# 電子カルテのためのポリシに基づく動的アクセス制御

# Policy-based Dynamic Access Control for Medical Records

山本由香理† 飯島正†
Yukari Yamamoto† Tadashi Iijima†
†慶應義塾大学　理工学部
† Department of Science and Technology, Keio Univ.

**要旨**

医療現場という緊急性を伴う流動的な状況において，柔軟に対応できるアクセス制御方式を提案する．MML(Medical Markup Language)文書によるデータ交換を前提とした Web アプリケーション型電子カルテに対し，拡張した XACML(eXtensible Access Control Markup Language)を利用して，ロールベースアクセス制御(RBAC)のためのアクセス制御ポリシを規定する．これにより，ある特定の状況下において，基本的なアクセス制御ポリシを，現場ユーザの要求に基づいて一時的に変更することが可能なアクセス制御方式を提案する．ここで基本アクセス制御ルールの動的な変更を引き起こす状況として，救急車搬送などの緊急時や，転院もしくは患者本人の希望によるセカンドオピニオン要求に伴う医療機関間の医療情報交換を想定している．アクセス権限を変更する際には，相応の許認可や義務行為の発生を伴わせることで，不正なアクセスから秘匿すべき情報を保護する．

## 1. はじめに

現在，ある程度以上の医療機関では広く電子カルテシステムが用いられている．2009 年 11 月 2 日には，厚生労働省において「医療情報ネットワーク基盤検討会」第 23 回会合[1]が開催されているが，この会合において，電子化された診療情報を安全にやりとりする際の「なりすまし」等を防ぐ為の認証方法や, 技術的なセキュリティ管理などの事項が含まれた認証用証明書ポリシ案が了承されている. また, 診療録等の保存を行う場所の規定に関しても「民間事業者等との契約に基づいて確保した安全な場所」へと改訂することが了承された．これらの改定は，今後システムの SaaS 化等の流れに電子カルテが対応していく上で，重要なものと認識されている．レセプトのオンライン請求義務化も数年後に迫る中，今や医療現場において，電子カルテシステムの普及利用はさらに促進されることは明らかであろう．その上で，より高度な利用を検討する時期に来ている．

しかし，電子カルテシステムには多くの課題も残されており，アクセス制御の柔軟性の欠如もその一つといえる．そこで本論文では，緊急時への対応や患者の意思に基づいた制御ルールの動的変更を可能とするアクセス制御方式を提案する．この方式は，XML 文書のためのアクセス制御ポリシを規定する XACML(eXtensible Access Control Markup Language)仕様[2][3]における義務(Obligation)記述を具体化することで，義務が満たされた場合には基本的なアクセス制御ポリシを他のポリシに動的に変更することを許すものである．具体的には，通常の ID/Password 方式の認証よりも強度の高い ID カード(RFID)の提示による認証の義務や，電子カルテシステムや電子メール等の外部メディアを介した上位権限者への承認を求める義務などが考えられる．この提案方式を評価するためには具体的事例の蓄積が不可欠であり，本方式を導入した評価用の簡易的な電子カルテシステムを構築中である．既に上述のような義務記述を組み込んだ事例については実装し，その機能を確認した．しかし，こうした利活用の事例は引き続き継続的に蓄積していくことが必要である．

本論文の構成は以下の通りである．まず，続く第 2 節において，本提案方式に関連した前提知識である電子カルテ，アクセス制御等の概念と，XML 文書にアクセス制御ポリシを与えるための XACML 仕様について紹介する．さらに，第 3 節で本論文で提案するアクセス制御方式について述べ，第 4 節では評価用に構築中の簡易的な電子カルテシステムを紹介して，導入して確認できた評価事例を示す．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従来の紙のカルテを電子的なシステムに置き換え, 電子情報としてカルテ（診療録や検査記録など）を編集・管理し，データベースに記録する仕組みである．2001 年に e-Japan 構想の一環として厚生労働省が電子カルテ普及を掲げており，当時「2006 年までに全国の 400 床以上の病院および全診療所の 6 割以上」と設定された目標普及率には現在も達していないものの, その普及率は年々高まっている.

電子カルテ導入のメリットは主に，(1) ペーパレス化によるデータの長期かつ大量の保存が可能になること，(2) 診察のみならず防疫対策策定や研究を目的とした集計および統計処理など，多様な目的で使用する際のデータ処理の容易さ，(3) 医療機関同士や地方自治体などとの医療連携へ向けた診療データ交換の実現，(4) 患者にとって検査画面を見ながら診察を受けることができわかりやすい，といった点が挙げられる.

デメリットとしては，(1) 紙のカルテと比べ操作性が落ちる，それに伴い扱いに習熟が求められること，(2) 停電などの災害時には使用できないこと，(3) データ漏洩等の被害が拡大しやすいこと，(4) システムが高価であることなどが挙げられる.

