4 ユビキタス情報社会のプライバシーとその保護技術

吉浦 裕[1] 越前 功[2]
1 電気通信大学 2 国立情報学研究所

ユビキタス情報社会のプライバシー

コンピュータとセンサおよびそのネットワークがいたるところに存在して人々の活動を支える社会すなわちユビキタス情報社会の実現が進んでいる．本稿では，ユビキタス情報社会の重要な問題であるプライバシーについて述べる．プライバシーの定義には諸説があるが，情報の視点からの古典的な定義としては，「個人にかかわる情報の扱いを当該個人が制御できること」が知られている．ここで，情報の扱いには，情報の提供，利用目的・範囲，提供した情報の確認・修正・棄却，提供先からの2次提供などが含まれる．プライバシーの対象となる情報とは何だろうか．その範囲を厳密に定義することは困難であるが，1134人へのアンケートを通じて，個人情報またはプライバシー情報に相当すると感じる32種類の情報を列挙した例がある[1)]．そこには，氏名，住所，学歴職歴，病歴，スケジュールなどのテキスト情報に加え，顔写真，指紋などの画像情報も含まれている．

ユビキタス情報社会のプライバシー問題の発端は1970年代にまでさかのぼる．当時すでに，ディジタル化されたプライバシー情報が本人の知らない間に収集され，使用されるという懸念が有識者たちによって表明されていた．その後，電子商取引などのネットワークサービスの普及に伴って，問題が徐々に顕在化したが，2000年頃からユビキタス情報社会の実現によって，プライバシー問題は新しい局面を迎えた．

ユビキタス情報社会以前では，プライバシー情報を提供する場面が電子商取引などに限定されていたが，以後では，センシングネットワークによって，生活のあらゆる時間・空間でプライバシー情報を提供するようになった．たとえば，GPSやRFIDを通じた位置情報，監視カメラを通じた顔や動作の情報，情報家電の利用を通じた健康管理に関する情報の提供が挙げられる．なかでも，各種のセンサを内蔵し，そのAPIを公開した携帯端末の普及は，プライバシー漏洩の機会を飛躍的に増大させている（図-1）．

ユビキタス情報社会がもたらしたもう1つの大きな変化は，人間という知的センサによって絶えず監視され，プライバシー情報を取得・開示されるようになったことである．動画や写真の投稿・配信サービス，ブログ，Microblog，ソーシャルネットワーキングサービス（SNS）などが続々と現れ，数億人の個人が，自分自身や友人，さらには直接関係のない人のプライバシー情報を安易に開示するようになった．

ユビキタス情報社会のプライバシーはトレードオフの問題と見なすこともできる．高度なネットワークサービスを享受するためにプライバシー情報の提供が必要になる一方で，リスクも生じる．プライバシーのリスクには下記が含まれる．

- 人格のリスク：主に不特定多数へのプライバシー情報の暴露により，人格の尊厳を失う．
- 人権のリスク：主に機関や企業によるプライバシー情報の取得によって，不当な差別や支配を受ける．
- 犯罪のリスク：主に特定の個人や団体によるプ

