電子的に流通する構造化情報へアクセス制御ポリシを定義するための利用者指向インタフェース

User -Centered Interface to define Access Control Policy for Structured Documents on the Internet

雨宮美奈帆† 飯島正‡
Minaho Amemiya† Tadashi Iijima‡
†慶應義塾大学　理工学部
† Department of Science and Technology, Keio Univ.

要旨

最近の情報システムでは，リレーショナルモデルよりも複雑な構造と多彩なタイプのデータが混在したコンテンツを使う機会が急速に増え，複雑な構造を持たせたまま電子的に流通させる必要性も高まっている．そうしたコンテンツに対してもアクセス制御機構を導入することは，不可欠である．

本発表では，XML で構造化された電子カルテ等の構造化文書へ，XACML(XML Access Control Markup Language)とその実現アーキテクチャに従って，RBAC(Role-Based Access Control)，ABAC(Attribute-Based Access Control),および，それらの拡張モデルに基づいたアクセス制御ポリシを定義するための利用者指向のインタフェースを備えた支援ツールの設計とプロトタイプに関して報告する．同プロトタイプシステムでは，QBE(Query By Example)等で提案されたいわゆる例示インタフェースの考え方の適用を試みている．

1. はじめに

一般に情報システムでは複数人で情報が共有されるが，個人情報が様々な人によって閲覧され書き換えられるためアクセス制御が重要である．近年では，そうした情報システムが組織内専用の通信システムで閉じることなく，広く，インターネットを介して相互利用されるようになってきた．さらに，個人情報はその当人の所有物であり，必ずしも専門技術を備えていない本人がインターネットを介して自由にアクセスできるとともに，情報のセキュリティ制御を自由に設定できることが必要となりつつある．また，最近の情報システムでは，従来よりも複雑なデータを扱う機会が増え，個別の情報ごとに固有の複雑なデータ構造を備えた情報に，確実で的確なアクセス制御を設定できることが求められている．

たとえば，医療機関で作成蓄積されるカルテ（診療記録）のような情報は，患者の氏名/住所/生年月日といった個人情報から，医師の所見，時系列的な治療行為の記録，投薬記録/指示，画像を含む検査結果といった多様なタイプの情報が構造を持って含まれている．こうした情報の一部が，一つの医療機関の中の各診療科の診察室，検査室，経理部，病棟といった各部署で共有されるばかりではなく，他の医療機関や，保健所，健康組合といった外部機関との間で流通されることが推進されている．また，そのカルテの所有者は，そのカルテを作成した医療機関であるという考え方から，その対象となる患者に帰属するという考え方に移り変わっており（別途，医師が著作権を主張するケースもありうる），患者本人の管理下で本人の意思に基づいて開示されるように変化してきている．

しかし，一般に，アクセス制御ポリシの定義はそう簡単なものではない．たとえば，XML 文書のための XACML というアクセス制御ポリシ記述言語では，ポリシは，XML の形式で記述し，複雑な構造を持った文書に適用される場合，実際にどのような制御が定義されているのかが分かりにくい．

そこで本論文では「ポリシの視覚化と例示プログラミングによる定義」のための手法を提案する．ポリシ定義者が実際にアクセス制御の対象となる画面でアクセス制御の例を与えることによって，アクセス制御ポリシ定義を生成する．定義者は実際の画面に対して具体的な制御を定義するだけでよいので，より容易にアクセス制御ポリシを指定できると考えている．実際に電子カルテを例として上記システムを構築し，その機能を確認した．現在は，具体例を通したポリシ定義をデータマイニング手法として知られている連関規則(Association Rule)の考え方で，一般化する機構を開発中である．

本論文の構成は以下の通りである．まず第 2 節で本提案に関連した電子カルテ，アクセス制御の概要や XML 文書にアクセス制御ポリシを与える XACML 仕様について紹介する．更に第 3 節で例示プログラミングの考え方を紹介し本論文で提案するポリシ定義方式について述べる．後続の第 4 節で実装した

