2010 年度第 6 回情報処理学会東北支部研究会（山形大学）
資料番号 10-6-B4-3

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

佐藤 晋也† 伊藤 仁† 和泉 諭†† 高橋 薫†
† 仙台高等専門学校 †† 東北大学

概　要

個人や組織の情報，およびそれらの関連情報をオントロジーによって表現し，それらへのアクセス制御を RBAC モデルに基づいたロールオントロジーを用いて行う手法を提案する．さらに，アクセス権限の委任や禁止を動的に行い，場面に応じた柔軟な情報アクセスを可能にする方法についても併せて与える．

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[4]に基づいたアクセス制御についても検討してきた[2][3]．

しかし，アクセス対象となる個人・組織情報はオントロジーで表現しているが，アクセス制御の基盤となるRBACのロールやパーミッションなどの情報をオントロジーで表現していないため，システムに適用する上で管理・運用に非統一性が残ることや，オントロジーの特長をロールやパーミッション情報に活用できていないといったことが改善点として挙げられる．また，オントロジーは関係情報を記述することに優れているので，ロール同士の関係をオントロジーを用いて有効に記述することにより，幅広いアクセス制御に繋げることができるのではないかと考えられる．これは，組織に所属する人々の役職による上下関係や人同士の横の関係を指している．

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細かい関係付けを行えるほか，対象となる個人・組織情報オントロジー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（例えば，[12]）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ことや，情報へのアクセスを一時的に規制するといった際のユーザの持つ権限の変化と，それらから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や禁止を動的に行うものである．

以下，2節ではプライバシーを考慮した個人・組織情報の表現を述べ，3節ではRBACモデルに基づいたロールオントロジーを与える．4節では，ロールオントロジーに基づいた各情報への動的なアクセス制御の手法について述べる．5節ではロールオントロジー及び動的なアクセス制御の適用例を示し，最後に6節でまとめと今後の課題を述べる．

2. 個人・組織情報の表現 [2]

2.1 個人・組織情報定義

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[8][9]とOWL[10]を用いオントロジーで表現する．

個人をfoaf:Person[6]クラスのインスタンスとし

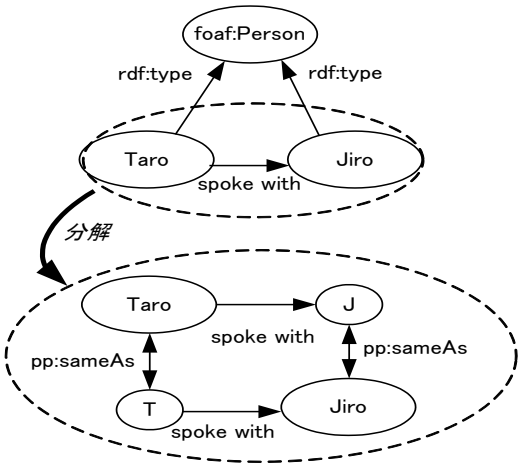

図 1 個人情報分解例

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．

また，情報の内容や閲覧する人に応じて情報の扱いが異なる．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．図1は，個人情報のα，β基準による分解の例を示している．α基準で記述された“Taro spoke with Jiro”に対してβ基準による分解を行うと，“Taro spoke with J”および“T spoke with Jiro”と別々の情報として表現することができる．

2.2 個人・組織情報閉包

上述した個人・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，組織内の情報などの情報範囲を組織情報閉包とする．

例えば，学校（SNCTと呼称）の事務部門の情報が図2の実線部分のように与えられていたとすると，SNCTの組織情報は以下となる：

SNCT pp:gMember AdministrativeOffice

OWLのプロパティ定義を用い拡張された情報から成る組織情報閉包G1は以下の通りになる．

SNCT pp:gMember AdministrativeOffice
SNCT pp:gMember General Affair
SNCT pp:gMember Financial Affair

また,組織内の情報を含む組織情報閉包をG2 とする．G2 では，組織の情報や，所属している個人の情報を組織情報閉包とし，以下の通りとなる．

SNCT pp:gMember AdministrativeOffice
SNCT pp:gMember General Affair
SNCT pp:gMember Financial Affair
General Affair phone +81-22-391-5508
General Affair pp:pMember Mike
Financial Affair phone +81-22-391-5517

さらに，組織に所属している人の個人情報を含む情報を組織情報閉包G3とする．G3は以下の通りとなる．

SNCT pp:gMember AdministrativeOffice
SNCT pp:gMember General Affair
SNCT pp:gMember Financial Affair
General Affair phone +81-22-391-5508
General Affair pp:pMember Mike
Financial Affair phone +81-22-391-5517
Mike ID f003