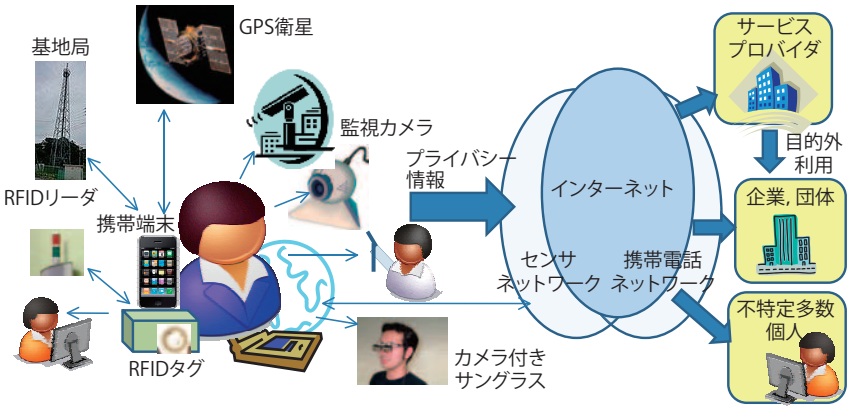
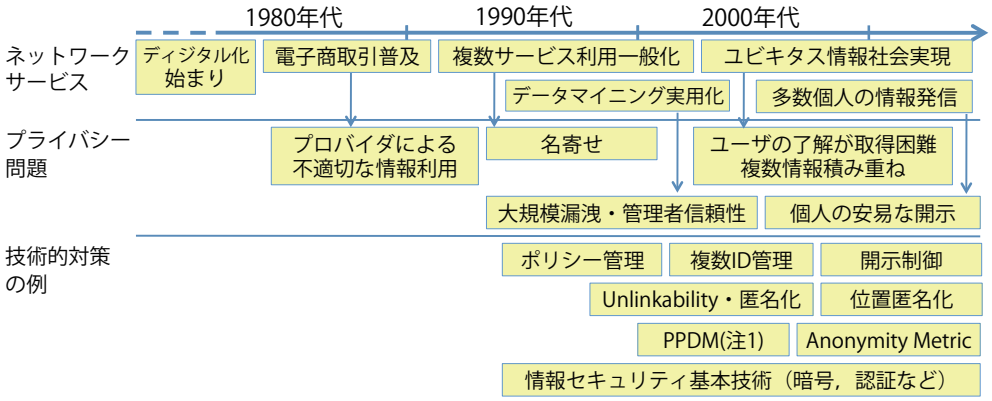


図-1　ユビキタス情報社会のプライバシー問題



注1) Privacy Preserving Data Mining.
注2) 保護技術はいずれも現在まで活発な検討が続けられている.

図-2　ネットワークサービスの発展とプライバシー問題の拡大

ライバシー情報の取得によって，成りすましやストーカー犯罪の標的となる.

このようにネットワークサービスが高度化し普及する中で，その利便性を維持しながら，個人にかかわる情報の扱いを制御することが，ユビキタス情報社会のプライバシー保護の本質的な課題である.

ネットワークサービスの発展とプライバシー問題の拡大

プライバシーは，ネットワークサービスの利便性とトレードオフの関係にある．それは，サービスの発展とともに顕在化し，サービスのユビキタス化に伴って大きな社会問題になった．そこで，本章では，1980年頃から現在までのネットワークサービスの発展と，それに伴うプライバシー問題，技術的対策を概観する（図-2）．その上で，ユビキタス情報社会のプライバシー問題の特性について述べる.

1980年以降の最初の重要なネットワークサービスは電子商取引であった．そこでは，顧客の氏名，住所，カード番号などのプライバシー情報を，当該顧客の了解を得ないでサービスプロバイダが扱うことが懸念された．これに対し，プライバシー情報の扱いに関して，顧客とプロバイダの双方がポリシーを定め，その整合性を検証する技術（たとえばPlatform for Privacy Preferences：P3P）が提案され，現在も検討が続けられている.

1990年代になると，1人のユーザが複数のネットワークサービスを利用するようになり，サービスごとに開示したプライバシー情報を名寄せすること

で，プロバイダなどが広範囲のプライバシー情報を入手する懸念が生じた．そこで，サービスごとに異なるIDを利用可能とする技術が提案され，検討が続けられている．関連して，複数のプライバシー情報・複数のIDが同一人物であると推定できないこと（Unlinkability）や，匿名化技術が検討されている．攻撃の立場からのUnlinkabilityや匿名性を破る技術も多数報告されている．

