論　文

SNSにおける新しい信頼モデルと図書館における応用

井上　創造*，堀　　優子**

〈抄　録〉

SNS（Social Networking Service）は、利用者間の社会的なつながりを重視したコミュニケーションシステムである。SNSは、図書館のような利用者を相手とするサービスにとって非常に有用である。ところが最近のSNSにおいては、迷惑なメッセージが徐々に増えていることが問題になりつつある。これは、利用者の登録時の認証を、既存利用者からの招待と、有効なメールアドレスを登録するというたった２点にのみ頼っている事が原因であると考えられる。本論文では、SNSを形式的にモデル化し、利用者間の情報アクセスのための基準を表す信頼という概念を導入する。さらにその記述を用いて、「所属による信頼」、「匿名での発言」という新たな信頼の概念を導入する。また特に前者について、所属を確実に認証するための方式を４章で述べ、その実装を示す。

A Trust Model of Social Networking Services and Their Applications for Libraries

INOUE Sozo*, HORI Yuko**

1. はじめに

近年、Webサービスの分野で、SNS（Social Networking Service）というサービスが注目されている。SNSは、友人や、コミュニティという名のグループといった、利用者間の社会的なつながりを重視したコミュニケーションシステムである。現実社会のつながりを重視することにより、いたずらや誹謗中傷、宣伝やスパムといった迷惑なメッセージが少なく安定したコミュニケーションを目指す物である。

一方、このような社会的な側面を重視したシステムは、図書館のような利用者を相手とするサービスにとって非常に有用である。なぜなら、

- サービス提供の際の利用者認証のために、所属を表すコミュニティの情報などを利用できる
- おすすめの本の紹介といった、サービス提供の際の、コンテンツの選択のために、趣味のコミュニティや友達関係などの情報を利用できる

からである。今後、SNSが図書館で利用される事により、利用者に対して綿密かつ柔軟なサービスを提供できるようになるであろう。

ところが最近の一般のSNSにおいては、迷惑なメッセージが徐々に増えていることが問題になりつつある。これは、利用者の登録時の認証を、既存利用者からの招待と、有効なメールアドレスを登録するというたった2点にのみ頼っている事が原因であると考えられる。これだけだと、一旦迷惑メッセージの発信者が加入すると、彼らが彼らなりの社会的ネットワークをSNS上に構成してしまうことが可能であり脆弱である。

本論文では、まず２章で一般的なSNSを形式的にモデル化し、３章でその上での利用者間の情報アクセスのための基準を表す信頼という概念を形式的に記述する方法を導入する。さらにその記述を用いて、

- 所属による信頼
- 匿名での発言

という新たな信頼の概念を導入する。また特に前者について、所属を確実に認証するための方式を４章で述べ、その実装を示す。５章はまとめである。

* いのうえ　そうぞう　九州大学附属図書館研究開発室准教授　E-mail:sozo@lib.kyushu-u.ac.jp
**ほり　ゆうこ　九州大学附属図書館図書館企画課企画係　E-mail:yukos@lib.kyushu-u.ac.jp

SNSにおける信頼モデルを形式的に定義した物は著者の知る限りない。本論文ではこれを定義することにより、SNSにおける様々な信頼を表現できるようにする。

また、実装したシステムは、所属を確実に認証することで、迷惑なメッセージが減るだけではなく、利用者の社会的な立場を把握した上でのコミュニケーションが可能になるという点で類を見ない物である。

大学に関連するSNSは、その多くが学生有志、または同窓会を運営母体としており、ここで論じる「実名制」を取り入れているSNSもいくつか見受けられる。例えば、東大OB.NET [1] は、その名のとおり東京大学のOBのためのSNSであるが、学士会が東大卒業生のデータと照らし合わせて認証を行い、完全実名制を維持することで信頼性とセキュリティを高めている。

また、文部科学省が募集している19年度「新たな社会的ニーズに対応した学生支援プログラム（学生支援GP)」には、SNSをキーワードとした応募が４件あり [2]、大学が、現実の人間関係を基盤としてSNSを活用していこうという動きが活発化していることが伺える。今後、大学を主体としたSNSが様々な形で登場してくることが予想される。