プロトタイプシステムを紹介し動作確認による評価を述べ，第 5 節において結論と課題をまとめる．

2. 電子カルテとアクセス制御

本節では提案方式で前提とする電子カルテ，アクセス制御，XACML といった概念について示す．

2.1. 電子カルテシステム

電子カルテシステムとは，医療機関で医師が記録するカルテを，コンピュータ上で電子的に編集・管理し，データベースに保存するシステムである．厚生労働省（旧:厚生省/労働省）は，1999 年に電子カルテを承認した．また 2001 年には e-Japan 構想の一環として電子カルテの普及促進を図るため，「2006 年度までに 400 床以上の病院及び全診療所のうち 6 割以上」という普及目標を掲げた．2006 年度時点での目標達成は実現されなかったが普及率は年々上昇している．また，2011 年度以降、レセプト（診療報酬明細書）のオンライン請求義務化が予定されており，その普及が一層，加速されると予想される．

2.2. アクセス制御

アクセス制御とは, 情報に対するユーザのアクセス可能範囲を制限することである. ある主体（subject）が，対象資源（object）に対して，そのアクセスができるかを許可したり拒否したりすることを指す．本研究で採用しているアクセス制御方式は，職務上の役割（role）によってアクセス権を決定するロールベースアクセス制御（RBAC）を基本にして属性ベースアクセス制御(ABAC)やそれらの拡張モデルに基づくものである．

2.3. XACML

XACML（eXtensible Access Control Markup Language）[1]とは，XML ベースのマークアップ言語で，インターネットを通じた情報アクセスに関する制御ポリシを記述するための言語仕様のことである．2003 年 2 月に XML 関連技術の標準化団体である OASIS（Organization for the Advancement of Structured Information Standards）によって標準化された．XACML は，特定の情報に対して誰が（主体），どのデータ（資源）に，どのような動作（action）が出来るのかを記述することができ，例えばユーザの年齢や職業（ロール）などによってアクセスできる資源や動作を変更することができる．

XACML は，要求に対する許可・不許可を決定する PDP（Policy Decision Point：ポリシ判定部），PEP（Policy Enforcement Point：ポリシ強制部），PAP（Policy Administration Point：ポリシ管理部），PIP（Policy Information Point：ポリシ情報部）の 4 コンポーネントからなり，アクセス制御を施行している(図 1).

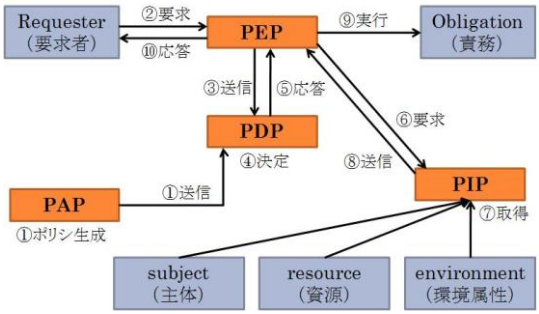

図 1　XACML を用いたアクセス制御モデル

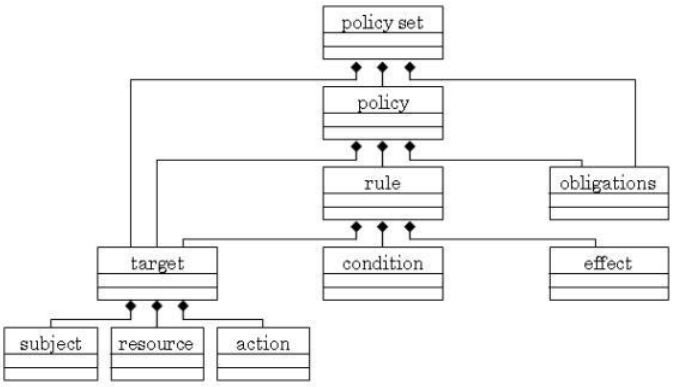

図 2　ポリシ言語モデル[2]

また，ポリシ言語モデルの構造を図 2 に示す．ルールには，「主体が 15 歳以上の場合」などといった条件（Condition）を付加することができ，またポリシやポリシセットには，「上司に確認メールを送る」などといった責務（Obligation）を付加することができる．