このように，カルテの電子化においては，データの利用交換が容易であるというメリットと，相反して，データ漏洩の危険性の高さというデメリットが共存しており，その不安感が普及を妨げている部分もある．しかし今後の医療・介護．福祉機関の相互連携の未来像を考えた場合，安全かつ柔軟なデータ交換の実現は不可欠であるといえる.

### 2.2. アクセス制御

アクセス制御とは，システム内の情報へのユーザのアクセス可能範囲を制限することである．具体的には，ある主体(subject)が，どの対象データ(object)に対し，どの種類のアクセスができるか，許可・拒否する機能とみなすことができる．アクセス制御においては，認証，認可，説明可能性という三つの要素が必要となる．アクセス制御における認証とは，ユーザの正当性を検証する作業のことであり，一般的には利用者 ID とパスワードの照合などで行われる．IC カードや生体認証など複数の認証要素との組み合わせで認証強度を上げることが可能であり，その強度はアクセスする情報の重要度に応じて設定される．アクセス制御における認可とは，ユーザがそのシステム上で出来る行為をシステム側が決定することである．アクセス対象，アクセスする人，アクセスする時間帯，アクセスしている場所，アクセス手段の五つの要素に関して決定を行う．例えば，A というファイルに対し，ユーザ B はシステムの置かれた施設内ネットワークから 12 時～24 時までの間アクセスを許される，というような決定がなされる．説明可能性とは，ユーザによってどのような操作が行われたか説明ができることを意味する．たとえばアクセス履歴の取得が可能でなければならない．第 4 節で示す事例では，認証を ID/Password と RFID カードで，認可を XACML の拡張により実施しており，実際に評価用に試作した簡易版の電子カルテシステムに組み込んで，動作を確認している.

アクセス制御には幾つかの種類があるが，今回はロールベースアクセス制御(RBAC)を用いる．RBAC では，主体のロール(役割)に基づいて，オブジェクトへのアクセスを制御する．ロールとは，例えば外科医師，看護婦，などの組織における仕事上の役割のことである．つまり個々のユーザに対してアクセス許可を与えるのではなく，外科医ならばアクセスできる，と云うようにユーザのロールを通して与えるため，各ユーザのアクセス権の管理は各ユーザの適切な割り当てに単純化できるメリットがある.

### 2.3. XACML

XACML（eXtensible Access Control Markup Language）は，XML ベースのマークアップ言語であり，情報にアクセスする際の制御ポリシを記述するためのポリシ記述言語仕様である. XML 関連の標準化団体 OASIS(Organization for the Advancement of Structured Information Standards) により，2003 年 2 月に

OASIS 標準[2]として承認された．SAML（Security Assertion Markup Language）の仕組みを拡張するものとして企画され，XACL（XML Access Control Language）をベースとすることで，認可決定のためのポリシ記述の柔軟性と拡張性を高めたものとなっている．

XACML では特定の情報に対して，誰が（主体），どのデータ（資源）に，どのような動作ができるのかを記述し制御する．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設定できる．「18 歳以上のユーザ」「医師であるユーザ」など，こういった一つ一つのアクセス条件をルールと呼び，このルールに適合した場合に決定する値(許可(Effect)，不許可(Deny)) を結果(Effect) として設定しておく．複数のルールを結合したものをポリシと呼ぶ．

XACML では複数のルールが存在し，状況に応じてそれらを組み合わせて働かせなければならないため，複数ルールの結合アルゴリズムも定義している（具体的には，Permit-overrides (許可優先)，Deny-overrides (拒否優先)，First-applicable (先行優先)といったものがある）．

XACML 仕様においては，ポリシ記述言語の単なる言語仕様を規定する上で前提とする，ポリシを取り扱うアーキテクチャが規定されており，コンポーネントとして，(1) PDP（Policy Decision Point）：定められたポリシに従い PEP が示したアクセス要求が正しい権限を持つものかどうかを判断し，許可，不許可の決定を行う「ポリシ判定部」，(2) PEP（Policy Enforcement Point）：アクセス要求者からの要求を受け，PDP に資源へのアクセス判断を問い，PDP の示す許可，不許可の決定に基づき資源へのアクセスの制御を実施する「ポリシ強制部」，(3) PAP（Policy Administration Point）：PDP が参照するアクセス制御のルールを定義し，ポリシやポリシ集合を生成する「ポリシ管理部」，(4) PIP（Policy Information Point）：PEP の問合わせに対し，主体や資源や環境に関する属性値を提供する「属性情報提供部」，がある．また，PEP と PDP 間で，認可要求と認可決定（応答）の正規化したプロトコルの構文を Context と呼ぶ．それらコンポーネント間でのデータの流れを図 1 に示す．図 1 において PEP(ポリシ強制部)から⑥として義務行為の強制（と確認）を行うコンポーネント(Obligation)が与えられている．これが本論文における提案方式において具体化する部分である．

