケーションを促進している．しかしながら SNS の利用は個人情報を公開することで円滑に行えることも多く，利用者は気付かないうちに多くの個人情報を公開している場合がある．現在，利用者が気付かないうちに公開していた情報が第 3 者に取得され個人が特定される 「サイバーストーキング」 が多く報告されている．

そこで我々は利用者が公開している情報をサイバーストーカーが収集していく過程を提示し，自身の公開情報の制御を促すシステム **Account Reachability Checker** (ARChecker) の提案をする．我々は，サイバーストーキング事例 [1] より，サイバーストーカーは利用者が持つ複数の SNS アカウントを見つけ出し関連付けることで，利用者に関する様々な情報を取得していくことに注目した．そして複数の SNS アカウントが同一人物であると第 3 者に推測される可能性を**アカウント到達**

(注1)：http://www.facebook.com
(注2)：https://twitter.com/

可能性（ **Account Reachability** ）と定義した．

ARChecker はアカウント到達可能性計算し，提示するシステムする．本システムを利用することで，サイバーストーカーが利用者の持っている複数の SNS アカウントを関連付け，どれだけの情報が収集できるか知ることができる．利用者は自身が公開している情報を制御し，自分自身を守れるようになることが期待される．

我々はアカウント到達可能性の算出方法を定義し，利用者のプロフィール情報を利用した算出プログラムを実装した．また，算出結果を利用者にわかりやすく提示するためのヒントの提示を実装した．

本稿では，第 2 節でサイバーストーキングの過程とそこから得られた個人が特定されやすい状況について述べる．第 3 節では開発したシステムの利用方法と仕様について述べ，第 4 節ではユーザテストの結果と考察を述べる．

2. サイバーストーキングによる個人情報の流出

2.1 サイバーストーカーによる個人情報取得の手法

サイバーストーキングとはインターネットを利用して特定の人物にしつこく付きまとうストーカーのことである [2] ．サイバーストーキングは SNS 利用時における揉め事による憎悪や，公開されたプロフィール情報などから恋愛感情を抱いたりすることがきっかけとなり始まっていく．サイバーストーキングの被害はインターネット上だけにとどまらず，実世界における被害も多く報告されている．

具体的にサイバーストーカーが個人を特定していく過程を，参考文献 [3] をもとに分析を行った．実際に起きた炎上事件 [1] の過程を示す．この炎上事件は，ある Twitter ユーザが Twitter 上で不適切な発言を繰り返し行い，これが原因となって起きた事件である．

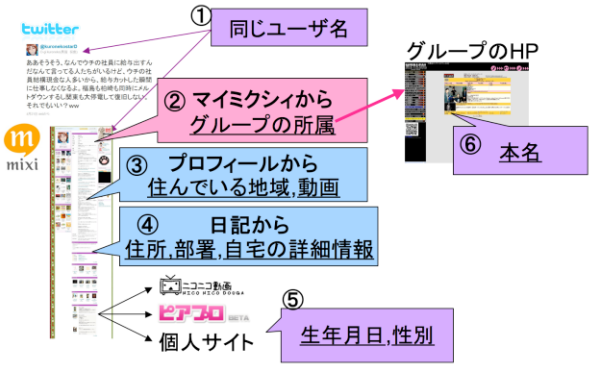

図 1　個人情報特定の流れ

（1） Twitter と mixi で同じユーザ名を使っていたことから mixi のページが特定された．

（2） mixi から趣味の所属グループが明らかになった．

（3） mixi のプロフィールから居住地が判明し，公開動画から本人の顔が特定された．

（4） mixi の日記から，住所や会社の部署，自宅の間取りなどが判明した．

（5） mixi から個人サイトをはじめとする複数の SNS アカウントが判明した．これらから性別，生年月日などが特定された．

（6） (2) で明らかになったグループのホームページが特定され，本名が明らかになった．

このようにサイバーストーキングの過程を分析すると，ある 1 つの SNS を起点として，利用者が利用している他の SNS や Web ページを特定していくことで，更なる個人情報を収集していることがわかる．この調査より，利用している複数の SNS や Web ページのつながりからより多くの個人情報が流出してしまうことが分かった．

