基般

オンラインサービスと匿名性

折田明子（関東学院大学人間環境学部）

インターネットは匿名性が高い?

自分の買い物を人に知られたくないとき，皆さんは店頭での買い物を選ぶだろうか．それとも，ネット通販による買い物を選ぶだろうか．実名を隠したソーシャルメディアならば，職場の愚痴を書いても大丈夫だろうか．

インターネットを使えば，自分の顔を見せずにサービスを利用したり，コミュニケーションを図ったりすることができ，名乗れる名前の自由度も高い．それゆえ，インターネットの利用は，匿名性が高いものであると捉えられてきた．

たしかに，相手と対面せずに利用できるという観点では，インターネットを介して提供されるサービスの利用や，そこで行われるコミュニケーションは，匿名性が高いものと言える．互いに姿を見ることがなければ，見かけから判断される年齢，性別，人種といった手がかりを秘匿することができる．社会生活において使っている名前（実名）や，所属組織を隠すことができれば，生活に対する影響も避けることができる．一方で，インターネットを介して銀行口座の取引を行うならば，顔が見えないとはいえ，身元を明確にし，かつ当人であることが確認できなければならない．また，買い物であれば支払い者と届け先の情報が必要であり，ソーシャル・ネットワーキング・サービス（SNS）であれば，友人との人間関係において互いに誰なのかが分かる必要がある．このように，インターネットを介した非対面の状態がすべて匿名というわけではなく，サービスによって利用者を特定する度合いは異なる．これらを混同することによって，匿名性を過信して多くの情報をばら撒いてしまったり，あるいはいたずらに恐れてサービス利用を避けてしまったりといった事態が発生し得る．

インターネット利用における匿名性は，「匿名だから悪い」「匿名か，実名か」といった二択の考え方に陥りがちである．しかし，これは実名，匿名の状態は，異なる文脈であれば影響も異なるということに過ぎない．匿名であることによって，性別や年齢，身なりや所属組織といった，本人の属性に起因するステレオタイプが解消される可能性もあるが，それはその人物に関する背景情報が不足することでもある．匿名性が高ければ率直に物事が言いやすいということは，相談ごとなどにおいて自己開示が促進されると同時に，コミュニケーションがこじれた際に他者への攻撃を容易にすることでもある．このように，同じ特徴であっても，文脈や場面によってもたらされる影響は異なるため，匿名性を善悪の二択で捉えるよりも，そのメリットを高めつつ，デメリットを減じたサービスづくりやコミュニケーションを考える必要があろう．

本稿では，インターネット利用における匿名性を，「名前」という観点から，その構造とサービスへの適用について整理することを試みた．

インターネット利用における匿名性の種類

インターネット利用における匿名性は，本人を見ることができるか否かという非対面状況ゆえに発生するものと，本人を特定できるか否かという本人到達性に関するもの，そして同一人物であるか否かというリンク可能性に関するものの3つに分類できる．1つ目はメディアの特性によるものであり，後者2つは利用者の名乗りと，情報のひもづけに関するものである．

