SNS 上のプライバシーセンシティブ情報の漏洩検知に基づく公開範囲の設定方式

町田 史門 [1]　**嶋田 茂** [2]　**越前 功** [1,3]

[1] 総合研究大学院大学 〒101-8430 東京都千代田区一ツ橋 2-1-2
[2] 首都大学東京 産業技術大学院大学 〒140-0011 東京都品川区東大井 1-10-40
[3] 国立情報学研究所コンテンツ科学研究系〒101-8430 東京都千代田区一ツ橋 2-1-2
E-mail: {shmachid, iechizen}@nii.ac.jp, shimada-shigeru@aiit.ac.jp

あらまし SNSが幅広い年齢層に普及し，多くの人々がSNSを楽しむ一方，SNS投稿に起因したプライバシー侵害のトラブルが多く発生している．その原因の1つとして，SNSユーザ自身によるプライバシーセンシティブ情報の漏洩がある．本稿では，このような情報の漏洩検知の為に，公文書の公開におけるプライバシー侵害に関連した公開基準をSNS投稿記事に適用検討し，SNSにおけるプライバシー侵害等情報分類表の定義と評価を行った．更にこのプライバシーセンシティブ情報の漏洩検知に基づく公開範囲の設定方式を提案した．

Settings of Access Control by Detecting Privacy Leaks in SNS

Shimon MACHIDA [1]　Shigeru SHIMADA [2]　Isao ECHIZEN [1,3]

[1] The Graduate University for Advanced Studies
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430 Japan
[2] Tokyo Metropolitan University AIIT
1-10-40 Higashi Ohi, Shinagawa-ku, Tokyo, 140-0011 Japan
[3] National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430 Japan
E-mail: {shmachid, iechizen}@nii.ac.jp, shimada-shigeru@aiit.ac.jp

Abstract People of all ages are enjoying Social Networking Services in these days. Posting messages through SNS increases privacy invasion since private information is leaked during the process. One of the reasons, SNS users often leak own privacy information by themselves. In this paper, we define and evaluate the classification table of privacy sensitive information for Social Networking Services will be based on the classification table of official archives. Besides, we propose the method of access control in SNS to be based on detecting privacy leaks.

1 研究背景と目的

1.1 研究背景

Twitter, Facebook に代表される SNS（Social Networking Service）が幅広い年齢層に普及し[1], SNS に投稿される日々のライフログを通じて，多くの他ユーザとのコミュニケーションを楽しんでいる. このような状況で SNS 投稿に起因したプライバシー侵害のトラブルが多く発生している．例えば，不用意な SNS 投稿により, 職を失う SNS ユーザも出ており[2], 何気ない投稿が予期しないトラブルへと発展する可能性がある．その原因の 1 つとして，SNS ユーザによる自身のプライバシーセンシティブ情報の漏洩がある．プライバシーセンシティブ情報とは, 本人/他人のプライバシーに関連した慎重に扱われるべき情報を指す. Y. Wang ら[3]の研究によると，自らプライバシーセンシティブ情報を漏洩してしまった SNS ユーザは，投稿後に自ら気付く，または他ユーザからの指摘により問題に気付き，その投稿行為に後悔する．更に，場所を含めた現在の状況が推測されやすい情報などのプライバシーセンシティブ情報が漏洩した場合，犯罪に繋がる恐れもあり[4]，投稿内容に細心の注意を払う必要がある. これら SNS への投稿はインターネット上に瞬時に流れていき，友人関係性の弱いユーザや面識の無いユーザも含めた広範囲に拡散していく．更にその投稿はインターネット上に長期間残り続ける危険性もはらんでいる．SNS 側では不用意な投稿への対応策として，投稿に対する”公開”・”友達”等の公開範囲を設定する機能を提供しているが，ユーザの中には面識の無いユーザが参照可能となるデフォルト設定：公開を使用し続けていたり，過去に設定変更をしていたが，SNS 側の機能拡張・改変時にデフォルト設定へ戻り，その後気付かずに意図していないユーザが投稿を参照可能となっているケースもある[5]．また，SNS ユーザは現在提供されている友達・大学・会社等の特定グループといったユーザの属性情報をベースとした公開対象以外に，投稿内容によって特定の個人や興味を持つグループに対して，安全に効果的に公開したいと考えている[6]．この投稿内容に応じた公開範囲を設定したいというユーザ要求を満たす為に，新しい機能が必要とされている.