2.2 SNS 利用者の実情

SNS の利用者が実際にどのように SNS を利用しているのか調査した．参考文献 [4] より， SNS を利用している利用者のうち約 6 割の利用者が複数の SNS を利用していることが報告されている．これらの利用者のうち各 SNS を使い分けて利用している利用者も多く存在し，それぞれの SNS で公開している情報は異なる場合が多い．使い分けで多いのは「仕事用・学校用」と「趣味用」などのような使い分けである．これらの使い分けをする理由として，仕事や学校関係の人たちに自身の趣味を公開したくないという欲求があることが考えられる．主に仕事用では本名や所属など自身が特定されやすい情報を多く公開している．しかし趣味用の SNS では仕事用の SNS と異なり，自身が特定されないよう公開する情報を制限している．もしも利用者が趣味用の SNS がきっかけとなりサイバーストーキングの被害にあった場合，これらの SNS が関連付けられてしまうと，サイバーストーカーに本名など個人が特定されやすい情報までも取得されてしまう．このように各 SNS が関連付けられることで，より多くの個人情報が取得されてしまう可能性のある利用者は少なくないことがわかる．

我々はなぜ使い分けをしているはずの SNS が関連付けられてしまうのか考察した．サイバーストーキングの過程の中で SNS を関連付けるために用いられたキーワードの多くは，利用者自身が投稿内容中に気が付かないうちに公開していたり，本名とアカウント名が同一人物だと推測されやすいものを利用するなど利用者自身が公開していることが多いことが分かった．しかしながら，利用者が普段 SNS を利用しているときには自身が想定している公開情報と実際の公開情報の差になかなか気づかず，実際にサイバーストーキングの被害にあってから気が付くことが多い [1] ．被害になってからでは遅く，個人が特定されてしまう前にこの差に気付き，対策することが必要となる．

3. Account Reachability Checker

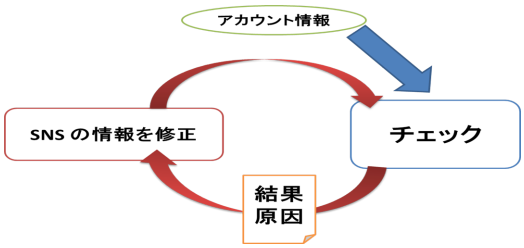

図 2　ARChecker における操作の流れ

ARChecker を使って利用者が公開情報を改善する流れを図 2 に示す．利用者はまずアカウント到達可能性をチェックしたい SNS にログインを行う．するとシステムがアカウント到達可能性を算出し，利用者に提示する．予想していた以上の結果が出た場合，利用者は SNS 上で公開している情報の修正や制御を行い，想定していた通りの結果になるよう本システムを繰り返し利用できる．

現在のシステムは利用する SNS を Facebook と Twitter としている．

3.1　フレームワーク

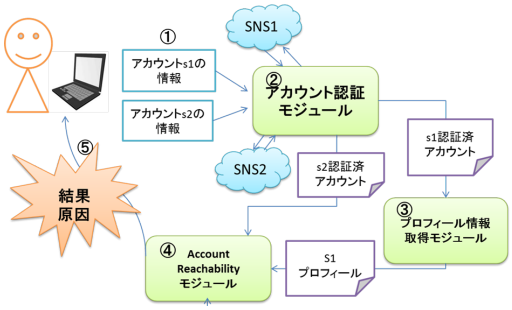

図 3　システムの構造

ユーザ U1 が 2 つの異なる SNS のアカウント同士のアカウント到達可能性を調べたいと仮定し，本システムの流れを図 3 に沿って説明していく．ここで利用する SNS を Facebook と Twitter と仮定する．

（1）　U1 は Facebook (アカウント S1)，Twitter (アカウント S2) 両方にログインをする．

（2）　アカウント認証モジュールにて 2 つの SNS の認証をシステムが行う．

（3）　認証されたアカウント S1 をプロフィール情報取得モジュールに渡し，プロフィール情報を取得する．

（4）　プロフィール情報とアカウント S2 の情報を Account Reachability 評価モジュールに渡しアカウント到達可能性を算出する．Account Reachability 評価モジュールは 3 つのサブモジュールを持つ．各モジュールについては後述する．

（5）　アカウント到達可能性の算出結果と原因をユーザ U1 に提示する．

提示された結果と原因をもとに，利用者自身が公開している情報を制御していく．

以下各モジュールを説明していく．モジュールは大きく 3 つに分かれている．アカウント認証モジュール，プロフィール情報取得モジュール，Account Reachability 評価モジュールである．