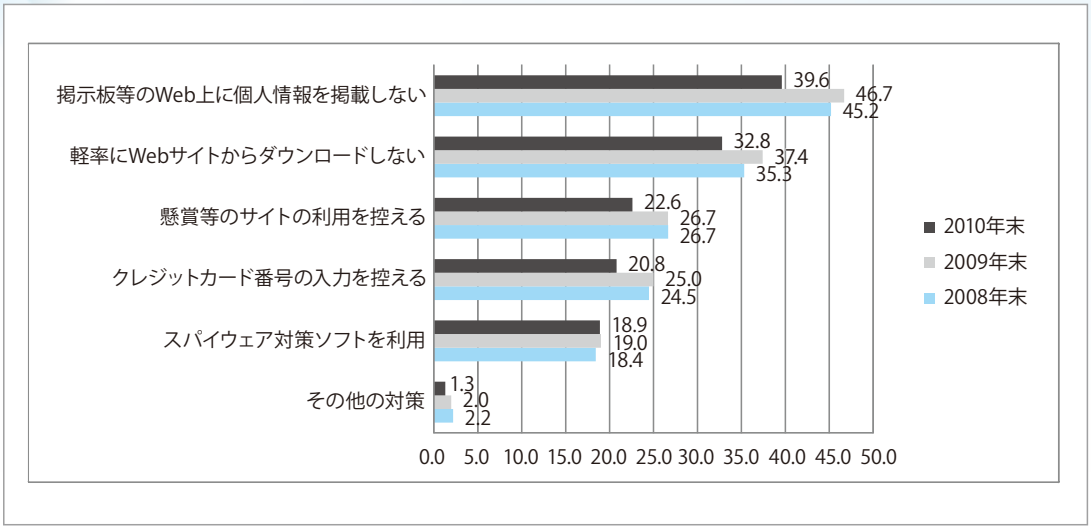

図-1　世帯における個人情報保護対策（平成23年総務省情報通信白書）

◆視覚的匿名性：相手の姿を見られるか

1つ目は，オンラインでコミュニケーションするゆえに相手を直接見ることができない「視覚的匿名性」（visual anonymity）である．これを分かりやすく表現したのが，1993年のNewYoker誌に掲載された風刺画である．端末の前に2匹のイヌがいて"On the Internet, nobody knows you're a dog"とあり，現実とオンラインのコミュニケーションではまったく異なる人格（動物？）でいることすらできるということを表現したものである．現在では動画を伴うチャットや会議が普及しつつあるが，テキストベースのコミュニケーションは依然として多く行われており，利用者が自らについて記述したことが，その人物を知る手がかりになる．なお，視覚的匿名性は，相手が実名を名乗っているか否かとは無関係に発生する．

視覚的匿名性がある状況では，個人はコミュニケーションにおいて自分自身に関してより詳細に記述する傾向があり，同時に受け手も限られた情報から相手に関する手がかりをできるだけ得ようとする傾向があるという[1)]．そのため，一見逆説的ではあるが，オンラインでのコミュニケーションでは，対面のコミュニケーションに比較して，むしろ自分に関して詳細に情報を発信してしまう可能性がある．

◆本人到達性：相手が誰かを特定できるか

2つ目は，本人が誰であるかを特定できるか否か，「本人への到達性の有無」という意味での匿名性である．言い換えれば，個人情報保護法第二条に定義されている個人情報，つまり「生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの」が明らかであれば本人到達性があるといえる．

日本語の「匿名」は，本人到達性の有無によるものであり，「自分の名前を隠して知らせないこと．また，本名を隠してペンネームなどの別名をつかうこと」（大辞泉）とされている．これに対し，英語では本人到達性がない状態を，さらにanonymous（匿名・無名性）とpseudonymous（仮名性）に区別している．

なお，これまで，日本ではインターネット利用において，主に個人情報保護の理由から利用者が実名を秘匿する傾向があった．情報通信白書によれば，インターネット利用時の不安として「個人情報の保護の不安」を感じるという回答が約70%を占め例年上位に上がっている．また，個人情報保護への対策実施状況を見てみると，6割から7割の回答者が何らかの対策を行っており，特に「Web上に個人情報を記載しない」という回答が多数を占めており，コミュニケーションサービスの利用において，実名や電話番号，住所などを記載しないことに注意がはらわれている（**図-1**）☆1．

☆1 ただし，その割合は2010年にはいったん減少しており，Facebookなど実名での利用をうたったサービス利用との関係を検討する必要があろう．

◆リンク可能性：相手を他者と識別できるか

3つ目は，複数の行為が同一人物によるものだと識別できるかどうかの「リンク可能性の有無」である．リンク可能性（Linkability）は，ドレスデン大学のPfitzmannらが1999年以来とりまとめてきた匿名性に関する用語集（anon terminology）において，匿名性の程度を決める重要な要素として位置づけられている[2]．

