

医療・健康情報の利用許諾モデルの提案

藤田 邦彦[†]

塚田 恭章[‡]

[†] 日本電信電話株式会社
NTT コミュニケーション科学基礎研究所
243-0198 神奈川県厚木市森の里若宮 3-1
fujita.kunihiko@lab.ntt.co.jp

[‡] 日本電信電話株式会社
NTT コミュニケーション科学基礎研究所
243-0198 神奈川県厚木市森の里若宮 3-1
tsukada.yasuyuki@lab.ntt.co.jp

あらまし EHR に代表される医療・健康情報活用サービスにおいては、重要な個人情報が含まれることから漏洩を防ぐ必要がある反面、適切な医療行為を受けるために医師や看護師などの医療情報取扱者への適切な開示が必要である。本稿では、医療情報を患者が権利を保有するコンテンツとみなし、医療情報取扱者に対して患者が利用を許諾するというモデルを提案する。本モデルでは、医療情報へのアクセス権が適切に設定されることは、対応する利用許諾の互換性として定式化される。互換性の厳密かつ機械的判定のため、利用許諾は一階述語論理の枠組みで記述される。

A Proposal of License Model for Medical and Healthcare Information Services

Kunihiko Fujita[†]

Yasuyuki Tsukada[‡]

[†]NTT Communication Science Laboratories,
NTT Corporation
3-1 Morinosato Wakamiya, Atsugi-shi,
Kanagawa Pref, 243-0198 JAPAN
fujita.kunihiko@lab.ntt.co.jp

[‡]NTT Communication Science Laboratories,
NTT Corporation
3-1 Morinosato Wakamiya, Atsugi-shi,
Kanagawa Pref, 243-0198 JAPAN
tsukada.yasuyuki@lab.ntt.co.jp

Abstract In medical information services such as EHR, it is necessary to prevent information leakage because important individual information is involved. On the other hand, it is also necessary to achieve an appropriate release of information to medical information handlers such as doctors and nurses. In this study, we propose a model in which (1) medical information is considered to be contents to which patients retain their rights, and (2) patients license medical information for its handlers. In our model, appropriate settings of access rights to medical information are formulated as corresponding license interoperability. To verify license interoperability strictly and automatically, licenses are expressed in first-order logic.

1 はじめに

2009 年 7 月に政府の IT 戦略本部によって策定・公表された i-Japan 戦略 2015[1] においては、三大重点分野の一つに医療・健康分野が挙げられ、日本版 EHR (仮称) が言及されている。EHR とは Electronic Health Record の略であり、医療情報のネットワーク化や情報共有のた

めのサービスなどを指す。EHR において扱われる情報は、第一に、医療機関が管理するカルテ・処方箋・調剤録などの医療情報である。この他に、フィットネスクラブなどで行った運動の内容や、歩数・体重・心拍数・血圧の記録などの健康情報を、両者の密接な関連を考慮して広義に EHR と呼称して考える場合もあれば、健康

情報を扱うサービスを PHR (Personal Health Record) として、狭義の EHR とは別物として議論する動きもある。

このような医療・健康情報活用サービスを実現するには、個人に帰属する医療・健康情報を、医療従事者などにどのように適切に開示できるようにするかが重要な検討課題となる [2]。i-Japan 戦略 2015 で示されている日本版 EHR (仮称) の基本構想においても、医療過誤の低減や過去の記録に基づいた継続的医療、不要な検査の回避、セカンドオピニオンの活用のため、「個人が医療機関等により入手・管理する健康情報を医療従事者等に提示する」ことを目指しており、医療情報を保有・管理する主体が医療機関などから個人へと移行することを志向している。一方で、医療・健康情報はプライバシーに関わる重要な個人情報である。取り扱いのミスが個人にとって大きな損害につながる場合もあり、その流通と開示は必要最小限に留めることも求められる。そのため、従来型の個人情報を扱うシステムにおいては認証技術により本人確認を行い、個人に係る情報はその個人のみが参照することが一般的であった。

