Vol.2010-GN-74 No.5
2010/1/21

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

大野浩[†]　中村亨[†]　爰川知宏[†]　宮島麻美[†]　前田裕二[†]

EHR に代表される医療・健康情報活用サービスにおいては，重要な個人情報を扱うことを考慮しながら，他のユーザに対してデータへのアクセスを許可する手段が必要となる．本稿では，医療・健康情報活用サービスに適用可能なデータアクセス制御のしくみについて，要件を整理しながら，その実現方法を提案する．

A Proposal of Method for Data Access Control on Medical and Healthcare Information Services

Hiroshi Ohno[†] Toru Nakamura[†] Tomohiro Kokogawa[†]
Asami Miyajima[†] and Yuji Maeda[†]

In medical and healthcare services such as EHR, it is required to control data access strictly, because these services handle high-level personal information. To utilize medical and healthcare information effectively, an easy method to disclose information is also required. In this study, we discuss the requirements and propose a method for data access control in medical and healthcare information services.

1. はじめに

現在日本では，行政，教育，医療等の公共性の高い分野において，ネットワーク技術活用への期待が高まっている．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，エンドユーザである国民に向けた具体的サービスとして，国民電子私書箱(仮称)，および日本版 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，情報共有のためのサービスを指す．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，処方せん，調剤録といった医療情報である．このほか，医療機関が管理していない健康情報，例えば，自宅あるいはフィットネスクラブ等で行った運動や，歩数，体重，心拍数，血圧等の記録等も含めて考える動きもある．こうした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れば，両者の密接な関連を考慮して広義に EHR と呼称して議論される場合もある．本稿では，広義の EHR サービスとして，医療情報と健康情報を区別せず，さまざまな機関・団体が管理する医療や健康に係る情報を通信ネットワーク経由で流通・共有する医療・健康情報活用サービスについての議論を行う．

このような医療・健康情報活用サービスを実現する際には，個人に帰属する医療・健康情報を，医療従事者等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．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」ことを目指している[1]．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．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度にとど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）で目指され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，活用することが必要である．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ユーザ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相手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．

[†] NTT サービスインテグレーション基盤研究所
NTT Service Integration Laboratories

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ためのデータアクセス制御のしくみについて，以上のような要件を整理しながら，その実現方法を提案する．

2. 要件

2.1 情報開示に関する要件

先の章にて述べた通り，医療・健康情報活用サービスにおいては，

a. 医療・健康情報を情報の帰属者の許諾に基づいて，他のユーザがアクセス（読み取りまたは書き込み）できること
b. a において，医療・健康情報の帰属者が，IT リテラシの低い者，高齢者，子供，乳幼児である場合など，情報の帰属者本人による許諾手続きの実施が困難な場合に，アクセス許諾手続きを代行する手段があること
c. a, b において，他ユーザに対するアクセス可否を設定する手続きが容易であり，情報開示したい相手に確実に開示できること

が求められている．ここでは，上記項目を起点に要件の詳細化・再構成を図る．

a のユースケースとしては，図 1 のように，

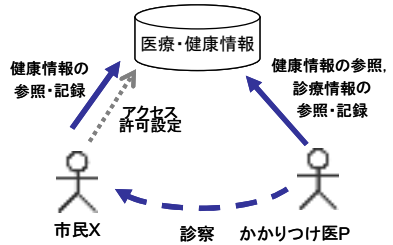

図 1 情報帰属者のアクセス許可に基づいて他ユーザからアクセスするケース

i) 市民 X: かかりつけ医 P に対し，自身の日常の健康情報を開示し，診察の記録については読み書きを許可する
ii) かかりつけ医 P: 市民 X の日常の健康情報を参照しながら，診察を実施し，その結果を市民 X の医療情報として記録する