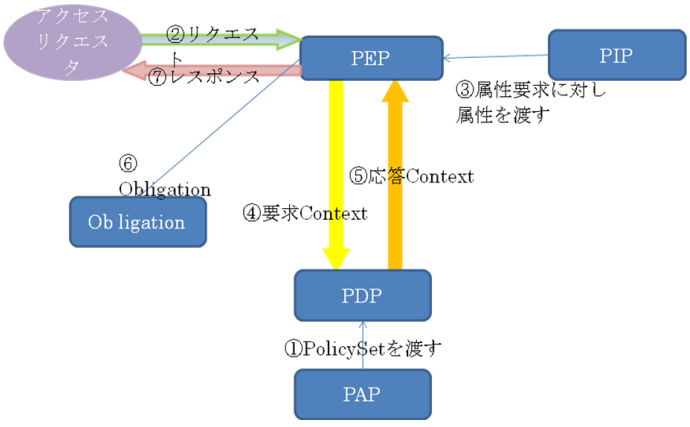


図 1　XACML のデータフローモデル

## 3. 義務記述による動的アクセス制御方式

第 1 節で示したように，電子カルテにはアクセス制御の柔軟性が足りないという問題点がある．そこで本論文では「義務行為を伴う動的なアクセス制御方式」を提案する．これは，XACML における Obligation を具体化したものであり，　基本的なアクセス制御ポリシはロールベースアクセス制御に基づいて行うが，特定の状況下においては，義務行為の実施と引き換えに動的なアクセス制御ポリシの変更を可能とするものである．具体的な状況として(1)緊急時対応，(2)現場の判断，(3)患者の希望，といったカテゴリの事例について検討している．

まず，一つ目の「緊急時対応」というカテゴリの状況は，患者の救急搬送などが該当し，その場合，緊急時には通常と異なるポリシ生成を行う．例えば他の医療機関からの情報の授受や，同病院の他の科

の情報の授受を可能にする．外科医が，患者が現在内科に掛かり薬を服用していることがわかった場合に，薬の飲み合わせなどを勘案するために許可を求める．この場合，緊急事態であるという条件の証明や上位の職位者からの承認を必要する．

二つ目の「現場の判断」というカテゴリの状況では，現場の医師などの希望があった時に，上位職種からの許認可を得るといった義務行為の実施によって一時的にアクセス権限の拡大する．例えば，担当医不在時の診察において，必要に応じ上位職種（院長等）や担当医の承認により，他の医師による担当医権限でのカルテ操作を許す

第三の「患者の希望」というカテゴリの状況では，医療情報の主体である患者の希望に基づいて，予め規定した範囲内において，アクセス権限の変更を可能にする．例えば，患者の希望により担当医でない医師にも，担当医同等の情報閲覧権限を与えることができる．但し予め情報保護の観点からシステム側で規定されたアクセス範囲を超えない範囲での裁量とする．

このような状況に対応するために，その状況ごとの承認，認可に必要な義務記述(Obligation) の提案を行う．義務記述(Obligation) とはポリシ言語において，ポリシが認可されたときに PEP が行わなければならない義務のことであるが，ここでは，関係者(ステークホルダ)に対して実施を求める行為（義務行為）に相当し，PEP には(1)関係者への義務行為の遂行を促し，(2)義務行為の遂行を確認する，といった機能が必要となる．本提案には Obligation 記述のための書式やオントロジを含むが，本論文では紙数の都合上，詳細を省く．基本的な書式は下記のような Obligations タグで囲んで記述する

```
<Obligations>
  <Obligation Id="activity:askApprovaltoReadTreatmentRecord"  FulfillOn="Permit">
    ここに，activity を書く．
  </Obligation>
</Obligations>
```

## 4. 評価用の簡易電子カルテシステム

本提案を評価するために，簡易電子カルテシステムを構築中であり，前述のような一部の義務記述への対応を組み込んで，その動作を確認した．この簡易電子カルテシステムは，あくまで本提案の評価用であるため，実運用に必要な機能の多くを実装する予定はない．図 2 に示すように XACML が前提としている認証/認可用のため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/)をベースに実現し，主に Servlet/JSP で実装されている Web アプリケーション型の電子カルテシステムから利用している．この電子カルテシステムでは，医療情報の国際標準規格 HL7[5]に準拠した MML ( Medical Markup Language)[4]で記述されたデータ交換用の電子カルテデータを読み込むことができ，そのスキーマに対応した形で，JAXB(The Java Architecture for XML Binding)を利用して内部オブジェクトにマッピングする．MML は地域医療連携システム Dolphin Project でも実装されているフォーマットである[6]．さらに，そのマッピングに対応する形で，リレーショナルデータベース JavaDB へもマッピングさせることを試みている．これにより，XACML によるポリシ記述を電子カルテ内のデータに適用させることを目指している．

