Vol.2009-EIP-44 No.4
2009/6/5

ソーシャルメディアにおけるなりすまし問題に関する考察

折田明子†

ブログや SNS、掲示板などのソーシャルメディアにおける匿名性の高いコミュニケーションにおいては、会員登録や仮名利用によって利用者の識別性が確保されている。だが、第三者が、ID そのものを乗っ取るまでにいかないものの、趣味や嗜好を真似て特定のユーザに「なりすます」という問題が発生している。長らく使っていた仮名を他者が意図的に名乗り出してコミュニケーションに混乱を招いたり、個人のブログやサイトの管理者であるかのようにふるまうといった行為だ。本稿では、ネット上の匿名性と識別性の整理を踏まえた上で、こうしたなりすまし問題についての考察を試みる。

A Report on the Username Squatting Problem of Social-media

Akiko Orita†

Social-media, such as blogs, SNS and BBS is the place that users tend to hide their real name but register their IDs. Username squatting is occurred on such social-media not only as identity-theft but as pretending to be a particular user. This paper firstly shows the classification of identity representation on the web, then,consider several cases of username squatting based on the classification.

1. はじめに

インターネット上で、他人の名前や ID を使う「なりすまし」という言葉は、一般には ID とパスワードの盗用や不正アクセスによる行為を指して用いられている。こうした行為は不正アクセス禁止法違反として処罰の対象となると同時に、セキュリティの問題として扱われている。一方、ID やパスワード盗難以外の手段実現される「なりすまし」も存在する。この場合、ID やパスワードは必ずしも不正に得られたものではなく、本人性の確認はより困難となる。特にブログや SNS、掲示板などのソーシャルメディアは実名を秘匿した利用が主流であり、本人確認の難しさと自己情報に対する警戒感の薄れが問題を深刻化させると言えるだろう。本稿では、後者の「なりすまし」において、現在どのような問題が発生しつつあるのかを明らかにするとともに、今後の研究設計に貢献するための問題提起を試みる。

2. ネット上の「名乗り」構造

ブログや SNS、掲示板など、利用者が情報を発信したり閲覧したりするソーシャルメディアの利用は増加しており、その約 7 割が実名を秘匿したコミュニケーションを志向している[1]。ソーシャルメディアは匿名性の高い場としてとらえられているが、Web2.0 と称されるサービスの多くは利用時に会員登録を求めており、利用者の同一性は確保される。また、利用者もニックネームやハンドルなどの「仮名」によって自己を表現し、コミュニケーションをはかっている[2]。

実名を秘匿したコミュニケーションが主流であるゆえに、全ての人が認証された実名を名乗っていない環境下でなりすましが発生する余地があると言えるだろう長らく使っていた仮名を他者が意図的に名乗り出してコミュニケーションに混乱を招いたり、著名人のブログやサイトの管理者であるかのようにふるまうといった行為は、ID を取得するプロセスに本人確認が含まれない限り、「誰が本物か」を証明しづらいという点でも問題をはらんでいる。

本節では、まず匿名性が高いとよばれるソーシャルメディア利用における「名乗り」の構造を整理する。匿名性の程度は、情報の発信者が誰であるかを特定するという要素と、情報の発信者を他者と識別する、すなわち同一人物を同識別するという要素によって左右される。谷口らは前者を「実社会の人格」、後者を「ネット社会の人格」と定義し、ネット社会の人格が特定されるが実社会の人格が特定されない状態を「仮名

† 中央大学大学院戦略経営研究科（ビジネススクール）
Chuo Graduate School of Strategic Management, Chuo University

性」(pseudonymity)と定義しており[3]、実社会とネット空間を区別している。

本稿では、 (1)本人が誰であるかを特定する「本人到達性」、(2)行為が同一人物であるかどうかを判別する「リンク可能（不能）性」という二軸、および(3) 誰の観点からの「名乗りなのか」という観点を前提に、名乗りの構造を整理する。