２．SNS

本章では、SNSの一般的であると考えられる形態を集合論を用いてモデル化する。図１と図２はその概念図である。

２.１　利用者のネットワーク

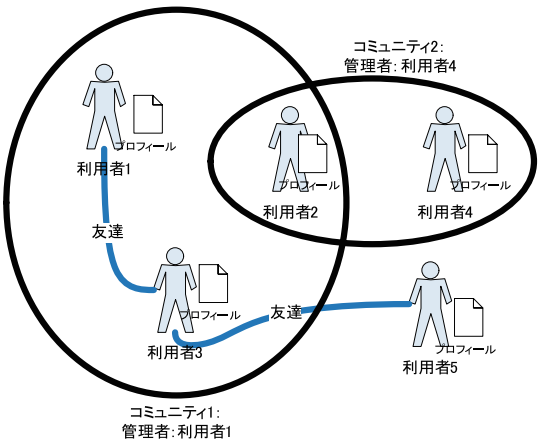

図１　利用者のネットワークの例

SNSにおいては、システムはそれぞれの利用者に対するシステム上の人格であるアカウントを持つ。利用者は、自信の個人情報や紹介文といったプロフィールを持つ。

定義 １ （利用者とプロフィール）

*Uは、利用者のアカウントの集合である。以降特に区別する必要がない場合には、利用者のアカウントのことを**利用者**と呼ぶ。また任意の利用者$\forall u \in U$ は、利用者の情報を表す文字列である**プロフィール**profile(u)を持ち、Pを$\forall u \in U$ についてのprofile(u)の集合とする。逆にプロフィールpについて、from(p)=profile^{-1}(p)とする。*

*from(p)*は、プロフィールの当事者のことである。

SNSにおいては、現実の世界における面識などに対応して、利用者間での合意に基づいて友達という関係を結ぶことができる。

定義 ２ （友達）

*友達関係Fは、$u \neq v$であるような利用者$\forall u$、$\forall v \in U$ について (u,v) の集合である。このとき、uとvは**友達**と呼ぶ。*

友達は、互いの利用者の合意によってシステムに登録することができる。

また同じ興味や所属を持つ利用者が集まって、コミュニティという集まりを作ることができる。コミュニティには管理者と呼ばれる利用者がいて、コミュニティに対する各種の運用を行う。

定義 ３ （コミュニティ）

***コミュニティ集合**Cは、**コミュニティ**c=(admn(c), Member(c))の集合である。ただし**コミュニティ管理者**admn(c)∈Member(c)，Member(c)⊆Uとする。*

コミュニティの登録や削除は、コミュニティ管理者が行うことができる。またコミュニティへの利用者の参加は、コミュニティ管理者が行う設定により、自由に参加できたり、コミュニティ管理者の同意が必要だったりする。

2.2 発言

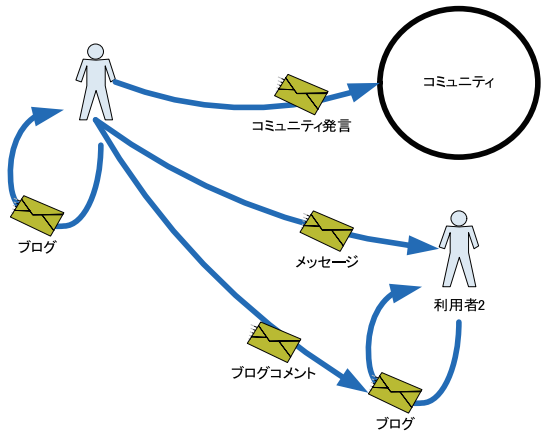

図2　利用者の発言の種類

SNSにおいては、利用者は様々な種類の発言をすることができる。それは、自信の日記に相当するブログ、ブログに対するコメント、利用者間でのメッセージ、コミュニティ内での発言といった物である。以下ではこれらを一括して定義する。

定義 4 （ブログ・コメント・メッセージ）

Mは、発言

m=(date(m), from(m), to(m), vontent(m))

の集合である。ただしdate(m)を日付時刻、from(m)∈U, to(m)∈U∪C∪Mとし、content(m)は文字列を初めとする任意のオブジェクトとする。