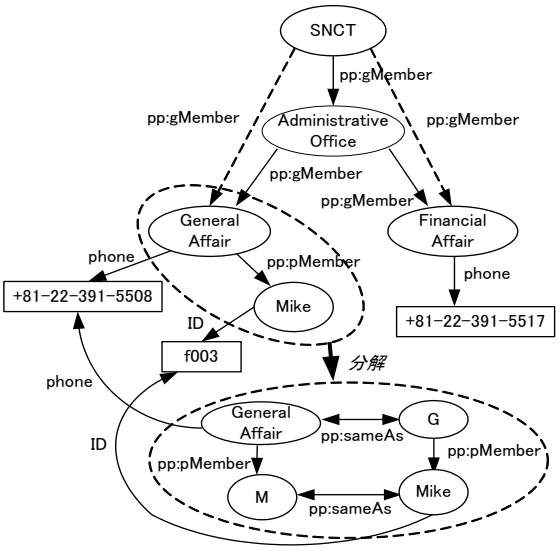

図 2 組織情報閉包例

図2の例で

General Affair pp:pMember Mike

はγ基準で記述されているが，これをδ基準により分解を行うと別々の情報として表現することができる．このように，各閉包により情報公開の範囲をきめ細かに定義することを可能としている．

3. ロールオントロジー

我々は，前節で述べたオントロジーを用いた個人・組織情報の表現に基づき，これにRBACの考えを組み合わせ，ロールとパーミッションの関係の記述を行った[2][3]．これはロールに割り当てられるパーミッションの中にα～δ基準，個人情報閉包，組織情報閉包の記述を行うものである．これにより，きめ細かに情報へのアクセスを可能としているが，これらの情報はオントロジーとして表現していないため，オントロジーの特長を活用していない．ここで，ロールとパーミッション情報にもオントロジーを用いることでロール同士の関係などをより詳しく記述することや各情報を体系的に表現できると考えられる．さらに，各情報をオントロジーによる統一を行うことで,管理における不統一性も解消される．

本節では,OWLによるRBACの表現に関する先行研究[14]の考え方を組み合わせ，ロール及びパーミッションとパーミッションに記述される各基準や各閉包をRDFとOWLを用いて，ロールオントロジーとして表現を行う．

ロールオントロジーにおけるロール情報を図3に示す.RBACにおけるロールをrbac:Roleクラスとして記述する．また，個人と組織ごとにロールを分けるため，サブクラスとしてrbac:P_Roleとrbac:G_Roleを設ける．このクラスのインスタンスにユーザのロールを記述することで，個人と組織ごとにロールを設定することを可能にしている．

また，ロールに階層を導入するためにrbac:Role

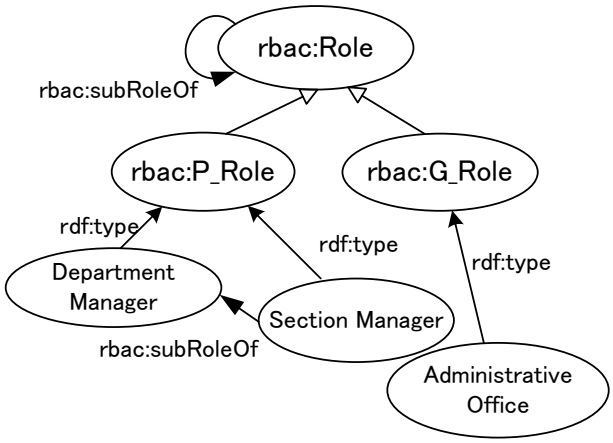

図 3 ロールクラス

クラスにrbac:subRoleOfを推移的オブジェクトプロパティとして記述する．ロールに階層関係を記述することによって，これらのロールを持っているユーザ同士の上下関係も同時に表現可能となる．

例えば，ある企業における部長と課長ロールを記述する際のロールとその階層は以下のように記述することができる（図3インスタンス部）．

DepartmentManager rdf:type rbac:P_Role
SectionManager rdf:type rbac:P_Role
SectionManager rbac:subRoleOf DepartmentManager

このように階層を記述することで，部長と課長のロールの上下関係を記述できるほかに，これらロールを持っているユーザ同士の関係も同時に表すことが可能である．

図4に個人・組織情報とロールの関係を示す．ユーザはロールを持つという関係を記述しなければならないので，rbac:hasRoleをオブジェクトプロパティとして，foaf:Agentとrbac:Role間に記述する．ここでのfoaf:Agentクラスはアクセス対象となるオントロジーに記述されており，個人や組織の情報が記述されているクラスのスーパークラスとなっている．

図5にユーザとロールの関係の例を示す．破線はロールオントロジーと対象となる情報のオントロジーとの境界線となっている．ここでのBobはfoaf:Agentクラスのインスタンスとして扱う．オントロジーに記述されている情報から，Bobは X-CompanyのGeneralAffairに属しているという関係を得ることができる．図4の関係から，

Bob rbac:hasRole DepartmentManager

が成り立つ．これにより，BobはDepartmentManagerロールを持つことができる．このように，アクセス対象となるオントロジーではユーザの所属している組織の情報が詳しく記載されているため，ロール自体に所属先などの記述を行わなくても，ユーザがそのロールを持つという関係だけから推移的にロールがどの部署に適用されているかを得ることができる．これらから，ロールオントロジーにはシンプルにロール情報を記述することができる．

