情報処理学会論文誌 Vol.55 No.9 2092–2103 (Sep. 2014)

推薦論文

SNSにおけるセンシティブデータの漏洩検知に基づく公開範囲の設定方式

町田 史門[1,a)] 梶山 朋子[2] 嶋田 茂[3] 越前 功[1,4]

受付日 2013年11月29日, 採録日 2014年6月17日

概要：SNS（Social Networking Service）が幅広い年齢層に急速に普及し，SNS に投稿されるライフログにより，多くの人々がコミュニケーションを活発化している一方，SNS 投稿に起因したプライバシ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 ユーザによる，個人に関する情報の漏洩がある．本論文では，SNS ユーザの不用意な投稿による個人に関する情報の漏洩が，実際に発生していることを確認するために，Twitter アーカイブにおけるこのような情報漏洩の存在率の試算評価を行った．次に，本試算評価を受け，SNS 投稿時に発生する情報漏洩を自動検知する第一歩として，非公開とすべき情報の内容分類と開示レベルを対応付けた，SNS におけるプライバシ侵害情報分類表の提案とその評価を行った．さらに本分類表の特性を活かし，センシティブデータの漏洩有無の通知と，SNS 投稿者を中心としたネットワーク内における公開対象者の自動設定を提供するシステムを提案した．

キーワード：プライバシ，センシティブデータ，SNS，Twitter，公開範囲

Settings of Access Control by Detecting Sensitive Data Leaks in SNS

Shimon Machida[1,a)] Tomoko Kajiyama[2] Shigeru Shimada[3] Isao Echizen[1,4]

Received: November 29, 2013, Accepted: June 17, 2014

Abstract: Social Networking Service is rapidly becoming popular for all ages nowadays. Users communicate by posting messages in SNS. On the other hand, posting messages through SNS increases invasion of privacy. One of the reasons is SNS users themselves often leak their sensitive data unintentionally. In this paper, to confirm leakage of sensitive information by unintentional posts, we evaluate the abundance ratio of sensitive data in Twitter archive. As a result, we define and evaluate a classification table of invasion of privacy for SNS that is based on classification according to contents of information which should be kept private, and disclosure level as the first step to detect privacy leaks automatically. We also propose a system that provides automatic configuration of disclosure target based on SNS egocentric network.

Keywords: privacy, sensitive data, SNS, Twitter, access control

1. 研究背景

Twitter，Facebook に代表される SNS（Social Networking Service）が幅広い年齢層に急速に普及し [1]，SNS に投稿されるライフログによる友人や他ユーザとのコミュニケーションが活発化している一方で，SNS 投稿に起因した

1 総合研究大学院大学
The Graduate University for Advanced Studies (SOKENDAI), Chiyoda, Tokyo 101–8430, Japan
2 青山学院大学
Aoyama Gakuin University, Sagamihara, Kanagawa 252–5258, Japan
3 首都大学東京産業技術大学院大学
Tokyo Metropolitan University Advanced Institute of Industrial Technology, Shinagawa, Tokyo 140–0011, Japan
4 国立情報学研究所コンテンツ科学研究系
National Institute of Informatics, Chiyoda, Tokyo 101–8430, Japan
a) shmachid@nii.ac.jp

本論文の内容は 2013 年 10 月のコンピュータセキュリティシンポジウム 2013 にて報告され，コンピュータセキュリティ研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

プライバシ侵害のトラブルが多く発生している．不用意なSNS投稿により，職を失うSNSユーザが出る等 [2]，何気ない投稿が予期しないトラブルへと発展している．その原因の1つとして，友人や他ユーザだけでなく，SNS投稿者自身によって，個人に関する情報を漏洩させていることがあげられる．

総務省主催のパーソナルデータの利用・流通に関する研究会 [3] では，個人に関する情報を“パーソナルデータ”と定義している．パーソナルデータは，プライバシに抵触する可能性のある性質を表すプライバシ性の高低により，(1) 一般パーソナルデータ，(2) 慎重な取扱いが求められるパーソナルデータ，(3) センシティブデータの3種類に分類されている．“一般パーソナルデータ”とは，保護されるパーソナルデータのうち，プライバシ性が高くないものと定義されている．氏名等の公知情報，本人の明確な意図で一般に公開された情報，名刺に記載されている情報等のビジネス関連情報を指す．“慎重な取扱いが求められるパーソナルデータ”は，一般パーソナルデータよりもプライバシ性が高いものと定義されており，GPS等の位置情報や継続的に収集される購買・貸出履歴等を指す．“センシティブデータ”とは，思想・信条等に関する情報，健康情報等の慎重に扱われるべき，最もプライバシ性の高い情報を指す．これら3種類のパーソナルデータのうち，プライバシ性の高くない一般パーソナルデータは，氏名等保護される情報が定まっているため，パーソナルデータに該当するか否かの判断がつきやすく，SNSにおいてメールアドレス等の個人識別性を有する単純な情報が投稿されることは稀であるとされている [4]．また，慎重な取扱いが求められるパーソナルデータの中でも，SNS投稿に付帯する情報としてGPS等位置情報は，FoursquareやGoogle Maps等の位置情報サービスに主に利用されているが，ユーザは状況に応じて位置情報機能のON/OFFを使い分ける等，その危険性を認識している [5]．しかし，分類のプライバシ性が高まるにつれ，保護すべき情報の定義が曖昧となり，パーソナルデータであるかの判断が難しくなる．最もプライバシ性の高いセンシティブデータは，保護対象とすべき情報を，諸外国や国際機関等におけるパーソナルデータの範囲の定義や，日本国内の各省庁の個人情報保護法に基づくガイドライン等もふまえて，検討されているが [3]，実社会において，個人情報保護に対する誤解や理解不足が指摘されており [6]，SNS投稿時にセンシティブデータが含まれていることに気付きにくい．実際に，自らセンシティブデータを漏洩してしまったSNSユーザは，投稿後に自ら漏洩に気付いたり，友人や他ユーザからの指摘によって漏洩を認識し，その不用意な投稿行為に後悔している [7]．このことから，センシティブデータの漏洩がSNSにおけるプライバシ侵害のトラブルを引き起こす原因の1つになっていると考えられる．

