組織間情報アクセス制御ポリシーのための FCA によるロール自動調整とルールの設計洗練化支援

Auto adjustment of role for -policy of access control among multiple organization by using FCA and support to sophisticate to design rule

尾崎稜太 †, 飯島正 ‡
Ryota Ozaki†, and Tadashi Iijima‡
† 慶應義塾大学大学院　理工学研究科開放環境科学専攻
‡ 慶應義塾大学 理工学部
†Graduate School of Science and Technology for Open and Environmental Systems, Keio Univ.
‡Department of Science and Technology，Keio Univ.

要旨

近年では，個人情報であっても複数の組織にまたがって管理されており，アクセス制御サーバを外部化し，多様な連携利用を可能とすることが求められている．そうした複数の組織で個人情報を管理するには全ての組織で一元化されたアクセス制御モデルにて整合性のとれたアクセス権限を付与する必要がある．

そのため，本研究では RBAC をベースとするアクセス制御モデルのロールに対して形式概念分析を用いてロール同士の関係を可視化し，不適切なルールを付与されたロールを見つけたり，近い内容のロールのすり合わせを提案したりすることでルールの洗練化を試みている．

本報告では簡単な例題を通して形式概念分析を用いたロール同士の関係の可視化の結果を, ルールの設計洗練化に活用が可能であることを示す.

1. 研究背景

近年，ネットワーク技術の発達に伴い,SNS などが普及し, インターネット上に誰でも個人情報を作成することができるようになった. しかし, これらの個人情報は様々なユーザにより閲覧される可能性がある. つまり, 個人情報が見知らぬユーザに悪用されてしまう危険性が大きくなっている. 例えば, 医療施設では, 従来は紙で作成されていたカルテや処方箋が電子化されてきている. また, 情報が電子化されることによって従来は行うことが困難であった施設間での情報の共有が考えられるようになる. 例えばこれを医療施設などで導入することができれば, セカンドオピニオンとして別の病院を受診する際, 患者側の許可のもとでカルテを共有することができ, 繰り返しの診察による手間や再検査を行うことによる身体的なリスクを低減させるなどのメリットが考えられる. しかし, セキュリティや法律の問題で未だ実用に至ってはいない.

本研究プロジェクトにおけるアクセス制御モデルでは, 特に複数の組織にまたがって分散されている情報にアクセスすることを想定している. 従来はあるデータベースにアクセスするとき, そのデータベース管理システムにアクセス制御モデルを組み込むことでアクセス制御を実現していたが, 今後はアプリケーションソフトウェアが複数のデータ管理組織にアクセスし, 組織をまたがった情報の移動が行われる状況が想定される. そのアクセスに対して制御を行う際には, 個々のデータベース管理システムでのアクセス制御ではなく, 外部化されたシステム上でのアクセス制御が求められる. しかし, 外部化されたシステム上でのアクセス制御では, 従来のように個々の施設だけではなく, 複数の施設のルールを扱うことになり, ルールの数が膨大となり, 管理が煩雑になる.

そこで, 本研究ではロールベースアクセス制御 [1] をベースとした外部化されたシステム上でのアクセス制御におけるロールの管理の簡略化を目的として, 形式概念分析 (Formal Concept Analysis : FCA)[2] を用いて膨大になることが予想されるロールのうち近い内容となるものを可視化し, すり合わせることを提案してきた. FCA とは, 物事の概念構造を数学的に解析する手法で, 対象に属性を与えることでその対象の上下関係を導き出すことができる. この点で, 前述の複数のデータ管理組織を扱う外部化されたシステム上でのアクセス制御でのロールの管理という目的に当てはまることから, 本研究では形式概念分析を採用している. この論文では, この手法を用いることでロール同士の関係を可視化することができることを示す.

2. 関連知識

2.1.RBAC(Role-Based Access Control)

アクセス制御は, 一般に, 主体・対象・操作の 3 つの組のうち, 許可されている組の集合で制御される. 特に RBAC[1] は, 情報にアクセスする主体にアクセス権限を設定するのでなく, ロールに対してアクセス権限を設定し, 各主体をそのロールにそれぞれ割り当てるものである. ロールごとにアクセス権限を設定することで. アクセス権限の定義数を大幅に減らすことができる. 例えば, 病院の場合であれば, 従業員それぞれに権限を設定するのではなく, 医者や看護師のようなロールごとにアクセス権限を設定する.

