

F-036

OWLによる個人・組織情報のモデル化とプライバシーの取扱い

A Privacy-based Personal and Group Information Modeling in OWL

佐藤 加奈[†]

Kana Sato

佐藤 晋也[†]

Shinya Sato

加藤 靖[†]

Yasushi Kato

高橋 薫[†]

Kaoru Takahashi

1. はじめに

インターネットの利用が爆発的に普及し、様々な機関でデータの収集・蓄積が進んでいる。こうした情報が無制限に利用できると、個人のプライバシーに関わる内容までが第三者に容易に把握されてしまう危険が高まってきた。

本稿では、プライバシーの対象となる情報をOWL[1]とRDFを用いたオントロジーで表現する。これにより情報範囲を定め、アクセスを制御する方法について検討する。

個人の情報、グループの情報およびそれらに関連した情報をプライバシーの対象とし、個人やグループと情報との関係等をオントロジーで明確に記述する。個人情報のモデル化には文献[2]を基にし、更に、グループに関する情報のモデル化を行う。個人情報やグループ情報をモデル化することでプライバシーの対象となる情報の範囲を定める。更に、オントロジーとして表現された情報へのアクセスをどのように制御するかの方法を併せて提案する。

2. 個人・グループ情報のモデル化

2.1. 個人情報

2.1.1. 個人情報定義

FOAF[3]の語彙を用い、個人をfoaf:Personクラスのインスタンスとして定義し、個人情報をfoaf:Personのインスタンスを含むオントロジー中のトリプル(文)とする。個人情報の記述には2つの種類がある:

- (1) 一人の個人が記述される原始的な個人情報。例えば、「太郎 likes an apple.」が個人情報となる。
- (2) 複数人(二人)の個人が記述されている複合的な個人情報。この場合、以下の2つの基準の選択を可能とする: α 基準は両者の情報をそのまま同時に表現する。 β 基準は別々の個人情報として表現する。例えば、「太郎 spoke with 次郎」は複合的な情報であり、 β 基準では、「太郎 spoke with J」, 「T spoke with 次郎」という2つの原始的な情報(太郎と次郎、それぞれの個人情報)に分解する。 α 基準は個人情報に他の個人情報も含めるという考え方であり、 β 基準は厳格に各個人情報を分離するという考え方である。

2.1.2. 個人情報閉包

これまでの個人情報は、インスタンスとプロパティが関連付けられる距離1の範囲内の情報、つまり一つのトリプルに関してのみしか記述しなかった。しかし、人を取り巻く情報は、他にも多数存在する。個人に関係するすべての情報を個人情報の範囲とし、このような個人情報の範囲を個人情報閉包とする。個人情報の範囲を広げるものとして、例えばowl:TransitivePropertyなど、OWLやRDFの基本概念を用いる。

2.2. グループ情報

2.2.1. グループ情報定義

情報は個人情報だけではなく、会社などの組織・グループに関する情報がある。そのため、グループに関する情報もプライバシーの保護対象とする。グループをfoaf:Groupクラスのインスタンスとして定義し、グループ情報をfoaf:Groupのインスタンスを含むオントロジー中のトリプルとする。グループ情報の記述には3つの種類がある:

- (1) 一つのグループが記述されている原始的なグループ情報。例えば、「X社 phone 0120-*****」がグループ情報となる。
- (2) 二つのグループが記述されている複合的なグループ情報。個人情報と比べグループ情報はプライバシーレベルが低くなると考える。そのため、二つのグループが記述されているグループ情報は分解せず記述する。例えば、「X社 pp:gMember Y部」がそうである。
- (3) グループと個人が記述されている複合的なグループ情報。これは情報の内容や閲覧する人に応じて情報の扱いが異なる。そのため、グループと個人を同時に表現する γ 基準と、複合的な情報を分解し表現する δ 基準の2つに分けて考える。例えば、「太郎 経営 X社」は γ 基準に基づく情報である。また、 δ 基準では、「T 経営 X社」, 「太郎 経営 X」という2つの情報(X社と太郎、それぞれのグループ情報)に分解し記述する。

[†] 仙台電波工業高等専門学校
Sendai National College of Technology

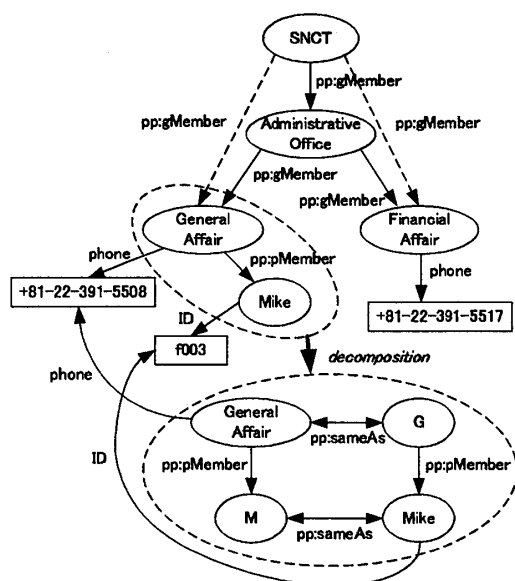


図 1: グループ情報閉包 (学校の事務部門の情報例)