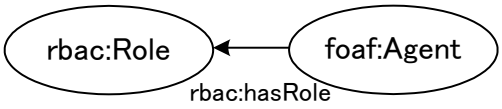

図 4 個人・組織情報とロールの関係

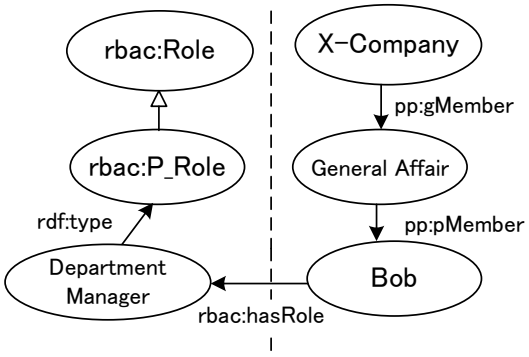

図 5 ユーザとロールの関係

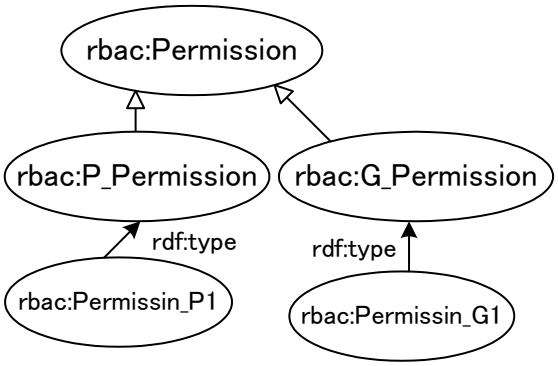

図 6 パーミッションクラス

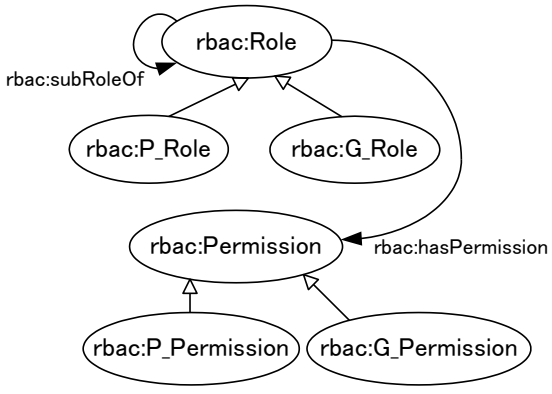

図 7 ロールとパーミッションの関係

次にパーミッション情報を図6に示す．RBACにおけるパーミッションをrbac:Permissionクラスとして記述する．また，rbac:Roleクラスと対応させるため，サブクラスとしてrbac:P_Permissionとrbac:G_Permissionクラスを記述している．このクラスのインスタンスに各ロールに割り当てられるパーミッションを記述する．

図7にロールとパーミッションの関係を示す．パーミッションをロールに割り当てるという関係がある

ので，この関係を記述するためにrbac:hasPermissionをオブジェクトプロパティとしてrbac:Roleとrbac:Permissionクラス間に記述する．この関係を記述することによって，各クラスにインスタンスとして記述されるユーザのロールとパーミッションにも同様の関係が成り立つ．ロールオントロジーでは様々な種類のパーミッションをインスタンスとして記述しているので，複数のパーミッションを割り当てる際もrbac:hasPermissionプロパティを用いることで分り易く表現することができる．このインスタンスに記述されるパーミッションは，適用される組織のロールの数などにより変化する．これらも上述のrbac:hasRoleプロパティの記述によって，ユーザや組織の情報から推移的にパーミッションの適用範囲などを得ることができる．したがって，パーミッションも記述を簡略化することができる．

rbac:Permissionクラスのインスタンスには，α～δ基準や個人情報閉包と組織情報閉包の記述を行うためにデータタイププロパティを用いて各情報を記述する．前節で述べた個人・組織情報のα，β基準はrbac:PersonCriterion，γ，δ基準はrbac:GroupCriterionとして記述している．個人，組織情報閉包はそれぞれ，rbac:PersonClosure，rbac:GroupClosureとして記述している．これら閉包が適用される情報の範囲に関する記述は，rbac:PersonRangeとrbac:GroupRangeとして記述している．

例えば，図8のようなパーミッションが割り当てられたロールを持つユーザの各情報へのアクセスの範囲は以下の通りとなる．

(1) 個人情報のアクセス

rbac:Permission_P1 rbac:PersonClosure ALL
rbac:Permission_P1 rbac:PersonRange self
rbac:Permission_P1 rbac:PersonCriterion α

つまり，α基準に従い全ての自分自身の情報を閲覧可能である．

(2) 組織情報へのアクセス

rbac:Permission_P1 rbac:GroupClosure G1,G2,G3
rbac:Permission_P1 rbac:GroupRange X-Company
rbac:Permission_P1 rbac:GroupCriterion γ