2.2. 形式概念分析 (Formal Concept Analysis : FCA)

FCA はデータ分析手法の一つであり, 数学的に概念構造の分析を行う. FCA の用語としての概念とは一般的に使われるものと異なり, 以下のように数学的に定義されたデータとして扱われる.[5]

- オブジェクト G

  現象や事象に出現する対象

- 属性 M

  オブジェクトの持つ性質

- 二項関係 I$\subseteq$ G$\times$ M

  gIm であるとき,g は m の属性を持っていることになる

- 文脈 $\boldsymbol{K}$ = (G,M,I)

  対象と性質の関係の集合

- 外延 X$\subseteq$ G

  共通の属性を持つ対象の集合

- 内包 Y$\subseteq$ M

  共通の対象を持つ属性の集合

- 概念 (X,Y)

  必要十分な関係にある外延と内包のペア

また, ある文脈に対して複数の概念が出現するが, それらの概念の包含関係を図で表したものを概念束と呼ぶ.

例えば, 対象と属性をそれぞれ「脊椎動物の分類群」と「恒温動物であるか・成体が肺呼吸であるか・卵生であるか」とし, その文脈を表した表を図 1 とすると, 以下の図 2 のような概念束が形成される. なお, この概念束は Concept Explorer [3] というツールを使用して作成した. この概念束の円一つ一つが概念を表している. 例えば, 爬虫類と両生類がかかっている円は外延が「爬虫類・両生類・鳥類」、内包が「卵生・成体が肺呼吸」である概念となっている. これは, 爬虫類・両生類・鳥類に共通する特徴が卵生・成体が肺呼吸であり, 卵生・成体が肺呼吸という特徴を共通して持っているのが爬虫類・両生類・鳥類であることから, 外延と内包が必要十分な関係にあるため, 概念となる. 図 1 から, 今回扱う属性では爬虫類と両生類の特徴は同じであり, それは図 2 の概念束から容易に判断できる. 実際に成体だけに着目するとヘビやヤモリとカエルやイモリは類似している.

また, この形式概念分析では対象の包含関係も可視化することができ, 今回扱った図 2 の概念束では図の上にある概念ほど上位の概念, つまり汎化されている概念で, 下にある概念であるほど下位の概念, つまり特化されている概念であることがわかる. 例えば, 魚類の特徴である卵生という属性は爬虫類や両生類や鳥類も持っており, 上位の概念が持っている属性は多くの対象が持っていることがわかる.

	恒温動物	成体が肺呼吸	卵生
哺乳類	×	×	
爬虫類		×	×
鳥類	×	×	×
魚類			×
両生類		×	×

図 1: 対象と属性の関係

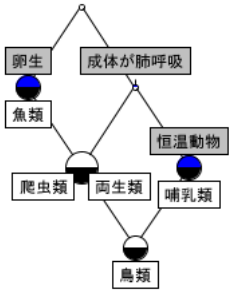

図 2: 概念束の例

2.3. 既存研究と本研究の位置付け

本研究は FCA という手法を用いて施設間でのアクセス制御を適切に行うものである. 同様に FCA を RBAC のロールに適用している研究に,Ravi Sandhu 氏による RBAC のロール階層を FCA を用いた図で可視化しているもの [6] や, Aswani Kumar 氏らによる FCA を用いて複数の施設間での RBAC のモデルを作成するもの [7] があるが, 前者は RBAC のロールの関係を「操作」を属性とした概念束を用いて可視化を行い, 操作に基づいたロールの関係をわかりやすくすることを目的としたもので, 後者は施設間でのアクセス制御に RBAC を用いる際, 複雑化しがちなロールのアクセス権限を FCA を用いて簡易化して扱いやすくすることを目的としたものである., 本研究は FCA を用いてロールの関係を可視化して, 近いルールや不適切なルールを見つけ, より適切なルールを提示したり, ルールの統合や継承階層構造の導入により保守性を高めることを目的としており, それぞれ目的が異なっている.