1990年代後半になると，企業等が多数のユーザからプライバシー情報を集めてデータマイニングを行うようになり，データベースからの大規模なプライバシー漏洩および管理者の信頼性が問題となった．そこで，Privacy Preserving Data Mining（PPDM）の研究が始まった．PPDMは，個々のプライバシー情報を特定できないようにしながら，その集合に対してマイニングを可能とする技術である．また，PPDMのプライバシー保護を保証するために，プライバシー情報が誰のものか分からないことの判断基準としてAnonymity metricが検討されている．たとえば，k-匿名性と呼ばれるmetricは，対象データ内の任意のプライバシー情報について，該当する個人をk人未満に絞り込めないことを保証する基準である．

さて，前章で述べたように，2000年頃からユビキタス情報社会の実現が進み，センシングネットワークを通じて，生活のあらゆる時間・空間でプライバシー情報の提供が行われるようになってきた．その結果，下記の問題が顕在化した．

(1) プライバシー情報が，ユーザの了解なしに取得される可能性が高まる．
(2) 逆に，毎回ユーザの了解を得ようとすると，ユーザにとって煩雑となる．
(3) 多数の断片的なプライバシー情報の積み重ねが，意図しないプライバシー情報の開示につながる可能性がある．

次章では，センシングネットワークを用いた代表的なサービスである位置情報サービスを取り上げ，具体例を述べる．

ユビキタス情報社会がもたらしたもう1つの大きな変化は，多数の個人による情報発信である．人間は，システムとしてみると，きわめて知的である一方，制御することは困難である．この制御困難な知的センサによって絶えず監視され，プライバシー情報を公開されるようになった．今後，カメラ付きサングラスなどの機器やライフログなどのサービスが普及するに従って，この問題はさらに拡大する可能性がある．次々章では，多数の個人による情報発信の代表例として，SNSを取り上げ，具体例を述べる．

以上，ネットワークサービスの発展に沿ってプライバシー問題が拡大する様子を概観したが，他の大きな問題領域として，悪意によるプライバシー情報の盗用がある．外部からのハッキング，内部からの情報漏洩，通信路の盗聴，成りすましによる情報詐取（フィッシング等）などの問題があり，これらは情報セキュリティの一環として対策が講じられている．ユビキタス情報社会のセキュリティとプライバシーを包括的に論じた文献として2)，3)があるので参照いただきたい．

位置情報サービスのプライバシー

位置情報サービスのプライバシー問題

本章では，センシングネットワークを用いた代表的なサービスである位置情報サービスを取り上げ，そこでのプライバシー問題と対策技術について具体例を述べる．ケータイ白書2010によると，日本における2009年のGPS機能付き携帯電話の保有率は，全携帯電話の5割を超えており，GPS機能付き携帯電話所有者のうち，約4割が位置情報に基づくサービス（位置情報サービス）を利用して，自分の位置情報を開示したり，他人の位置情報を取得している．最近では，Twitterのジオタグ☆1やfoursquareのチェックインなどの位置情報追加・登録機能により，自分の位置情報を公開して他のユーザとのつながりを楽しんだり，Google Mapsにより最寄りのレストランを探したりすることが可能になった．このようにユー