【アカウント認証モジュール】

ログインされた SNS アカウントの認証を行うモジュールである．各 SNS との認証に OAuth を利用しているため安全な認証を行っている．アカウント認証時にアカウント名と ID の取得を行う．

【プロフィール情報取得モジュール】

認証されたアカウント情報をもとに SNS に公開しているプロフィール情報を取得する．プロフィール情報の取得には各 SNS が提供する API を利用している．

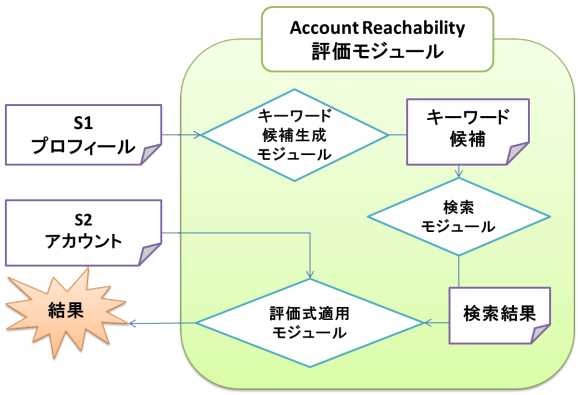

図 4　Account Reachability 評価モジュール

【Account Reachability 評価モジュール】

このモジュールは 3 つのサブモジュールを持つ (図 4)．キーワード候補生成モジュール，検索モジュール，評価式適用モジュールである．

（1）　キーワード候補生成モジュール

取得した S1 のプロフィール情報からアカウント到達可能性を算出するために必要となる情報を取得し，キーワード候補を生成する．ここで，取得した情報をそのままキーワードとして用いるだけでなく，学校名を略称に変更する略称データベースや，名前から作られるアカウント名の推測や誕生日を用いたアカウント名を生成する「言い換え API」を用いてキーワード候補を生成する．

（2）　検索モジュール

SNS2 上でキーワード候補を検索していき，S2 の候補となるアカウントを取得するモジュール．

（3）　評価式適用モジュール

検索結果をアカウント到達可能性の算出式に適用し，アカウント到達可能性を算出する．

以下アカウント到達可能性の算出方法について述べる．

3.2　アカウント到達可能性の算出方法

サイバーストーカーはある SNS 上に公開している情報からキーワードを抽出し，検索エンジンなどを利用して別の SNS の

アカウントを見つけ出している．我々はこの方法を利用してアカウント到達可能性を求めている．アカウント u1 からアカウント u2 に対するアカウント到達可能性の算出式を以下に示す．

$$AccountReachability\,(u1 \rightarrow u2) = max_{K \subseteqq Kef} \left(Match(u2) * \frac{Score\,(K, u2)}{\sum_{a \in A} Score\,(K, a)} \right)$$

$$Kef = \{k | k \in KeyEnt\,(u1)\}$$

$$A = \{a | a \in Search(k)\}$$

$$Match(u2) = \begin{cases} 1 & if\ u2 \in A \\ 0 & else \end{cases}$$

$KeyEnt(u1)$ は u1 から得られたキーワード候補の集合である．$Search(k)$ はキーワード k で検索を行った結果である．各キーワードをそれぞれ検索した結果，その中に u2 のアカウントが見つかった場合，検索結果で得られたすべての候補アカウントに対し類似度のスコアリングを行う．スコアリングの方法は様々存在するが，我々は一番簡単なスコアリング方法である以下を採用した．

$$Score\,(k, a) = \frac{1}{Rank\,(k, a)}$$

$$Rank\,(k, a) = \{\text{k で検索を行った時の a の順位 }\}$$

検索キーワード候補すべてでのスコアを算出し，これより得られたスコアの合計値を 1 としたときの u2 のスコアの割合をアカウント到達可能性とする．

3.3 結果と原因の求め方と提示方法

図 5　Account Reachability Checker

本システムの出力画面を図 5 に示す．利用者が 2 つの SNS にログインし (図 5 ①) ，チェックボタン (図 5 ②) を押すとシステムがアカウント到達可能性を算出する．検索結果のうち自身のアカウントがどの程度見つかるか提示する 「結果」 を出力画面左側のエリア (図 5 ③) に，利用者が見つかるきっかけとなったキーワードである 「原因」 を出力画面右側のエリア (図 5 ④) に提示する．