日本版 EHR (仮称) で目指しているサービス実現のためには、医療従事者が自身のアカウントの権限において、個人の医療・健康情報を参照・活用する事が必要である。このため、基本的なセキュリティ対策に加えて、情報にアクセスできる他者を厳密に制御できなくてはならない。すなわち、個人が情報開示したい他者を適切かつ簡単に指定でき、その個人の意図を正しく反映した情報アクセス制御が必要である。またその際、EHR サービスが公共サービスとしての性質を持つことから、IT リテラシの高いユーザだけでなく、高齢者や子供・乳幼児の利用を考えると、他者による設定代行のしくみも必要であると考えられる。

本稿においては、他者に医療・健康情報を開示して活用する方法について、以上のような要件を整理しながら利用許諾モデルを提案する。本稿の構成は以下の通りである。2 章では、医療情報活用サービスにおいて求められる要件について検討する。3 章では、2 章で挙げられた要件を実現する方法として、医療情報の利用許諾モデルを提案する。4 章では、3 章の提案モデルに基づき、医師・看護師・技師・医療事務職

の利用許諾の例を挙げる。5 章では、提案モデルを RBAC (Role Based Access Control) と比較して議論する。最後に 6 章で結論と今後の課題について述べる。

2 要件

1 章で述べた議論に基づけば、医療情報活用サービスにおいて求められる要件は、以下のようになるとまとめられる。

要件 1 医療情報の利用の権利は第一義的には患者が有する。

要件 2 患者の許諾に基づき、他の医療情報取扱者が医療情報を利用することができる。

要件 3 患者による許諾の手続きの実施が困難な場合、当該手続の代行の手段が用意されている。

ここで、要件 3 が設けられている理由について説明する。要件 1,2 に基づく場合、利用許諾の付与の様子は図 1 に示す例のようになる。しかし、一般に患者は、看護師や技師が、医療情報のどの項目を閲覧したり編集したりするか、アクセス権を設定するに足る十分な知識を持っていないのが通常である。また、一般的に IT リテラシの低い傾向にある高齢者や子供・乳幼児による本サービスの利用を考えると、他者による設定代行の仕組みも必要であると考えられる。

この要件 3 を実現するため、本稿では、医療並びに本サービスに関する知識を持つ「かかりつけ」の医師に、患者が、通常の医療情報の利用許諾を与えるとともに、他の医療情報取扱者に対し当該医師が利用許諾を与える、いわゆる再許諾の権利を与える、という方法を提案する。この方法により、許諾の手続きの代行手段を実現できる。この場合の利用許諾の付与の様子を図 2 に示す。