2.1 本人到達性

本人到達性とは、基本四情報などの個人情報によって、情報の発信者が誰であるかを特定できる状態と定義できる。一般的に匿名という言葉で指し示されるのは、本人へ到達性が失われた状態である。本人への到達の困難さは、ある集合におけるユーザの数、多様性、そしてユーザに対する事前知識によって決定する [4]。すなわち、コミュニティなどのある集合に属するユーザの数が少なかったり、それぞれのユーザに多様性があれば（均質でなければ）、本人を特定できる可能性は高くなる。逆に、集合に属するユーザの母数が大きく、かつユーザの性質が均質であるほど本人への到達性は低下する。

例えば、「A 氏」「B 氏」といった均質な仮名や、番号順にリニアに付与される ID は、本人のイニシャルや嗜好を反映させたものと比較して本人到達性は低い。また、参加者が少数のコミュニティは、参加者が多数のコミュニティよりも本人を特定できる可能性が高い。

2.2 リンク可能性

リンク可能性(Linkability)とは、複数の行為を同一人物のものとして識別できる状態を指す[5]。なお、Linkability は PIA(プライバシー影響評価)関連の翻訳では「データ結合性」とされるが、本稿ではリンク可能性という訳語を採用する。リンク可能性は複数の行為に対する行為者の識別子（ログイン名、アクセス元など）によって判別でき、この識別子は広義の仮名(pseudonym)といえる。仮名によって行為と行為者は関連づけ（リンク）られる。

行為がリンク可能な状態であれば、行為者を識別することができ、リンク不能な状態であれば行為者は識別できない（図 1)。たとえば「通りすがり」という名の書き込みが複数表示されている掲示板において、その書き込みがすべて同一人物によるものなのか、複数の人物によって書き込まれているのかが区別できない状態は、リンク不能な状態であり、匿名性は高い。

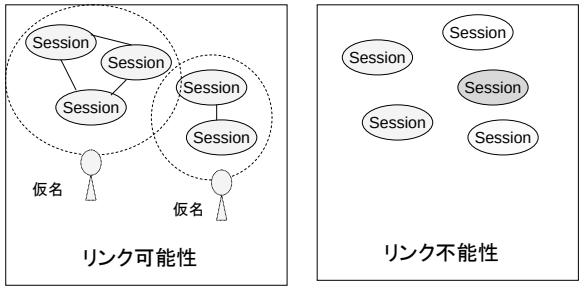

図 1　リンク可能性とリンク不能性

以上の二つの軸の関係を図に示す（図 2)。CMC 研究等で用いられている用語と併せて説明するならば、本人への到達性がある状態は、一般的には匿名ではないと状態、すなわち実名と位置づけられる。一方、本人への到達性がない状態である第三および第四象限は、リンクが可能であればハンドルやニックネーム、ID による「仮名」”pseudonym”、リンクが不能であれば名無し、通りすがりといった「完全匿名」”anonymity”と位置づけられる。

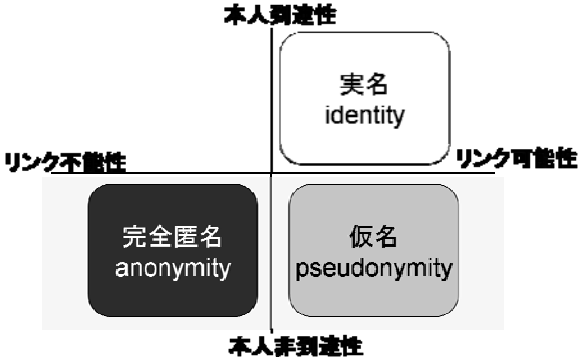

図 2　匿名性の構成

2.3 名乗りのレイヤ構造

こうした名乗りの違いは、取り扱う者の観点によって異なる。利用者は自分自身を匿名性の高い状態にあると考えていても、実際にはシステム上全ての行為がリンク可能であるという状況は珍しくない。たとえば、多くのソーシャルメディアが会員登録を求めており、決済を必要とするサイトでは支払い情報の登録を含んでいるが、ユー