つまり，組織情報閉包G1～G3で表現されたX-Companyクラスに記述された情報をγ基準に従い閲覧可能である．

このようにして，各情報へのアクセスの基準となるパーミッションの記述を行う．

組織のロールに割り当てられるパーミッションには，施設の利用に関する記述が行えるrbac:facilityをデータタイププロパティとして用意している．

このようにして，ロールやパーミッションに詳細な記述を行い，関係付けを行うことでより柔軟で細かいアクセス制御を可能としている．また，オントロジーを用いて体系的にロールやパーミッションを記述することで，より分り易く各関係を表現している．

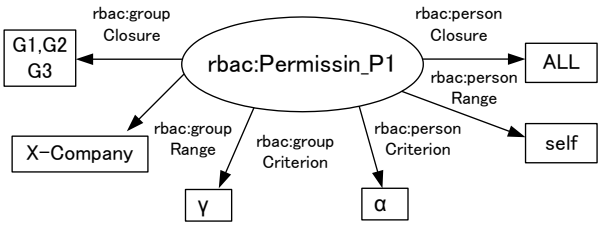

図 8 パーミッションの例

4. 動的なアクセス制御

4.1 アクセス制御の基本的考え方

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ことや，情報へのアクセスを一時的に規制するといった際のユーザの持つ権限の変化と，それらから生じるアクセス権の変更に対して柔軟に対処した方が良い場面が考えられる．そこで，前節で示したロールオントロジーに基づいて，権限の委任や禁止を動的に行うアクセス制御を導入する．

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) [11]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．これらアクションを行う際には，予め期間や時間の指定を行う．また，各アクションを行った後に取り消しを行うことも可能としている．

アクセス制御として次の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同士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．このアクセス制御は，対象となるオントロジーを主に用いており，ロールオントロジーは間接的に用いているので，ロール階層に基づいたアクセス制御と比較すると限定的なアクセス制御となっている．

これらの動的なアクセス制御は，制御を行う際はアクションごとに記述されたルールに沿って，一時的なアクセス情報を作成する．したがって，システムに適用する際には高いレベルの情報となるロールオントロジーの書き換えは行わずに制御を行う．

以下では，これら2つのアクセス制御の概要と導入したルールについて述べる．

4.2 ロール階層に基づいたアクセス制御

ロール階層に基づいたアクセス制御の基盤となるのはロールオントロジーにおけるrbac:subRoleOfであり，対象となるユーザは，このプロパティで関係付けされたロールを持つユーザとなる．つまり，上下関係の上位にいるユーザが，下位に位置するユーザに特定の情報へのアクセスの一時的な許可などを行うことがこの制御の大きな目的となっている．このアクセス制御では，ユーザの権限などに直接関わるロールオントロジーに基づいているため，ロールとパーミッションへのアクションを可能としている．

ここでは，Delegation，Admission，Prohibitionの3つのアクションを用いる．下位のユーザが自身の権限ではアクセスできない情報に権限を超えてアクセスをしたい場合に，上位のユーザが自身の権限を一時的に下位のユーザに委任をすることができれば，より柔軟な情報のアクセスに繋がる．そこで，委任に関するアクションを考察する．結果的に，ロールに割り当てられたパーミッション情報も含まれる．これを委任に関するアクションとしてDelegationとする．

なお，このアクションで権限を超えたアクセスを満たすことはできるが，一部の情報のみへのアクセスを許可するといったことはできない．そこで，制御をパーミッションに限定したアクションをAdmissionとする．これは，上位のロールに割り当てられたパーミッションの一部を下位のロールに割り当てることで，一部の情報に限定しアクセスをさせることを可能としている．また，このアクションはロール自体の一時的な許可も合わせて行うことができる．

また，Admissionとは逆に一時的に情報へのアクセスを規制したいといった状況も考えられる．そこで，権限の行使を規制するアクションをProhibitionとする．このアクションはロール自体へ行うこともできるが，パーミッションに限定して行うことも可能となっている．

これらアクションをオントロジーと対応してルール記述可能な言語SWRLに従いルールとして定式化する．図9は，アクションの対象となるオントロジーの例であり，図10は，DepartmentManagerに割り当てられたパーミッションの例である．

このオントロジーにおけるMikeとBobはfoaf:Agentクラスに記述されたインスタンスであり，各ロールはrbac:Roleクラスに記述されたインスタンスである．DepartmentManagerに割り当てられたパーミッションは前節で示した例と同様のものとなっている．ルールで個人・組織情報に対応した各基準や閉包を扱う際は，個人に関する情報(rbac:PersonCriterion，rbac:PersonClosure，rbac:PersonRange）をP_Inf，組織に関する情報（rbac:GroupCriterion，rbac:GroupClosure，rbac:GroupRange)をG_Infとし，一つの情報として定義する．