以上の要件を満たすモデルを次章以降で説明する。

3 提案モデル

本稿では、医療情報を患者が権利を保有するコンテンツとみなし、医療情報取扱者に対して

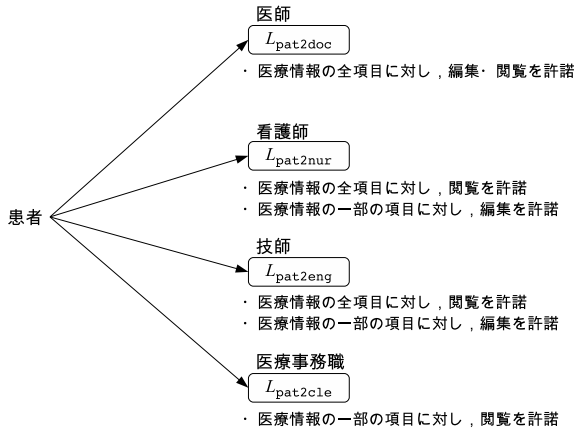


図 1: 患者が各医療情報取扱者に対して、直接に医療情報の利用許諾を与える場合

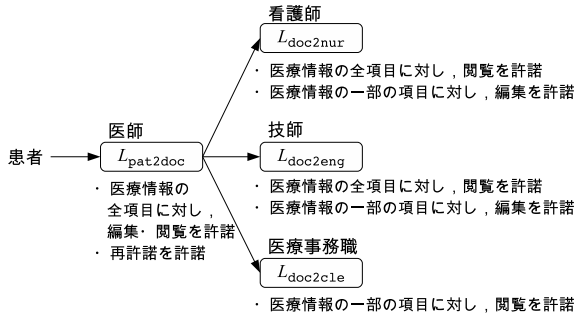


図 2: 患者が医師に対して、医療情報の利用許諾と、再許諾（医師が他の医療情報取扱者に対して、医療情報の利用許諾を与えること）の権利を与える場合

患者が利用を許諾するというモデルを提案する。本モデルにおいては、「適切なアクセス権の設定＝利用許諾の互換性成立」を基本概念とする。互換性の厳密かつ機械的判定のため、利用許諾の内容は一階述語論理の枠組みで記述される。

3.1 構文規則

利用許諾を一階述語論理で記述する場合の構文規則を、以下のように定義する。

利用許諾は、次の論理式で表現される。

$$r_1 \wedge \cdots \wedge r_n$$

各 r_i は、ルールを表す。すなわち、利用許諾はルールの連言により表現される。また、ルールは、以下の形をとる。

$$f_1 \wedge \cdots \wedge f_m \rightarrow p$$

ここで、各 f_j は条件を表し、 p は結論を表す。各 f_j は任意のリテラルである。各条件 f_j を全て満たしたときに許諾される権利を表すのが p である。 p は、適用される分野に依存しない一般的な述語 Perm または Owner を用いて、許諾される内容を規定する。Perm(x, w, act, c) は、エージェント x がエージェント w に対しアクション act をコンテンツ c に対して行うことを許諾することを表す述語である。Owner(x, C) は、エージェント x がコンテンツの集合 C の所有者であることを表す述語である。

3.2 対象領域の定義

ここでは定式化の際に使用するソートとなる対象領域を定義する。すなわち、本稿で用いる体系は正確には多種一階述語論理である。

- $D_{contents}$ 医療情報の集合。この集合上の変数として c などを用いる。
- $D_{contents_set}$ 医療情報の有限集合の集合。この集合上の変数として C などを用いる。
- D_{action} コンテンツに対するアクションの集合。複製 (copy)、閲覧 (browse)、編集 (edit) など。この集合上の変数として act などを用いる。
- D_{agents} 医療情報取扱者の集合。患者 (patient)、医師 (doctor)、看護師 (nurse)、技師 (engineer)、医療事務職 (clerk) などに分類される (文献 [3] 表 1 より例を抜粋)。この集合上の変数として $holder, recipient, originalHolder$ などを用いる。

3.3 利用許諾の種類

利用許諾の定式化にあたっては、ロールをアサインする条件が与えられている利用許諾 RAL と、与えられていない利用許諾 L の 2 種類を用意する。医師から看護師への利用許諾を例に、両者の関係を以下に示す。

$$RAL_{doc2nur}(holder, recipient, act, c, C) \iff IsDoctor(holder) \wedge IsNurse(recipient) \rightarrow L_{doc2nur}(holder, recipient, act, c, C)$$

ただし, $\text{IsDoctor}(holder)$ は $holder$ が医師であることを表す述語, $\text{IsNurse}(recipient)$ は $recipient$ が看護師であることを表す述語である。

3.4 互換性の定義

L_1 と L_2 を 3.1 節で定義した構文規則に則って記述された, ロールをアサインする条件が与えられていない利用許諾とする。 L_1 は L_2 に対して互換性を有するとは, 論理的な含意の関係 $L_1 \rightarrow L_2$ が成り立つことと定義する。