また、発言mは、to(m)の種類によって以下のように呼ばれる。

- *ブログ：to(m)=from(m)の時。*
- *メッセージ：to(m)∈Uかつ、to(m)≠from(m)の時。*
- *ブログコメント：to(m)∈Mかつ、to(m)がブログまたはブログコメントの時。このとき、mの**ルート発言者** root(m)=to(to(…to(m)…))と定義する。*
- *コミュニティ発言：以下のいずれかの時。*
  - *to(m)∈Cの時、または、*
  - *to(m)∈Mかつ to(m)がコミュニティ発言の時。*

このとき、mのルートコミュニティroot(m)=to(to(…to(m)…))=c∈Cと定義する。

上記において、ルート発言者は、コメントの元となったブログ、ルートコミュニティは、発言の元となったコミュニティ発言を意味する。

また、発言*m*の生成、削除は、利用者*from(m)*が行うことができる。

2.3 利用者の招待

SNSにおいては、まだアカウントを作っていない利用者をすでに作った利用者が招待するという機能がある。この機能を使い利用者*u*が利用者*v*を招待し、その結果*v*がアカウントを作ると、*(u,v)*が*F*に*追加される。*

3. SNSにおける信頼モデル

本章では、SNSにおける信頼モデルを、閲覧許可と信頼条件という概念を導入する事によりモデル化する。この信頼モデルは、既存のSNSの情報アクセス制御を表現することができるが、本章では新たに、

- 所属による信頼
- 匿名での発言

という新たな信頼を、定義した信頼モデルにより導入する。

3.1 閲覧許可

発言をどの利用者が閲覧して良いかは、発言の種類に応じてシステムや利用者が設定する。

そのためにここでは閲覧許可の記述を導入する。閲覧許可は、対象である発言またはプロフィールを閲覧することのできる主体を記述することで表現する。主体の記述としては、利用者、コミュニティのメンバー、友達の友達といった数段先の友達といった場合が考えられる。これらを、以下のように定義する。

定義 5 （閲覧許可）

閲覧許可集合Rは、閲覧許可r=(subject, trget)の集合である。ただし、subject∈U∪C∪{'ALL', 1,2,…}とし、 trget∈M∪Pとする

閲覧許可の意味

上記で定義した閲覧許可のシステムにおける意味は以下の通りである。

閲覧許可*r=(subject, trget)*に対して、利用者は*trget*を以下のように閲覧できる：

- *subject*∈*U*の時：利用者*subject*が見ることができる。
- *subject*∈*C*の時：*subject*に属する利用者∀*u* ∈*Menber(subject)*が見ることができる。
- *subject*∈{1,2,…}の時：利用者*u, v, w*∈*U*について、*u*と*v*が友達であるときに*u*と*v*を１ホップ、さらに*u*と*w*が友達であるときに*u*と*w*を2ホップの友達と呼び、以下同様に呼ぶとすると、利用者*from(trget)*の*subject*ホップ以内の友達が見ることができる。
- *subject='ALL'*の時：すべての利用者が見ることができる。

システムにおける既定の設定

メッセージは、その発言者と受信者しか読むことができない。つまり、メッセージである発言

∀*m=(date, from, to, content)*∈*M*

について、*(subject, m)*∈*R*となる*subject*は、*from*と*to*のみであるという制限が、システムによって与えられる。

閲覧許可の変更権限

閲覧許可は、発言の種類に応じて以下の者が追加・削除することができる：

任意の∀*trget*∈*M*∪*P*および∀*subject*∈*U*∪*C*∪{*'ALL', 1,2,…*}について、*(subject, trget)*の*R*への追加と削除は、

- *trget*がプロフィール*profile(u)*の場合は、本人*u*が行うことができる。
- *trget*がメッセージあるいはブログの場合は、発言者*from(trget)*のみが行うことができる。
- *trget*がブログコメントである場合は、ルート発言者*root(trget)*のみが行うことができる。
- *trget*がコミュニティ発言である場合は、ルートコミュニティの管理者 *admn(root (trget))*のみが行うことができる。

3.2 信頼

日常において、「あなたは信頼のおける人だから情報を教えよう」と言うように、信頼とは、ある人が他の人に何らかの行為をする際に基準となるものであると考えられる。これをSNSにおける閲覧という行為に限定すれば、信頼は、閲覧許可の集合と等価変換することができると言える。この考えを元に、信頼を以下のようにモデル化する。まず個々の閲覧許可に対応した信頼の記述である信頼条件を導入する。これを信頼の主体と対象についてあつめることで信頼をモデル化する。