SNSでの投稿はインターネット上に瞬時に流れ，友人関係性の弱いユーザや面識のないユーザも含めた広範囲に拡散していくため，長期間残り続ける可能性が高い．投稿に含まれる現在の所在や状況が推測されやすい情報を含むセンシティブデータが漏洩した場合，犯罪につながる恐れも指摘されているため [8]，投稿内容には細心の注意を払う必要がある．しかし，地域や家庭における文化やその背景等からユーザのプライバシへの理解に多様性があり，SNSユーザが投稿内容にセンシティブデータが含まれるか否かを共通認識のもと，判断することはきわめて難しい．

現在，SNSサービスにおいて，このような不用意な投稿によるプライバシ侵害のトラブルを軽減するための手法として，投稿に対する公開範囲の設定が用意されている [9]．しかし，SNSユーザの中には，(1) 面識のないユーザが参照可能であるデフォルト設定のまま使用し続ける，(2) 過去に友人等の特定の人のみに公開できるよう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ってしまったことに気付かず，自身の投稿を面識のないユーザが参照可能な状態で使用し続ける [10] 等の問題が発生している．ユーザのITリテラシの低さから，意図していないユーザへの情報が漏洩する場合もあるため，SNSサービス提供者側は，ユーザが投稿する前の投稿予定記事にセンシティブデータが含まれているかどうかを自動検知し，ユーザに提示する仕組みが必要である．

本論文では，実際にSNSで発生しているセンシティブデータの漏洩を確認するために，過去1年間分の1億4,000万件のTwitterアーカイブを用いて，センシティブデータの漏洩有無とその検知手法を試算評価する．また，この評価結果を受け，SNS投稿予定記事に含まれるセンシティブデータを自動検知するための第一歩として，非公開とすべき情報の内容分類と開示レベルを対応付けたSNSにおけるプライバシ侵害情報分類表を提案する．さらに，本分類表の妥当性を評価するために，一対比較法を用いた評価調査を実施する．本分類表を適用することにより，センシティブデータが含まれたSNS投稿記事の内容から漏洩の有無と開示レベルを判断できるようになる．この特性を活かし，センシティブデータの漏洩有無の通知と，投稿者を中心としたネットワーク内における公開対象者の自動設定を提供するシステムを提案する．

2. センシティブデータの漏洩検知

SNSにおけるセンシティブデータ漏洩の既存研究において，感情の高ぶりを含む感情に起伏があるとき，アルコール等の影響があるときのSNS投稿は，自らセンシティブデータを漏洩させてしまい，後日後悔するとしている [7]．また，必要以上にセンシティブデータを公開してしまったうえに，意図していないユーザにまでその情報が漏れていたことに気付き，さらに後悔している [11]．そして，SNS

表 1 個人の内心に関する情報の分類結果
Table 1 Classification results of information relating to inner nature of individuals.

分類	検出率
肯定	1%
否定	13%
中立	10%
無関連	76%

ユーザはこのような後悔を防止するために，投稿予定内容に応じた様々な投稿可否の判断基準を持っている [12]．そこで，このような SNS ユーザの不用意な投稿によるセンシティブデータの漏洩が実際に SNS で発生していることを確認するために，前述の SNS ユーザの後悔事例 [7], [11], [12] をもとに，Twitter アーカイブにおけるセンシティブデータの存在率の試算評価を行った．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 137,877,745 件とした．この Twitter アーカイブに対して，これらの後悔事例より，(1) 個人の内心に関する情報としての “宗教”，(2) 個人の心身の状態に関する情報としての “病歴” と “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の “行動傾向” および “写真” に関連した情報の含有を分析し，センシティブデータの漏洩が実際にどの程度発生しているのかを確認した．

2.1 個人の内心に関する情報の検知

個人の内心に関する情報として，“個人の宗教観” を検出した．キーワードマッチング処理後のツイートに対して，SNS ユーザ自身が肯定的な意見を持つ，または否定的な意見を持つ場合に，個人の宗教観が表現された投稿であると判断した．また，投稿が肯定・否定のどちらでもない場合は，中立的な意見として一般的な宗教観とし，個人の宗教観には含めないものとした．処理手順は以下である．

(1) 137,877,745 件の Twitter アーカイブから Wikipedia：宗教一覧 [13] より，キリスト教や仏教の各宗派名，新興宗教名等をキーワードとして，キーワードマッチングを行う．
(2) SNS 投稿記事内に投稿ユーザ自身の意見を含まないことが多いと考えられるハッシュタグ・リツイート・URL 付きのツイートを除去する．
(3) 抽出された 17,123 件のツイートから，ランダムに 1,000 件をサンプル抽出する．
(4) 抽出された 1,000 件のツイートを (1) 肯定，(2) 否定，(3) 中立，(4) 無関連の 4 値で分類する．調査の確度を高めるために，2 人により上記分類を行い，2 人が同値で判別したツイートを正しい判定と見なす．

表 1 は，上述の 4 分類に対する検出率を示している．個人の宗教観は，肯定と否定の合計より 14%が該当した．

表 2 個人の心身の状態に関する情報の分類結果
Table 2 Classification results of information relating to physical and mental state of individuals.

自ら漏洩有無	分類	病気・疾患名	検出率
あり	個人の病気・疾患（重度）	癌	0.97%
		脳梗塞	0.21%
		その他	0.45%
	個人の精神的な症状	鬱	0.5%
		その他	0.17%
	個人の病気・疾患（軽度）	血尿	0.25%
		その他	1.68%
なし			95.77%

2.2 個人の心身の状態に関する情報の検知

個人の心身の状態に関する情報として，“個人の病気・疾患（重度）”，“個人の精神的な症状”，“個人の病気・疾患（軽度）” を検出した．キーワードマッチング処理後のツイートに対して，SNS ユーザ自ら情報漏洩させているか否かを判断した．処理手順は以下である．

(1) Yahoo! 家庭の医学 [14] より，癌，鬱，エイズ等の病気・疾患に対して，医療の要・不要により，重度（不治の病，医療者がかかわらないと治癒に至らない）・軽度（医療者にかかわらなくても自然治癒力や本人の努力次第で改善する）の分類 [15] を行う．軽度に分類された病気・疾患の中でも精神疾患については，精神症状として分類する．
(2) 137,877,745 件の Twitter アーカイブから，医療の要・不要により分類した病気・疾患名をキーワードとして，キーワードマッチングを行う．
(3) SNS 投稿記事内に投稿ユーザ自身の意見を含まないことが多いと考えられるハッシュタグ・リツイート・URL 付きのツイートを除去する．
(4) 抽出された 96,318 件のツイートから，ランダムに 10,000 件をサンプル抽出する．
(5) 抽出された 10,000 件のツイートを，2 人により，(1) 自ら漏洩あり，(2) 自ら漏洩なしの 2 値で分類する．