1.2 研究目的

SNS へのプライバシーセンシティブ情報の漏洩を検知する為には，SNS 投稿する際に，このような情報を含むか否かの判断基準が必要となるが，実社会においても同様の判断基準が必要とされている．今日までの歴史的な史料や公的文書である公文書の管理・公開の役割を担う機関として，国・都道府県・市町村が管轄する公文書館が存在する．公文書館では公文書などの公開にあたり，公開基準を設けており，その基準の 1 つにプライバシー侵害がある. これは公開対象となる公文書に，プライバシー等の人権侵害，個人・法人の権利権益を不当に害する恐れのある情報が含まれている場合に考慮が必要なためである[7]. そこで，前研究[8]では，公文書館が管理・公開する公文書に対して, SNS 投稿記事は, SNS ユーザによって作成されるテキストや画像，位置情報等の属性情報を含む私文書であることから, デジタル私文書と定義した. そして，「プライバシー等侵害の度合い」を区分しつつ，保護期間を定める公文書館での試み[9]である，戸嶋によるプライバシー等侵害情報分類表（私案）[7]を基にデジタル私文書におけるプライバシー侵害等情報分類表を定義した.

本稿では，このデジタル私文書におけるプライバシー侵害等情報分類表を蓄積された過去の SNS データアーカイブに適用し, プライバシーセンシティブ情報の漏洩検知が可能であるかの評価を行う．そして，その評価結果を基に，プライバシーセンシティブ情報の漏洩検知に基づく公開範囲の設定方式を提案する．以降，2 章でデジタル私文書におけるプ

ライバシー侵害等情報分類表について述べ, 3 章ではこの分類表を適用した SNS データアーカイブの分析，4 章ではプライバシーセンシティブ情報の漏洩検知に基づく公開範囲の設定方式の提案を行う.

2 プライバシー侵害分類表

2.1 公文書のプライバシー情報の取扱

歴史的な史料や公的資料などの公文書を管理する公文書館では，所蔵資料を可能な限り一般に公開することを理想としているが，公文書を公開するにあたり，プライバシー侵害の恐れのある情報が含まれているか考慮する必要がある．その試みの 1 つである戸嶋によるプライバシー等侵害情報分類表（私案）[7]では，縦軸を非公開とすべき情報の内容による 6 分類，横軸を非公開とすべき情報の重要度による 3 分類，及びその非公開期間の 2 軸から構成されるが，縦軸の非公開とすべき情報の内容では，SNS において発生し難い分類が含まれていること，横軸の分類の重要度に応じた非公開期間においては，SNS 投稿時では原則，非公開期間を待たずに即時公開であることが問題となる．そこで，この分類表を基に, SNS ユーザが SNS 投稿後に後悔する事象を反映させた非公開とすべき情報の内容による分類と，非公開とすべき情報の重要度による非公開期間を，重要度による公開範囲に置き換え，デジタル私文書版のプライバシー等侵害分類表を定義する.

2.2 投稿の後悔と非公開とすべき情報

デジタル私文書におけるプライバシー等侵害分類表の縦軸の非公開とすべき情報の内容による分類を検討するにあたり，SNS ユーザが SNS 投稿後に後悔する事象を分析する．Y. Wang ら[3]によると，感情の高ぶりを含む感情に起伏がある時やアルコール等の影響がある時の SNS 投稿は, 自らプライバシーセンシティブ情報を漏洩し，後日後悔している．また，必要以上のプライバシーセンシティブ情報を公開してしまった上に，意図していないユーザにまで情報が漏れていたことに気づき, 更に後悔する[10]. これら過去の研究[3, 6, 10]から後悔を伴った SNS 投稿の分類とその内容は，以下であった.