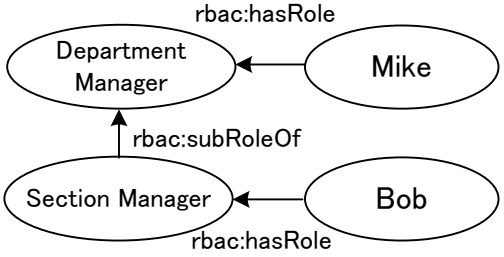

図 9 階層関係の例

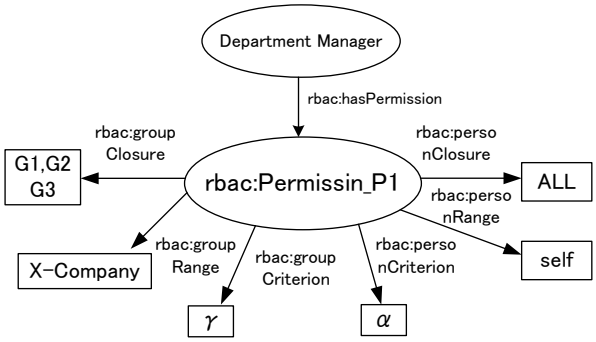

図 10 パーミッション例

以下に各アクションに対応するルールを示す．

ルール1：ロールの委任

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

ルール2：ロールの許可

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

ルール3：ロールの禁止

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

ルール4：特定のパーミッションの許可

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

ルール5：特定のパーミッションの禁止

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

各ルールはrbac:subRoleofとrbac:hasRoleによって記述された情報を対象としてアクションを適用する．よって，図9で示した例のような関係が成り立っ

ている時に，各アクションを適用することできる．各変数は，?aと?bはfoaf:Agentクラスに記述されたユーザ,?xと?yはrbac:Roleクラスに記述されたロールとなる．これを図9の例を用いて説明する．?aをMike，?bをBobとする．図9からMikeとBobはrbac:hasRoleとして各ロールを持っている．これらのロールはrbac:subRoleofによって階層関係が表されているので，ルール1～ルール3では条件に従いMikeからBobへのロールの委任，許可，禁止を行うことができる．同様にパーミッションに関するルールも,アクションの対象となるパーミッション(P_Inf, G_Inf）を記述することで，ルール4ではMikeがBobへ自身の個人情報を閲覧させる許可，ルール5ではMikeがBobの持つ組織情報の閲覧に関するパーミッションの禁止のアクションを行うことができる．ここでは示していないが，対象となる情報（P_Inf, G_Inf）は随時選択することができる．このように，ロールオントロジーに記述された情報から高いレベルのアクセス制御を可能としている．

4.3 ユーザの関係に基づいたアクセス制御

個人・組織情報には様々な関係性が存在する．オントロジーはこれら関係を記述することに優れている．そこで，オントロジーに記述された関係情報を利用して制御を行うユーザの関係に基づいたアクセス制御について示す．手法は前節で示したものと同様となっている．このアクセス制御において基盤となるのは，ユーザ及び組織間に記述された各プロパティとなる．これらプロパティは，アクセスの対象となるオントロジーに記述されているので，ロール階層に基づいたアクセス制御と比較すると限定したレベルの制御となる．よって，前節ではロールそのものを委任するといったルールを示したが，本節で示すアクセス制御では，アクションの対象となる情報はパーミッションのみとなっている．

ユーザ同士の関係は複数存在する．1つ目として，ユーザ同士の信頼関係を用いたアクションを示す．図11はアクションの対象となるオントロジーの例である．パーミッションの例は図10を用いる．この例では，対象となるオントロジーに記述されているオブジェクトプロパティのpp:trustを用いたアクションとなる．このpp:trustは記述されたユーザ同士の信頼関係を示している．また，この信頼関係の深さを示すために，pp:trustにはサブプロパティとしてpp:trust1とpp:trust2が記述されている.pp:trust2まで記述されている時が信頼の度合いが一番高いものとしている．

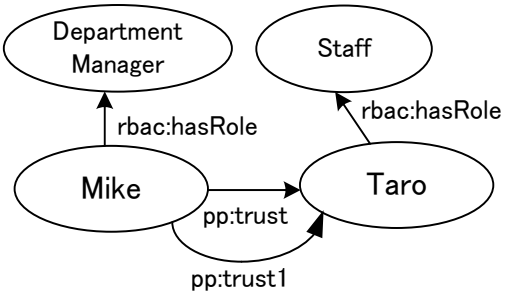

図 11 オントロジーの例

図11を用いて各アクションに対応するルールを示す．ここでのアクションは，Admissionのみとなっている．

ルール6: 信頼関係を用いたパーミッションの許可

$$Agent(?a) \wedge Agent(?b) \wedge trust(?a,?b) \wedge trust1(?a,?b) \Longrightarrow Allow\_P\_Admission(?a,?b,P\_Inf(?a))$$

各変数は，?aと?bはfoaf:Agentクラスに記述されたユーザとなる．このルールでは，pp:trustだけではなくpp:trust1が記述されていなければ許可のアクションを適用することができない.図11の例では，MikeはTaroに自身の個人情報を閲覧する許可を与えることができる．ここでは，trsut1まで記述された場合についての例だが，適用される情報によってこの値は変化する．