3. 提案

本研究プロジェクトでは,FCA によるロールの自動調整とそれによるルールの洗練化支援を提案している. 本研究では, ベースとするアクセス制御モデルとして RBAC を採用し, そのロールの関係を導き出すために FCA[2] によって表される概念束を用いる.

3.1.RBAC ベースのアクセス制御

本研究では以下の 3 つをセットとしたものをルールの表現として扱っている.

- 主体：SVO の S にあたる部分. 医者や事務員など, アクセスを行う側がこれに該当する.
- 対象：SVO の O にあたる部分. カルテや在庫情報など, アクセスされる側がこれに該当する.
- 操作：SVO の V にあたる部分. 閲覧や編集など何を行うかがこれに該当する.

この 3 つの組, 主体-対象-操作を一つのルールとし,RBAC で扱うロールはこのルールを持つことでアクセス権限を得ることになる. 例えば,「医者」というロールに,「医者」という主体と「カルテ」という対象と「閲覧」という操作を持つルールが与えられた場合, その医者というロールはカルテを閲覧する権限を持っていることになる. なお, このルールは複数持つことも可能で, 一般的にロールは複数のルールを持つことでアクセス可能な対象を決定する.

3.2. ロールの上下関係の導出

許可されている内容を属性とすることで, ロールに属性がついているかついていないかに基づいてロールの上下関係を決定することができる. この上下, または等しい関係からどのロールが近く, どのロールが同じなのかを分析することができる. 同じ内容のルールを統合することはもちろん, 施設間で同じ名前の役職であったとしても, 少しだけ異なる権限が付与されている場合も考えられる. そういった場合にその差異を示すことによってルールの洗練化に利用することもできる.

4. 設計と実装

4.1. ポリシーの構成

RBAC をベースにしたアクセス制御では 4.1. で述べた通り, 主体・対象・操作の組の集合をルールとし, 許可されているアクセスを表す. ルールについては図 3 のような形式で記述しており, この記述をもとにアクセス制御を行っている.

```
<Rule Effect="Permit" RuleId="0">
<Subject> A病院の薬剤師</Subject>
<Resource>担当外患者のカルテ</Resource>
<Action>閲覧</Action>
</Rule>
```

図 3: ルールの表現

また, 今回は図 4 に示すように, ルールの集合をポリシーとしてロールに持たせることでルールの表現を行っている.

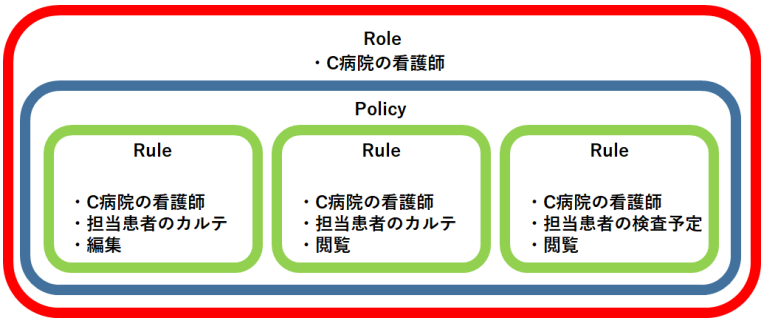

図 4: ルールの表現

4.2.FCA によるロール階層構造の分析

本研究では 2.2. で示した FCA を用いて得た概念束で表される概念の関係から, 類似しているロールや同じであるロールを導出したり, ロールの上下関係を表すことで秘匿レベルの高いアクセスやそうでないアクセス, アクセス権限の強いロールとそうでないロールの可視化を行っている. その際には 4.1. で述べた RBAC で扱う主体を対象とし, アクセス対象と操作のペアを属性としている. このように定義することで, アクセス権限の違いの観点から概念束を形成することができ, ロールの上下関係を表すのに適しているためである. これの適用例については 6. で示す.

4.3. ルールの洗練化

5.2. で導出したロールの関係から以下のようにルールの洗練化を提案することができる.