検索した結果の全体から自身のもう 1 つのアカウントが見つかってしまったことを直感的に分かりやすくするために，アイコンを用いて結果を提示する．全体の検索結果で得られたすべての候補アカウントを，利用者のアイコンを色つき，他の候補アカウントを灰色で表示する．アイコンの色を変えて表示することで一目で自身のアカウントを見つけることができる．またアイコンの大きさを類似度のスコアをもとに決定し，類似度に比例した大きさでアイコンを表示する．もしも表示されているアイコンの数が少なく，また自身のアイコンが大きく表示されていると，自身のもう一つのアカウントの見つかりやすさが視覚的かつ直感的にわかる．

また自身が見つかる原因となったキーワードをタグクラウドを用いて提示することで，自身が見つかる可能性の高いキーワードを他のキーワードより大きく表示することができ，どのキーワードが危険であるのかが分かりやすくなった．各キーワードの大きさは，それぞれのキーワードで得られたアカウント到達可能性の値により決定している．タグクラウドを用いた提示方法により大きく表示されたキーワードを自身の公開情報から削除するなど対策もしやすくなった．

これらのインターフェースにより，利用者は自身のアカウント到達可能性を直感的に理解できると考えられる．また繰り返し利用することで SNS を利用する上で危険なことや，上手な SNS の使い方を身に着けることができるなど，リテラシの向上も期待される．

4. ユーザテスト

我々は ARChecker の有用性をはかるユーザテストを行った．被験者は Facebook と Twitter のアカウントを持つ 6 名 (20 代女性：4 名，30 代女性：1 名，20 代男性：1 名) で，実際に ARChecker を利用し，以下の質問の回答を得た．

（1） アカウント到達可能性の値
（2） 自身が想定していた結果との比較
（3） 結果がアイコンによってわかりやすく提示されていたか
（4） 原因となったキーワードがタグクラウドによってわかりやすく提示されていたか
（5） システム自体が使いやすかったか

質問 1 と質問 2 の回答を以下の図 6 に示す．

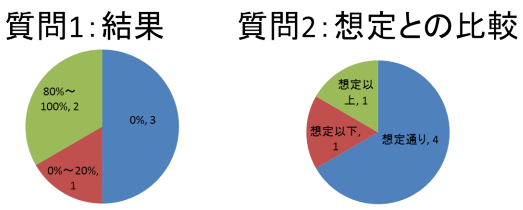

図 6　ユーザテストで得られた回答

アカウント到達可能性の値が 0% と回答した被験者が 3 名おり，それぞれの被験者の Facebook と Twitter の公開情報を比べてみると，アカウント名のみ公開しているなど特定されやすい情報を公開していないことが分かった．しかしながら 80% から 100% の値が算出された被験者は，公開している情報が同じであり，また被験者特有の情報を公開しているということが分かった．また想定との比較をみてみると，想定通りと答えた被験者のほとんどがアカウント到達可能性 0% の被験者であった．それぞれの被験者はアカウントが特定されないように対策を行っていた．この結果から対策がうまくいっていることがわかる．

質問 3 に対して全被験者がわかりやすいと回答した．しかしながらアイコンの大きさがどれほど大きければ危険なのかがわからないという意見を得た．また質問 4 に対しても全被験者がわかりやすいと回答したが，キーワードがどの情報をもとにして得られたものなのかがわかりにくいという意見を得た．

今後より多くの被験者に対しユーザテストを行い，利用者が危険と感じる値の特定を行っていく．

5. 関 連 研 究

SNS を利用した著者やプロフィール推定の研究は数多くされている．文献 [5] ではブログの内容から書き手の属性推定や著者の推定を行っている．またターゲットユーザのプロフィールを推定する手法として，文献 [6] では友人のプロフィールを利用したプロフィール推定方法の提案，文献 [7] では写真を利用したプロフィール推定手法が提案されている．また利用者の行動範囲の推定を行う研究も数多くされ，文献 [8] では Twitter のつぶやきから利用者がメッセージを発信した場所を推定する手法を提案している．

また第 3 者によってプロフィールが推定されることを利用者に提示するシステム提案されている．文献 [9] では SNS でのコメントや投稿内容から利用者が意図しない個人情報が漏洩してしまうことを利用者に提示するシステムを提案している．また Please Rob Me.com(注3) では Twitter のつぶやきから自宅にいない時間帯を抽出したり，ICanStalkU.com(注4) では GPS タグのついている写真の履歴をマップに表示して行動履歴を見せるなど，利用者に注意喚起を促すシステムも多く運用されている．