2.2.2. グループ情報閉包

グループ情報に関係する情報は、個人情報閉包のような OWL の基本概念を用いて派生するグループ情報や、グループの中のグループ情報が考えられる。これらグループ情報の範囲を段階的に定めることで、閲覧する人に応じて、公開できる情報の範囲を制限するのに有効に利用できる。このようなグループ情報の範囲をグループ情報閉包とする。

以下では、学校組織の例を通して、グループ情報閉包を説明する。学校 SNCT があり、この学校の事務部門の情報が図 1 の実線部分のように与えられていたとする。

SNCT のグループ情報は、“SNCT pp:gMember AdministrativeOffice” となる。

派生情報から成るグループ情報閉包を $G1$ とし、これは、OWL のプロパティ定義を用い拡張された情報から成る。この例では、「pp:gMember」は owl:Transitive Property である。これより、“SNCT pp:gMember GeneralAffair” と “SNCT pp:gMember FinancialAffair” が $G1$ に含まれる。

また、グループの中のグループ情報を含むグループ情報閉包を $G2$ とする。 $G2$ では、グループのメンバーであるグループの情報や、所属している個人の情報をグループ情報閉包とする。そのため、この例では、 $G2$ は上の $G1$ に加え、“AdministrativeOffice pp:gMember GeneralAffair”、“AdministrativeOffice pp:gMember FinancialAffair”、“GeneralAffair phone +81-22-391-5508”、“FinancialAffair phone +81-22-391-5517”、“GeneralAffair pp:pMember Mike” (γ 基準のとき)、“GeneralAffair pp:pMember M” (δ 基準のとき)、“GeneralAffair pp:sameAs G” (δ 基準のとき) となる。

3. プライバシーを考慮した情報アクセス

前節で、プライバシーの対象となる個人情報とグループ情報のモデル化を行った。モデル化を行うことで、プライバシーの対象である情報の範囲を定義した。範囲には、個人情報や個人情報閉包、グループ情報やグループ情報閉包がある。情報の範囲を定めたことで、誰が情報にアクセスするかによって公開する情報を制御することができる。

情報の範囲を定めたオントロジーに対して、オントロジー閲覧者の役割 (ロール) や権限に応じたアクセス制御を行う。この制御の基本的な考え方は、前節で定義したモデルを RBAC (Role Based Access Control) [4] と組み合わせて用いることである。

プライバシーを考慮した図 1 のような学校オントロジーがあると、アクセス制御の例を述べる。この学校オントロジーは学校に関するグループ情報、グループに関連する情報、グループに所属している人の情報が記述されており、それにアクセスするユーザに対してロールを割り当てる。例えば、ロールとして、学長や情報管理者、学生などがある。そして、ロールとパーミッションの関係を決める。パーミッションはオントロジーの定義した情報範囲へのアクセス承認である。例えば、情報管理者や学長にはすべての情報に対してパーミッションを割り当てる。また、学生には自身の個人情報とグループ情報閉包 $G1$ へのパーミッションを与える。更に、 α , β , γ , δ 基準をパーミッションに与えることもできる。例えば、情報管理者は α 基準と γ 基準で表現されたすべての情報に対してアクセスすることができる。また、学生は自身の個人情報と β 基準と δ 基準で表現されたグループ情報閉包 $G1$ にアクセスすることができる。

4. おわりに

本稿では、個人情報とグループ情報のモデル化、特に閉包を定義したことで、プライバシーの対象となる情報の範囲を定め、これを RBAC と組み合わせることによって、プライバシーを考慮したオントロジーアクセスの方法を提示した。

今後の課題として、具体的なアクセス制御環境を構築し、その有効性を評価することがあげられる。

参考文献

- [1] W3C, OWL Web ontology language reference, <http://www.w3.org/TR/owl-ref>.
- [2] S. S. Al-Fedaghi and M. Y. Ahmad, Personal information modeling in Semantic Web, *ASWC (Asian Semantic Web Conference) 2006, LNCS 4185*, pp.668-681, 2006.
- [3] The Friend of a Friend (FOAF) project, <http://www.foaf-project.org/>.
- [4] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, Role-based access control models, *IEEE Computer*, 29(2), pp.38-47, 1996.