- ✓ 宗教
  信仰している宗教・思想の情報
- ✓ 病気・疾患
  精神症状・身体情報を含む個人や家族の病歴情報
- ✓ 個人の特定情報
  自身や他者が特定される可能性のある写真や個人・家族に関する情報
- ✓ 行動傾向
  犯罪を含む非常識的な行動，日常生活における個人の活動状況や趣味嗜好等の情報

これらの結果を戸嶋によるプライバシー等侵害情報分類表を基にまとめ，表 1 に示す．本分類表により，投稿内容に含まれる非公開とすべき情報の分類とその重要度を表現した.

2.3 重要度に応じた開示範囲

次に，非公開とすべき情報の重要度による投稿の開示範囲を定義する．公文書では，意図していないユーザに情報が公開される事を防ぐために，文書内容による非公開対象者を設定する基準はなく，一定の非公開期間と文書の部分公開によりプライバシー情報が漏れることを防ごうとしている．これは原則，即時公開 且つ, 投稿内容の部分公開を無しとする SNS 投稿記事には適用出来ない公開基準となる. そこで, 非公開とすべき情報の”重要度による非公開期間”に置き変わる指標として, ”重要度による公開範囲”を定義する. SNS ネットワーク内の公開範囲の研究として，M.Gala ら[11]による SNS エゴネットワークにおける友人分類の研究がある．エゴネットワークとは，社会ネットワーク分析における特定のユーザを中央に配置したネットワークを指し，例えば Facebook や LinkedIn における友達リストは自分自身を中心としたエゴネッ

表 1： デジタル私文書におけるプライバシー侵害等情報分類表

非公開とすべき情報の内容による分類 ＼ 非公開とすべき情報の重要度による分類及び公開範囲		個人の特に重大な秘密であって，当該情報を公にすることにより，当該個人の生存中の権利・利益を不当に害する恐れがある	個人の重大な秘密であって，当該情報を公にすることにより，当該個人の社会生活上の権利・利益を不当に害する恐れがある	個人の秘密であって，当該情報を公にすることにより，当該個人の権利・利益を不当に害する恐れがある
		開示レベル 1 家族＋ 親友（1-5 人） 週 1 回以上の コミュニケーション	開示レベル 2 友達 （6-15 人） 月 1 回以上の コミュニケーション	開示レベル 3 知人以上 友達未満 （16-50 人） 半年 1 回以上の コミュニケーション
個人の内心に関する情報	思想，信条	個人の信条主張		一般的な社会信条
	宗教	個人の宗教観		
個人の心身の状態に関する情報	病歴	個人の病気・疾患（重度）		個人の病気・疾患（軽度）
	心身の記録		個人の精神的な症状	個人の身体情報（身長・体重など）
個人の基本情報，生活の状況に関する情報	戸籍，外国人，登録，写真		個人特定可能な写真	
	家庭状況			家族構成や家庭状況等の家族情報
	行動傾向	非常識な行動傾向，活動状況		日常的な行動傾向，活動状況
個人の経歴，社会的活動等に関する情報	犯罪及び不法行為	犯罪行為（重度）	犯罪行為（軽度）	

トワークを構成していると見なす．この研究では，SNS エゴネットワークに対して，Dunbar’s circle [12]を適用し，エゴネットワーク内の友達との関係性の強弱に SNS 内のコミュニケーション頻度を用いている．そして，関係性の強弱から導出された 4 サークルへの分類結果が現実世界の分類と似ている事を示した．Dunbar’s circle では，認知科学の観点から人間にとって，それぞれの人間と安定した関係を維持可能な上限数は平均 150 人程度としている．例えば，Facebook において友達が 150 人以上存在する場合，自身の”友達”リスト内に友人関係が非常に弱いユーザが含まれていることを意味し，即ちプライバシーセンシティブ情報の漏洩に繋がる可能性がある．この Dunbar’s circle と M.Gala らの SNS 内コミュニケーション頻度による分類をベースに，非公開とすべき情報の重要度による公開範囲として，新たに開示レベルを定義する．表 2 に SNS エゴネットワークにおける開示レベルを示す．