これらの手法は単一の SNS を対象としているが，我々のシステムは複数の SNS が関連付けられることによる個人情報の流出に着目している点が関連研究とは異なる．複数の SNS を利用したアカウントの推定手法として長谷川ら [10] の研究では，SNS の友人関係からアカウントの関連付けを行う手法が提案されている．この手法ではペアワイズ類似度を用いて，未だリンクを持たない 異なる SNS アカウント同士のペア間のエッジを予測している．我々の提案システムである ARChecker は，一つの SNS から別の SNS アカウントの候補を見つけ出し，それぞれのアカウントが利用者のアカウントであるか類似度を用いて探し出す手法であり，長谷川らのアプローチとは異なる．しかしながら類似度を算出する手法として，長谷川らの手法を用いることができると考える．

(注3)：http://pleaserobme.com/

(注4)：現在運用停止

6. まとめと今後の課題

近年サイバーストーキングによる個人情報取得が多く行われ，それらの被害から身を守る手段を考察した．サイバーストーカーは複数の SNS を関連付けることで多くの個人情報が取得していることが分かった．そこで我々は複数の SNS が関連付けられることによる個人情報の流出を防ぐために，自身が公開している情報を正しく認識できているか確認できるシステム Account Reachability Checker を開発した．本システムはアカウント到達可能性をチェックし，原因を利用者に提示するという簡単な仕組みである．これらの結果から，利用者自身が対策を行い身を守っていくことが期待される．また繰り返し利用することで対策がきちんと効果を出しているのか確認することもでき，対策方法を身に着けていくことで SNS を利用する上でのリテラシの向上が期待される．

アカウント到達可能性を求めるために用いられる情報は多くある．今後はプロフィール情報だけでなく，投稿内容から得られる情報を用いたアカウント到達可能性の考察を行く．また，より効果的にプライバシの露出度を意識させるインターフェースの考察，実装を行う．

謝　　辞

本研究は独立行政法人情報処理推進機構の 2012 年度未踏 IT 人材発掘・育成事業に採択され，支援を受けて開発を行いました．

文　　献

[1] 小林直樹: “ソーシャルメディア炎上事件簿,” 日経 BP 社, 200p., 2011.

[2] Cyber Stalker: http://www.jiten.com/dicmi/docs/k11/16720s.htm マルチメディア・インターネット事典 Dictionary of Multimedia and Internet

[3] 石澤恵, 渡辺知恵美: “複数のオンラインソーシャルネットワーク間におけるアカウント到達可能性を利用したプライバシ攻撃の調査と考察,” 電子情報通信学会第 2 種研究会資料,, WI2-2012-18, pp.51-52, 2012 年 3 月

[4] 総務省情報通信国際戦略局情報通信経済室 “次世代 ICT 社会の実現がもたらす可能性に関する調査研究報告書, ” 2011 年 3 月

[5] 奥村学: “ブログにおける偏り補正のための書き手のプロファイリング,” 人工知能学会誌,23 巻 6 号, pp.798-802, 2008 年 11 月

[6] Alan Mislove, Bimal Viswanath, Krishna Gummadi and Peter Druschel: “You are who you know: Inferring user profiles in Online Social Networks,” WSDM2010, pp.251-260, 2010 年 2 月

[7] Yu-Heng Lei, Yan-Ying Chen, Bor-Chun Chen, Lime Iida, Winston Hsu: “Where Is Who: Large-Scale Photo Retrieval by Facial Attributes and Canvas Layout,” SIGIR2012, 2012 年 8 月

[8] 伊川 洋平, 榎 美紀, 立堀 道昭: “マイクロブログのメッセージを用いた発信場所推定,” DEIM Forum 2012, F7-2, 2012 年 3 月

[9] 孫尚君: “SNS からの意図しない個人情報漏えい検出システムの開発 -アナライザ用周辺機能の開発及び GUI の設計-,” 筑波大学大学院博士課程 システム情報工学研究科特定課題研究報告書, 2012 年 3 月

[10] 長谷川聡, 佐久間淳: “異種ネットワーク間リンクのペアワイズ類似度に基づくリンク予測法,” The 26th Annual Conference of the Japanese Society for Artificial Intelligence, 2012
[11] Pfitzmann, Andreas and Hansen.: “A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management,”