☆1 カメラ付き携帯電話で撮影した写真やTwitterへの書き込み（ツイート）などにタグとして追加できる位置情報．緯度と経度を表す数値データで構成される．

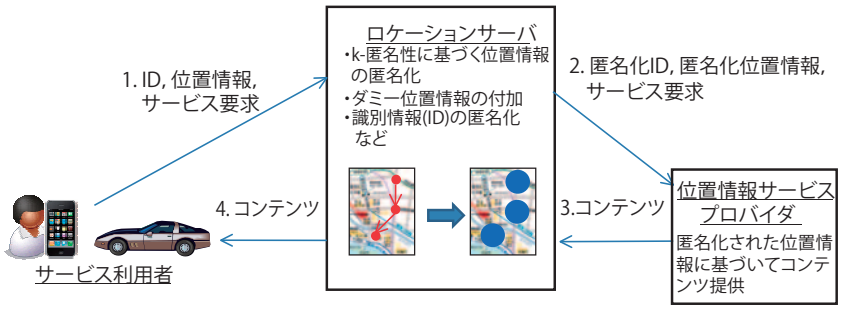


図-3　位置情報サービスのプライバシー保護モデル

ザの位置情報を利用したさまざまなサービスが提供され始めている一方で，ユーザの位置情報や移動経路が第三者によって不当に把握されることで，ユーザが不利益を被ることが問題となっている．米国では，レンタカー会社が貸し出した車の位置をGPS経由で不当に監視し，利用エリア外を走行した車に追加料金を課した事例(2001年)や，休暇を取って旅行に出ていることをTwitterで公開したところ，自宅に置いてあった数千ドルを盗まれたといった事例(2009年)などが報告されている．また，位置情報の解析を通じて個人情報が推測できる可能性も報告されている．Hohらは，65人のドライバーの車に装着したGPSを被験者に1週間観測させたところ，85%のドライバーについて，自宅らしき場所を発見できたという報告を行っている．

さらに，位置情報のプライバシーに関して，ユーザの意識が低いことも問題となっている．USA TODAYの記事によると，長期休暇で旅行に出た米国人の多くは，旅行中に自宅への泥棒の侵入を恐れて，留守番電話の設定を意図的に解除したり，新聞や郵便物の送付を停止したりしているが，旅行中のSNSの利用に対しては警戒心が薄く，自宅から何百マイルも離れた旅行先の位置情報や写真をリアルタイムで掲載したり，『ここに1週間滞在の予定です』などといった情報を安易に投稿してしまう問題があると専門家が指摘している．

このように，位置情報サービスの利用者が増大する中で，利用者(特に位置情報のプライバシー意識が低い利用者)が，第三者により位置情報や移動履歴を過度に取得されないようにすることが，位置情報サービスのプライバシー保護の本質的な課題である．次節では，位置情報サービスのプライバシー保護技術を概観する．

■ 位置情報サービスのプライバシー保護

位置情報のプライバシーの主な目的は，ユーザの位置情報そのものの保護(position privacy)，移動経路情報の保護(path privacy)，位置や経路の情報から推測できる個人情報の保護(identity privacy)である．位置情報サービスの普及に伴い，位置情報のプライバシー保護の研究は近年盛り上がりを見せており，実用化に向けたさまざまな手法が提案されている[4]．

図-3は，位置情報サービスにおけるプライバシー保護モデルの代表例を示す☆2．このモデルでは，(信頼できる第三者機関である)ロケーションサーバがサービス利用者から受信した位置情報を匿名化するので，サーバの信頼性やコストの問題を解決することが実用上の課題となる．これに対し，ロケーションサーバを設置せず，サービス利用者と位置情報サービスプロバイダの間で，匿名化した位置情報とコンテンツを送受信する構成も考えられる．しかし，サーバを設置しないモデルの場合，個々の利用者側で位置情報を匿名化するため，複数利用者の位置情報に基づいて個々の情報を匿名化するk-匿名化などの手法が適用できず，匿名化手法が限定されるといった問題

☆2　具体的なプロトコルについては，IETFのGeopriv ワーキンググループによるRFC 3693[5]を参照のこと．

や，利用者から位置情報サービスプロバイダにIDを直接送信するため，個人の行動履歴が特定されやすくなるといった問題があり，サーバを設置するモデルとの優劣は一概には言えない．

図-3のモデルにおいて，利用者によるサービス要求からコンテンツ受信までの流れは以下のようになる．位置情報サービスの利用者は，最初にGPSを搭載した無線通信デバイスを通して，現在の位置をロケーションサーバに送信するとともに，サービス要求を行う．