2.1 節と同様に調査の確度を高めるために，2 人による分類を行い，2 人が同値で判別したツイートを正しい判定と見なし，各分類に対する検出率を算出した．**表 2** は，各分類に対する検出率を示している．サンプル抽出全体の 4.23%のツイートが，いずれかの分類に該当する結果となった．個人の病気・疾患（重度）は，癌・脳梗塞等の合計から 1.63%，個人の精神的な症状は，鬱・パニック障害等の合計から 0.67%，個人の病気・疾患（軽度）は 1.93%であった．

2.3 個人の基本情報，生活状況に関する情報の検知

個人の基本情報，生活状況に関する情報として，“非常識

表 3 個人の基本情報，生活状況に関する情報の分類結果
Table 3 Classification results of information relating to basic and life situations of individuals.

分類	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%
その他	99.46%

な行動傾向”，“個人特定可能な写真”，“日常的な行動傾向”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ときの SNS 投稿は，自らセンシティブデータを漏洩させやすいといわれている [7] 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し，感情の高ぶりを検知した．感情極性の判別には，日本語評価極性辞書 [16] を利用した．処理手順は以下である．

(1) Twitter アーカイブに対して，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ごとの P/N 判定を行う．
(2) 単語ごとの P/N を集計し，ツイートごとの 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) ポジティブ傾向・ネガティブ傾向にあるツイートを取得するため，P/N スコアに閾値（0.75 以上，または 0.25 以下）を設定し，対象ツイートを絞り込む．
(4) 感情の高ぶりがあるときの画像付きの SNS 投稿は，平常時と比較して，センシティブデータが含まれるか否かを判断することが，より難しいと仮定し，Instagram や Twitpic 等の画像共有サービスの URL 付きツイートに絞り込む．
(5) 抽出された 876,976 件のツイートから，ランダムに 7,000 件をサンプル抽出する．
(6) 抽出された 7,000 件のツイートを，2 人により，投稿テキストに紐づく画像の確認を行い，(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 値で分類する．

本節も同様に，2 人による分類を行い，双方が同値で判別したツイートを正しい判定と見なし，各分類に対する検出率を算出した．**表 3** は，各分類に対する検出率を示している．非常識な行動傾向は検出できなかったが，個人特定可能な写真，日常的な行動傾向は計 0.54%の検出率であった．

2.4 検知結果と考察

これまでのサンプルツイートに対する検知結果を，137,877,745 件の全ツイートに適用すると換算した場合，センシティブデータの漏洩として，計 0.008%の検知となった．センシティブデータの漏洩検出率は，いずれの分類も低い結果であったが，一度漏洩してしまった情報をなかったことにすることは難しく，また，失職や損害賠償等社会的な制裁を受ける可能性を考慮すると，ごく少数であっても，SNS 提供者側に未然にその漏洩を検知・指摘する仕組みが必要である．

3. プライバシ侵害情報分類表の提案

3.1 公文書のプライバシ情報の取扱い

2 章の試算評価を通じ，SNS においてユーザ本人がセンシティブデータを漏洩させてしまうことが確かめられた．したがって，投稿前にユーザの記事の内容を検査して，情報漏洩を防止するシステムを構築することは重要である．当該システムの構築にあたり，ユーザの投稿予定記事の中にセンシティブデータを含むか否かを判定するための客観的な判断基準が必要である．実社会において同様の判断基準を必要とする文書として，今日までの歴史的な史料や公的文書である公文書があげられる．公文書の管理・公開の役割を担う機関として，国・都道府県・市町村等が管轄する公文書館が存在する．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しているが，公文書等の公開にあたり，公開基準を設けており，その基準の 1 つにプライバシ侵害がある．これは公開対象となる公文書に，プライバシ等の人権侵害，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 [17]．

公文書館の公開基準は，主に，情報公開条例方式と国立公文書館方式の 2 種類に分類ができる．前者の情報公開条例方式は，非公開とすべき情報を詳細に分類し，その分類ごとに非公開期間を設定する．後者の国立公文書館方式では，非公開とすべき情報の詳細分類はせずに重み付けを行い，状況に応じた柔軟な対応をとる．この両方式の利点を取り入れた公文書の公開基準として，戸嶋によるプライバシ等侵害情報分類表（私案）[17] があげられ，プライバシ等侵害の度合いを区分しつつ，保護期間を定めている．

このプライバシ等侵害情報分類表では，縦軸は情報公開条例をベースとした「非公開とすべき情報の内容による分類」を表し，6 つの分類が定義されている．一方，横軸は「非公開とすべき情報の重要度による分類及び非公開期間」を表し，国立公文書館利用規則 [18] の個人プライバシ等侵害の重さをベースとした 3 つの分類と，分類に応じた非公開期間が定義されている．本分類表を，SNS に適応するためには，(1) 上述の分類表の縦軸にあたる，非公開とすべき情報の内容による分類に，SNS において発生し難い分類が含まれていること，(2) SNS 投稿では原則，投稿後に非公開期間を待たずに即時公開となるため，分類表の横軸が表す，分類の重要度に応じた非公開期間に置き換わる指標が必要であることが課題となる．

本論文では，本分類表をもとに，SNS 投稿時に発生する

表 4 SNS における非公開とすべき情報の内容による分類
Table 4 Classification in accordance with information that should be kept private in SNS.