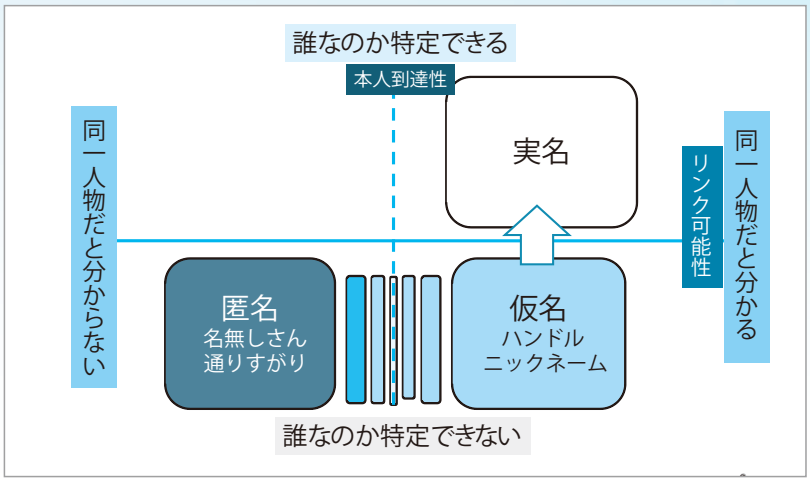

図-2　本人到達性とリンク可能性

たとえば，「名無しさん」という名前の投稿が並んでいる場合，それがすべて同じ人物によるものか，すべて違うのか，あるいはどれとどれが同じ人物かは，一見区別することができない．これがリンク不能な状態である．もし，これらの投稿に投稿元IPアドレスが付与されていれば，少なくとも同一IPアドレスからの投稿をリンク可能なものとしてくくり，ほかのものと識別することができる．これがリンク可能な状態である．

リンク可能性によって，同一人物としての情報が蓄積されるということは，個人を特定するに至らなくとも，ある人物と別の人物が識別されていることが前提であり，蓄積された情報によってある人物像がつくられることでもある．匿名性を考えるにあたり，本人到達性の有無という軸だけでは，継続的に利用するハンドルや利用IDといった仮名と，「匿名希望」や「名無しさん」と言った使い捨ての名前や，IDが付与されない状態が区別できなかった．そこにリンク可能性という軸を加えることによって，オンラインでの名前は，次のように整理できる（**図-2**）☆2．

- 実名：本人到達性およびリンク可能性がある状態
- 仮名：本人到達性はないがリンク可能性がある状態
- 匿名：本人到達性とリンク可能性がともにない状態

これらは，明確な境界線によって区別できるものではなく，程度を持つものであるし，その状態は遷移するものである．たとえば，ある掲示板の話題スレッドにおいて「通りすがり」と名乗る匿名の利用者が互いにコミュニケーションをはじめると，相手と自分を区別するために，投稿番号を継続的に使ったり，「通りすがりA・B」といった識別子を付与したりするといった行動がある．これは，その話題の中でのみリンク可能な状態を作っているが，その話題を超えて掲示板全体，サイト全体，あるいは複数のサイトやサービスでも同じ名前を使ったり，自ら同一人物であるとひもづけるといったように，リンク可能な範囲をどこまで広げるかによって，その利用者に関連づけられる情報量は変化する．関連づけられる情報量が多ければ，特定の人物像を再構成することになる．また，個人情報保護法第二条に書かれている「他の情報と容易に照合することができ，それにより特定の個人を識別することができる」という状態になることで，本人を特定する可能性も高くなるといえる．

誰に何を見せるのか

前章で整理した，本人到達性とリンク可能性の組合せは，実名・仮名・匿名等，利用者同士で互いに「見える」名乗りを前提としている．しかしインターネット上のサービス利用に際して登録する情報は，利用者間での名乗りと必ずしも同じではない．決済