ロケーションサーバは，利用者IDと位置情報の匿名化を行い，サービス要求とともに所定のサービスプロバイダに送信する．サービスプロバイダは，匿名化された位置情報とサービス要求に基づいて，コンテンツを生成し，ロケーションサーバを経由してユーザに送信する．

ロケーションサーバによる位置情報の匿名化手法としては，ある時間帯における単位エリアに少なくともk人が存在するように，位置情報の粒度を変更する統計的手法(k-匿名性を利用した手法)や，実際の位置情報に架空の位置情報(ダミー情報)を加えて撹乱データを作成する手法などが代表的である．しかし，利用者から取得した任意の位置情報の集合に対して，これらの手法が匿名性を効果的に高めるとは限らないことが知られている．Kidoらは，位置情報の匿名性を高める性質として，遍在性(利用者がいたるところにいる)，稠密性(一定の範囲に利用者がたくさんいる)，一様性(利用者が一様に分布している)を挙げており，これらの性質に基づいて位置情報の匿名性の客観的な評価指標を定めている[6]．

SNSのプライバシー

SNSのプライバシー問題

本章では，ユビキタス情報社会のもう1つの特徴である，多数の個人による情報開示の代表例として，SNSを取り上げ，そこでのプライバシー問題と対策技術について述べる．SNSのプライバシー情報には，ユーザプロフィール(名前，性別，年齢，所属など)，日記・コメント，写真などがある．ユーザプロフィールはユーザ本人が開示するが，それ以外は本人だけでなく友人によっても開示され，また毎日のように継続的に開示される．

プライバシー情報	直接開示		間接開示		合計
	本人	閲覧者	本人	閲覧者	
病歴	14	2	1	0	17
電話やメールの通信履歴	3	0	1	0	4
アドレス帳の内容	12	0	3	0	15
家族に関する具体的な事柄	26	3	6	0	35
学歴職歴	39	1	11	0	51
身長や体重	3	0	0	0	3
電話やメールの通信の内容	3	0	3	0	6
家族構成	38	8	5	0	51
氏名	5	1	10	0	16
住所	7	1	4	1	13
生年月日	13	0	10	0	23
職業	104	19	47	1	171
出身地	7	5	2	0	14
Webサイトの閲覧記録	1	0	0	0	1
スケジュール	91	6	5	0	102
知人や友人に関する具体的事柄	8	0	2	0	10
商品やサービスの購入記録	10	1	0	0	11
合計	384	47	110	2	543

表-1　特定ユーザのSNS日記7047文の分析

これらのプライバシー情報の漏洩問題と対策については，ACM系，IEEE系の国際会議を中心に多数の研究発表がある．たとえば，ユーザプロフィールについては，Facebookサンプルユーザ232人のうち誕生日を公開しているユーザは84%，携帯電話の番号および配偶者の名前を公開しているユーザは各々39%および28%などの調査報告[7]，ユーザの1/3は「友人まで」などの公開制限を設定しているが，2/3は「全体公開」にしているといった報告[8]がある．

日記・コメントについては，ブログを対象とした調査報告があり，ユーザの55%は自分の実名をブログの中で公開している，91%は友人の何らかのプライバシーを公開した経験がある，21%は友人の実名を公開，66%は当該友人の了解を得ていないとしている[9]．SNSでも同様の傾向があると考えられる．

Facebook社の統計によれば，2010年7月時点の1ユーザあたりの平均「友人」数は130である．そこで，開示範囲を「友人まで」としても130人への開示となり，「友人の友人まで」とすると130^2人への開示となる(厳密には重複があるので130^2より少ない)．「全体公開」は数億人への開示となる．