といったものが考えられる．このケースにおいて，市民 X としては，特定の病院のかかりつけの医師にのみアクセスを許可したい場合もあれば，複数の病院を含めて，アクセスを許可したい場合もあると考えられる．また，開示する健康情報については，一定期間分のみにとどめたいといった要望もあると考えられる．また，かかりつけの医師だけでなく，担当の保健師や看護師も含めて開示したい場合もあると思われる．これらのことから，医療・健康情報活用サービスにおいては，アクセス制御する情報ごとに，アクセスを許諾・非許諾とするデータの範囲，組織（A 病院，B 診療所等），ロール（医師，保健師，看護師等），人間関係（かかりつけ等）といった区分に基づいたアクセス制御を実現すべきと考えられる．入院患者を対象とした調査においても，医療従事者の職種や患者との関係性によって，自身のカルテ情報を「見せたくない」と思う程度が大きく異なっていることが示されており[2]，医療・健康情報へのアクセス制御における，ロールや人間関係といった区分の重要性が伺える．

また，b に関わるケースとしては，図 2 のように，

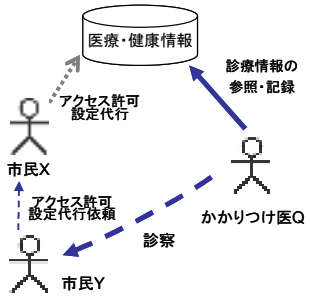

図 2 代行者のアクセス許可に基づいて他ユーザからアクセスするケース

iii) 市民 Y: 市民 X の親．高齢で IT 利用に不慣れなため，自らの医療・健康情報へのアクセス可否の設定については，離れて暮らす子（市民 X）に任せる
iv) 市民 X: 市民 Y の子．親である市民 Y に代わり，市民 Y のかかりつけ医 Q について，市民 Y の医療・健康情報へのアクセス可否の設定を実施する
v) かかりつけ医 Q: 市民 Y の過去の診療記録を参照しながら，診察を実施し，その結果を記録する

といったものが考えられる．このケースからは，第一に，各医療・健康情報へのアクセス可否を設定可能とするだけでなく，そのアクセス可否情報に対するアクセス可否設定を可能にするしくみが必要であることが導き出される．また，市民 Y としては，自分の特定の子に対し，設定代行を依頼したい場合もあれば，家族に含まれる子ならば，誰でもよいので，設定代行を依頼したいという場合もあるだろう．また，子供がいない高齢者の場合には，信頼関係にある特定の人に設定代行を依頼する場合もあり得る．また，乳幼児の場合は，親が設定代行をするのが妥当と思われる．先のユースケースからは「かかりつけ」といった人間関係を扱うことが導き出されたが，そうした医療に関わる関係のみならず，家族，親，子といった人間関係を扱う必要がある．

c の要件は，アクセス可否の設定に関わるユーザインタフェースによって実現すべきところが大きいと思われる．今回は，ユーザインタフェース設計には踏み込まず，

その設定作業に過ちが生じる可能性が高まるケースを想定し，基本的なデータアクセス制御機構の設計に反映すべきポイントがないか検討した．例えば，

vi) 市民 X: これまで A 病院に通院していたが，引っ越しに伴い，B 診療所に通院することにした．それに伴い，かかりつけ医が P 医師から Q 医師に変更になったため，Q 医師に対し，新たに（P 医師と同様の）アクセス許可設定を実施する

といったように，新たにアクセスを許可するユーザを変更・追加するケースが考えられる．この場合，市民 X が医療・健康情報ごとに Q 医師に対するアクセス可否の設定をすべきである．しかし，設定作業にはある程度の手間がかかり，一定の確率で設定ミスが混入するものと考えられるため，極力その作業は回避されるか，他のより単純な作業に置き換えられることが望ましい．ここで，a の要件の詳細化で導出された「人間関係」の区分に基づく，データへのアクセス制御が，設定作業の容易化に寄与すると考えた．例えば，P 医師に医療・健康情報へのアクセス許諾をする際に，「かかりつけ」という人間関係に P 医師を含めるものと設定し，「かかりつけ」という人間関係を持つユーザに対するアクセス可否を設定する．この場合，仮に転院によって，かかりつけ医が P 医師から Q 医師に変更になったとしてもアクセス可否設定については追加作業が発生せず，「かかりつけ」という人間関係から P 医師を削除し，Q 医師を追加する作業のみを実施すればよい．つまり，このケースでは，市民 X はかかりつけ医に自身の情報を開示したいのであり，それがたまたま P 医師であったと解釈する方が適切であると考える．