定義 6（信頼）

信頼条件集合Tは、信頼条件t=(v,Trget(u), condition(v, u, g))の集合である。ここでvは利用者を値に持つ変数、Trget(u)はM∪Pの部分集合を値に持つ利用者uの式であり。condition(v, u, g)は真または偽の値を持つvとuとgの論理式である。ただしgはM∪Pを変域に持つ変数である。また利用者uの利用者vに対する信頼Trust(u,v)を、信頼条件

∀*(v, Trget(u), condition(v, u, g))*∈*T*

の集合とする。

さらに、信頼条件を閲覧許可に反映させるために、以下の制約を付加する。

閲覧許可と信頼条件の対応

任意の∀***u***, v*∈ *U, 任意の*∀*g*∈*Trget(u)、および任意の信頼条件*∀*(v, Trget(u), condition(v, u, g))*∈*Tについて、条件式condition(v, u, g)が真ならばそのときに限り、 以下のいずれかでなければならない：*

1. *任意の*∀*trget*∈*Trget(u)について (v, trget)*∈*R、または*
2. *任意の*∀*trget*∈*Trget(u)とv*∈*Member(c)であるようなあるcについて (c, trget)*∈*R、または*
3. *任意の*∀*trget*∈*Trget(u)とhop(u, v)以上のある自然数nについて (n, trget)*∈*R、または*
4. *任意の*∀*trget*∈*Trget(u)について ('ALL', trget)*∈*R。*

ただし、利用者u、vの間の最小のホップ数をhop(u,v)と書く。

関数*trust*の与え方はいろいろ考えられるが、例えばよく用いられるような、友達の友達までブログへの閲覧許可を与える場合は、

(v, Blo(u), hop(u,v)≤*2)*∈*T*

とすればよい。ただし*Blo(u)*は利用者*u*が書いた

ブログの集合とする。

また、前節で述べたメッセージを発言者か受信者しか読むことができないという信頼条件は、

$$(v, Message(u), (v=from(g))\vee(v=to(g)))\in T$$

と書くことができる。ただし$Message(u)$は利用者uが書いたメッセージの集合とする。

3.3 所属による信頼

SNSを図書館の利用者のような特定の組織に適用する場合には、上記のような友達の友達といった関係以外にも、利用者の所属による信頼が存在すると考えられる。例えば、「この人は九州大学の人間だから互いに実名を明かして良い」といった具合である。近年、巷のSNSでは利用者が実名を避けるようになり、知人を実名で検索することが難しくなってきているが、所属による信頼は、この問題への打開策にもなりうる。

ここでは、組織をコミュニティで表すことで所属による信頼を表現する。例えば、コミュニティcに入っている人にだけプロフィールを見せるという信頼条件は、以下のように表すことができる。

$$(v, \{profile(u)\}, v\in Member(c))\in T$$

ただしこの場合、コミュニティに加入する際の認証をどう行うかが問題となることに注意が必要である。４章において、我々が実現した利用者認証の方法を述べる。

3.4 匿名での発言

前節で導入した所属による信頼により、SNSにおける利用者間の信頼が既存の方法より柔軟かつ現実に近い形で管理できると考えられる。しかし一方で、例えば「自分が経験した病気の療法を他人と議論したい。しかし身近な人には自分の病歴を知られたくない」といった場合には、これまでに述べた友達による信頼や所属による信頼がそぐわないことがある。このような場合も、例えばプロフィールを公開していない相手にのみ発言を読ませるような信頼条件を以下のように定義できる。

$$(v, Comment(u), (v, profile(u))\notin R)\in T$$

ただしこれは、いわゆる匿名の発言を許すことになる。このような信頼条件を制限なく利用者に与えると、一般の掲示板のような濫用につながる可能性があるため、例えばシステム管理者には特別な権限を与えるといった配慮が必要であろう。

ここまで、SNSにおける信頼モデルを導入し、そのモデルの上でいくつかの新しい信頼の概念を定義した。提案したモデルをすべて実装するには、信頼や閲覧許可の評価や、更新をさらに定義する必要がある。