ザ同士のコミュニケーションにおいては実名や支払い情報をはじめとする個人情報は秘匿され、匿名性は保たれる。

そこで、本稿では折田[6]によるアイデンティティ表出のレイヤ構造をもとに、名乗りの構造を整理する。ソーシャルメディアにおける名乗りは、(1)ユーザ同士のインタラクションが発生する「ユーザ間レイヤ」、(2)利用登録や履歴管理を行う「サービス提供者レイヤ」、 (3)支払い情報およびアクセス元情報を管理する「本人確認レイヤ」という 3 つのレイヤに大きく分けることができる（図 3)。これにより、ユーザ間では匿名性が保たれているが、サービス提供者にとってはユーザの行為がリンク可能であるなど、異なるレイヤによって異なる程度の匿名性を提供する可能性が見えてくる。

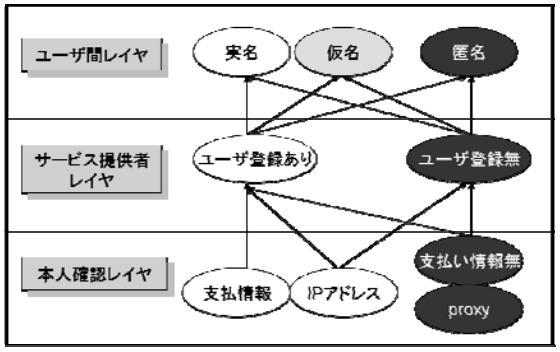

図 3　アイデンティティのレイヤ構造

3. なりすましの実例

本節では、ID やパスワード盗難以外の状況で発生するなりすましの事例を整理しつつ紹介する。

3.1 偽プロフィール

第一に、氏名、生年月日、住所、性別と言った基本四情報と言った本人確認情報を入手し、偽のプロフィールを作成した他人になりすますという方法である。著名人の場合、氏名や生年月日も公知となっていることからこ名前を騙られやすく、著名人を装った Twitter アカウントが迷惑メッセージの温床として悪用されるという事態も発生している [7]。

一般的な利用者にもこうしたリスクは存在する。世界的に利用されている SNS である Facebook では友人の名を騙り、同性愛者であるかのようにプロフィールを作成した男が名誉毀損で訴えられるという事件があった[8]。また児童や生徒が本人になりすまして「プロフ」を作成し、援助交際しているかのようにみせかけるといった悪質ないじめの報告もある[9]。

その背景には、ブログをはじめとするソーシャルメディアにおける個人的な情報の開示がある。ソーシャルメディアの利用において実名を秘匿する傾向は高いものの、その他の個人的な情報はむしろ詳細に開示されている。佐藤らによるブログにおける個人情報開示状況によれば、県／市レベルの住所は 70%のブログから読み取ることができ、生年月日に関しては学生層の 50%、一般層の 20%強から読み取ることができる[10]。また、インターネットという互いに顔を見ながらコミュニケートしない「視覚的匿名性」が提供される場所においては、むしろ自分自身について詳しく言及する自己開示が促進されるという見方もある[11]。

こうして得られた情報から、その人物になりすましたプロフィールを再構成することは難しくない。2.3 で述べたレイヤの観点からも、サービス提供者に会員登録をする際にも有料サービスなどで身元確認をしない限り、本人性の真偽を判定することはできない。ユーザ間レイヤにおいて、実名を互いに公開しないのであれば、なおさら実名を知らずともなりすますことは容易だ。こうした問題について、教えて!Goo や Yahoo!知恵袋などの Q&A サイトには、相談が寄せられている（表 1）

表 1　Q&A サイトに見るなりすまし相談の例

ブログのコメントでトラブルになった相手が、ブログ管理者と同じハンドル名で別のブログを立ててなりすまし、名誉を毀損するような内容の記事を掲載し続けて困っている
自分と同じハンドルを名乗り、なりすまして他者のブログのコメント欄を荒らしている人がいる
自分になりすまし、顔写真、住所や電話番号などをプロフに掲載された