2つ目として,組織に纏わる関係を用いたアクションのルールを示す．信頼関係の他にもユーザが所属している組織との関係などからもアクションを行うことができる．例えば，ある組織を管理しているユーザとその組織に所属しているユーザ間を階層関係で表せないといった場合もある．このような場合に階層関係を用いずに，組織に纏わる関係を用いて行うアクションのルールを以下に示す．ここでのアクションも，Admissionのみとなっている．図12はアクションの対象となるオントロジーの例となる．パーミッションの例は図10を用いる．

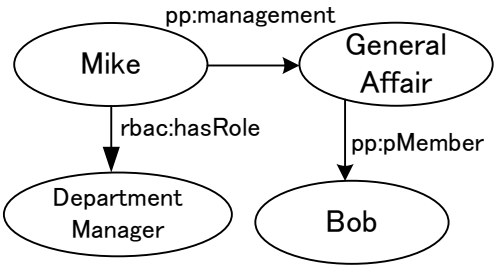

図 12 ユーザの関係を表した例

ルール7: 組織に纏わる関係を用いたパーミッションの許可

$$Agent(?a) \wedge Agent(?b) \wedge Group(?x) \wedge management(?a,?x) \wedge pMember(?x,?b) \Longrightarrow Allow\_P\_Admission(?a,?b,P\_Inf(?a))$$

各変数は，?aと?bはfoaf:Agentクラスに記述されたユーザとなる．?xは対象となるfoaf:Groupクラスに記述された組織情報となる．これを図12の例を用いて説明する．?aと?bはMikeとBobとなり，?xはGeneralAffairとなる．MikeとGneralAffairにはpp:managementで関係付けされているので，GeneralAffairとpp:pMemberで関係付けされているBobへアクションを行うことができる．つまり，MikeはBobへ自身の個人情報を閲覧する許可を与えることができる．この例では組織を管理するユーザとの関係をpp:managementとして説明をしたが,対象のオントロジーによってこの値は変化する．しかし，ルールの形式はルール7に沿うことになる．

このように，ロール階層に基づいたアクセス制御では行うことができない制御を，限定したレベルの中ではあるが行うことが可能となる．

5. 適用例

本節では，3節と4節において示したロールオントロジーと動的なアクセス制御を学校を例としたオントロジーに適用する．

5.1 学校オントロジー

学校オントロジーには，個人情報として教員や学生，事務職員の情報などが記述されている．組織情報は学科やクラス，研究室などの情報が記述されている．図13にロール及びパーミッションの適用例を挙げる．

教員や学生といった個人に関するロールはrbac:P_Roleクラスに記述する．図13では，インスタンスとして，Head_Dept（学科長），Teacher(教員)が記述されており，それらに割り当てられるパーミッションはrbac:hasPermissionによって記述されている．例では，各ロールはrbac:Permissin_P2と関係付けがされている．また，学科長ロールと教員ロール間には階層関係を表現することができるので，rbac:subRoleOfが記述されている．学科や事務といった組織に関するロールはrbac:G_Roleクラスに記述する．例では，Dept_IS(IS学科)インスタンスとして記述されている．組織のロールに関しても個人のロールと同様にパーミッションが割り当てられている．例では，IS学科ロールはrbac:Permissin_G1が割り当てられている．

次に学校オントロジーとロールオントロジーの関係の例とパーミッションの詳細の例を図14に示す．foaf:Agentのサブクラスでとなるsnct:Teacherクラスのインスタンスとして記述されたSuzuki(教員)は