3.5 アクションの可否判定

各利用許諾から, 該当するコンテンツに対し, だれがどのようなアクションを実施することができるかを判定する手続きは以下の通りである。具体的な事実の集まりを環境 E とし, 正リテラルの論理積で表されているものとする。環境 E とロールをアサインする条件が与えられている利用許諾 RAL から, $\text{Perm}(x, w, act, c)$ が論理的に導出されることを,

$$E, RAL \vdash \text{Perm}(x, w, act, c)$$

と書く。このとき, E と RAL のもとで, w は c に対して act を実施することを x から許諾される。

4 医療情報の利用許諾の例

図 2 に示す利用許諾の例を, 提案モデルに従い記述した例を以下に示す。また, アクションの可否判定の例と利用許諾の互換性についても述べる。

4.1 各医療情報取扱者の利用許諾例

4.1.1 医師

患者により以下の内容が許諾される。

- ・ 医療情報の全項目に対し, 編集・閲覧を許諾
- ・ 再許諾を許諾

利用許諾 $L_{\text{pat2doc}}(holder, recipient, act, c, C)$

$$\begin{aligned} & (\text{ActType}(act, \text{browse}) \\ & \wedge \text{Owner}(holder, C) \\ & \wedge \text{Element}(c, C) \\ & \rightarrow \text{Perm}(holder, recipient, act, c)) \\ & \wedge (\text{ActType}(act, \text{edit}) \\ & \wedge \text{Owner}(holder, C) \\ & \wedge \text{Element}(c, C) \\ & \rightarrow \text{Perm}(holder, recipient, act, c)) \\ & \wedge (\text{FamilyDoctor}(holder, recipient) \\ & \wedge \text{Owner}(holder, C) \\ & \rightarrow \text{Owner}(recipient, C)) \end{aligned}$$

ただし, $\text{ActType}(act, x)$ は変数 act がアクション x であることを表す述語, $\text{Element}(c, C)$ は c が医療情報 C のフィールドであることを表す述語である。また, $\text{FamilyDoctor}(holder, recipient)$ は, $recipient$ が $holder$ のかかりつけ医であることを表す述語である。

4.1.2 看護師

医師により以下の内容が許諾される。

- ・ 医療情報の全項目に対し, 閲覧を許諾
- ・ 医療情報の一部の項目に対し, 編集を許諾

利用許諾 $L_{\text{doc2nur}}(holder, recipient, act, c, C)$

$$\begin{aligned} & (\text{ActType}(act, \text{browse}) \\ & \wedge \text{Owner}(holder, C) \\ & \wedge \text{Element}(c, C) \\ & \rightarrow \text{Perm}(holder, recipient, act, c)) \\ & \wedge (\text{ActType}(act, \text{edit}) \\ & \wedge \text{Owner}(holder, C) \\ & \wedge \text{Element}(c, C) \\ & \wedge \text{Actable}(recipient, act, c) \\ & \rightarrow \text{Perm}(holder, recipient, act, c)) \end{aligned}$$

ただし, $\text{Actable}(recipient, act, c)$ は $recipient$ が c に対してアクション act を実施することができることを示す述語である。

4.1.3 技師

医師により以下の内容が許諾される。

- ・ 医療情報の全項目に対し, 閲覧を許諾
- ・ 医療情報の一部の項目に対し, 編集を許諾

利用許諾 $L_{\text{doc2eng}}(\text{holder}, \text{recipient}, \text{act}, c, C)$
 $(\text{ActType}(\text{act}, \text{browse}))$
 $\wedge \text{Owner}(\text{holder}, C)$
 $\wedge \text{Element}(c, C)$
 $\rightarrow \text{Perm}(\text{holder}, \text{recipient}, \text{act}, c))$
 $\wedge (\text{ActType}(\text{act}, \text{edit}))$
 $\wedge \text{Owner}(\text{holder}, C)$
 $\wedge \text{Element}(c, C)$
 $\wedge \text{Actable}(\text{recipient}, \text{act}, c)$
 $\rightarrow \text{Perm}(\text{holder}, \text{recipient}, \text{act}, c))$