3.2 無断転載

第二には、メールマガジンやブログの内容を無断でコピーし、オリジナルの記事をあたかも自分が作成したかのように装う方法である。あるキーワードで検索した結果、同じ文章や内容に出くわすことは少なくないが、こうした無断転載は著作物に対する盗用といった問題であると同時に、元の著者を騙った名声や評判を悪用するなりすましの問題でもある。第三者がアフィリエイト目的で、読者数の多いメールマガジンの内容をコピーし、本人のサイトらしきものを作成した例[12]がある。

3.3 掲示板におけるなりすまし

第三には、掲示板などのコミュニケーションにおいて、他人になりすますという方法である。プロフィールといった全人格的な乗っ取りではないが、なりすましが容易にできることから話題や文脈の混乱を招いたり、誹謗中傷を引き起こすと言った問題がある。会員登録やログイン、すなわちサービス提供者レイヤにおけるリンク可能性が確保されない掲示板においては、なりすましが発生しやすい。そもそも、「通りすがり」と名乗った複数の投稿があった場合、それらの投稿は同一人物と判別できずリンク不能な状態である。本節では、匿名掲示板として知られる２ちゃんねるを例に、なりすましおよびその対策のための仕組みについて説明する。

２ちゃんねるへの投稿は会員登録や記名を必須とせず、投稿者は自分で名乗らない限りは「名無しさん」と言った掲示板ごとに定められた共通の名前が付与される。そのため、どの投稿が同一人物のものによるかは判別できず、投稿者は自分の初出の投稿番号をハンドルの代わりに名乗るなどして識別性を確保していた。しかし、他者が同じ番号をあたかも本人であるように名乗り「偽物」を発生させる行為や、もしくは複数の人間がそれぞれ別人であるかのように振る舞う「自作自演」が発生したため、これを防止するために利用者を識別する工夫がなされるようになった。

識別のための第一の工夫は、アクセス元 IP アドレスと時刻を暗号化した ID の生成と付与である。2007 年現在、２ちゃんねるの約 8 割弱の掲示板において、24 時間以内の同一 IP アドレスからの投稿に ID が付与され、cookie で判別できる限りにおいて同一性を表示している[13]。第二の工夫は、ニックネームの後に 8byte 以内のパスワードから生成した暗号化文字列を表示させる「トリップ」と呼ばれる仕組みである。特に、相談事などで自分の発言の連続性や同一性を確保したいと考える利用者は、自分の仮名（最初の投稿番号やニックネームなど）に加えてトリップを表示させる。ID 機能では日付やアクセス元の IP アドレスの変化に対応できないが、トリップを併用することによって投稿している利用者の同一性、すなわちリンク可能性は高まる。

こうした仕組みの実装によって、「この投稿は自分によるものだ」という証明は比較的容易になったが、トリップに用いたパスワードが見破られ、なりすまされた際に「この投稿は自分では*ない*」と証明することは困難だ。２ちゃんねるには「トリ（トリップ）テスト」と呼ばれる、パスワードからトリップへの変換を試せる掲示板も存在しており、推測可能なトリップは悪意のあるユーザによって試みられる余地がある。実際、相談事を扱う掲示板において、相談者になりすまして投稿に割り込み、話を混乱させるという例が見られる。それでも自分と偽物を区別するために、アクセス元の IP アドレスを表示させるというローカルルールを持つ掲示板も存在するが、その IP アドレスを検索エンジンによって検索し、検索結果を第三者が再投稿するといった例も少なくない。この場合、２ちゃんねる外の行為とのリンク不能性が犠牲になる。

図 4　２ちゃんねるの固定ハンドルとトリップ

3.4 その他のなりすまし

その他、趣味や創作活動のコンテンツを載せたサイトに対し、自分がさもその著者であるかのように振る舞うという事例について、ネット上に相談が寄せられている。例えば、立ち話で友人達に「これは自分が作ったサイトだ」と、著名なサイトの作者を騙ってふれまわるというエピソードが見受けられた。