2.4. アクセス制御の問題点

XACML によるアクセス制御は，柔軟なポリシを定義することができ，様々なシステムに拡張しやすいという利点があるが，いくつかの問題点がある．例えば，(1)アクセス制御ポリシの記述が難しい，(2)情報漏えいなど不足のないアクセス制御実施が不確実である，といった問題である．

本論文では, これらの問題点の中から「アクセス制御ポリシの記述の難しさ」に焦点を当てる. XACML によるアクセス制御のポリシ定義は，(1)ポリシを記述する XML 文書が複雑である，(2)制御後の画面を具体的に想定しながら記述できない，(3)ポリシ中の制御対象資源（resource）と画面の対象部分が直接結びつかない，といった理由により困難度が高いと考えられる．XACML ではアクセス制御ポリシを XML ファイルへ記述しなければならず，実際の画面と関連付けたり，具体的なイメージを持ちながら定義したりすることが難しい．これらの課題を解決し，簡単に確実性の高いアクセス制御ポリシを定義することが求められている.

3. 例示プログラミングによるポリシ定義

3.1. 例示プログラミング

例示プログラミングとは，ユーザが明示的にシステムに具体例を与えることでプログラムを自動で生成させることである[4]．実用例としては，キーボードマクロや Edition By Example などが挙げられる．キーボードマクロとは，ユーザが実際のキー操作を行いながらその走査列をマクロとして登録できる機構であり，Edition By Example とは，テキストファイルの修正前と修正後をユーザが示すことでシステムに変換規則を推論させるものである．例示プログラミングは，ユーザがプログラムを書くかわりに具体例を与えることで自動的にプログラムを生成するので操作系やスタイルの設計等に有効である[5].

例示プログラミングの利点としては，(1)プログラミングの知識がなくても作成できる，(2)操作に対する具体的な結果を確認しながら作業できる，などが挙げられ，問題点としては，(1)例からのプログラム作成の困難さ，(2)実用的な例示プログラミングシステムはほとんどない，といった点が挙げられる.

3.2. 例示プログラミングによるポリシ定義

第 2 節で示したように, XACML によるアクセス制御の問題点として「ポリシ記述の難しさ」がある. そこで本論文では「ポリシの視覚化と例示プログラミングによる定義」を提案する．従来，XML ファイルに直接記述しなければならなかったポリシ定義を，実際にアクセス制御を行う画面で例を通して定義できるようにした．画面上の文字の濃さ・薄さによって読み書きの許可・不許可を可視化し（図 3），その定義に従うアクセス制御ポリシを XML ファイルとして生成する（図 4）．具体例を通して直観的にアクセス制御のポリシを定義することができ，意図通りアクセス制御を容易に定義できると考えている.