最も厳しい開示レベル 1 の公開対象としては，”家族”＋”親友”とし，親友とは週に 1 回以上のコミュニケーションがあり，その人数は 1～5 人とするが，この人数に家族は含めないこととする．次に，開示レベル 2 の公開対象は，”友達”とし，月に 1 回以上のコミュニケーションがあり，その人数は 6～15 人とする．開示レベル 3 は”知人以上 友達未満”を指し，半年に 1 回以上のコミュニケーションがある．同様にその人数は 16～50 人とする．そして，開示レベル 4 は”知人”とする．この開示レベルでは，プライバシーセンシティブ情報を含まない投稿内容であるため，本プライバシー侵害等情報分類表に未記載であるが，その人数は 51 人～150 人とする．最後に開示レベル 5 を他人とし，全くコミュニケーションが無い・もしくは，数年音沙汰が無いケース等を指す．なお，下位の開示レベルは，上位の開示レベルの公開対象も含むものとし，分類表において複数の分類が該当した場合は，より厳しい開示レベルを採用することとする．

表 2: SNS エゴネットワークにおける開示レベル

開示レベル	公開対象	人数（人）	コミュニケーション頻度
1	家族＋親友	1～5	週 1 回以上
2	友達	6～15	月 1 回以上
3	知人以上 友達未満	16～50	半年 1 回 以上
4	知人	51～150	年 1 回以上
5	他人	151～	年 1 回未満

次節では，本プライバシー侵害等情報分類表を Twitter アーカイブに適用し，プライバシーセンシティブ情報の漏洩検知の評価を行う．

3 評価

3.1 センシティブ情報の漏洩検知

SNS ユーザの投稿内容に対して，プライバシーセンシティブ情報の含有を検知する為に，デジタル私文書におけるプライバシー等侵害情報分類表を適用した判別評価を行う．対象データは，過去 1 年間（2012/6/19～2013/6/13）に蓄積された日本語 Twitter アーカイブ 約 1 億 4000 万件とする．この Twitter アーカイブに対して，①個人の内心に関する情報として，”宗教”，②個人の心身に関する情報として，“病歴”・”心身の記録”，③個人の基本情報・生活状況に関する情報として，“行動傾向”に関連した情報の含有を分析し，プライバシー漏洩がどの程度発生しているのか確認する．

3.2 個人の内心に関する情報（宗教）

個人の内心に関する情報における個人の信仰宗教の漏洩として，分類表の開示レベル 1：個人の信仰宗教を検出する．個人的/一般的の判断としては，キーワードマッチング処理後のツイートに対して肯定的な意見を持つ，または否定的な意見を持つ場合に，個人の宗教観と判断する．また，肯定/否定のどちらでも無い場合は，中立的な意見として，一般的な政治観とするが，その場合は分類表に沿い，開示レベルの設定は無しとなる．

最初に全ツイートから Wikipedia:宗教一覧[13]を使用しキーワードマッチングを行う．次に，ハッシュタグ・リツイート・URL 付きツイートのフィルタリング処理を行った結果，17,123 件のツイートを抽出した．このツイートからランダムに 1000 件を抽出し，①肯定，②否定，③中立，④無関連の 4 値分類を 2 名で実施し，同値の分類としたツイートを正しく分類出来たものと見なす．このツイートの分類内訳を表 3 に示す．

表 3: 個人の内心に関する情報（宗教）の内訳

	検出率
肯定	1%
否定	13%
中立	10%
無関連	76%

上記結果より，開示レベル 1： 個人の宗教観は，肯定・否定の合計より 14%が該当した．

3.3 個人の心身の状態に関する情報

次に，個人の心身の状態に関する情報における，病歴・心身の記録の漏洩として，分類表の開示レベル 1：個人の病気･疾患（重度），開示レベル 2：個人の精神的な症状，開示レベル 3：個人の病気・疾患（軽度）を検出する．対象とする病症は Yahoo! 家庭の医学[14]を使用するが，予め対象とする病気・疾患に対して，重度・軽度，精神的症状のカテゴリ分けを行った．

最初に全ツイートからこれらの病症を使用しキーワードマッチングを行った．次にハッシュタグ等，前項と同様のフィルタリング処理を行った結果，45,383 件のツイートを抽出した．更に，このツイートから人手により SNS ユーザ自ら情報漏洩しているか否かを判別した結果，418 件であった．そのツイートの分類内訳を表 4 に示す．この結果より，開示レベル 1： 個人の病気・疾患（重度）は，癌・脳梗塞等の合計から 38%，開示レベル 2：個人の精神的な症状は，鬱・パニック障害等の合計から 16%，開示レベル 3：個人の病気・疾患（軽度）は 46%であった．

