アカウント到達可能性に着目した SNS における個人情報漏洩の考察

理学専攻　情報科学コース　石澤　恵　（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）が普及しおり，それに伴い利用者も増加している．それと同時に SNS における個人情報漏洩が深刻な問題になっており，サイバーストーカーによる SNS ユーザの身元特定等の事態が起こっている．サイバーストーカーはターゲットとなるユーザが利用している複数の SNS アカウントを紐付けていき，そこで公開している情報を組み合わせることで身元を特定していく．しかし，SNS ユーザは複数の SNS アカウントが同一人物のものであると特定されることで，どれだけの情報が漏洩するかを認識していないことが多い．つまり，SNS ユーザは自身を守る為に，自身が持っている複数 SNS アカウントでの情報の漏れを認識する必要がある．我々はこのユーザの認識を助ける為に，サイバーストーキングの手法を調査し，その要素を考察した．そしてそれを基に，1 つの SNS アカウントから同一人物が利用しているもう 1 つの SNS アカウントがどの程度絞り込めるかを示す可能性「アカウント到達可能性(Account Reachability)」を定義した．本稿では，このアカウント到達可能性の定義と計算式について説明する．また実際に複数のアカウントにおいてアカウント到達可能性についての予備実験 を行ったのでこれを報告する．

2. サイバーストーカーによる個人情報の収集

サイバーストーカーは，ターゲットとなるユーザを決めてそのユーザの個人情報を収集し，その情報をインターネットに公開したり現実の世界でストーキングをするといった行為を行う．きっかけは，サイバーストーカーを行う人がターゲットとなるユーザのプロフィールや投稿などを見てネット上で好意や憎悪といった感情を持ってしまう等の一方的なものである．我々はネット上で一方的に憎悪の感情を持ってしまいネットストーキングに発展してしまう例として，炎上事件による個人情報の特定方法を調査した．炎上事件は SNS 上で道徳に反するコメントをしたり，ニュースなどによって取り上げられ注目されるなど，ユーザの予測しない何らかのきっかけで開始される.最近では，本人が書いた覚えのない架空のコメントをもとに炎上が発生する事象 確認されている．その際，通常の利用では特に意識していなかった，既に公開されている個人情報が，利用者とは面 識のない第 3 者によって自らの想定以上に収集してまとめ られ，全くの他人に晒されてしまう．

本節では書籍[2]に掲載されていた炎上事件の 1 つに関して個人情報の収集の過程を中心に述べる．2011 年 4 月末に，あるユーザが twitter 上で原子力発電所のメルトダウンをちらつかせる発言を繰り返した．これが原因となって炎上事件が発生し，tweet を行ったユーザの個人情報を特定する動きが起こった．図 1 はその時に起こった個人情報の収集の流れである．

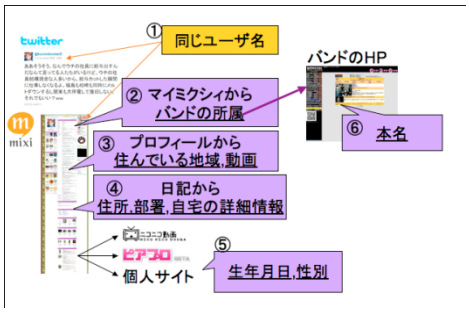

図 1:個人情報特定の流れ

①twitter 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．
②mixi 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．
④mixi の日記から，住所や会社の部署，自宅の間取り等が判明した．
⑤mixi 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，本人が登場する動画がさらに流出した．
⑥②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．

この例の個人情報特定の流れで注目すべきは，特定される SNS や web ページが増えるにつれて知られてしまう個人情報が増えていくという点である．炎上の元である twitter から，mixi や個人サイト，グループの web ページが明らかになることによって漏洩する個人情報の数が加速的に増加している．このことから我々は複数の SNS や Web ページが同一人物のものと推測され，更なる個人情報を特定されるという傾向に注目した．

3. アカウント到達可能性

前節に述べたように複数の SNS がたどられ，それらが同一ユーザのものであるとどの程度絞り込めてしまうかを示す可能性を，我々は**アカウント到達可能性(Account Reachability)**と定義する．これは，攻撃者の観点から，複数の行為を同一人物が行っていると関連付けられるかも

しくは関連づけられないかを十分に識別できる状態であることを意味する「到達可能性」(Reachability)の定義[1] に基づいている．(図 2).

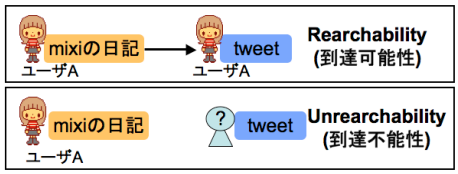

図 2:Reachability と Unreachability

到達可能性を求める式をいかに示す.