4．システム実装

我々は、既存のSNSであるVarry[3]に対して、３.３節で述べた所属による信頼を実装した[4]。本章では、この実装方法を述べる。

4.1 所属の認証

本実装では、

１．九州大学附属図書館の利用者にのみ実名を公開する

２．すべての利用者に対して、九州大学のメンバー（図書館の利用者）であることを公開する

という閲覧許可を採用した。

これらはそれぞれ、以下の信頼条件で表すことができる：

$$(v, \{name(u)\}, v\in Member(c))\in T$$

$$(v, \{name(c)\}, TRUE)\in T$$

ただし、$name(u)$を利用者uの実名、cを九州大学に対応するコミュニティとし、$name(c)$をcの名前とする。

これらにより、

- 九州大学のメンバー同士では実名を明かすことにより、現実の利用者の特定ができ、日常生活に近いコミュニケーションを行う事ができる
- 九州大学以外の人間は、利用者の実名を知ることができなくとも、九州大学のメンバーかどうかを判別できるため、九州大学の社会的信頼に即した信頼を九州大学のメンバーに対して持つことができる
- このことは九州大学のメンバーにとっても、九州大学の社会的信頼を九州大学以外の人間に対して利用することができる

というメリットがある。

4.2　システムの構成

本システムにおいては、Varry、つまり既存システムへの改造の他に、九州大学附属図書館の利用者であることを認証する**九大所属認証システム**を構築した。

九大所属認証システムは、九州大学附属図書館の全利用者についての

- 利用者番号と
- 氏名

の集合をデータベースとして持つ。ただしこれらは、暗号学上逆変換が難しい、ハッシュ化された値として保存される。このため、九大所属認証システムのデータが万が一漏洩しても、利用者番号と名前がデータベースから漏洩することはない。

4.3　システムの動作

既存システムと九大所属認証システムは、扱う利用者が既存システムのアカウントをすでに持っているかどうかによって、連携して異なる動作をする。

既存システムのアカウントを持たない場合

1．利用者は九大所属認証システムにアクセスし、
   - 自分の図書館利用者番号
   - 氏名
   - メールアドレス

   を入力する。
2．九大所属認証システムは、
   - 入力された利用者番号のハッシュ値
   - 入力された氏名のハッシュ値

   の組がデータベースに存在するかを判定する。
3．存在しなければ、そのような図書館利用者が存在しない旨を表示して終了する。
4．存在すれば、既存システムに
   - 氏名
   - メールアドレス

   を通知する。
5．既存システムは上記を受け取ると、上記メールアドレスが既存のアカウントの物ではない事を確認した上で、このメールアドレスに対し招待状を送ることでその利用者を招待する。
6．その利用者が招待状に応じてSNSのアカウントを生成すると、既存システムはそのアカウントの氏名を４の物に設定し、九州大学のコミュニティに自動的に加入させる。

