B-016

ロールオントロジーに基づいた個人・組織情報への動的なアクセス制御

A Dynamic Access Control for Personal and Group Information based on Role-Ontology

佐藤 晋也† 伊藤 仁† 和泉 諭‡ 小林 秀幸† 高橋 薫†
Shinya Sato Jin Itoh Satoru Izumi Hideyuki Kobayashi Kaoru Takahashi

1. はじめに

筆者らは，個人の情報，組織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，個人や組織と情報との関係をモデル化し，オントロジーで明確に表現する方法を提案してきた[1]．また，これらのオントロジーとして表現された個人・組織情報に対して，RBAC（Role Based Access Control）モデル[2]に基づいたアクセス制御についても検討してきた．しかし，ロールやパーミッション情報にオントロジーの特徴を活用できないことなどが改善として挙げられる．

そこで，本稿ではオントロジーを個人・組織情報の対象として，RBACにおけるユーザのロールやパーミッションを表現したロールオントロジーを提案する．このオントロジーの表現により，ロールとパーミッション情報を体系的に表現できることや，個人・組織情報との関係付けも容易に行えるという利点が生まれる．

さらに，情報への動的なアクセス制御をロールオントロジーに基づいて行う手法についても併せて述べる．これは，ある情報へアクセスする際に，権限を超えてそれらの情報にアクセスするといった際に生じる，アクセス権の変更に対して柔軟に対処するためのロールの委任，許可，禁止を動的に行うものである．

2. 個人・組織情報の表現 [1]

個人や組織の情報，そしてそれらに関する情報をプライバシーの対象とし，これらの情報をRDFとOWLを用いオントロジーで表現する．

個人をfoaf:Personクラスのインスタンスとして定義し，これを含むオントロジー中のトリプル(文)を個人情報とする．同様に，組織をfoaf:Groupクラスのインスタンスとして定義し，これを含むトリプルを組織情報とする．

これら個人・組織情報は距離１の範囲内の情報のみの記述である．しかし，人や組織を取り巻く情報は，他にも存在する．個人に係る情報を個人情報閉包とし，OWLやRDFの基本概念を用いて表現する．また，組織情報も同様にOWLの基本概念を用いて派生する情報や，組織の中の情報など情報範囲を組織情報閉包とする．図１に組織情報閉包の例を示す．OWLのプロパティ定義を用い拡張された情報を組織情報閉包G1，組織の中の組織情報を含む組織情報閉包をG2とする．また，電話番号などの所属している個人の情報を含む組織情報を組織情報閉包G3とする．

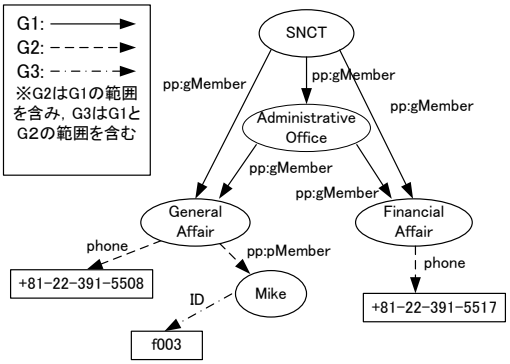

図 1 組織情報閉包の例

一方，情報の内容や閲覧する人に応じて情報の扱いは異なる．複数人の個人が記述されている複合的な個人情報は，両者の情報をそのまま同時に表現するα基準と，別々の個人情報として表現するβ基準がある．また，組織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基準がある．

3. ロールオントロジー

RBAC におけるユーザのロールやパーミッションを OWL と RDF を用いてロールオントロジーとして表現する．

ロールオントロジーを用いた例として，図２に学校情報を表現したオントロジーの一部を示す．このオントロジーにおいて，ロールとパーミッションはクラスとして記述される．また，これらのクラスに個人・組織を分けたロール及びパーミッションを，サブクラスとして記述する．これらクラスのインスタンスとして，ユーザのロール及びパーミッションが記述される．また，ロール階層を表現するために，ロールクラスに rbac:subRoleOf をオブジェクトプロパティとして記述する．

ロールとパーミッションクラス間にはオブジェク

† 仙台高等専門学校
Sendai National College of Technology
‡ 東北大学電気通信研究所/情報科学研究科
Research Institute of Electrical Communication /
Graduate School of Information Sciences, Tohoku University