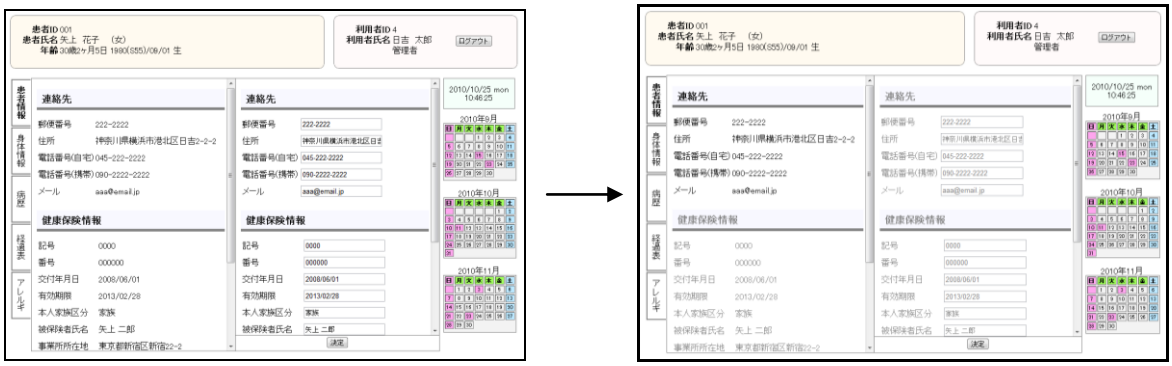

図 3　アクセス制御ポリシの定義画面

図 4　自動的に生成されたアクセス制御ポリシの内容

4. 実装・評価

本提案に際して，電子カルテを例に例示プログラミングによるポリシ定義のためのシステムを実装した．図 5 に示すように XACML が前提としている認証/認可用のアーキテクチャを，オープンソースの“Sun’s XACML Implementation”(http://sourceforge.net/projects/sunxacml/) をベースに実装している．アクセス制御ポリシを画面上で定義すると，PAP において XML 形式のポリシを生成し，そのポリシに従ってユーザのリクエストに対する制御を行っている．現在は Java アプリケーションとしてプロトタイプを実装しているが, Servlet/JSP を用いた Web アプリケーション型の電子カルテシステムを開発予定である．

現状では，下記のような状況での動作確認ができている．

1．画面上で定義した通りにポリシが記述できるかを確認した．ポリシ定義画面において，ロール・対象資源・動作それぞれに関して許可・不許可の設定を行い，ポリシを定義した．

2．定義したポリシ通りにアクセス制御ができているかを確認した．１．の動作を行った後，各ロールでログインし，各資源に対して閲覧及び変更ができるかを試した．結果，１．で定義した通りの挙動を示し，正確にポリシ定義ができていることが確認できた．

今回実装した簡易電子カルテのポリシ定義システムによって，第 2 節で述べた「アクセス制御ポリシ記述の難しさ」という問題を軽減できた．実際の画面で具体的にポリシ定義をすることができ，またプログラミングの難しさも解消することができた．しかし，XML ファイルに直接記述できることを十分に網羅できたわけではなく，ポリシ定義者が熟練者である場合はより柔軟な制御が可能であり，必ずしも本提案が優れているとは言えない．

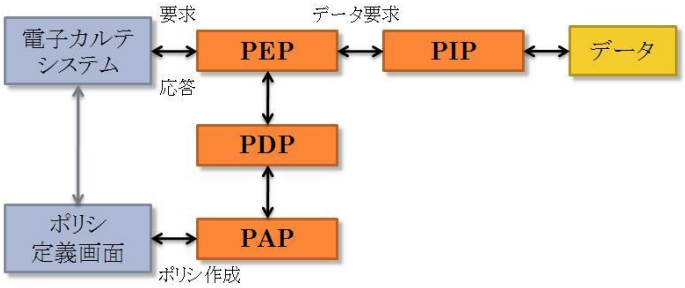

図 5　実装した簡易カルテシステムの概要

5. おわりに

容易なアクセス制御ポリシの定義を目標に，例示プログラミングによるポリシ定義を提案し，それに基づく簡易電子カルテシステムを実装することで，その評価を行った．本来の記述方式に比べより具体的に簡単にポリシを定義することができ，XACML やプログラミングに関する知識が全くなくてもポリシの定義をすることができるようになった．

しかし，課題も残されている．まず，より柔軟なアクセス制御ポリシの定義が必要である．XACML によるアクセス制御は許可・不許可を与えるだけではなく，アクセス条件によって制御を変えたり，責務を課すことでアクセス範囲を拡張できたり，またロール・資源・動作を新規に作成できるといった，柔軟なアクセス制御が可能であるところに特徴がある．その特徴を十分に活かせるポリシ定義ができなければ十分であるとは言えない．この課題に関しては今後も継続して研究していく予定である．また，現在，連関規則（Association Rule）による学習機能を開発中である．

参考文献 (WWW ページの最終確認日:2010 年 11 月 5 日)

[1] OASIS, “XACML 仕様書 2.0,” http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml .
[2] 道村唯夫, “技術解説 -XACML-,” http://www.xmlconsortium.org/websv/kaisetsu/C11/content.html .
[3] MedXML コンソーシアム, “MML Version 3.0 規格書,” http://www.medxml.net/mml30/mmlv3_index.htm .
[4] 増井俊之, “予測/例示インタフェースの研究動向,” コンピュータソフトウェア, Vol.14, No.1, 1997, pp.1-16.
[5] 小柳光生, 小野康一, 堀雅洋, “XSLT スタイルシート生成のための例示インターフェース - 編集モデルと生成ツール - ,” 第 3 回インターネットテクノロジーワークショップ WIT2000, 2000, pp.163-170.