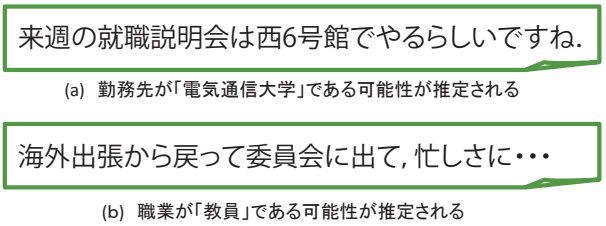


図 -4　間接開示の日記文例

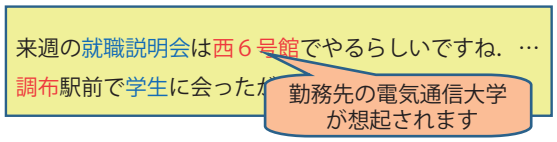


図 -5　DCNL の機能

表-1は，特定ユーザがSNSに投稿した日記・コメントを取り上げ，最初の章で述べた32種類の分類[1]に沿って筆者らが分析した結果である．2005年10月から2007年5月までに投稿された日記（149件）と日記に対するコメント（本人の記述375件，閲覧者の記述618件），文章数にして7047文を対象とし，そこでのプライバシー情報の開示件数を数えた．日記・コメント中にプライバシー情報が直接記載されている場合（直接開示）と，直接記載されていないが，記載された情報からWeb検索などにより人がプライバシー情報を推定できる場合（間接開示）があり，その比率は4：1であった．

図-4に間接開示の日記文例を示す．文例1では，「就職説明会」から，ユーザは高校か大学に所属している可能性が高いと推定される．「西6号館」をキーワードとしてWeb検索を行うと，検索結果の上位30件のうち東京工業大学に関する記事が13件，電気通信大学が12件，東北大学と早稲田大学が各2件，学校に関係しない記事が1件であり，投稿者の所属を推定することができる．文例2はより微妙であり，文例1のように，特定のキーワードからの推論やWeb検索によって職業が推定できるわけではないが，投稿者が教員である可能性が感じられる．

■ SNSのプライバシー保護

SNSのプライバシーを保護する代表的な技術は，ユーザによる開示範囲の指定であり，指定された開示制御をSNSサーバが実行する．「友人まで」，「友人の友人まで」などの階層的な範囲指定に加えて，各々の友人や友人グループに対する開示の可否を指定することができる☆3．

筆者らは，SNSのプライバシー情報のうち日記・コメントの部分を対象とした開示制御技術DCNL（Disclosure Control of Natural Language information）を開発している[11]．ユーザがSNSシステムに日記・コメントを入力すると，DCNLはその内容を検査し，色分けなどによってプライバシー漏洩の危険度を示す（図-5）．ユーザが着色部分をクリックすると，どのようなプライバシー漏洩の可能性があるかを表示する．DCNLでは，文書エディタの自動英文添削のような実用化を目指している．初期の自動英文添削は，的外れな指摘が多かったが，文章の色を変える等の目障りにならない指摘であり，時には有益な指摘もあったので利用された．そして継続的な利用を経て精度が高まり現在では非常に有用になっている．DCNLもこのように育てたいと考えている．

DCNLは，ユーザのプライバシーを表す語句（電気通信大学，教員など）をプライバシー知識として蓄積する．日記文章を入力すると，文中の語句とプライバシー知識内の語句の照合により，プライバシー漏洩を直接的に検知する．しかし，この照合では，大学名や職業名などが直接記述されている場合（直接開示）は検知できるが，人が文章から間接的に推定できる場合（間接開示）は検知できない．そこで，間接開示の検知および直接開示の検知漏れに対する補完のために，Web検索を利用した検知（想起検知）を行う．

