5ZB-3

プライバシー保護機能付きブログ解析ツールの開発

川場　真理子　　兼子　愛　　小舘　亮之

1. はじめに

mixi を始めとする SNS やブログの普及によって、個人が自身の行動履歴を開示するケースが増えている。しかし、その手軽さ故に本来開示すべきではない自身の個人情報や他人のプライバシーに関わる情報を記載してしまい、トラブルに巻き込まれることも少なくない。例えば、顔写真を公開した上で、自分の行きつけの店や住んでいる町のことなどブログに書いていた女性が、見知らぬ男性に後をつけられたり、「あなたのことは何でも知っている」といったメールを送り付けられたりしたというように、ブログからストーカーに発展するような事例[1]がある。既に個人情報の漏洩を防止する目的で開発された製品としては、野村総合研究所の”TrueTller”[2]やデジタルアーツ社の”i-フィルター”[3]が存在する。そこで、本稿では情報を掲示板に書き込む際に、個人情報を含んでいる可能性がある情報であるか否かを検地する機能を有するプライバシー保護機能つきブログ解析ツールを提案し、そのシステムについて検討を行った結果について報告する。

2. 提案手法

ブログはその性質上、口語や特殊な表現(いぃ友達に、なれたカもしれないｏ)が多く用いられる。一般に個人が書く文体には個人の癖が出やすいと考えられる。そこで、投稿者が書いた文章内容をベイズ定理に基づく解析エンジンを実装して個人情報らしき情報が含まれている可能性を検地する手法を試みた。尚、本稿に置ける個人情報とは、住所、氏名、電話番号、カード番号、メールアドレスとする。また、ニックネーム、や学校名、顔写真なども個人情報と考えられる。また、本システムが想定する利用者は学生や OL 等の未成年、または若年女性としている。を用いて解析する手法を試みた。図１にこれらの利用者によると思われるブログの文例をしめす。

Blog content analysis tools for privacy protection
Marriko Kawaba, Ai Kaneko and Akihisa Kodate
Dept.of Mathematics and Computer Science, TsudaCollege

> おととぃと、昨日ゎ、あゃゃと遊んだヵラ、ｲﾝﾀｧﾈｯﾄを見れませんでした ｏ＜中略＞変なｺﾒﾝﾄもあったｹﾄﾞ、応援のｺﾒﾝﾄもぃっぱぃあって、嬉しかったです ｏ

図１：小学生が書いたブログの抜粋

2.1 要素技術

ベイズフィルタのライブラリとして Classfier4J[3]を用い、また、形態素解析ツールには Java で書かれた Sen[4]を用いた。しかし検討を進めるにあたって、住所、電話番号、郵便番号、個人名、地名といった個人情報にはパターンがあり、表記方法も限られていることが解った。たとえば、人名、地名は形態素解析することによってほぼ読み取ることができる。更に、郵便番号電話番号カード番号などの番号であらわされる個人情報にも数字の並びや数字の接続記号などに特定のパターンが現れる。更にメールアドレスも@マークを中心とした記号の羅列を読み取ることで抽出可能である。

また、ベイズフィルタのみでは個人情報が書かれている個所を正確に特定することが難しい。よって、文書を形態素解析した後で、住所、氏名、電話番号、カード番号、メールアドレスを抽出し、ブログの投稿画面でユーザに注意を促すことにした。