表 4: 個人の心身の状態関する情報の内訳

	検出率
癌	23%
鬱	12%
血尿	6%
脳梗塞	5%
その他	54%

3.4 個人の生活状況に関する情報

最後に，個人の生活に関する情報として，行動傾向の漏洩を検知するために，分類表における開示レベル 1： 非常識な行動傾向，開示レベル 3：一般的な行動傾向を検出する．SNS ユーザが感情の高ぶりを含む感情に起伏がある時の SNS 投稿は，自らプライバシーセンシティブ情報を漏洩しやすい [3]ことから，ツイートがポジティブ（P）/ネガティブ（N）であるかの感情極性を判別する．感情極性の判別には，日本語評価極性辞書[15]を利用する．処理手順は以下である．

① 全ツイートに対して，形態素解析器 Mecab を用いて形態素解析し、日本語評価極性辞書を基に単語毎の P/N 判定を行う．

② ツイート毎の P/N スコアを 1.0 ～0.0 で算出する．ポジティブ傾向であれば，より 1.0 に近づき，ネガティブ傾向であれば，より 0.0 に近づいた値となる．

③ P/N スコアに閾値（0.75 以上，または 0.25 以下）を設定する
全体の 12%のツイートが閾値以上（N は閾値以下）であった．

④ 画像共有サービスの URL 付きツイートに絞り込む
感情の高ぶりがある時の写真付き投稿は，よりプライバシー情報に対する判断が緩くなると仮定し，画像共有サービスと紐付いたツイートにフィルタリングする．

上記手順で実行した結果，70,364 件を抽出した．更に，このツイートからランダムに 7000 件を抽出し，分類表の開示レベルに沿い，①非常識な行動傾向，②個人特定可能な写真，③日常的な行動傾向，④その他の 4 値分類を実施した．分類内訳を表 5 に示す．

表 5:個人の生活状況に関する情報の内訳

	検出率
非常識な行動傾向	0%
個人特定可能な写真	0.35%
日常的な行動傾向	0.19%

開示レベル 1：非常識な行動傾向は検出できなかったが，開示レベル 2，3 は計 0. 5%の検出率であった．

3.5 検知結果と考察

開示レベル毎のプライバシーセンシティブ情報の漏洩検出率を表 6 に示す．これまでの分析により，1 億 4000 万件のツイートから開示レベル 1-3 の情報漏洩として，0.002%を検知した．

表 6:開示レベル毎の検出率

	検出率
開示レベル 1	0.0002%
開示レベル 2	0.0017%
開示レベル 3	0.0001%

プライバシーセンシティブ情報の漏洩検出率は，どの開示レベルも低い結果であったが，一度漏洩してしまった情報を無かったことにすることは難しく，また，職を失う等社会的な制裁を受ける可能性も考慮すると，ごく少数であっても，SNS 提供者側で未然にその漏洩を検知・指摘する必要がある．

4 公開範囲の設定方式の提案

4.1 投稿内容に応じた公開範囲の提案

2013 年 8 月現在, Facebook では投稿時の公開範囲の設定機能として，”公開”・”友達”・”SNS 側で作成される特定グループ”・”ユーザによりカスタマイズ可能なグループ”を提供している. Twitter においては, ”公開”・個別ユーザに対する”ダイレクトメッセージ”機能を提供している．しかし，多くの SNS ユーザは通常，公開範囲：友達を設定しているが[5]，F.Stuzman ら[16]によると，公開範囲：

友達には関係性の弱い友人が含まれており，依然としてプライバシー関連の危険性があるとしている．また，ユーザによっては，投稿内容によって公開対象として望ましいユーザの選択や望ましくないユーザの除外を行なっているが[17]，投稿の都度行なっていくことは難しい．この事から，SNS ユーザは現在提供されている公開範囲の設定以外に，投稿内容によって特定の個人や興味を持つグループに対して，安全に効果的に公開したいと考えている[6]．そこで，ユーザが投稿する情報は原則全公開として，SNS の特徴である他ユーザとの繋がりを尊重しつつも，プライバシーセンシティブ情報を含む場合のみ，2 章にて説明したデジタル私文書におけるプライバシー侵害等情報分類表を用いてその重要度と開示レベルを判別し，プライバシーセンシティブ情報の漏洩有無の通知と，自身を中心としたエゴネットワーク内における開示レベルに従った公開範囲の設定方式を提案する．