「電気通信大学」の検知を例として，想起検知のアルゴリズムを説明する．まず検査対象の文に含まれるすべての名詞から最大m個までの組合せを求

☆3　Facebookの開示制御について，Gursesらの詳細な分析がある[10]．

検索キーワード	電気通信大学の出現回数	検索キーワード	電気通信大学の出現回数
就職西 6	1	6 号館説明就職	1
就職 6 西	1	就職説明 6 号館	1
西就職 6	1	6 号館西就職	3
西 6 就職	1	就職西 6 号館	3
6 就職西	1	就職説明会 6 号館西	1
6 西就職	1	6 号館就職説明	1
6 号館就職	1	就職 6 号館説明	1
就職 6 号館	1	説明 6 号館就職	1
6 号館西	6	6 号館就職西	3
西 6 号館	4	就職説明会西 6 号館	1
西 6 号館就職	4	6 号館西就職説明会	1
説明就職 6 号館	1	6 号館就職説明会西	1
就職 6 号館西	3	西 6 号館就職説明会	1
西就職 6 号館	3	西就職説明会 6 号館	1

表 -2　文例（a）からの「電気通信大学」の想起の過程

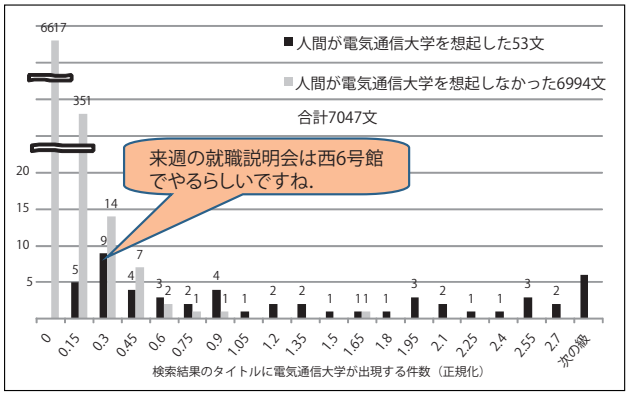


図 -6　「電気通信大学」の想起度の分布

め，それをキーワードとしてWeb検索APIを起動する．このとき，文中の名詞の総数をnとし，そこから選択する名詞の数を$i(1\leq i\leq m)$とすると，検索回数Rは$\sum_{i=1}^{m} {}_nC_i$となる．検索結果の上位k件までのタイトルを検査し，その中の「電気通信大学」という語句の出現回数Aをカウントする．このとき，検査するタイトル数TはRkとなる．

「電気通信大学」の出現回数Aを検索回数Rで割って正規化した値（A/R），すなわち検索1回当たりの「電気通信大学」の出現回数を想起度とする．m=3，k=24の場合に，図-4の文例（a）ではA/R=0.32，文例（b）では0.0であり，文例（a）は文例（b）よりも，「電気通信大学」を想起しやすいと判定する．表-2は，文例（a）の想起度を求める過程での検索キーワードと，そのキーワードで検索した際の「電気通信大学」の出現回数を示す．ただし出現回数が1以上の場合のみを記載している．

図-6は，前述した特定ユーザの日記・コメント7047文における「電気通信大学」の想起度の分布を示す．横軸は想起度，縦軸は文の数を表している．検出しきい値をA/R=0.30に設定すると73文を検知し，その中には人間が「電気通信大学」を想起した53文のうちの48文を含む（適合率=0.65，再現率=0.91）．

本アルゴリズムは図-4文例（a）から「電気通信大学」を想起できた．これは，「就職説明会」や「西6号館」に着目しWeb検索に基づいて判断する過程を自動化できる可能性を示している．また，「調布駅前で学生に会ったが，…卒研で悩んでいるようだった」という文例からも，想起度0.35で「電気通信大学」を想起できた．

また，本アルゴリズムは，上記と同じパラメータを用いて，図-4文例（b）から，想起度0.56で「教員」を想起することができた．本アルゴリズムの実用化に向けて，他ユーザの日記を用いた評価・改良および効率化（検索APIの起動回数の低減等）を進めている．

