5Y-4

SNSにおける個人情報の保護に関する研究

北野光一† 寺口敏生† 田中成典‡ 大谷和史† 小泉陽子‡
関西大学大学院総合情報学研究科† 関西大学総合情報学部‡

１．はじめに

近年，Web 上でコミュニティを形成する SNS（Social Networking Service）の普及に伴い，SNS 上で情報を発信するユーザが増加している．しかし，SNS には，知人同士のコミュニティであるという安心感から，個人情報に対する配慮が疎かになり，無意識のうちに自身の個人情報を漏洩するという問題[1]がある．そのため，個人情報の漏洩をユーザに警告し個人情報を保護する仕組み[2][3]が望まれている．そこで，SNS の日記中で個人情報に該当する部分を別の表現に書き換える研究[4]や，SNS における個人情報の漏洩レベルを定量化する研究[5]が行われている．しかし，既存研究[4][5]には，コーパスや単語の係り受けルールに依存しているため，SNS の日記の様に記述形態多様な文章では，情報の抽出精度が低下するという問題や，抽出した情報がユーザ自身の個人情報かどうかを特定できないという問題がある．そこで，本研究では，個人情報の抽出モデルを構築することで，コーパスやルールに依存することなく対象ユーザ自身の個人情報を抽出する手法を提案する．本提案手法を用いて抽出した個人情報から個人情報の漏洩状況を分析し提示することで，個人情報の漏洩を警告するシステムを実現する．

２．研究の概要

本研究では，SNS の日記に記述された個人情報を抽出し，ユーザに個人情報の漏洩を警告する手法を提案する．本システムの概要を図 1 に示す．本システムは，1）個人情報識別モデル構築機能，2）個人情報抽出機能，3）個人情報特定機能により構成される．入力データは，対象ユーザの日記群とし，出力データは，個人情報一覧と個人情報漏洩度とする．

２．１　個人情報識別モデル構築機能

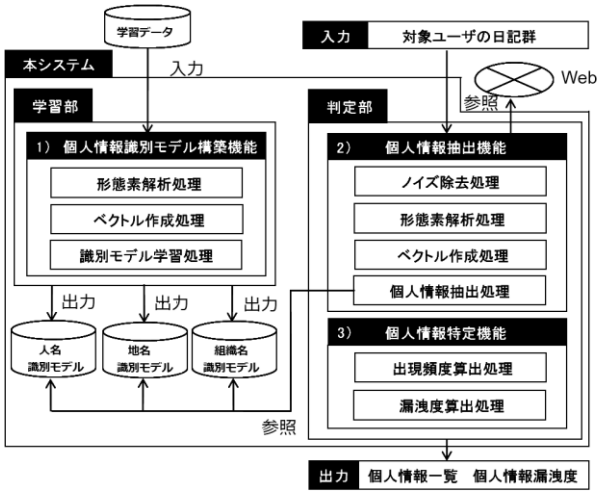

図１　システムの概要

本機能では，人名，地名と組織名を識別するためのモデルを構築する．学習データには，SNS の日記を用いる．学習の素性には，形態素解析により分割した形態素，形態素の品詞細分類，文字種と，チャンクの開始位置や終了位置を示す Chunk タグの 4 つを用いる．形態素毎に素性ベクトルを作成し，SVM（Support Vector Machine）を用いて識別モデルを学習し，各識別モデルを構築する．

２．２　個人情報抽出機能

本機能では，対象ユーザの日記群から個人情報を抽出する．まず，HTML タグ及び日記に記述された店舗情報などを除外する．次に，個人情報識別モデル構築機能と同様に，形態素毎に素性ベクトルを作成する．そして，パターンマッチルールを用いることで抽出可能な個人情報を抽出する．最後に，各識別モデルを用いて人名，地名，組織名を抽出する．

２．３　個人情報特定機能

本機能では，個人情報抽出機能で抽出した個人情報が対象ユーザ自身のものであるかの特定と個人情報の漏洩度の算出を行う．まず，出現頻度の高い個人情報をユーザ自身のものであると捉えるため，個人情報の種類毎に出現頻度を算出し，上位 3 件を特定し出力する．そして，抽出した個人情報の組み合わせから個人情報の漏洩度を 4 つのレベルで算出し出力する．

Research of Classification of Word of Mouth Based on Advertising Characteristic
† Koichi Kitano, Toshio Teraguchi, Kazufumi Otani
Graduate School of Informatics, Kansai University, 2-1-1 Ryouzenji-cho, Takatsuki-shi, Osaka 569-1095, Japan
‡ Shigenori Tanaka, Yoko Koizumi
Faculty of Informatics, Kansai University, 2-1-1 Ryouzenji-cho, Takatsuki-shi, Osaka 569-1095, Japan