分類	分類説明	後悔例
個人の内心に関する情報	個人の思想や信仰宗教の情報	自身の信仰宗教に関することを投稿後，仕事上で好ましく思われなかった
個人の心身の状態に関する情報	個人や家族の精神症状・身体情報を含む病歴情報	個人・家族の病歴や病状を軽々しく公開した
個人の基本情報，生活状況に関する情報	自身や他者が特定される可能性のある写真，個人や家族に関する情報	友人が写り込んだイベントの写真を無断で投稿した
	非常識な行動，日常生活における個人の活動状況や趣味趣向などの情報	感情に任せて，ネガティブ/攻撃的なコメントを投稿した
個人の社会的活動等に関する情報	自身が気付いていない場合を含む犯罪行為などの情報	未成年にも関わらず，アルコールを飲み，それを投稿した

事実に基づいたプライバシ侵害情報分類表を提案する．上述の 2 つの課題を解決するために，(1) SNS 投稿後に感じた後悔理由をもとに，プライバシ侵害情報分類表の縦軸の「非公開とすべき情報の内容による分類」を定義し，(2) 非公開期間に代わる指標として，「重要度に応じた公開範囲」を定義する．

3.2 非公開とすべき情報の内容による分類の定義

SNS におけるプライバシ侵害情報分類表の，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 投稿時に発生する事実に基づいて修正するため，ユーザが SNS 投稿後に感じた後悔事例から SNS で発生するセンシティブな事象を分析する．本論文では，2 章の Twitter アーカイブにおけるセンシティブデータの存在率の試算評価で使用した既存研究 [7], [11], [12] より，SNS 投稿後の後悔理由を抽出し，SNS 投稿時の非公開とすべき情報の内容による分類を行った．**表 4** は，SNS における非公開とすべき情報の内容による分類と，その後悔例を示している．

3.3 重要度による公開範囲の定義

公文書では，意図していないユーザに情報が公開されることを防ぐために，文書の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，即時公開かつ投稿内容の部分公開をなしとする SNS 投稿記事には適用できない公開基準となる．そこで，横軸の非公開とすべき情報の「重要度による非公開期間」に置き変わる指標を検討した．IT 時代におけるプライバシ管理の主要事項として，Palen らは，Altman の Privacy Regulation Theory [19] をベースに，(1) 開示境界，(2) 識別境界，(3) 時間境界の 3 種類を提唱している [20]．(1) 開示境界とは，その情報が一般に公開可能事項であるかの境界を指し，(2) 識別境界とは，その情報における特定の個人や事象の識別性の境界を指す．(3) 時間境界とは，過去，現在そして未来等の時間経過における境界を指す．時間境界に関する SNS のプライバシ保護を目的とした既存研究として，記事公開後の公開期間に期限を設け，投稿記事の公開を制限する手法 [21] があるが，前述のように SNS では原則，メッセージを即時公開とすることから，記事公開前の非公開期間を設ける手法は提案されていない．そこで本論文では，「重要度による非公開期間」に置き変わる指標として開示境界に着目し，情報の「重要度による公開範囲」を用いて，当該情報が公開可能な事項であるかの境界として定義した．

SNS ネットワーク内の公開範囲に関する既存研究として，La Gala ら [22] による SNS エゴネットワークにおける友人分類に関する研究があげられる．エゴネットワークとは，社会ネットワーク分析における自身を中央に配置した他ユーザとの関係構造を表現したネットワークを指す．たとえば Facebook や LinkedIn における友だちリストは自分自身を中心としたエゴネットワークを構成していると見なされる．既存研究では，SNS エゴネットワークに対して，Dunbar's number [23] を適用し，SNS 内のコミュニケーション頻度を対応付けることにより，SNS エゴネットワーク内と実社会における友人分類が似ていることが示されている．Dunbar's number 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 人程度としており，SNS においてもこの維持可能な友人数が変わらないとされている [24]．たとえば，Facebook において友だちが 150 人以上存在する場合，自身の友だち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，誤ってセンシティブデータを投稿してしまった場合に，これら紐付きの弱いユーザにも情報が漏洩することになる．

この Dunbar's number と La 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，新たな開示レベルを定義した．**表 5** は，SNS エゴネットワークにおける開示レベルを示している．

最も厳しい開示レベルを示す開示レベル 0 では，公開対象を “家族” と定義し，コミュニケーション頻度とその人数は未設定とした．開示レベル 1 では，公開対象は，“親友” と定義した．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 人とした．開示レベル 2 の公開

表 6 SNS におけるプライバシ侵害情報分類表
Table 6 Information classification table for invasion of privacy in SNS.

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		開示レベル 1 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 友だち （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 友だち未満 （16-50 人） 半年 1 回以上の コミュニケーション
		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
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・体重含む）
個人の基本情報，生活の状況に関する情報	写真		個人特定可能な写真	
	家庭状況			家族構成・家庭状況等の家族情報
	行動傾向	非常識な行動傾向		日常的な行動傾向
個人の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）	

表 5 SNS エゴネットワークにおける開示レベル
Table 5 Disclosure level in SNS egocentric network.

開示レベル	公開対象	人数（人）	コミュニケーション頻度
0	家族	–	–
1	親友	1〜5	週 1 回以上
2	友だち	6〜15	月 1 回以上
3	知人以上 友だち未満	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

対象は，“友だち” とし，月 1 回以上のコミュニケーションがある 6〜15 人と定義した．開示レベル 3 は “知人以上 友だち未満” とし，半年に 1 回以上のコミュニケーションがある 16〜50 人と定義した．開示レベル 4 は “知人” とし，その人数は 51〜150 人とした．最も公開範囲が緩い開示レベル 5 は，まったくコミュニケーションがない，もしくは，1 年以上音沙汰がないケースを指す “他人” とした．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．

3.4 SNS におけるプライバシ侵害情報分類表の提案

戸嶋により提案された公文書におけるプライバシ等侵害情報分類表 [17] に，3.2 節で定義した縦軸の非公開とすべき情報の内容による分類と，3.3 節で定義した横軸の重要度による公開範囲の定義を適用することによって，SNS におけるプライバシ侵害情報分類表を提案した．**表 6** は本論文において提案したプライバシ侵害情報分類表を示している．

適用にあたり，縦軸の非公開とすべき情報の内容による分類では，SNS 投稿後の後悔事例の確認ができなかった分類に関して，SNS では発生し難い分類として，本分類表の対象から除外した．また，横軸の重要度による公開範囲では，開示レベル 0〜5 を定義したが，クローズド SNS である Path [25] では，サービス開始当初，より深いつながりを持つ少ない人数として，家族を含めた友だちリストの上限を 50 人に設定し，閉ざされた SNS エゴネットワークを表現した．これにより，Facebook 等のオープン SNS からプライバシを保ちたいユーザを多く獲得してきたことを考慮し，本分類表では，開示レベル 0 の “家族” をすべての開示レベルに含むものとし，50 人を開示範囲の上限として，開示レベル 1〜3 を分類の重要度に応じて設定した．