2.2　システムの流れ

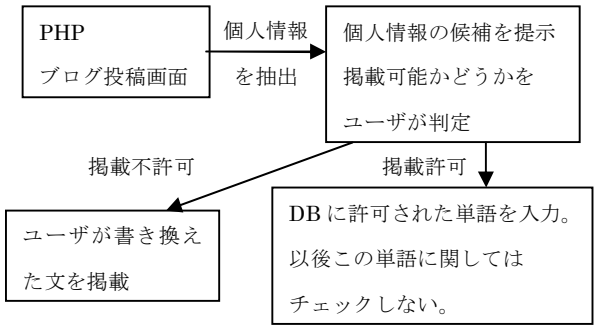

図２：システムの流れ

ユーザが文章を入力すると通常のブログの場合は、そのまま投稿されるが、本システムの場合、ユーザの文章から個人情報候補を抜き出し、ユーザに投稿

をしてよいかの確認を求める。この時、抜き出す個人情報候補は、住所、名前、電話番号、カード番号、メールアドレスに限られる。その抽出法として、住所氏名は、形態素解析された段階で、地名、人名と辞書に登録されているものを抽出する。電話番号、カード番号については、電話番号は、携帯電話の番号の場合、11 桁の数字の羅列、もしくは 11 桁の数字を 3 桁 4 桁 4 桁と記号で区切られているものを抽出し、固定電話の場合は、10 桁の数字の羅列、もしくは 10 桁の数字を記号で区切ったもの（例：0120－444－444）を抽出する。メールアドレスは@マークを中心とした半角英数字と記号の羅列を抽出する。また、ユーザが投稿を許可した場合は、許可された言葉を DB に入力し、以後その言葉に関してはチェックを入れないようにする。さらに、ユーザが投稿を許可しなかった場合は、ユーザが正しいと思う文章に書き換えられた文章が投稿される[図 2]。以下に、ユーザの投稿する文の例[図 3]と、ユーザへの注意を促す文の例[図 4]を示す。

今日は、新宿で梅子と会った。久しぶりに同窓会をすることになったので、参加者は umeko@tsuda.ac.jp まで！

図 3 ：ユーザが書いた文章

今日は、**新宿**で**梅子**と会った。久しぶりに同窓会をすることになったので、参加者は **umeko@tsuda.ac.jp** まで！

図 4 ：ユーザに注意を促す文章

3.システムの評価

表 1 に、ユーザが書いた文章例と、その文章から抜き出された個人情報を示す。

今日は、津田さんと池袋でオムライスを食べた。すっごくおいしかったので店の電話番号を書いておきます。123-4567-8900	津田 池袋 123-4567-8900
愛ちゃんとなっちゃんと出かけた。渋谷は超混んでてつかれたよー。	愛 渋谷
ゆうこりんとさっちゃんと映画を見に行ったよ。OO7 格好よかった～。	

表 1 ：ユーザの文章と個人情報

苗字や、名前、○○さん、○○ちゃんなどと書かれたものは、抽出されるが、「なっちゃん」「ゆうこりん」などのあだ名は抽出されない。また、電話番号や渋谷、新宿、池袋、などの地名は正しく抽出されることがわかった。

4. まとめ

個人情報のパターンを分析することでブログに書かれる個人情報を得ることができた。しかし、ユーザの嗜好を反映させるニックネームや学校名などの個人情報の抽出は不十分である。Sen を用いた形態素解析も一見に付き、10 秒から 20 秒近くの時間がかかるため、ユーザにストレスを与えやすく、実用的とはいえない。また、ユーザが許可したデータを DB に登録するやり方ではなく、機械学習で、個人情報の抽出を行い、個人の嗜好を反映させたい。以下に、今後の課題を挙げる。

- ニックネームや学校名などの個人情報の抽出
- 形態素解析にかかる速度の改善
- 機械学習による個人情報の抽出

参考文献

[1]読売ウイークリー,”大流行「ブログ」でストーカーに狙われる”,
http://www.yomiuri.co.jp/atmoney/yw/yw05041701.htm
[2]野村総合研究所,”テキストデータの文章中に存在する個人情報を自動的にマスク処理する「TRUE TELLER 個人情報フィルタ」を発売”,
http://www.nri.co.jp/news/2005/050303.html
[3]デジタルアーツ株式会社,”i-フィルター”,
http://www.daj.co.jp/cs/ifpe/index.htm
[4]Classifier4J,
http://classifier4j.sourceforge.net/
[5]Sen,
http://ultimania.org/sen/