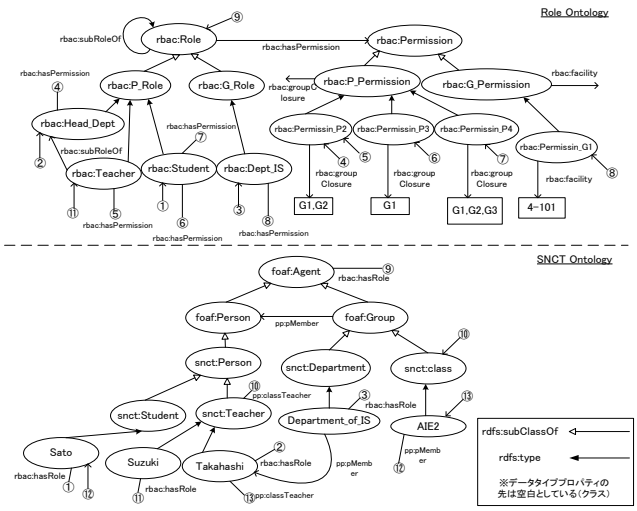

図 2　ロールオントロジーと学校オントロジー

トプロパティとして rbac:hasPermission が記述される．パーミッションクラスのインスタンスには上で述べた，きめ細やかなアクセスを可能とするための α，β，γ，δ 基準と各情報閉包とその範囲をデータタイププロパティとして記述する．図２の例では，組織情報閉包についての記述が行われており，各パーミッションに組織情報閉包 G1～G3 をそれぞれ記述している．また，グループパーミッションのインスタンスには，使用することができる施設の情報を記述する rbac:facility をデータタイププロパティとして記述する．

これらロールオントロジーのロールと図２の下部にある学校オントロジーに記述されているユーザ及びグループの関連付けを行うために，rbac:hasRole をオブジェクトプロパティとして記述する．これによって，図２の様に Sato は rbac:Student ロールを持つといった関係を記述することができる．

4. 動的なアクセス制御

前節で示したロールオントロジーに基づいて，ロールの委任，許可，禁止を動的に行うアクセス制御を適用する．制御の際のアクションの種類は，Delegation(委任)，Admission(許可)，Prohibition(禁止)の 3 種類を扱う．これらのアクションに基づき，オントロジーと対応してルール記述が可能な言語 SWRL(Semantic Web Rule Language) を用い，動的なアクセスを行うための各ルールを導入する．アクセス制御としては次の 2 つを導入する：

(1) rbac:subRoleOf で記述されたロール間で行うロール階層に基づいたアクセス制御
(2) 対象となるオントロジーに記述されたユーザの関係に基づいたアクセス制御

一つ目は，ロールオントロジーを直接用いて行う高いレベルのアクセス制御となっている．二つ目は，ユーザが所属している組織の情報や，ユーザ間の信頼の度合いなどの関係に基づいている．これらを基に動的なアクセス制御を行うための各ルールを導入する．以下にルールの例を示す．

ルール例1： 階層に基づいたロールの委任

$$Role(?x) \wedge Role(?y) \wedge Agent(?a) \wedge Agent(?b) \wedge subRoleOf\ (?x,?y) \wedge hasRole(?a,?y) \wedge hasRole(?b,?x) \Longrightarrow Allow\_P\_Delegation(?a,?b)$$

図２に対応して考えると，変数$?a$がTakahashi，$?b$がSuzuki となる．ロールに関する変数は$?x$がTeacher，$?y$がHead_Deptとなる．オントロジーから，各ロールはrbac:subRoleOfで階層関係が表現されている．したがって，ルールに基づいてTakahashiからSuzukiへのロールの委任が可能となる．

ルール例2： ユーザの関係に基づいた個人情報へのアクセス許可

$$Teacher(?a) \wedge Student(?b) \wedge Class(?x) \wedge classTeacher(?a,?x) \wedge pMember(?\mathrm{x},?\mathrm{b}) \Longrightarrow Allow\_P\_Admission(?a,?b,P\_Inf(?a))$$

各変数は，$?a$がTakahashi，$?b$がSatoとなる．クラスに関する変数は$?x$がAIE2となる．オントロジーから，TakahashiとAIE2の間には担任である関係を表すpp:classTeacherが記述されている．また，SatoがAIE2に所属することを表すpp:pMemberも記述されている．したがって，ルールの条件を満たしているのでTakahashiはSatoへ自身の個人情報へのアクセス許可を与えることができる．

このように，ロール階層に基づいたアクセス制御では広い範囲で権限の変更などを可能とし，ユーザの関係に基づいた制御では狭い範囲ではあるが，許可の受け渡しが可能となる．

5. まとめ

本稿では，ロールオントロジーの表現とそれらに基づいた動的なアクセス制御の手法について述べた．ロールオントロジーによって，ロールやパーミッション情報を体系的に表現することが可能となる．

今後は動的なアクセス制御を行う為のアーキテクチャの設計と，これらの有効性を評価するために学校オントロジーを対象として，情報検索システムを構築することが考えられる．

【参考文献】

[1] K.Sato, S.Izumi, Y.Kato and K.Takahashi, "A Privacy-based Personal and Group Information Modeling in Semantic Web," Proc. the 13th IASTED International Conference on Internet and Multimedia Systems and Applications (IMSA 2009), 655-035, 2009.

[2] R.S.Sandhu, E.J.Coyne, H.L.Feinstein and C.E.Youman, "Role-based Access Control Models," IEEE Computer, Vol.29, No.2, pp.38-47, 1996.