4.1.4 医療事務職

医師により以下の内容が許諾される．
 ・医療情報の一部の項目に対し，閲覧を許諾

利用許諾 $L_{\text{doc2cle}}(\text{holder}, \text{recipient}, \text{act}, c, C)$
 $(\text{ActType}(\text{act}, \text{browse}))$
 $\wedge \text{Owner}(\text{holder}, C)$
 $\wedge \text{Element}(c, C)$
 $\wedge \text{Actable}(\text{recipient}, \text{act}, c)$
 $\rightarrow \text{Perm}(\text{holder}, \text{recipient}, \text{act}, c))$

4.2 アクションの可否判定の導出例

以下に示す環境において看護師のアクションの可否判定の導出の例を以下に示す．

環境 E

$\text{IsPatient}(\text{originalHolder})$
 $\wedge \text{IsDoctor}(\text{holder})$
 $\wedge \text{IsNurse}(\text{recipient})$
 $\wedge \text{ActType}(\text{act}', \text{browse})$
 $\wedge \text{Owner}(\text{originalHolder}, C)$
 $\wedge \text{Element}(c', C)$
 $\wedge \text{FamilyDoctor}(\text{originalHolder}, \text{holder})$

医師のロールをアサインする条件が与えられている利用許諾を

$RAL_{\text{pat2doc}}(\text{originalHolder}, \text{holder}, \text{act}, c, C)$

とし，看護師の利用許諾を

$RAL_{\text{doc2nur}}(\text{holder}, \text{recipient}, \text{act}', c', C)$

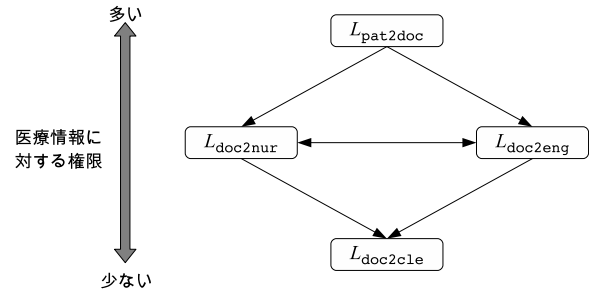


図 3: 利用許諾の互換性

とする（自由変数は適宜置換した．また，以後は引数を省略する）．このとき，医師の利用許諾と環境より

$E, RAL_{\text{pat2doc}} \vdash \text{Owner}(\text{holder}, C)$

となる．この導出結果を環境に含め，これと看護師の利用許諾より，

$E, \text{Owner}(\text{holder}, C), RAL_{\text{doc2nur}} \vdash$
 $\text{Perm}(\text{holder}, \text{recipient}, \text{act}', c')$

となり，医師 holder が看護師 recipient に対し，医療情報 c' にアクション act' を施すことを許諾する，という結論が導出される．

4.3 利用許諾の互換性

第 4.1 節で列挙した各利用許諾について，互換性を分析すると，図 3 が結果として得られる． L_{pat2doc} が医療情報に対するアクセスの権限が最も多く， L_{doc2cle} は最も制限されている． L_{doc2nur} と L_{doc2eng} はその中間に位置し，利用許諾を文法的に解釈した場合は同値である．同値である理由は，通常は看護師と技師では編集できる項目が異なる（例：看護師は血液検査の結果の編集権限を持ち，技師は X 線撮影の結果の編集権限を持つ）が，両者の利用許諾では $\text{Actable}(\text{recipient}, \text{act}, c)$ と捨象されて表現されるためである．

以上のように，利用許諾の互換性を分析することにより，医療情報に対する適切な権限を当該医療情報取扱者に付与しているかどうかを判定することができる．

5 議論

本研究の先行研究としては、コンテンツの循環的な流通の促進のために実施された、ライセンスに形式意味論を与える試み [4] やライセンスの互換性の分析 [5] が挙げられる。