AccountReachability(u1 -> u2)
= 1 -(1-*ReachabilityByLink*(u1 -> u2))
* (1-*ReachabilityByIdentifier*(u1 -> u2))
*(1-*ReachabilityByQuasiIdentifier*(u1 -> u2))

リンクによる到達可能性である ReachabilityByLink，名前やアカウント名などの特定属性による到達可能性である ReachabilityByIdentifier，所属，性別，居住地の情報などによる準特定属性（属性値を組み合わせると個人が特定できる可能性のある属性）による到達可能性である ReachabilityByQuasiIdentifier，ユーザの友人関係による到達可能性である ReachabilityByRelationship の 4 項目によって構成される．以下各項について述べる．

- *ReachabilityByLink* (u_1->u_2):
  SNS_1 のアカウント u_1 のページから SNS_2 の u_2 に直接リンクが貼られていることによって第 3 者がアカウント u_2 にたどりつく可能性である．直接リンクがある場合は 1，無い場合は 0 を返す.

- *ReachabilityByIdentifier*(u_1->u_2):
  u1 の特定属性(アカウント名，氏名)から u2 が特定される可能性を表す値であり，以下の式で表される．

$$\mathrm{Re}\,achabilityByIdentifier(u_1 \rightarrow u_2) = \max_{c \in Cand(u_1,n)} \frac{Match(c,u_2)}{Rank\ (c,SNS_2)}$$

Cand(u_1, *n*)は u1 のアカウントから予測される． u2 の検索キーワードの候補である． Rank(*c*, *SNS*$_2$)は検索キーワード候補 c を SNS_2 上で検索した時の結果件数中で該当ユーザが現れた順位を表し， *Match*(*c*, u_2)は検索キーワード候補 c によって u_2 が検索された時は 1 を返し，検索されなかった時は 0 を返す.

ReachabilityByQuasiIdentifier (u_1->u_2):
u_1 の準特定属性から u_2 が特定される可能性を表す値であり，以下のように定義される．.

$$\mathrm{Re}\,achabilityByQuasiIdentifier(u_1 \rightarrow u_2) = \max_{c \in QCand(u_1,n)} \frac{Match(c,u_2)}{Rank\ (c,SNS_2)}$$

4. Reachability の調査

我々は予備調査として，mixi と twitter もしくは mixi とアメーバブログの両アカウントを持つ利用者に協力を得て，到達可能性を計算した．表 1(a)は mixi のアカウントを起点とした twitter への到達可能性，表 1(b)はアメーバブログへの到達可能性である．本予備調査では，ReabhabilityByRelationship を除く 3 項目にて計算を行った．表 1 中，"byLink" は ReachabilityByLink，"byID" は ReachabilityByIdentifier，"byQuasiID" は ReachabilityByQuasiIdentifier の値を示している．なお表 1(a)，(b)の各ユーザは同一人物ではない．表 1 を見て，わかるように直接リンクを張っていないものでも，特定属性によって到達できたり，リンクや特定属性での到達可能性は 0 でも準特定属性によって高い可能性で到達できてしまうアカウントが見られた．これらのアカウントは SNS によって使い分けをしており，書かれる内容が異なっていたため，万が一第 3 者によって情報が収集された時想定以上の情報が集められる可能性が高いことが予想される．

twitter

ユーザ	*ByLink*	*ByID*	*ByQID*
u1	1	$\frac{1}{258}$	1
u2	0	1	1
u3	0	1	0
u4	0	$\frac{1}{21}$	$\frac{1}{2}$

アメーバブログ

ユーザ	*ByLink*	*ByID*	*ByQID*
u1	0	0	1
u2	0	$\frac{1}{35}$	$\frac{1}{65}$
u3	0	1	$\frac{1}{2}$
u4	0	$\frac{1}{2}$	$\frac{1}{2}$

図 3:AccountReachability を適用した結果

5. まとめ

本稿では SNS におけるプライバシ保護を Reachability という観点から考察し，Reachability を求める式であるアカウント到達可能性を定義した．さらに実際の SNS データに対してアカウント到達可能性の式を適用し，我々が当初想定したより高い可能性で到達できてしまうことが示された．今後は，直接リンク，特定属性，準特定属性以外にもアカウント到達可能性を生む要因を調査したいと考えている

6. 謝辞

この研究は「独立行政法人情報処理機構　未踏 IT 人材発掘･育成事業」の支援を受けて実現しました.

参考文献

[1] Pfitzmann, Andreas and Hansen: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf Ver. 0.34, 2010.
[2] 小林直樹: ソーシャルメディア炎上事件簿, 日経 BP 社, 200p., 2011.