4. 考察

4.1 なりすまし構造

2 節で述べた「名乗りの構造」を元になりすまし問題の考察を試みる。

なりすましの加害者 F が被害者 T になりすます場合を想定する。F が T と名乗る状態を $F(t)$　と表す。F の観点からは T という名が実名であれど $F(t)$は F にとっての「仮名」であり、T が $T(t)$ と名乗る「実名」とは区別される。また、$F(t)$という名前から F の現実のアイデンティティに到達することはできないため、F にとって $F(t)$とは図 2 における第三象限に位置すると見なすことができる。

しかし、新規ブログを作成する際などの会員登録において、Ft が F に届くアドレスを設定するならば、メールアドレスにて認証されるはずの T は F に置き換えられ、ネット上では $F(t)$は $T(t)$としてなりすますことができ、第一象限の「実名」状態にあると見なすことができてしまう。

こうした事態を防ぐためには、本人確認によって $F(t) \neq T(t)$を示す必要がある。しか

し、本人確認のための情報をインターネット上の提供することは、なりすます側の F に対してさらなるなりすまし情報を与え、いたちごっこに陥る可能性がある。

ここで、2.3 節で述べたレイヤ構造を援用する。ユーザ間レイヤにおいて $F(t) \neq T(t)$ を示すためには、サービス提供者レイヤ以下のレイヤで本人確認が行われる必要がある。言い換えれば、ユーザ間レイヤにおいて実名をはじめとする本人確認情報の提示がなくとも、サービス提供者とユーザの間で本人であると確認されればよい。

多くのソーシャルメディアでは、同一の ID や仮名の登録を認めていないため、同一サイト内でのなりすましは比較的避けられると考えられる。だが、異なるサイトがが提供するブログまでその効力を及ぼすことはできない。OpenID のように、異なるサイトにおいて有効な本人認証の手段を導入することで、異なるサイトではユーザ間レイヤにおいてそれぞれ違う「名乗り」をしつつも、本人確認レイヤにて同一性を確保するという可能性は考えられる。

4.2 なりすまし対策に向けて

このような、不正アクセスではないが、他者になりすますという行為に対する対策を、二つの観点から考察する。

4.2.1 情報の開示による解決と非開示による解決

第一には実名開示および個人情報開示の有無である。実名をはじめとする自分の情報を積極的に開示することによって、なりすましを防ぐ方策だ。実名を開示することは、サイトのいわば「正本」を作ることであり、かつその本人性が本人確認レイヤによって保証されていれば正当性は高いと考えられる。米国初の実名制 SNS である LinkedIn は、本人性を保つために人脈およびクレジットカードの支払い情報を用い、転職やビジネス利用に耐える信頼性を確保している[14]。

全く逆のアプローチとして、実名をはじめとする一切の情報を公開しない、もしくは複数の仮名を用いて情報のリンク可能性を低くするという方策も考え得る。これは、なりすましをするための情報を提供せず、また提供したとしても同一人物のものとしてリンクさせないことによる防止策である。

ネット上では「バルサン」と称される偽物撃退の方法がある。これは、なりすましを受けたときに、なりすまされた本人しか知らないエピソードに関する質問を浴びせたり、あるいは偽物に対しておとりになる要求（○○をしろ、と言った命令）をして、偽物の矛盾点をついたり、偽物であることをはっきりさせるというものである。これは、情報の開示による問題解決の一手段と解釈することができるだろう。

4.2.2 事前および事後確認

第二には、事前または事後の本人確認と情報開示である。ソーシャルメディアの利用に際して、事前に支払い情報などによる本人確認を徹底することはなりすましの防止策になりうるが、サイトそのものの安全性と信頼性が前提となる上、サイト利用に対する障壁が高まる恐れがある。ただし、本人確認がなく、他人になりすましたアカウントが正当な手続きによって取得された場合の問題を考慮するならば、本人確認の徹底は一つの解決策になりうるであろう。

