クラウド上に配備できる電子化文書管理システムの構築

Building an Electronic Document Platform which is deployable on Cloud Computing Environment

山上燦† 飯島正‡
San Yamagami† 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，より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．例えば，電子書籍は，従来の紙の書籍の制約を越えて，対話性と細粒度セキュリティが求められると考えられる．そうした要求を満たす電子化文書管理システムをクラウド環境上に展開することを提案する．

本論文では，今後，患者個人が管理し複数の医療機関で共有利用されることが期待される電子カルテ(EMR)，個人保健情報(PHR)を例として，主にセキュリティの観点から，構築中の試作システムを紹介する．

1. はじめに

一般に情報システムでは，複数の利用者の間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プライバシを保護する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．

特にセキュリティに関して慎重な扱いが求められる電子化文書として電子カルテが考えられる．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．しかし，従来はそうした電子カルテ（診療録）などは，外部機関と共有されることは少なく，一つの医療機関の管理下に置かれるのがごく一般的であった．しかし，こうした高いセキュリティを求められる情報の一部が，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，近年では推進されている．

また，カルテの所有者（所有権保持者）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りつつあり（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このことは，患者本人が複数の医療機関で受診しセカンドオピニオンを得る際にも有用であるとされ，また同じような検査を複数の医療機関で繰り返し受けることを避ける意味でも有用性が高いと考えられている．しかし，特に情報技術に関してトレーニングを受けていない患者本人が自らのカルテ情報を手元のハードディスクなどで管理することは困難であることは容易に想像がつく．そこで，電子カルテバンクといったビジネスが成立し，情報管理を委託する可能性が考えられる．

電子カルテは，高いセキュリティ品質が求められる，ある意味極端な事例であるが，一般に，遠隔地からも電子的なメディアを介してアクセス化可能な，電子書籍を含む電子化文書には，肌理細やかなセキュリティポリシーが適用できることが望まれている．そこで，あえて電子カルテを取り上げることで，電子化文書のセキュリティに関して多面的にとらえることを試みる．

そこで本論文では，利用者の役割に基づいた細粒度のアクセス制御ポリシを定義し，クラウドサーバ上で共有利用するための環境を構築のための手法を提案する．単なるロールによるアクセス制御のみならず，属

性に基づいたルールの定義，さらにはさまざまなアクションへの拡張を定義することで細粒度のセキュリティモデルを構築することを考える．

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，クラウド環境の概要について紹介する．更に第 3 節で細粒度アクセス制御ポリシ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 節で実装した電子カルテ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・クラウドコンピューティング

前提とする電子カルテ，アクセス制御，クラウドコンピューティング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).

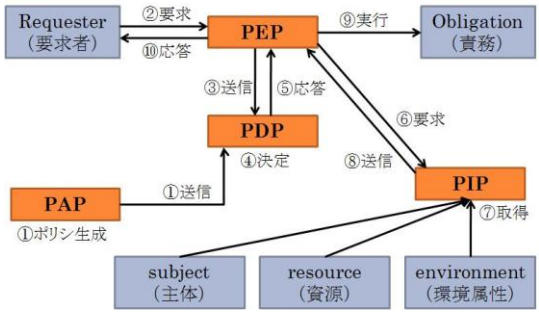

図 1　XACML を用いたアクセス制御モデル

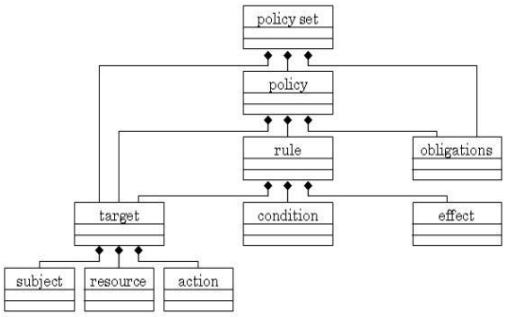

図 2　ポリシ言語モデル[2]