今後のプライバシー問題と技術課題

生活のあらゆる時間・空間でのプライバシー情報の提供，多数の個人によるプライバシー情報の開示は今後ますます増えていく．さらに，センサ情報やSNS情報がAPIを通じてプログラムによって利用されること，複数のネットワークサービスが自動的に連携することにより，プライバシー情報の取得・開示の機会およびその拡散の範囲が拡大すると考えられる．このような状況下で，ユーザの意思に沿ってプライバシー情報の扱いを制御する技術が求められる．

また，リスクの視点からは下記のような技術も必要になると考えている．

- 人格の尊厳が失われるリスクについては，不特定多数の個人によるプライバシー情報の開示を検

知し，警告・フィルタリングする技術．

- 人権が抑圧されるリスクについては，サービスの公平性を検証したり，アカウンタビリティを確保する技術．
- 犯罪の標的となるリスクについては，攻撃をシミュレーションする技術．たとえば多くの断片的なプライバシー情報の組合せによる推論の技術．

本稿では，主にユーザの視点からプライバシー問題を論じたが，プロバイダや監督官庁などの他のプレイヤの視点からの議論も重要である．また，本稿では技術を中心に論じたが，制度やビジネスの視点からの議論も重要である．ユビキタス情報社会のプライバシーは，これらの総合的な取り組みを必要とする複雑で面白い問題である．

参考文献

1) 現代人のプライバシー〜生活者アンケートの結果から〜，NEC総研，東京 (2005).
2) Stajano, F. : Security for Ubiquitous Computing, John Wiley & Sons, Chichester, England (2002).
3) Hutter, D., Mueller, G., Stephan, W. and Ullmann, M. (Eds.) : Security in Pervasive Computing, First International Conference, LNCS 2802, Boppard, Germany (2003).
4) Krumm, J. : A Survey of Computational Location Privacy, Personal and Ubiquitous Computing, Vol.13, No.6, pp.391-399 (2009).
5) Mulligan, D., Cuellar, J. and Morris, J. : Request for Comments : 3693 Geopriv Requirements (2004), http://www.ietf.org/rfc/rfc3693.txt
6) Kido H., Yanagisawa Y. and Satoh, T. : An Anonymous Communication Technique Using Dummies for Location-Based Services, International Conference on Pervasive Services, pp.88-97 (2005).
7) Acquisti, A. and Gross, R. : Imagined Communities : Awareness, Information Sharing, and Privacy on the Facebook, Workshop on Privacy Enhancing Technologies, LNCS 4258, pp.36-58 (2006).
8) Lewis, K., Kaufman, J. and Christakis, N. : The Taste for Privacy : An Analysis of College Student Privacy Settings in an Online Social Network, Journal of Computer-Mediated Communication, Vol.14, Issue 1, pp.79-100 (2008).
9) Viégas, F. B. : Bloggers' Expectations of Privacy and Accountability : An Initial Survey, Journal of Computer-Mediated Communication, Vol.10, Issue 3, Article 12 (2005).
10) Gurses S., Rizk, R. and Gunther, O. : Privacy Design in Online Social Networks : Learning from Privacy Breaches and Community Feedback, International Conference on Information Systems (2008).
11) 片岡春乃，内海　彰，広瀬友紀，吉浦　裕：意味と面白さを維持する自然言語情報の開示制御技術の提案―SNSのプライバシー保護への試適用―，情報処理学会第36回コンピュータセキュリティ研究会，pp.321-326 (2007).

（平成22年7月12日受付）

吉浦 裕（正会員）　yoshiura@hc.uec.ac.jp
1981年東京大学理学部情報科学科卒業．日立製作所を経て，現在，電気通信大学情報理工学研究科教授．情報セキュリティおよびプライバシー保護の研究に従事．博士（理学）．本会論文賞（2005年）など受賞．

越前 功（正会員）　iechizen@nii.ac.jp
1997年東京工業大学修士課程修了．日立製作所を経て，現在，国立情報学研究所コンテンツ科学研究系准教授．情報セキュリティ，コンテンツ保護の研究に従事．博士（工学）．本会論文賞（2005年）など受賞．