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　(指導教員：渡辺 知恵美)

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．SNS は他者とのコミュニケーションを促進しているが，個人情報を公開することで円滑に行えることも多く，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」の事例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する過程を提示し，自身の公開情報を制御を促すシステム Account Reachability Checker (ARChecker) を提案する．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により，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のものであると第 3 者に推測される可能性をアカウント到達可能性（ Account Reachability ）と定義した．ARChecker はアカウント到達可能性を計算し提示する．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アイコンを用いた可視化と，利用者が結果を改善するためのヒントの提示を実装した．

2　サイバーストーキングによる個人情報の流出

サイバーストーキングとはインターネットを利用したストーカー行為のことである．サイバーストーキングは SNS 利用時の揉め事による憎悪などがきっかけとなり始まり，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挙げられる．

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 [1] をもとに分析したところ，ある 1 つの SNS を起点として，ユーザ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おり，利用者が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．

調査 [2] によると，SNS の利用者のうち約 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，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分かる．

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の中に気が付かないうちに公開しているなど自身で公開していることが多いが，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

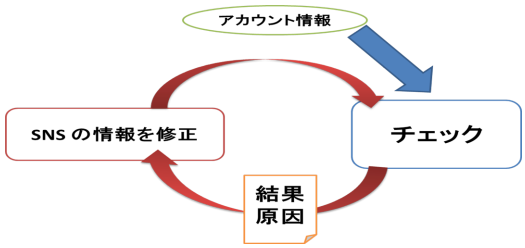

図 1: ARChecker における操作の流れ

ARChecker を使って利用者が公開情報を改善する流れを図 1 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 2: Account Reachability Checker

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ると仮定し，本システムの流れを図 2 に沿って説明していく．

1. U1 は アカウント S1 ，アカウント S2 両方にログインをする．
2. システムがアカウント到達可能性を算出する
3. 結果をユーザ U1 に提示する．
4. 原因となったキーワードを提示する．

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．アカウント到達可能性の求め方について 3.2 節で，提示される情報について 3.3 節で説明していく．

3.2 アカウント到達可能性の求め方

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．

$$AccountReachability\,(u1 \to u2) = \frac{\sum_{K \subseteq Kef} Score\,(K, u2)}{\sum_{K \subseteq Kef} \sum_{a \in Search(K)} Score\,(K, a)}$$

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

$KeyEnt(u1)$ は u1 から得られたキーワード候補の集合である．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アカウントに対し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のうち 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

本システムは，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」 を左側のエリア (図 2 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」 を右側のエリア (図 2 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アカウントをスコアをもとに大きさを決めて表示する．利用者のアカウントは色つき，他の利用者のアカウントは灰色で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．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．これ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 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，実装を行く．

謝辞

本研究は独立行政法人用法処理推進機構の 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．

参考文献

[1] 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

[2] 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