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. クラウドコンピューティング

クラウドコンピューティング（以下，クラウド）とは，ネットワーク上に存在するサーバが提供するサービスを，それらのサーバ群を意識することなしに利用できるというコンピューティング形態のことである．クラウドの概要図を図 3 に示す．クラウドは「アプリケーション」と「サーバ」の 2 つの層を内包している．

アプリケーション層の事例としては，Google 社の「Gmail」や「Google カレンダー」などクラウドのサーバを利用したアプリケーションが挙げられる．サーバ層の事例としては，Google 社の「Google App Engine」や Amazon 社の「Amazon Web Services」など大量の資源を備えたサーバ環境の利用が挙げられる．クラウドコンピューティングの利点としては，(1)情報の共有が容易，(2)開発コストが低い，(3)ビジネスのスケーラブルな拡大・縮小に伴って経営資源としてのハードウェアを購入/廃棄するリスクが低減する，などが挙げられる．一方, 欠点としては(1)セキュリティの不安 (情報漏洩のリスク), (2)サービス停止のリスクなどが挙げられる．

電子カルテといったデータを，クラウド環境で取り扱う利点は大きい．一つは共有の促進であり複数の医療機関からの参照更新が容易となる．もう一つは，物理的なハードウェアと，データとが切り離されることで地震等の災害によるハードウェア資産の損傷の影響を受けずに，多重化されたデータが遠隔地で安全に保持される可能性が高まることである（2011 年 3 月 11 日の東日本大震災での津波などによって，いくつかの自治体や医療機関において紙媒体の情報が失われたが，そうした損失を軽減する効果が期待される）．

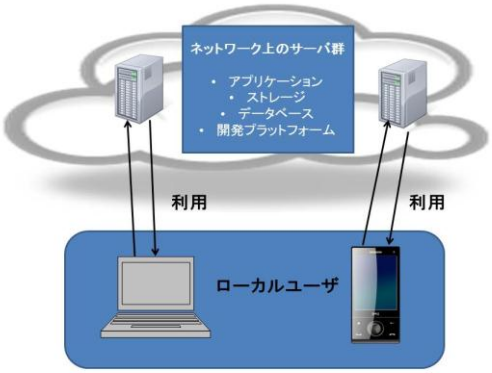

図 3　クラウドの概要図

3.　細粒度アクセス制御ポリシ定義

細粒度アクセス制御ポリシとは，通常のロールベースアクセス制御（RBAC）を基本にして，さらに細かい粒度でルールを定義することを意味する．アクセス制御の対象である，主体・資源・動作それぞれにおいて，モデルを拡張する．主体では，「医師」，「看護婦」，「事務員」などのロールが想定されるが，「どこの科に所属しているか」や，「対象患者の担当医であるか」などの属性情報に関する記述がなされる．資源においては「個人情報」や，「診療情報」などの粒度から更に細分化し，「電話番号」や，「住所」など粒度を対象とする．動作では，「Read」や，「Write」だけでなく，「上書き」，「変更」，「削除」などの動作が対象となる．

また更なる拡張として，緊急時等におけるアクセス権限の強度の変更を取り扱う．たとえば，「患者の担当医の許可が得られれば」「病院長の許可が得られれば」「患者本人が未成年の場合に保護者の承認が得られれば」といった条件付きのポリシにおいて，条件を満たす義務を課すことで，アクセス権限の対象範囲を変化させることを可能にする概念である．これは，XACML が本来持つ義務記述(Obligation)の機能をベースに導入が可能である．実際に，アクセスポリシを定義しアクセス制御を実行した様子を図 3～5 に示す．図 3～5 の順に，ロールが「医師」，「看護婦」，「事務」の場合の個人情報の見え方/操作権限が見て取れる．XML で表される情報（資源）に対して項目 1 つ 1 つにルールを定義することで，細粒度でアクセス制御を実施する．