4.2　関連研究

プライバシー漏洩を検知する研究として，H. Maoら[18]によるTwitterにおけるプライバシー漏洩情報の抽出とその原因分析がある．この研究では，プライバシーセンシティブ情報として，本稿と同様に感情が高まった際に投稿をするシーンとして，休暇・アルコール・病気に注目している．だが，これらのシーンに注目した経緯と漏洩検知後の漏洩防止方式に関して発展途上である．また，A.Squicciariniら[19]は，SNS投稿時の公開範囲設定に関連した研究として，新たにSNSへ投稿される画像を含む記事に対してプライバシー保護ポリシーを動的に生成し，そのポリシーを用いてプライバシー保護を行う方式を提案している．しかし，この方式による公開範囲の提案は，SNS側が提供する友達や特定グループを対象としており，依然として関係性の弱い友人が含まれ，且つ，公開対象が特定グループに縛られる問題がある．

4.3　システム概要

SNS投稿時に発生するプライバシーセンシティブ情報の漏洩検知に基づく公開範囲の設定方式を提案する．本システムでは，SNSユーザがSNS投稿を行う前に，事前利用する事で，投稿記事内にプライバシーセンシティブ情報が含むかどうか，含まれる場合に誰に対して参照可能とすべきかの公開範囲を算出し，その提案通知を行う．更にSNSユーザはこの公開範囲の提案に対して，公開対象者の追加・除外といった改訂することができ，最終的なSNSへの投稿はユーザに委ねることとする．また，その改訂情報は次回投稿時の公開範囲提案に考慮される．これにより，SNSユーザはプライバシーセンシティブ情報を意図していないユーザに対して公開されることなく，自身による公開範囲の管理が容易に可能となる．

4.4　システム内の分析プロセス

本システムの概略フローを図1に示す．

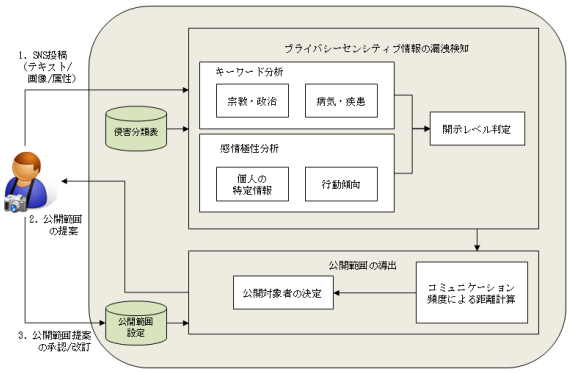

図 1：　システム概略フロー

本システムは大きく分けて，漏洩検知，公開範囲の導出，結果通知の3プロセスから構成される．以下では，そのプロセスを説明する．

Step1　プライバシーセンシティブ情報の漏洩検知

テキスト・画像・属性情報から構成される SNS 投稿記事を解析し，プライバシーセンシティブ情報を検知する．その判断基準として，２章で定義したプライバシー侵害等情報分類表を適用するが，非公開とするべき情報の内

容による分類により，分析方針が異なる．個人の内心に関する情報，個人の心身の状態に関する情報は，関連キーワードによる検知を行う．それ以外の個人の基本情報や生活状況に関する情報等に関する情報は，感情の高ぶりを含めた感情起伏が出ている時に判断が緩くなり投稿した場合，プライバシーセンシティブ情報の漏洩傾向がある為，投稿テキストにおける感情極性の分析によりポジティブ(P) / ネガティブ(N)を検知する．また，プライバシーセンシティブ情報の漏洩が検知された場合，プライバシー侵害等情報分類表に従い，投稿の開示レベルを決定する．