4. 評価

本章では，3 章で提案した SNS におけるプライバシ侵害情報分類表の妥当性の評価として，SNS 投稿時のプライバシ観点での情報の重要性の評価を行う．

4.1 プライバシの観点での情報の重要性の評価

提案したプライバシ侵害情報分類表の各分類が，SNS 投稿時にプライバシの観点からどの程度重要であるのか，一対比較法 [26], [27] を用いて評価調査を行った．

4.2 評価方法

一対比較法の評価方法に従って，下記の条件で評価を実施した．

(1) 被験者

被験者は，大学生，大学院生，教員，会社員，主婦から構成される 20 代～60 代の 39 人（男：21 人，女：18 人）とした．被験者の年代は，30 代（40%）が最も多く，続いて 20 代（33%），40 代（18%）・60 代（7%）・50 代（2%）である．

(2) 評価対象の分類

3 章で提案した SNS におけるプライバシ侵害情報分類表の 13 種類の分類を用い，各分類および，分類ごとにあらかじめ分類したサンプル Tweet メッセージに対して，SNS 投稿時のプライバシ観点での情報の重要性を，一対ずつ比較し，順位付けおよび，順位の信憑性評価を行った．その際，内心と行動傾向等，異なる性質の比較を極力避けるため，評価対象となる 13 種類の分類を 2 つの比較グループ（(A) 個人の内心・心身の状態に関する情報，(B) 個人の基本情報・生活の状況，および社会的活動等に関する情報）として，前者のグループ (A) を分類の (1)～(7)，後者のグループ (B) を分類の (8)～(13) に分けて実施した．**表 7** に本評価で比較対象とする分類を示す．

表 7 比較対象とする分類
Table 7 Classification as a target for comparison.

比較グループ	番号	分類名
(A) 個人の内心・心身に関する情報	1	個人の信条主張
	2	一般的な社会信条
	3	個人の宗教観
	4	個人の病気・疾患（重度）
	5	個人の病気・疾患（軽度）
	6	個人の精神的な症状
	7	個人の身体情報（身長・体重含む）
(B) 個人の基本情報・生活の状況，及び社会的活動等に関する情報	8	個人特定可能な写真
	9	家族構成・家庭状況等の家族情報
	10	非常識な行動傾向
	11	日常的な行動傾向
	12	犯罪行為（重度）
	13	犯罪行為（軽度）

4.3 評価手順

同一グループ内から異なる分類を 2 つ取り上げ，一方の分類を基準分類，他方の分類を比較分類とし，SNS 投稿時にプライバシの観点からどのくらい重要であるかを主観的に評価した．これを比較グループ A，B のそれぞれにおいて総当りに実施する．被験者は，基準となる分類を 0 ととらえたうえで，0 を含む −2（重要でない）から +2（重要である）までの 5 段階評価を行う．また，すべての分類を基準分類として評価する．評価手順を以下に示す．

Step 1. 被験者に 13 種類のプライバシ侵害情報の分類を提示し，分類の説明を行う．

Step 2. 被験者に，基準分類，比較分類の 2 分類を提示する．

Step 3. 被験者は，提示された基準分類を基準に，比較分類が SNS 投稿時にプライバシの観点からどの程度重要であるかを −2～2 の 5 段階の評価尺度により評価する．

Step 4. すべての分類を基準分類として提示し，グループ内の全分類と総当りに比較を行う．

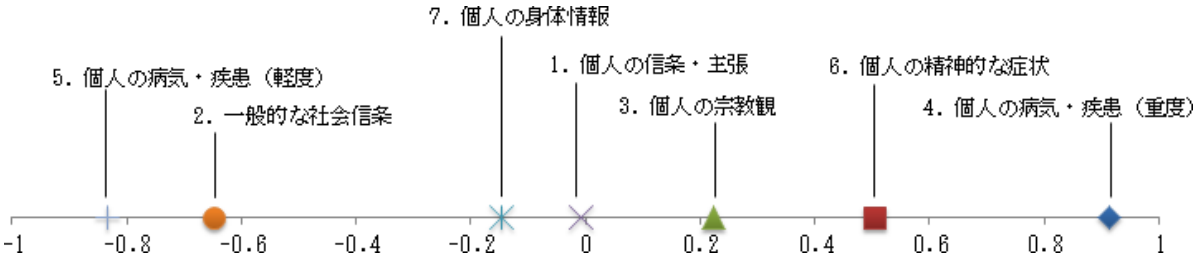
Step 5. 実際に過去に投稿され，あらかじめ各分類に分類したサンプル Tweet メッセージおよび，メッセージに紐付いた画像を提示し，Step 3，Step 4 を繰り返す．

Step 6. 全被験者の回答のうち，SNS を週 1 回以上利用する被験者 26 人（男：13 人，女：13 人）の回答に対して，一対比較法の評価方法[*1]に従い，グループごとに分類間の順位の算出と，分類間の有意差の有無を確認する．

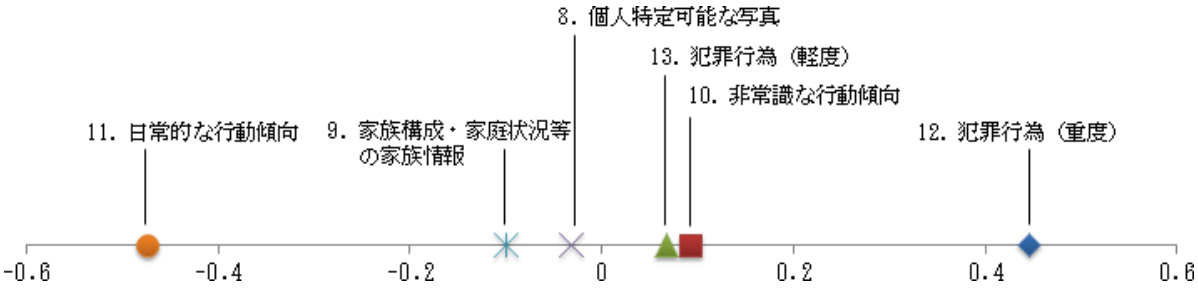
4.4 評価結果

比較グループ A，B におけるプライバシ観点での情報の重要性の評価結果を**図 1** に示す．図 1 の横軸は，分類ごとの尺度値を比較するために，数直線上に尺度表現している．プラス方向である右に行くほど，SNS 投稿時におけるプライバシ観点での情報の重要性が高いことを示しており，マイナス方向の左に行くほど，重要性が低いことを示している．(6) 個人の精神的な症状を除き，評価グループ A，B ともに，表 6 の SNS におけるプライバシ侵害情報分類表の開示レベルに沿った順位付けとなることが分かった．たとえば，評価グループ B：個人の基本情報・生活の状況，および社会的活動等に関する情報において，最も重

[*1] 一対比較法の最低被験者数は 20 人程度 [28] とされるため，本評価は成立すると考えられる．



a 評価グループ A：個人の内心・心身に関する情報の尺度値の比較



b 評価グループ B：個人の基本情報・生活の状況，および社会的活動等に関する情報の尺度値の比較

図 1 評価グループ別のプライバシ観点での情報の重要性の評価結果

Fig. 1 Evaluation result of the importance of information in the privacy point of view of evaluation groups.