1. 全く同じアクセス権限を持っているロールを統合して考える

2. 近いアクセス権限を持っているロールをまとめる

3. 不自然なアクセス権限を持っているロールを適正化する

1 に関しては概念束で同じセルに位置するロールに対して提案を行うことができる. これを行うことで新しく権限を与える際に, 同じようなロールであるのに毎回付与するかどうかを吟味する必要がなくなり, ルールの保守性が高まる.

2 に関しては概念束で近い場所に位置し, アクセス権限の差が小さいロールに対して提案を行うことができる. 全ての概念でこれを行うと非常に提案数が大きくなってしまうため, 一つのロールのみのセルから複数のロールがまとまっているセルへの統合だけを考える. これを行うことでいくつか施設がある中, ある施設のロールにだけ特定の権限が与えられている, または与えられていないといった不自然なアクセス権限を排除することができる. また, 必要に応じて 1 の統合も適用できるようになる.

3 に関しては上下関係が飛躍しており, 概念束で孤立しているセルにあるロールに対して提案を行うことができる. これを行うことで, 秘匿レベルの低いアクセス権限が中心のロールに 1 つだけ秘匿レベルの高いアクセス権限が付与されている状態といったほかのロールと大きく異なるルールが与えられている場合にそれを排除することができる.

なお, これらに関しては適切である場合も十分ありうるため, 自動的な統合などは行わず, 提案のみを行う.

4.4. ロールの継承階層構造

本研究では FCA を用いて求めたロールの上下関係に基づいて, ロールの継承階層構造を RBAC に導入したアクセス制御モデルを提案している. 例えば, 医療施設の場合, 医者や看護師や受付スタッフは全員従業員であるが, 従業員全員が許可されていることを各ロールに割り当てるのは記述量が多くなってしまう上に, 保守性の面にも問題がある. そこで, 図 5 に示すような継承構造を主体に持たせることで, より体系化することができる. この図では従業員にあるアクセス権限を付与すると医者や看護師など, その下位のロール全てにそのアクセス権限が付与されることになり, 保守的な運用を行うことができる.

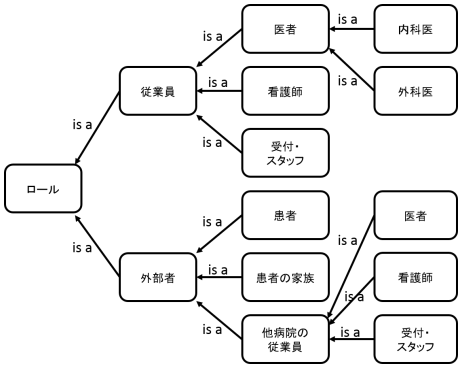

図 5: ロールの継承階層

5. 実験

今回, 病院同士での施設間アクセスを想定して, ロール間の関係を表す概念束を出力する実験を以下の条件下で行った.

- FCA を適用する際, 対象を「主体 (ロール名)」, 属性を「アクセス対象と操作のペア」とする.
- 対象と属性の関係については図 6 で示すものとする

また, 実験で使用したプログラムの中で Concept Explorer FX [4] の一部を使用している. 図 6 の内容を CSV 形式で与えたとき, 今回の実験は図 7 で示すような結果になった.

roletable	担当患者のカルテ閲覧	担当患者のカルテ編集	担当外患者のカルテ閲覧	担当外患者のカルテ編集	担当患者の検査予定閲覧	担当患者の検査予定編集
A病院の医者	○	○	○	○	○	○
B病院の医者	○	○	○	×	○	○
C病院の医者	○	○	×	×	○	○
A病院の看護師	○	○	○	×	○	○
B病院の看護師	○	○	×	×	○	×
C病院の看護師	○	○	×	×	○	×
A病院の薬剤師	○	×	○	×	×	○
B病院の薬剤師	○	×	×	×	×	×
C病院の薬剤師	×	×	×	×	×	×