図 3 ロール＝医師の場合

図 4 ロール＝看護婦の場合

図 5　ロール＝事務の場合

4. 実装・評価

本提案に際して，電子カルテを例に電子カルテ文書共有のためのシステムを実装した．実装したシステムのアーキテクチャを図 6 に示す．サーバーサイドは Java 言語，クライアントサイドは MXML と ActionScript 言語を使用した．セキュリティの部分では， 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．クラウド環境は，Google 社の「Google App Engine」プラットフォームを使用． 現時点では，対象主体は「医師」・「看護婦」・「事務」，対象資源については氏名などの「個人情報」を含む XML 文書，対象動作については，「閲覧」と「書き込み」のみを定義している．

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．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．具体的には，各ロールで ログインし，ポリシ通りの動作ができるかどうか確認した．
2．クラウド環境にて，画像も含め正しくデータが保存されているかを確認した（図 7）．具体的には，配備したアプリケーションのデータストア管理ページにて，エンティティが保存できているかを確認した．
3．電子カルテのコンテンツ記述のスキーマとしては，MedXML コンソーシアムの電子カルテシステム間の診療情報の交換のためのマークアップ言語 MML 仕様[3]を参考にした記述を使っている．

本稿執筆時点では，今回実装した電子カルテシステムによって，クラウド環境のもとで，電子化文書の共有ができる基盤が整備できた．しかし，セキュリティに関する検証は，未だ十分ではない．

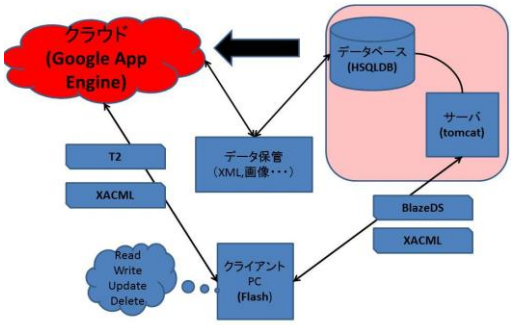

図 6　実装した電子カルテシステムの概要

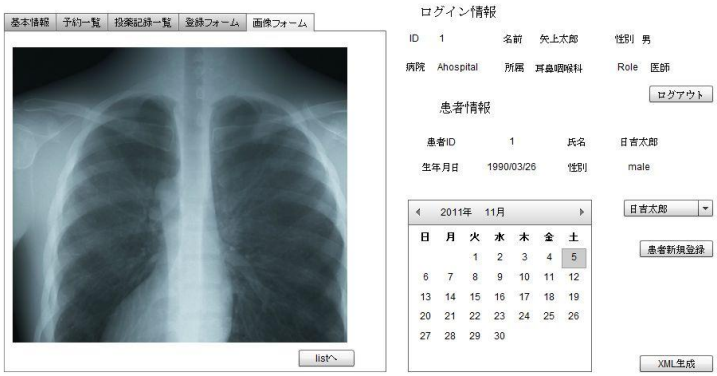

図 7 実装した電子カルテの画面（画像を含む）

5. おわりに

クラウド上に配備できる電子化文書共有システムの構築を目標に，そのシステムアーキテクチャやセキュリティ記述を提案し，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．クラウド上に配備できることで，より広範囲での文書共有が実現可能となった．

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とそのポリシ強制機構の実現が必要である．XACML によるアクセス制御は単に許可・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義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への拡張に特徴をもち，それを本研究では更に進めることを目指している．その具体的な定義の拡充と，実現性に関する検証が，直近の課題である．

参考文献

[1] OASIS, “XACML 仕様書 2.0,” http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml .
(最終閲覧/確認: 2011 年 11 月 4 日)
[2] 道村唯夫, “技術解説 -XACML-,” http://www.xmlconsortium.org/websv/kaisetsu/C11/content.html .
(最終閲覧/確認: 2011 年 11 月 4 日)
[3] MedXML コンソーシアム, “MML Version 3.0 規格書,” http://www.medxml.net/mml30/mmlv3_index.htm .
(最終閲覧/確認: 2011 年 11 月 4 日)
[4] Google,”Google App Engine,” http://code.google.com/intl/ja/appengine/ (最終閲覧/確認: 2011 年 11 月 4 日)