☆2　なお，ここでいう実名とは，社会生活上での名前を指し，必ずしも戸籍上の氏名に限らない．

を必要とするサイトでは，支払いに必要な情報（クレジットカード番号，口座番号およびその名義人など）を登録させるが，これらの情報は利用者間では当然参照できない．このように，誰にどの情報を見せるのかを整理したものが，**図 -3** である．

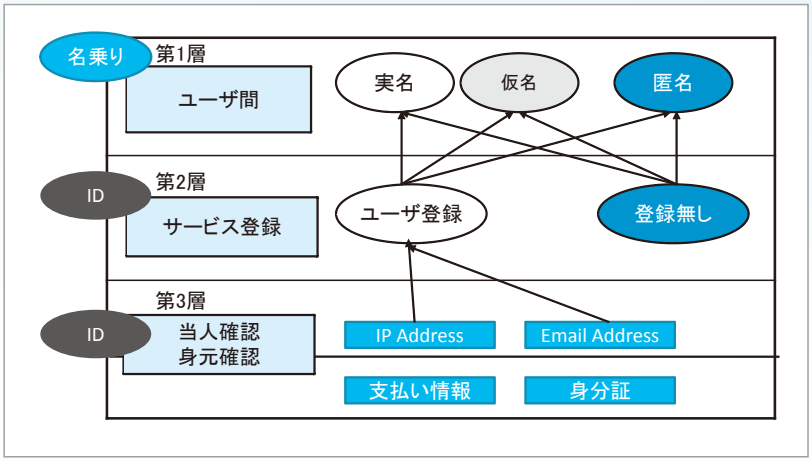

図 -3　3 層構造

第 1 の層は，利用者同士互いに見える名前であり，実名や仮名（ハンドル・ニックネーム），あるいは名無しといったものである．

第 2 の層は，サービス利用開始時に会員として登録し，ID を取得するか否かである．利用登録をすることにより，利用者がどのような名前を名乗ろうとも，あるいは利用時に複数の名前を使おうとも，同一人物としてのリンク可能性は保たれる．言い換えれば，利用登録がなければリンク可能性は担保されず，その上で名乗っている名前が実名である保証も，あるいは同一人物であるという保証もない．

第 3 の層はサービスを提供する側が，利用者について，それが当人であることを確認したり，当人の身元を確認したりするものである．メールアドレスへの到達性，すなわち登録した人が当人であるという確認のみを求めるレベルから，決済が必要であればそれに関するもの，公的な身分証を求めるものなど，用途によって当人および身元確認のレベルは異なる．なお，韓国で導入された実名登録制とは，第 3 層において身分証明書で身元を確認するものであり，第 1 層における実名の表示ではない．

このように整理すると，インターネット上のサービス利用およびコミュニケーションにおける匿名性とは，利用者同士に見える部分（第 1 層）だけでなく，むしろ第 3 層での身元確認のレベルにかかっていることが見えてくる．この身元確認は，日常生活で使う印鑑をイメージすると分かりやすいだろう．常に実印レベルのものを使う必要はなく，用途に応じて認印，スタンプ印と使い分けるのと同じである．

このように，利用者同士で見える「名乗り」と，ID，および確認手段を分けて捉えることにより，利用者同士では匿名性が高いが，サービス提供者に対しては本人への到達性があるという状況や，利用者の身元確認の厳密さを用途によって使い分けるという状況を作りだすことができる．たとえば，Yahoo! JAPAN では，1 つの Yahoo! JAPAN ID に対して，最大 6 つの異なるニックネームを設定し，掲示板やオークション，ブログなど，用途によって使い分けることができる．いわば，利用者間では用途ごとにリンク不能な状態を作ることができるが，サービス提供者からはそれらすべてがリンク可能なものとして把握できている状態である．かつ，有料サービスの利用者であれば支払者の情報が，オークションの利用者であれば住所も登録されているなど，高いレベルでの身元確認がなされているが，それが利用者同士で常に明らかにされるわけではない．