Step2 公開範囲の導出

Step1 にて決定した開示レベルに応じて, 自身を中心とした SNS エゴネットワーク内における友達とのコミュニケーション頻度による距離を測り，最終的な公開対象者を決定する．その際，以前の投稿に対する改訂情報を考慮し，公開対象者の追加・除外を行う．これにより，コミュニケーション頻度が少なくても，友人関係性が強いケース，またはその逆のケースに対する考慮となる．

Step3 結果通知

分析結果であるプライバシーセンシティブ情報の含有有無とその公開範囲をSNSユーザへ通知する. SNSユーザは本システムからの公開範囲の提案に対する投稿可否判断として，承認/改訂を行った後，SNSへ本投稿する．承認/改訂情報はシステム側に蓄積され，次回の投稿時の公開範囲提案に考慮される．

5 まとめと今後の活動

SNS 投稿時のプライバシーセンシティブ情報の漏洩を検知するため，公文書におけるプライバシーに関連した公開基準を SNS 投稿記事に適用し，デジタル私文書におけるプライバシー侵害等情報分類表を定義した．次にこの分類表を適用し，Twitter アーカイブからプライバシーセンシティブ情報の漏洩検知を行い，その漏洩検知に基づく公開範囲の設定方式の提案を行った．今後は，より多くの漏洩検知が可能となるような手法と，それらを自動検知する手法の検討を行う予定である．

参考文献

[1] 72% of Online Adults are Social Networking Site Users, http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_Social_networking_sites_update.pdf, 2013

[2] The Twitter Typo That Exposed Anthony Weiner, http://www.huffingtonpost.com/2011/06/07/anthony-weiner-twitter-dm_n_872590.html, 2011

[3] Y.Wang, G.Norcie, S.Komanduri, A.Acquisti, P.Leon, and L.Cranor, “I regreted the minute I pressed share”: A qualitative study of regrets on Facebook. SOUPS2011, 2011

[4] Twitter user says vacation tweets led to burglary, http://news.cnet.com/8301-1009_3-10260183-83.html, 2008

[5] F.Stutzman, R.Grossy, A.Acquisti, Silent Listeners: The Evolution of Privacy and Disclosure on Facebook, 2012

[6] M.Sleeper, R.Balebako, S.Das, A.McConahy, J.Wiese, J.Cranor, The Post that Wasn’t: Exploring Self-Censorship on Facebook, 2013

[7] 戸嶋明, 地方公文書館における公開をめぐる問題と対応について, アーカイブズ no.35, p.40-44, 2009

[8] 町田史門, 嶋田茂, 越前功, to be published, デジタル私文書におけるプライバシーセンシティブ情報の漏洩検知に基づく公開範囲の設定方式の提案, 2013

[9] 古賀崇, オープンガバメントとデータアーカイブ : 法制度的側面からの考察, ワークショップ「ビッグデータと“程よい”プライバシー」, 2013

[10] M.Sleeper, J.Cranshaw, P.Kelly, A.Acquisti, “I read my Twitter the next morning and was astonished” A Conversational Perspective on Twitter Regrets, 2013

[11] M.Gala, V.Arnaboldi, A.Passarella, M.Conti, Ego-net Digger: a New Way to Study Ego Networks in Online Social Networks, 2012

[12] R.I.M.Dunbar, The social brain hypothesis, 1998

[13] Wikipedia: 宗教一覧, http://ja.wikipedia.org/wiki/%E5%AE%97%E6%95%99%E4%B8%80%E8%A6%A7, 2013

[14] Yahoo! 家庭の医学, http://health.yahoo.co.jp/katei/, 2013

[15] 東山昌彦, 乾健太郎, 松本裕治, 述語の選択選好性に着目した名詞評価極性の獲得, 2008.

[16] F.Stuzman, J.Kramer-Duffild, Friends only: examining a privacy-enhancing bevavior in Facebook, 2010

[17] S.Kairam, M.Brzozowski, D.Huffaker, H.Chi, Talking in Circles: Selective Sharing in Google+, 2012

[18] H.Mao, X.Shuai, A.Kapadia, Loose Tweets: An Analysis of Privacy Leaks on Twitter, 2011

[19] A.Squicciarini, S.Sundareswaran, D.Lin, J.Wede, A3P: Adaptive Policy Prediction for Shared Images over Popular Content Sharing Sites, 2012