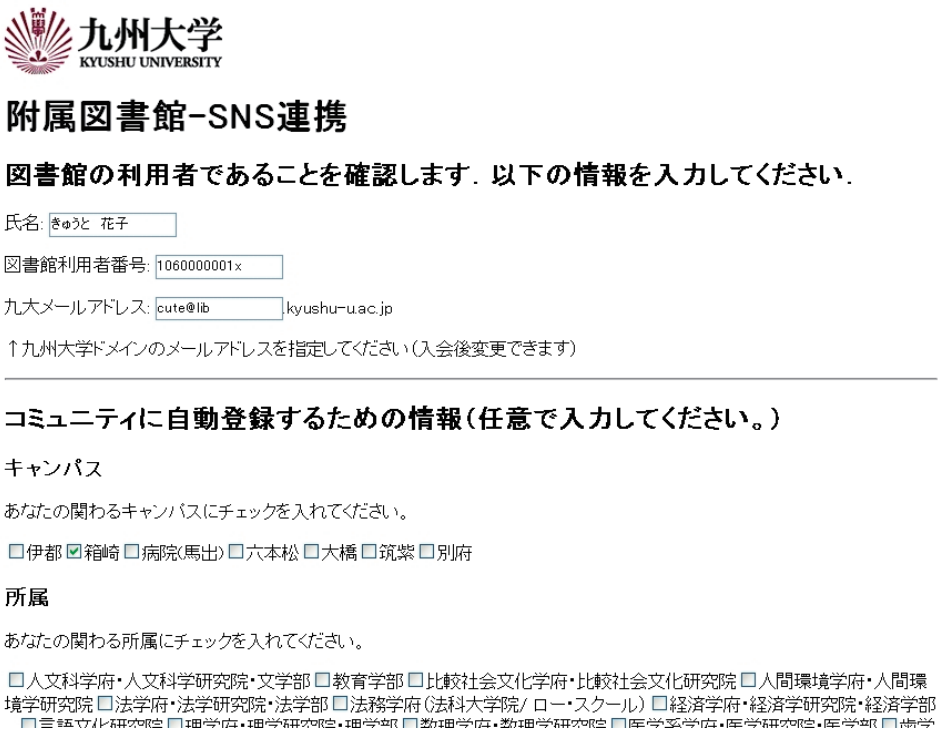

図３　九大所属認証システムの入力画面

図４　九大メンバーのプロフィール表示

７．なお、実は１の時点で利用者に、所属学部や興味のある学問分野などの任意選択項目を入力させており、それらに応じたコミュニティに自動的に加入させる。

既存システムのアカウントを持つ場合

この場合は、既存システムは前述の５を省略し、６において利用者がアカウントを生成せずともコミュニティへの自動加入を行う。

上記の２において、九大所属認証システムは、利用者番号と氏名の組しかチェックしていないため、例えば図書館利用者証を拾った人が不正に登録をできてしまうといった問題は残る。利用者番号は秘密にするよう周知されているため、問題は少ないと考えられる。

図３は、九大所属認証システムの入力画面である。

また、図４は、既存システムにおいて九州大学のメンバーがプロフィールを表示させた画面である。図４において表示される氏名は、九州大学附属図書館の利用者証に記載された物と同一である。九州大学の場合は、これは学生証と一致するので、氏名を偽ることは難しくなる。またこの氏名は、九州大学のメンバーにしか表示されない。これにより、４.１節の１番目の閲覧許可が実現できる。

一方図４の左側に表示される九州大学のロゴは、九州大学以外も含む全利用者に表示される。これにより、４.１節の２番目の閲覧許可が実現できる。

本実装では、九州大学という単一の所属についての認証を実現したが、複数の所属についても、それぞれの所属に応じた所属認証システムを用意し、それぞれの所属においてそのシステムを管理することで、比較的容易に実現できることがこの方法の利点である。

５．おわりに

本論文では、SNSにおける信頼モデルを導入し、そのモデルの上でいくつかの新しい信頼の概念を定義した。中でも所属による信頼について、それを扱うシステムの実装例を述べた。 提案したモデルをすべて実装するには、信頼や閲覧許可の評価や、更新をさらに定義する必要がある。

図書館におけるSNSの応用範囲は広い。例えば、

- 個人化された蔵書検索Webサービス MyLibraryにおいて、SNSの友達関係を利

用した協調フィルタリングを適用する。

- コンピュータ上で提供される書架である仮想書庫において、プロフィールや所属コミュニティを元にして利用者に適した自動配架を行う。
- 教室や会議室の予約や共有を利用者通しで自立的に行う、友達やコミュニティの情報を用いる。
- コミュニティにおいて、ゼミや共同執筆といった共同作業における資料の共有やバージョン管理を支援する。この際に電子資料へのアクセス許可を、コミュニティや友人関係を元に行えば、いちいち許可対象者の認証情報を管理する必要がない。

というように、諸々考えられる。

本システムの試験運用においては、現在150名ほどの九州大学のメンバーが存在する。本利用者や学外の利用者の交流の変遷を追いながら、今後本提案の是非を評価することが今後の課題である。

謝辞

本論文のシステム設計および実装にご協力いただいた、Varryを運営する案浦スミタカさん、NTT西日本の皆様、および九州大学e-worldプロジェクトの皆様に感謝いたします。

参考文献

［1］ 東大OB.NET，http://todai-ob.net/.

［2］文部科学省HP〉新たな社会的ニーズに対応した学生支援プログラム（学生支援GP）〉申請状況　http://www.mext.go.jp/a_menu/koutou/kaikaku/gakusei/07070619.htm

［3］Varry（ベイリー），http://varry.net/.

［4］http://sns.lib.kyushu-u.ac.jp/.