RBAC の医療情報への適用は過去に多く研究されている（例えば医療情報における RBAC のアクセス制御ポリシーの数理的定義に関する研究 [6] など）が、ここでは提案モデルと個別の研究との比較は行わず、RBAC との総合的な比較を論ずることとする。文献 [3] の表 1 では、医療情報取扱者として「医師」「看護師」をはじめとして 29 の役割が挙げられている。また、大規模な病院では診療科が 30 を超えることも珍しくなく、各診療科に、医師や看護師が所属しているため、RBAC におけるロールの設定が困難である。すなわち、医療情報にアクセスできる者を必要最小限に留めようとする、ロールの数が増大し、管理コストが増大する。一方、管理コストを軽減するためにロールの数を抑えようとする、医療情報にアクセスできる者を必要最小限に留めることができない。医療機関は職務の専門性が高く役割の分担が進んでいるため、各ロールに所属する人員数が少ないことが、このようなトレードオフの状況を招来していると考えられる。また、各診療科や検査科は並立しており、組織が階層的ではないため、階層型 RBAC の導入による管理コストの軽減効果も大きくないことが予想される。

また、1 章と 2 章で述べた通り、近年のプライバシー意識の高まりから、医療情報の保有・管理者は第一義的には患者である、とする傾向にある。提案モデルは、患者が保有する医療情報を、医療行為を遂行するための必要最小限の人員にその都度利用許諾を発行するという方針であり、このような傾向によく適しており、医療情報にアクセスできる者を必要最小限に留めることができる。以上の点を総合的に鑑み、医療・健康情報活用サービスへの適用に関しては、提案モデルが RBAC と比較して優位であると我々は考えている。

6 おわりに

本稿では、EHR のような医療・健康情報活用サービスにおける情報アクセス制御の要件を実現する方法について検討した。医療・健康情報を患者が権利を保有するコンテンツとみなし、医療情報取扱者に対して患者が利用を許諾するというモデルを提案した。また、互換性の自動的判定により、各医療情報取扱者の利用許諾の関係を明らかにする方法を示した。

今後は、本モデルの実装を通じ、要件やモデルの妥当性、利用許諾を記述する際のユーザインターフェースの検討、患者や医療情報取扱者の満足度などについて評価を進めたい。

謝辞

多くのご助言を頂いた、NTT コミュニケーション科学基礎研究所の真鍋義文氏、真野健氏、櫻田英樹氏に感謝いたします。

参考文献

- [1] IT 戦略本部：i-Japan 戦略 2015 (online). <http://www.kantei.go.jp/jp/singi/it2/kettei/090706honbun.pdf>.
- [2] 大野 浩, 中村 亨, 爰川知宏, 宮島麻美, 前田裕二: 医療・健康情報活用サービスにおけるデータアクセス制御方法の提案, 情処研報, Vol. 2010-GN-74, No. 5 (2010).
- [3] 山肩大祐, 野川裕記, 上田昌史, 田中 博: 医療情報におけるデータの取り扱いに関する情報学的考察, 情処研報, Vol. 2009-EIP-45, No. 5 (2009).
- [4] 藤田邦彦, 塚田恭章: クリエイティブ・コモンズ利用許諾の形式意味論, 情報処理学会論文誌, Vol. 49, No. 9, pp. 3165–3179 (2008).
- [5] Fujita, K. and Tsukada, Y.: An analysis of interoperability between licenses, *Proceedings of the 10th annual ACM Workshop on Digital Rights Management*, pp. 61–72 (2010).
- [6] Becker, M. and Sewell, P.: Cassandra: flexible trust management, applied to electronic health records, *Proceedings of the 17th IEEE Computer Security Foundations Workshop*, pp. 139–154 (2004).