要性が高いとされた (12) 犯罪行為（重度），次点の (10) 非常識な行動傾向は，開示レベル 1 に分類されている．また，最も重要性が低いとされた (11) 日常的な行動傾向は，開示レベル 3 に分類されている．分類表上で開示レベル 2 に分類される (6) 個人の精神的な症状は，より重要性が高くとらえられる結果となったが，評価手順 Step 5 で実施したあらかじめ分類したサンプル Tweet メッセージの評価結果においては，(3) 個人の宗教観よりも下位の順位であり，かつ，両分類の間には，有意差があった．以上の結果より，表 6 で提案した SNS におけるプライバシ侵害情報分類表が，SNS 投稿時のセンシティブデータであるかの判断基準として有効であることが分かった．ただし，本評価の被験者に偏りの可能性とその人数が十分とはいえないため，さらなる評価の充実を今後の課題とする．

5. 公開範囲の設定方式の提案

5.1 投稿内容に応じた公開範囲の提案

2014 年 6 月現在，Facebook では投稿時の公開範囲の設定として，“公開”，“友だち”，“自分のみ”，“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．多くの SNS ユーザは通常，公開範囲：“友だち” を設定している [10]．しかし，Stutzman ら [9] によると，公開範囲：“友だち” の中には，関係性の弱いユーザが含まれており，公開範囲を狭めたとしても，依然としてプライバシ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っているが [29]，投稿のつど行っていくことは難しい．このことから，SNS ユーザは，現在 SNS 側より提供されている投稿の公開範囲設定以外に，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 [12]．

そこで，ユーザが SNS へ投稿する前に，投稿予定記事に対して，表 6 の SNS におけるプライバシ侵害情報分類表を適用し，センシティブデータの検知を行う．センシティブデータを含まない場合，ユーザが事前に設定する公開範囲設定に従い，SNS へ投稿する．センシティブデータを含む場合，センシティブデータ漏洩の通知と，投稿者を中心とした SNS ネットワーク内における公開対象者の自動設定を提供するシステムを提案する．

5.2 関連研究

プライバシ漏洩を検知する研究として，Mao ら [30] による Twitter におけるプライバシ漏洩情報の抽出とその要因分析がある．この研究では，センシティブデータとして，本論文と同様に感情が高まった際に投稿をするシーンから，休暇・アルコール・病気に注目している．しかし，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，Squicciarini ら [31] 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保護ポリシを動的に生成し，そのポリシを用いてプライバシ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 側が提供する友だちや特定グループを

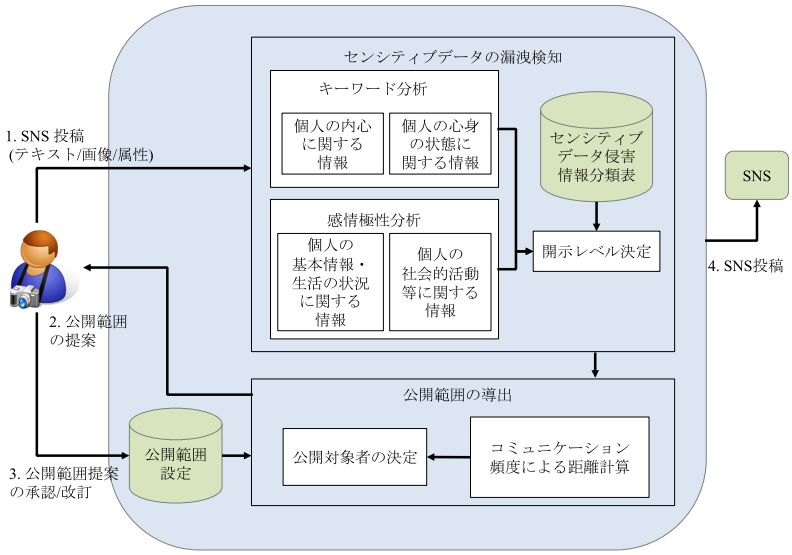


図 2 提案システムのプロセスフロー
Fig. 2 Process flow of proposed system.

対象としており，依然として関係性の弱い友人が含まれ，かつ，公開対象が特定グループにしばられるという問題がある．

5.3 システム概要

SNS ユーザの不用意な投稿によるセンシティブデータの漏洩を防止するために，センシティブデータ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，ユーザが SNS へ投稿を行う前に，事前利用することで，投稿予定記事内にセンシティブデータが含まれるか否かを判別する．含む場合に，センシティブデータの漏洩通知と，誰に対して参照可能とすべきかの公開範囲を導出し，提案を行う．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 への投稿判断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，ユーザはセンシティブデータを，意図していない他ユーザに対して公開することなく，公開範囲の管理が容易に可能となる．

5.4 システム内の分析プロセス

本システムのプロセスフローを図 **2** に示す．本システムは大きく分けて，センシティブデータの漏洩検知，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．

Step 1. センシティブデータの漏洩検知

テキスト・画像・属性情報から構成される SNS 投稿記事を分析し，センシティブデータの含有を検知する．その判断基準として，3 章で定義した SNS におけるプライバシ侵害情報分類表を適用するが，分類表の縦軸の非公開とす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，関連キーワードをベースとした検知を行う．それ以外の個人の基本情報，生活状況に関する情報，社会的活動等に関する情報等は，感情の高ぶりを含めた感情起伏が出ているときに判断が緩くなり投稿した場合，センシティブデータの漏洩傾向があるため，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，センシティブデータの漏洩が検知された場合，プライバシ侵害情報分類表に従い，投稿の開示レベルを決定する．

Step 2. 公開範囲の導出

Step 1 で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だち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．

Step 3. 結果通知

分析結果であるセンシティブデータの漏洩通知と，投稿に対する公開範囲として公開対象者を 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．