もう一つは、事後に本人と偽物を区別するための情報を開示させるという手段である。プロバイダー責任法の定めに従い、問題が発生した際に情報の開示請求を行うことが考えられるが、その際には開示請求に耐えうる理由と証拠が求められるだろう。

5. おわりに

自分になりすました他人が出現したとき、「本物」は自分であり、相手は「偽物」であると証明することは難しい。そもそも、現実に自分の身にそのようなことが起きた際には、何が起きているのか理解できない可能性は高い。本稿では、インターネット上のソーシャルメディアにおける「名乗り」の構造的な整理を前提に、なりすまし事例を探索的に考察した。なりすましに遭った際に、それがどのレイヤで発生しているのかを冷静に確認することは、適切な対策を取るための一助になると考える。

なりすまされないように実名を開示しない、という発想はある意味では正しいが、ある意味ではなりすましを防ぐための手段を放棄しているとも解釈できる。インターネット利用において、どのように名乗るかという選択の自由を確保しつつ、なりすまし問題の類型化と解決策を検証していくのが今後の課題である。

謝辞 本研究の一部は科研費若手 B(課題番号 19700241)および（課題番号 20338239）の助成を受けたものである。

参考文献

1) インターネット協会:インターネット白書 2008, インプレス,2008
2) Akiko ORITA”USERS’ ATTITUDES TOWARDS ANONYMITY IN USER GENERATED CONTENT: BASED ON STRUCTURE OF ANONYMITY”Proceedings of IADIS e-Society2009 pp163-170, 2009
3) 谷口展郎、千田浩司、塩野入理、金井敦「分散アイデンティティエスクローにおける匿名性／仮名性／本人性の管理に関する考察」電子情報通信学会技術報告 技術と社会・倫理研究会

(SITE) 2005-53 pp.7-12,2006
4) Kobsa, Alfred ”Privacy Through Pseudonymity in User-Adaptive Systems” ACM Transactions on Internet Technology, Vol.3 No.2 May2003 pp149-183, 2003
5) Pfitzmann, A. & Hansen, M Anonymity, Unlinkability, Undetectability, Unobservability,Pseudonymity, and Identity Management −A Consolidated Proposal for Terminology(ver.0.31 Feb. 15, 2008) 2008
http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf
6) 折田明子「Web 上の人物および行為の信頼性評価」人工知能学会誌 Vol. 24, No. 4（印刷中）,2009
7) Mrinal Desai「Twitter は MySpace になるのだろうか」TechCrunch Japan 2009 年 4 月 2 日,2009
8) “Man sues for Facebook defamation” 9NEWS Jul 1 2008
http://news.ninemsn.com.au/article.aspx?id=589603
9) 石田哲也「 想像を超えた"ネットいじめ"の世界に絶句… - 学校裏サイト対策講座が実施」マイコミジャーナル 2008 年 4 月 30 日,2008
http://journal.mycom.co.jp/articles/2008/04/30/netbullying/
10) 佐藤和紀, 安井良介, 針谷友彰,金井敦,廣田啓一,谷本茂明 “ブログにおける個人情報漏えいの状況調査” 情報処理学会研究報告 2009-EIP-43 pp1-8,2009
11) ウォレス,パトリシア（川浦康至、貝塚泉訳）「インターネットの心理学」NTT 出版(1999)
12) 「メルマガを全部コピペして使われてしまいました（悲）」2009.3.24 「竹内義晴の、しごとのみらい」ITmedia オルタナティブブログ,2009
http://blogs.itmedia.co.jp/takewave/2009/03/post-37fb.html
13) 折田明子”匿名性レベルの設計に向けて”智場 111 号 pp65-73 国際大学 GLOCOM, 2008
14) 折田明子「日本で実名制は受け入れられるか・ビジネス SNS の LinkedIn(3)」日経 NET IT-PLUS 2008.06.26