図 6: 対象と属性の関係

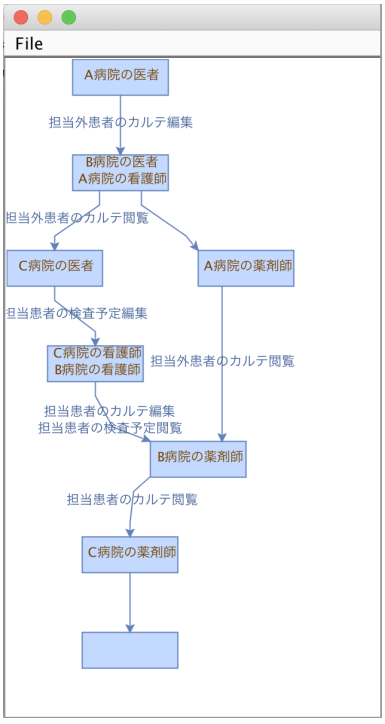

図 7: ロール同士の関係

この図からロール同士の関係を視覚的に読み取ることができる. 例えば,C 病院の薬剤師のアクセス権限に「担当患者のカルテ閲覧」を加えることで B 病院の薬剤師のアクセス権限と同じになり, 比較的近い内容のロールであることや, B 病院の看護師と C 病院の看護師はアクセス権限が全く同じロールであり, 統合して考えることができることや, A 病院の薬剤師は他のロールたちとフローが異なっており, 本当に適切なアクセス権限であるのか吟味する余地がある可能性があることなど, 多くのことが読み取れ, ルールの洗練化に役立てることができる.

また, 主体のアクセス権限の高さや, アクセス権限の秘匿レベルの高さを読み取ることもできる. 例えば. 最下位の最も特化されたロールである「A 病院の医者」は最も多くの権限を与えられており, 高いアクセス権を持っていることがわかる. さらに,「担当外患者のカルテ編集」や「担当外患者のカルテ閲覧」は比較的特化されたロールにのみ付与されていることから, 担当外患者のカルテへのアクセスは秘匿レベルが高く, 限られた人しかアクセスが許可されていないこともわかる.

この概念束は CSV 形式で与えたアクセス権限が変わるたびに他の設定などを変えることなく半自動的に書き換えることができるため, ロールやアクセス対象などの変更にも柔軟に対応することができる. さらに, アクセス制御に関しては継承階層構造の考え方を導入しているため, アクセス対象の追加があっても保守性を保ったままルールの追加をすることができる. 例えば,「担当患者の投薬情報閲覧」というアクセス内容が追加された場合, 図 7 での B 病院の薬剤師にそれへのアクセス権限を付与することで, C 病院の薬剤師以外の全てのロールにそのアクセス権限を付与することができ, 付与の漏れなどが生まれにくくなる.

6. まとめ

組織間でのアクセスを想定した際,FCA を用いてロールの関係の可視化を行った場合の結果を医療機関での簡単な例を用いて示した. 今回の実験結果からどのようなルールの洗練化が考えられるかを読み取ることができたが, これを概念束の内容から提示できるよう検討していきたい.

参考文献

[1] R. S. Sandhu, E. J. Coyne, et al: “Role-based access control models”, IEEE Computer, vol.29, no.2, pp.38-47, 1996.

[2] Rudolf Wille: “Restructuring Lattice Theory : An Approach Based On Hierarchies Of Concept”, Ordered Sets，vol.83, pp.445-470, 1982.

[3] Yevtushenko: Concept Explorer version 1.3, http://sourceforge.net/projects/conexp

[4] Francesco Kriegel: Concept Explorer FX, https://francesco-kriegel.github.io/conexp-fx/

[5] 鈴木治，室伏俊明 :“形式概念分析 -入門・支援ソフト・応用-”日本知能情報ファジィ学会誌 vol.19，no.2，pp.103?142，2007.

[6] Ravi Sandhu : “Role hierarchies and constraints for lattice-based access controls”, ESORICS : Computer Security ? ESORICS 96 pp. 65-79, Springer, 1996

[7] S. Chandra Mouliswaran ; Ch. Aswani Kumar ; C. Chandrasekar : “Representation of multiple domain role based access control using FCA”, IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) pp.1-6, 2015