現状では，下記のような事例において動作確認ができている．

1．まずはユーザのロールに応じて，適切な RBAC ができているかを確認した．今回は内科医・外科医などの医師ロールと事務員・患者などの医師でないロールで大別してその権限を変更した．結果，定められたポリシに従って，適切な RBAC が実現できていることを確認できた．
2．次に緊急時，現場判断が下された時に一時的にアクセス権限を拡大する方法について検証した．今回はその際の許認可操作の代わりとして，RFID カードの認証と，アクセス権限を拡大したという報告として院長への自動的なメール連絡の二つの行為を義務行為（Obligation）として義務付けた．
（ID カードの読み取りには，Phidgets 社(http://www.phidgets.com/)の RFID リーダを利用している．
今後はリーダが安価で入手できる Felica の利用や指紋認証の導入も計画している）

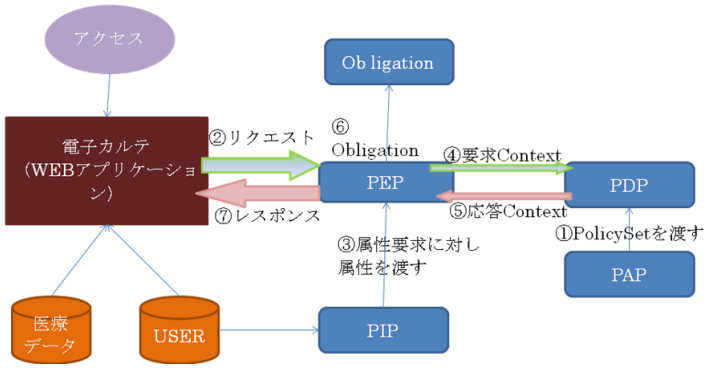


図 2　構築中の評価用簡易版電子カルテシステム

## 5. おわりに

電子カルテの柔軟なアクセス制御を目指して，緊急時にアクセス権限の動的変更を行い患者情報の提供を可能とする動的アクセス制御方式を提案し，評価用の簡易電子カルテシステムに組み込むことで，その動作を確認した．

しかし，残る課題も多い．ます，事例として義務行為を継続して蓄積していくことが必要である．また, 本論文で検討用に取り上げた事例についても, その妥当性についてはより深く検討する必要がある．例えば，(1) 通常時の ID/Password に追加して認証強度の高い RFID カードによる認証，(2)メールによる上位権限者への承認要求の送信と承認受領，といった義務行為を提案し実装したが，そうした義務行為自体を分類し体系化する必要がある．さらに，本研究で蓄積している単純化した事例と，実際の医療現場における現実との乖離を認識し，その差を埋めていかねばならない．たとえば，緊急性の有無の判断は，容易にできるものでもなく，誰もの判断が一致するとも限らない．多くの医療従事者からのヒヤリングによる情報収集や，法令順守といった面での整備も必要となる．また，医療機関毎に組織構造や職位区分が異なっていたり，カルテのフォーマットが異なっていることは当然ありうることであるが，医療連携のためのアクセス制御のためには，前提としているロールベースアクセス制御ロールのすり合わせやカルテ書式のマッピングが必要となる．これら課題への対応は引き続き継続して行っていく予定である．

## 参考文献

[1] 医療情報ネットワーク基盤検討会，独立行政法人　福祉医療機構
http://www.wam.go.jp/wamappl/bb13GS40.nsf/aCategoryList?OpenAgent&CT=30&MT=030&ST=080
[2] OASIS:　“XACML 仕様書 2.0,” http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml　(2005)
[3] 岩井原 瑞穂: “XML 文書のアクセス制御,”　オペレーションズ・リサーチ, Vol.50,　No.6,
日本オペレーションズリサーチ学会 (**2005**).
[4] 特定非営利活動法人 MedXML コンソーシアム: MML Version 3.0.2 規格書,
http://www.medxml.net/mml30/default.html　(2009)
[5] 木村 通男: “医療情報の国際標準規格 HL7 : その意義，解決される問題点, ”
情報管理, Vol. 50,　No. 5,　pp.258-265 (2007).
[6] 吉原博幸: “Dolphin Project 地域医療連携システムの現状,” 治療, Vol.90,　No.2,
日本医療ネットワーク協会(2008).