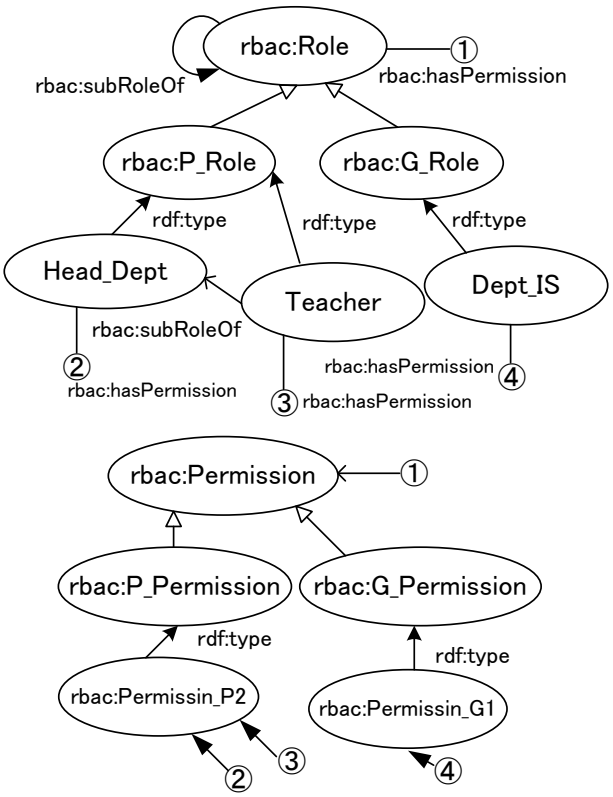

図 13 ロールとパーミッションの適用

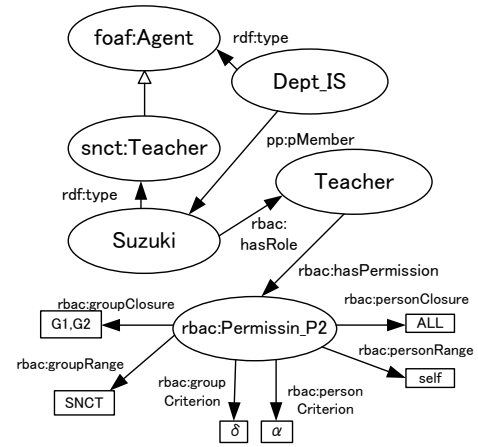

図 14 ロールとパーミッションの関係と詳細

rbac:hasRoleから，教員ロールを持つという関係が成り立つ．よって，教員ロールに割り当てられたパーミッションに記述されているプロパティから，各基準・閉包およびその閉包の範囲に基づき情報を閲覧することができる．例では，個人に関する情報は「α基準に従い全ての自分自身の情報を閲覧可能」となる．組織に関する情報は「組織情報閉包G1～G2で表現された，SNCTクラスに記述された情報をδ基準に従い閲覧可能」となる．このロールやパーミッション情報には，Suzukiの所属する学科の情報等は記述されていない．しかし，学校オントロジーに記述された Dept_IS pp:pMember Suzuki の関係から，「IS学科に属する教員のロール」という情報を推移的に得ることができる．このように，学校オントロジーとの関係付け行うことで，ロールやパーミッシ

ョンの記述を簡略化することができる．また，ロールオントロジーを適用することで，学校におけるロールやパーミッション情報も体系的に表現することを可能としている．

5.2 アクセス制御

上述の学校オントロジーを基に,4節で示した動的なアクセス制御を適用する．1つ目として，ロール階層に基づいたアクセス制御の適用例を示す．図15は学校オントロジーに適用した場合の階層関係の例となっている．各クラスの定義とロールに割り当てられたパーミッションの詳細は図13及び図14と同様とする．TanakaもSuzukiと同様にsnct:Teacherクラスのインスタンスとする．

学科長ロールを持つTanakaがSuzukiへロールの委任を行う場合，以下のルールに基づいた制御が行われる．

ルール(例1)： 学科長ロールの委任

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

各変数は，?aがTanaka，?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．よって，ルールに基づいてTanakaからSuzukiへのロールの委任が可能となる．

次に，学科長ロールを持つTanakaがSuzukiへ自身の個人情報に関する閲覧許可を行う場合の制御に用いるルールを示す．

ルール(例2)： Tanakaの個人情報の閲覧許可

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

各変数は，委任に関する例の時と同様となっている．先程の例と同様にルールの条件を満たしているため，Tanakaの持つ個人情報に関するパーミッションのSuzukiへの割り当てが可能となる．同様のルールを用いて，組織情報の閲覧許可も行える．

次にTanakaが教員ロールを持つSuzukiの組織情報の閲覧を禁止する場合に用いるルールを示す．

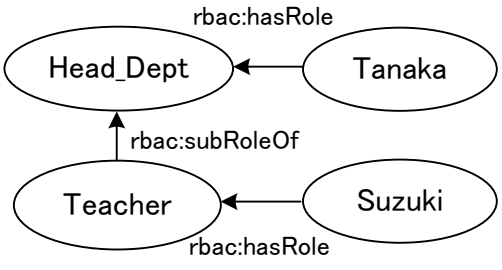

図 15 学校オントロジーにおける階層関係の例

ルール(例3)： Suzukiの個人情報の閲覧禁止

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

各変数は，委任や許可に関する例の時と同様となっている．この例も同様にルールの条件を満たしているため，TanakaがSuzukiの持つ組織情報に関するパーミッションを禁止することができる．

このようにして,4節で示したルールに基づいて階層関係で記述されたロール間で各情報の委任,許可,禁止が可能となる．

2つ目としてユーザの関係に基づいたアクセス制御の適用例を示す．図16は学校オントロジーにおけるユーザの関係の例となっている．Teacher及びSuzukiに関する定義は図13と図14と同様とする．また，snct:Classとsnct:Studentはそれぞれfaof:Agentクラスのサブクラスとなっている．このオントロジーは，学生が所属するAIE1クラスに纏わる情報を示している．SuzukiはAIE1クラスの担任をしている．また，SatoとMasudaはこのクラスに所属する学生となっている．SatoからMasudaには信頼関係を表すものとして,pp:trustからpp:trust2がプロパティとして記述されている．

まず，担任であるSuzukiが自身の個人情報をAIE1クラスに所属しているSatoに閲覧を許可する場合のルールを以下に示す．

ルール(例4)： Suzukiの個人情報の閲覧許可

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

各変数は，?aがSuzuki，?bがSatoとなる．クラスに関する変数は?xがAIE1となる.オントロジーから,SuzukiとAIE1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AIE１に所属することを表すpp:pMemberも記述されてい