オンラインサービスと匿名性に関する問題

◆どちらの方が匿名性が高いか？

視覚的匿名性，本人到達性，およびリンク可能性の組合せによっては，「顔が見えないが匿名性は低い」状態や，「顔が見えるけれども匿名性の高い」状態，「本人は特定されないが，ある人物像が形成される」状態が想定できる．誰に見せるかという層構造を加えると，さらに匿名性は一意ではないこと

が分かる．たとえば，店頭で現金で買い物する場合と，クレジットカードを使ったオンラインショッピングでは，どちらが匿名性が高いと言えるだろうか．前者では，顔が見えるために視覚的匿名性はないが，本人を知らない限り到達性はなく，現金で支払う限り同一人物としての情報も蓄積されない．ポイントカードを利用するならば，それまでの購買履歴は蓄積されるが，通常，そのデータは現場で顔を合わせている相手に参照されるわけではない．後者では，インターネットを介しており，顔が見えないという意味で視覚的には匿名だが，クレジットカードおよび記載されている実名（少なくとも決済はできる名前），そして配送先住所を提供しなければ買い物ができない．また，利用に際して会員登録をするならば，購買履歴が蓄積される．

医薬品のネット販売をはじめとする，ネット通販の安全性や本人到達性の問題，あるいは買い物におけるプライバシーの問題を論ずるにあたっては，異なる観点に立てば異なる匿名性が存在し，何を選択すべきかを考慮する必要があろう．

◆ 意図せず失われる匿名性

ソーシャルメディアをはじめとするコミュニケーションをはかるサービスでは，利用者本人が実名を秘匿したとしても，コミュニケーション相手との関係性や，その内容によって匿名性が失われてしまうことがある．たとえば，人間関係を表すソーシャルグラフにおいて，自分がつながっている相手が実名および所属先を明示した上で，自分のことを同僚とタグづけしたり，あるいは同僚と分かる内容のコミュニケーションをはかったとすれば，所属先が推測される状況になる．また，一般的なソーシャルメディアの利用には，会員登録が必要であり，サービス内の行動は同一人物のものとしてリンクされ蓄積されていく．その中には，位置情報を含むものもあり，また，投稿時刻も行動パターンを浮かび上がらせる手がかりになり得る．その結果，「早朝と深夜に投稿が多く，日中は火曜日のみ投稿するが，あとは投稿しない」といった情報と，人間関係を組み合わせることによって，自らが意図しないところで，本人に到達する手がかりを提供している可能性がある．他者との関係性および情報のリンク可能性によって，匿名性が失われることについても考慮する必要があろう．

また，このことは，いわゆる個人情報の保護だけでなく，プライバシーの保護といった問題にもかかわってくる．2012 年に米国ホワイトハウスが発表した行政文書，消費者プライバシー権利章典（CONSUMER DATA PRIVACY IN A NETWORKED WORLD）[3] では，特定の個人にリンク可能なデータの集合をプライバシー保護の対象としており，そこには特定のデバイスにリンクされるものも含めている．また，EU のデータ保護規則案（EU Protection of personal data）[4] においても，特定された自然人としつつも，その識別子にオンライン識別子（Online Identifier）を含めている．今後は，匿名性というものを，広く捉え直し，利用者が意識的に使っていくための整理が必要であろう．

参考文献

1) Wallace, P. : The Psychology of the Internet, Cambridge University Press (1999)（邦題 インターネットの心理学，NTT 出版）.
2) Privacy and Data Security : Anon Terminology Paper, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml
3) THE WHITE HOUSE “CONSUMER DATA PRIVACY IN A NETWORKED WORLD”, http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf
4) EU Protection of personal data, http://ec.europa.eu/justice/data-protection/

（2013 年 6 月 25 日受付）

折田明子（正会員）｜oritako@kanto-gakuin.ac.jp

博士（政策・メディア）（慶應義塾大学）．2008 年中央大学ビジネススクール助教，2010 年慶應義塾大学大学院政策・メディア研究科特任講師，2011 年米国ケネソー州立大学客員講師を経て，2013 年より現職．インターネット利用者の名乗りと ID，プライバシーに関する研究に従事．