３．システムの実証実験と考察

本システムの有用性を実証するために，SNS の mixi を解析対象として，対象ユーザ自身の個人情報の特定精度について，実験を行う．

３．１　実証実験

本実験では，正しく個人情報の抽出ができたのか，また，抽出した個人情報が対象ユーザの個人情報であるかの評価を行うため，mixi のユーザ 20 人の日記 1,491 件を対象として個人情報の特定精度を確認した．事前に目視で確認したところ，実験に使用した日記には 1,491 件中 536 件に対象ユーザに関連する個人情報が含まれていた．評価指標として，出力した上位 3 件に含まれる個人情報のうち，対象ユーザの個人情報が含まれていた確率を用いた．また，個人情報の漏洩度について，危険度の高い順にレベル 3 から 1 のレベルを設定し，手作業で抽出した個人情報を分類した結果を正解とし，個人情報抽出機能と個人情報法特定機能により抽出した個人情報を分類した結果との比較を行った．

３．２　結果と考察

個人情報特定の結果を表 1 に示す．上位 3 位までに 75%のユーザの個人情報を特定できたことが確認できた．従って，抽出した個人情報が対象ユーザのものであると判断する指標として出現頻度を用いることは，有用であると確認できた．ただし，人名については，未知語などによる誤判定も多く，出現頻度以外の指標を用いる必要があると考えられる．また，語句の出現パターンが類似しているため，地名と組織名の誤判定も見られた．本研究では，人名，地名と組織名につき約 600 件のベクトルを学習に用いたが，より多くの学習データを用いることで，識別精度が向上すると考えられる．パターンマッチルールを用いて抽出した個人情報については，高い精度で抽出できた．しかし，図 2 に示す漏洩度算出の結果より，危険度が高いレベル 3 の情報に取り溢しが見られた．これは，個人情報特定の結果において人名と組織名の抽出精度が低いためであり，更なる改善が必要である．

４．おわりに

本研究では，構築した個人情報識別モデルとパターンマッチルールを用いて，SNS の日記から個人情報を抽出し，提示することで個人情報の漏洩をユーザに警告する手法を提案した．そして，実証実験から提案手法の有用性を証明した．今後は，人名と地名の抽出精度の向上，パターンマッチルールの強化や情報を組み合わせることで想起できる個人情報を特定するなど，より粒度の細かい個人情報抽出を目指す．

表１　個人情報特定の結果

	1位	2位	3位	4位以降
人名	10%	10%	20%	80%
地名	69%	88%	94%	100%
組織名	6%	35%	59%	82%
メールアドレス	100%	100%	100%	100%
電話番号	100%	100%	100%	100%
生年月日	43%	43%	43%	43%
年齢	71%	86%	93%	93%
家族構成	82%	82%	88%	88%
総合	60%	68%	75%	86%

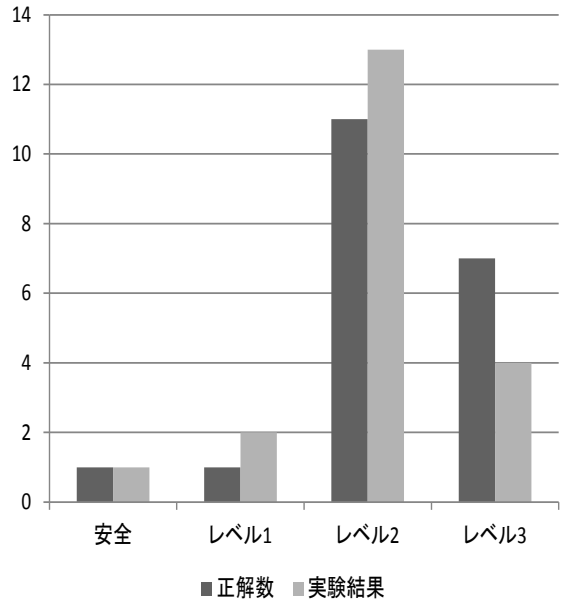

図２　漏洩度算出の結果

参考文献

[1] 谷本茂明，廣田啓一，山本太郎，千田浩司，畑島隆，高橋克己，金井敦：次世代プライバシ保護サービスのコンセプト提案，情報処理学会論文誌，情報処理学会，Vol.49，No.7，pp.2440-2455，2008.7.

[2] Ho, A., Maiga, A. and Aimeur, E. : Privacy Protection Issues in Social Networking Sites, 2009 IEEEACS International Conference in Computer System and Applications, IEEE, pp.271-278, 2009.5.

[3] Aimeur, E., Gambs, S. and Ho, A. : UPP ; User Privacy Policy for Social Networking Sites, 2009 Fourth International Conference on Internet and Web Applications and Services, IEEE, pp.267-272, 2009.5.

[4] 今田美幸，風間一洋：ソーシャルネットワーキングサービスを前提としたプライバシー侵害検出，ネットワークシステム研究会技術研究報告，電子情報通信学会，Vol.108，No.258，pp.71-76，2008.10.

[5] 片岡春乃，渡辺夏樹，水谷桂子，吉浦裕：自然言語情報の開示制御技術 DCNL の実現に向けてープライバシ検知手法ー，マルチメディア通信と分散処理研究会研究報告，情報処理学会，Vol.2008，No.21，pp.237-242，2008.3.