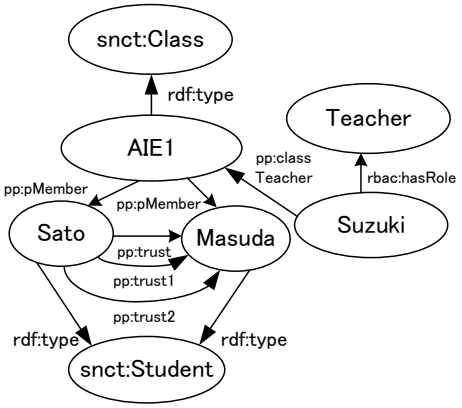

図 16 学校オントロジーにおける
ユーザ間の関係の例

る．したがって，ルールの条件を満たしているのでSatoへのSuzukiの個人情報の閲覧許可を行うことができる．

次に，SatoからMasudaへの個人情報の閲覧許可をする場合のルールを以下に示す．

ルール(例5)： Satoの個人情報の閲覧許可

$$Student(?a) \wedge Student(?b) \wedge trust(?a,?b) \wedge trust1(?a,?b) \wedge trust2(?a,?b) \Longrightarrow Allow\_P\_Admission(?a,?b,P\_Inf(?a))$$

各変数は，?aがSato，?bがMasudaとなる．この制御を行う際の基盤となるのは，SatoとMasudaの間の信頼関係となっている．SatoとMasudaの間にはpp:trust2まで記述されているので,ルールの条件を満たしている．したがって，MasudaはSatoの個人情報を閲覧することが可能となる．

このように，許可に関してのみだが，学校オントロジーに記述されているプロパティからアクセス制御を行うことを可能としている．この動的なアクセス制御は一時的な制御となっているが，これらを用いることでロールオントロジーに変更を加えなくても，範囲は狭いが場面に応じたアクセス制御が可能となる．

6. 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．また，動的なアクセス制御では場面に応じた柔軟な情報へのアクセス制御を可能としている．

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実装と，これらの有効性を評価するために学校オントロジーを情報の対象として，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] 佐藤加奈, 安田尚史, 加藤靖, 高橋薫, “個人・組織情報のモデル化とプライバシーの取扱い,” 2008年度第6回情報処理学会東北支部研究会, 資料番号08-6-A-3-4, 2009.

[2] 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.

[3] 佐藤加奈, 佐藤晋也, 加藤靖, 高橋薫, “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,” 第8回情報科学技術フォーラム(FIT2009), 3G-6, 2009.

[4] 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.

[5] W3C, “The Platform for Privacy Preferences 1.0 (P3P1.0) Specification,” W3C Recommendation 16 April 2002.

[6] “The Friend of a Friend (FOAF) project,” http://www.foaf-project.org/.

[7] S.S.Al-Fedaghi and M.Y.Ahmad, “Personal Information Modeling in Semantic Web,” Mizoguchi et al. (Eds.): ASWC 2006, LNCS 4185, pp.668-681, 2006.

[8] W3C, “Resource Description Framework (RDF),” http://www.w3.org/RDF/.

[9] W3C, “RDF Vocabulary Description Language 1.0: RDF Schema,” http://www.w3.org/TR/rdfschema/.

[10] W3C, “OWL Web Ontology Language Reference,” http://www.w3.org/TR/owl-ref.

[11] W3C, “SWRL: A Semantic Web Rule Language: Combining OWL and RuleML,” http://www.daml.org/2003/11/swrl/.

[12] L.Kagal, T.Finin and A.Joshi, “A Policy Based Approach to Security for the Semantic Web,” D. Fensel et al. (Eds.): ISWC 2003, LNCS 2870, pp.402-418, 2003.

[13] G.V.Lioudakis, E.A.Koutsoloukas, N.L.Dellas, N.Tselikas, S.Kapellaki, G.N.Prezerakos, D.I.Kaklamani and I.Venieris, "A Middleware Architecture for privacy protection," Computer Networks, Vol.51, pp.4679-4696, 2007.

[14] T.Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, W.Winsborough and B.Thuraisingham, "Role Based Access Control and OWL," Proc. the fourth OWL: Experiences and Directions Workshop, 2008.

[15] H.Chen, T.Finin and A.Joshi, "A Pervasive Computing Ontology for User Privacy Protection in the Context Broker Architecture," University of Maryland, Baltimore County TR-CS-04-08 TechReport, 2004.

[16] S.S.Yau and J.Liu, "A Situation-aware Access Control based Privacy-Preserving Service Matchmaking Approach for Service-Oriented Architecture," ICWS, pp.1056-1063, IEEE International Conference on Web Services (ICWS 2007), 2007.

[17] M.Hecker and T.Dillon, "Privacy Support and Evaluation on an Ontological Basis," Third International Workshop on Privacy Data Management with 23rd International Conference on Data Engineering (ICDE 2007), Apr 16 2007, pp. 221-227.

[18] E.Bertino, P.A.Bonatti and E.Ferrari, "TRBAC: A Temporal Role-Based Access Control Model," ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001, Pages 191-223.