5.5 投稿メッセージの処理手順

前節までの本システムの概要および，分析プロセスをふまえ，システムの実現時に必要となる基本機能および，データ処理手順を説明する．

5.5.1 基本機能

本システムでは，SNS ユーザのプライバシを保護する手法として公開範囲にフォーカスし，(1) SNS 投稿記事に含まれるセンシティブデータの漏洩検知，(2) 投稿記事の内容による適応的な開示範囲の提案手法の確立を目的としている．本手法の目的のために，システムの基本機能として以下の 6 機能が必要とされる．

- ユーザ視点
  1. 公開範囲として開示レベルを自由に設定できる．
  2. 設定した開示レベルに沿うようにユーザ単位で公開対象者を自由に選択できる．
- システム視点
  1. 投稿予定記事におけるセンシティブデータの含有を検知する．
  2. 検知したセンシティブデータに応じた公開範囲として開示レベルを導出し，ユーザへ提案する．
  3. 開示レベルの範囲内に指定された公開対象者のみに，投稿記事を公開する．
  4. 最終的に公開対象者としたユーザ情報を保持し，次回の開示レベル提案時に考慮する．

5.5.2 データ処理手順

データ処理手順として，基本機能のシステム視点 1〜4 を説明する．

Step 1. センシティブデータの漏洩検知

あらかじめ，プライバシ侵害情報分類表の分類ごとに，開示レベル 1〜3 および，その他として判別する多値分類器を作成する．分類器の作成方法としては，2 章の Twitter アーカイブにおけるセンシティブデータの存在率の試算評価と同様に，個人の内心に関する情報と個人の心身の状態に関する情報は，キーワード分析後の教師データから分類器を作成する．個人の基本情報，生活の状況に関する情報，個人の社会的活動等に関する情報については，感情分析後の教師データから同様に分類器を作成する．ユーザが SNS へ投稿予定記事を本システムに投稿した場合，あらかじめ作成されたすべての分類器を通し，最も狭い開示レベルを適用する．

Step 2. 公開範囲の導出

Step 1 より得られた開示レベルから，コミュニケーション頻度情報を得る．次に，友人ごとにユーザと友人のメッセージのやりとり等のコミュニケーション頻度から，自身と友人における紐帯の強度を算出し，友人の順位付けを行う．その際に，コミュニケーション頻度が少ないが公開対象者となりうるユーザが存在する可能性があるため，これまでの投稿履歴を考慮して，順位を決定する．最後に，開示レベルごとの人数上限に沿うように最終的な公開対象者を提案する．提案を受けたユーザは，基本機能のユーザ視点 1，2 にあるように，提案された開示レベルおよび公開対象者を自由に変更が可能である．

Step 3. SNS 投稿

ユーザから SNS 投稿依頼が行われた時点で開示レベルの範囲内に指定されたユーザのみに，投稿メッセージを限定公開する．また，公開の対象・対象外としたユーザ情報を保持し，次回以降に本システムを使用する際の初期値提案，および，Step 2 の公開範囲の導出時にも適用する．

6. まとめ

SNS ユーザの不用意な SNS 投稿によるセンシティブデータの漏洩が，実際に発生していることを確認するために，SNS 投稿後のユーザの後悔事例をもとに，137,877,745 件の Twitter アーカイブにおけるセンシティブデータの存在率の試算評価を行った．その結果，計 0.008%のセンシティブデータの漏洩を検知し，非常に少数であるが，センシティブデータを含んだ SNS 投稿が実際に行われていることを示した．本試算評価を受け，SNS 投稿時のセンシティブデータの漏洩を事前に自動検知するための第一歩として，非公開とすべき情報の内容分類と開示レベルを対応付けた SNS におけるプライバシ侵害情報分類表を提案した．本分類表の妥当性評価として，一対評価法を用い，SNS 投稿時のプライバシ観点での情報の重要性の評価を実施，その妥当性を示した．また，本分類表を用いることにより，センシティブデータが含まれた SNS 投稿記事の内容から漏洩の有無と開示レベルを判断し，センシティブデータの漏洩有無の通知と，投稿者を中心としたネットワーク内における公開対象者の自動設定を提供するシステムを提案した．

謝辞 本論文は，総合研究大学院大学学融合推進センターの助成を受けたものである．

参考文献

[1] 72% of Online Adults are Social Networking Site Users, available from ⟨http://www.senioragency.be/wp-content/uploads/2013/08/SOCIAL-MEDIA-WITH-ADULTS.pdf⟩ (accessed 2014-06-25).
[2] The Twitter Typo That Exposed Anthony Weiner, available from ⟨http://www.huffingtonpost.com/2011/06/07/anthony-weiner-twitter-dm_n_872590.html⟩ (accessed 2014-06-25).
[3] 総務省 パーソナルデータの利用・流通に関する研究会，入手先 ⟨http://www.soumu.go.jp/main_sosiki/kenkyu/parsonaldata/⟩（参照 2014-06-25）．
[4] Humphreys, L., Gill, P. and Krishnamurthy, B.: How much is too much? Privacy issues on Twitter, *Proc. ICA'10* (2010).
[5] Fastask：スマートフォンと位置情報に関する調査，入手先 ⟨http://www.fast-ask.com/report/report-gpsposition-20130509.html⟩（参照 2014-06-25）．
[6] 総務省：統計調査と個人情報保護，入手先 ⟨http://www.stat.go.jp/info/today/007.htm⟩（参照 2014-06-25）．
[7] Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P.G. and Cranor, L.F.: I regretted the minute I pressed share: A qualitative study of regrets on Facebook, *Proc.*

SOUPS'11, p.10, ACM (2011).
[8] Twitter user says vacation tweets led to burglary, available from ⟨http://news.cnet.com/8301-1009_3-10260183-83.html⟩(accessed 2014-06-25).
[9] Stutzman, F. and Kramer-Duffield, J.: Friends only: Examining a privacy-enhancing behavior in facebook, *Proc. SIGCHI'10*, pp.1553–1562, ACM (2010).
[10] Stutzman, F., Gross, R. and Acquisti, A.: Silent Listeners: The Evolution of Privacy and Disclosure on Facebook, *Journal of Privacy and Confidentiality*, Vol.4, No.2 (2012).
[11] Sleeper, M., Cranshaw, J., Kelley, P., Ur, B., Acquisti, A., Cranor, L. and Sadeh, N.: I read my Twitter the next morning and was astonished: A conversational perspective on Twitter regrets, *Proc. CHI'13*, pp.3277–3286, ACM (2013).
[12] Sleeper, M., Balebako, R., Das, S., McConahy, A.L., Wiese, J. and Cranor, L.F.: The post that wasn't: Exploring self-censorship on facebook, *Proc. CSCW'13*, pp.793–802, ACM (2013).
[13] Wikipedia：宗教一覧，入手先 ⟨http://ja.wikipedia.org/wiki/%E5%AE%97%E6%95%99%E4%B8%80%E8%A6%A7⟩（参照 2014-06-25）.
[14] Yahoo! 家庭の医学，入手先 ⟨http://health.yahoo.co.jp/katei/⟩（参照 2014-06-25）.
[15] 岡本　裕：9 割の病気は自分で治せる，pp.1–46, 中経出版 (2009).
[16] 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，言語処理学会第 14 回年次大会論文集，pp.584–587 (2008).
[17] 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, pp.40–44 (2009).
[18] 独立行政法人国立公文書館利用規則，入手先 ⟨http://www.mext.go.jp/b_menu/hakusho/nc/k19720425001/k19720425001.html⟩（参照 2014-06-25）.
[19] Altman, I.: *The environment and social behavior: Privacy, personal space, territory, crowding. Monterey*, Brooks/Cole Publishing Company (1975).
[20] Palen, L. and Paul, D.: Unpacking privacy for a networked world, *Proc. CHI '03* (2003).
[21] Ayalon, O. and Toch, E.: Retrospective privacy: Managing longitudinal privacy in online social networks, *Proc. SOUPS'13*, p.4 (2013).
[22] La Gala, M., Arnaboldi, V., Conti, M. and Passarella, A.: Ego-net digger: A new way to study ego networks in online social networks, *Proc. HotSocial'12*, pp.9–16, ACM (2012).
[23] Dunbar, R.I.M.: The social brain hypothesis, *Evol Anthropol*, Vol.6, pp.178–190 (1998).
[24] Goncalves, B., Perra, N. and Vespignani, A.: Validation of Dunbar's number in Twitter conversations, *ArXiv preprint* (2011).
[25] Path, available from ⟨https://path.com/⟩ (accessed 2014-06-25).
[26] 中前光弘，田畑洋二，大賀泰文，角田充弘，宇都文昭，奥西孝弘，越智　保，前田　要：Scheeffe の一対比較法による主観的評価法，日本放射線技術学会雑誌，pp.1561–1565 (1996).
[27] 沈　潔如，稲葉由之，伊藤　一：一対比較法を用いた観光客の期待度に関する調査と分析：台湾人観光客の事例，日本経営工学会論文誌，pp.273–282 (2004).
[28] 福田忠彦，福田亮子：増補版 人間工学ガイド 感性を科学する方法，pp.73–123, サイエンティスト社 (2011).
[29] Kairam, S., Brzozowski, M., Huffaker, D. and Chi, E.: Talking in circles: Selective sharing in Google+, *Proc. SIGCHI'12*, pp.1065–1074, ACM (2012).
[30] Mao, H., Shuai, X. and Kapadia, A.: Loose tweets: an analysis of privacy leaks on twitter, *Proc. WPES'11*, pp.1–12, ACM (2011).
[31] Squicciarini, A.C., Sundareswaran, S., Lin, D. and Wede, J.: A3P: Adaptive policy prediction for shared images over popular content sharing sites, *Proc. Hypertext'11*, pp.261–270, ACM (2011).

推薦文

本研究は，SNS におけるプライバシ侵害を情報の内容・重要度によって家族から複数の他人までに分類した 5 段階の開示レベルを策定し，大規模な Twitter のアーカイブを対象とした実証分析により評価した．さらに，SNS へ投稿する際に開示レベルを自動検出するシステムを提案している．近年の社会問題を課題対象とした重要なテーマであり，これを解決するための大規模なデータ分析を通した実証評価・システム提案は，意欲的な研究であり，今後の発展が期待できる研究領域である．よって，今後の同研究分野の発展に有用であるため，推薦論文として推薦したい．

（コンピュータセキュリティ研究会主査　西垣正勝）

町田 史門　（学生会員）

2013 年首都大学東京産業技術大学院大学産業技術研究科情報アーキテクチャ専攻専門職修士課程修了．同年より総合研究大学院大学複合科学研究科情報学専攻博士後期課程在学中．2013 年コンピュータセキュリティシンポジウム 2013 優秀論文賞，同シンポジウムコンセプト論文賞各受賞．

梶山 朋子　（正会員）

2001 年津田塾大学情報数理科学科卒業．2004 年慶應義塾大学大学院理工学研究科前期博士課程修了．2007 年総合研究大学院大学複合科学研究科情報学専攻後期博士課程修了．博士（情報学）．早稲田大学人間科学学術院助手を経て，2010 年青山学院大学理工学部助手，2013 年同大学同学部助教．マルチメディア検索インタフェース，知識創造活動支援に関する研究に従事．

嶋田 茂 （正会員）

1975 年名古屋工業大学大学院工学研究科生産機械専攻修士課程修了．同年（株）日立製作所入社．中央研究所にてパターン認識技術による地図・図面入力システム，空間情報システム，ユビキタスシステム等の研究開発に従事．1997 年東京大学大学院工学系研究科情報工学専攻より学位取得，博士（工学）．2007 年より首都大学東京産業技術大学院大学教授．IEEE，ACM，電子情報通信学会各会員．

越前 功 （正会員）

1997 年東京工業大学大学院理工学研究科修士課程修了（応用物理学）．同年日立製作所入社，システム開発研究所を経て，現在，国立情報学研究所コンテンツ科学研究系教授．総合研究大学院大学複合科学研究科情報学専攻教授を兼務．2010 年ドイツ・フライブルグ大学客員教授．2011 年ドイツ・マルティン・ルター大学（ハレ大学）客員教授．コンテンツセキュリティの教育研究に従事．博士（工学）．2005 年本学会論文賞，2006 年 IEEE IIH-MSP06, Best Paper Award，2010 年映像情報メディア学会藤尾フロンティア賞，画像電子学会画像電子技術賞，2011 年本学会長尾真記念特別賞，2014 年本学会論文賞各受賞．IEEE，ACM，電子情報通信学会，映像情報メディア学会，画像電子学会各会員．