以上の検討より，以下①～④が医療・健康情報活用サービスにおけるデータへのアクセス制御実現の要件となると考えられる．

① 各医療・健康情報について，データの範囲，組織，ロール，人間関係といった区分に基づいて，データへのアクセス制御情報（アクセス可否）を設定できること
② 各医療・健康情報へのアクセス可否を設定可能とするだけでなく，そのアクセス可否設定情報に対するアクセス可否も設定できること
③ アクセス可否を管理するための，データへのアクセス制御情報と，アクセス制御情報内で利用する，ユーザの人間関係を定義する情報とを分離して管理することにより，アクセス制御情報の編集負荷を低減できること
④ 設定されたアクセス制御情報と人間関係の定義情報に基づいて，医療・健康情報へのアクセス制御を実施できること

3. データアクセス制御方法の提案

3.1 アクセス制御ルールリスト（ACL）と関係情報に基づくアクセス制御

前章にて導出された①～④の要件を踏まえ，アクセス可否に関する情報として，アクセス制御ルールリスト（ACL）を設定するものとし，医療・健康情報を管理するサーバが，アクセス要求時に ACL を参照し，読み取りまたは書き込みを許可するしくみを提案する．

ACL の例を表 1 に示す．ACL を構成する項目は，①の要件より，アクセスを許可する対象組織，対象ロール，対象（人間）関係，データの対象範囲（対象期間の開始～終了）を含むものとする．以上に加えて，読み取り・書き込みの可否を設定する項目を具備するものとする．

②の要件より，「ターゲットデータ」項目には，健康記録や診療記録といった医療・健康情報だけでなく，ACL 自体を設定できるものとする．

また，③の要件より，表 1 のような ACL とは別に，ユーザごとに人間関係を設定するための情報（ユーザ関係情報）を保持するものとする．ユーザ関係情報の例を表 2 および表 3 に示す．ユーザ関係情報は，「かかりつけ」や「家族」といった関係名と，その関係に該当するユーザから構成されるものとする．

④の要件を満たすために，前提として，各ユーザの属性情報として組織とロールに関する情報を保持しているものとする．そして，あるユーザへの医療・健康情報アクセス要求があった際には，ACL を参照し，「人間関係」項目に特定の関係名が設定されている場合には，ユーザ関係情報を参照した上で，アクセス要求ユーザのデータ読み取りまたは書き込みを許可するか否かを判定する．判定の結果，許可された場合にはアクセス要求ユーザがデータの読み取りまたは書き込みを実施する．

表 1 アクセス制御ルールリスト（ACL）の例

	データ帰属ユーザ	ターゲットデータ	対象期間（開始）	対象期間（終了）	対象ユーザ	対象組織	対象ロール	対象関係	読み取り	書き込み	認証種別	有効期間（開始）	有効期間（終了）
ルール 1	市民 X	健康記録	2008/1/1	2011/12/31			医師	かかりつけ	可	否	IC カード		
ルール 2	市民 X	診療記録				A 病院		かかりつけ	可	可	PW		
ルール 3	市民 Y	診療記録						かかりつけ	可	可	PW		
ルール 4	市民 Y	ACL						家族	可	可	PW		
ルール 5	市民 Y	健康記録			市民 Z				可	否	PW	2009/10/1	2009/12/31

表 2 ユーザ関係情報の例（市民 X）

	かかりつけ	家族
ユーザ	P 医師（※A 病院） Q 医師（※B 診療所）	

表 3 ユーザ関係情報の例（市民 Y）

	かかりつけ	家族
ユーザ	Q 医師 J 保健師	市民 X

例えば，表 1 のルール 1 は，市民 X の健康記録のうち，2008 年 1 月 1 日から 2011 年 12 月 31 日のデータについては，かかりつけの医師に対して読み取りを許可することを示している．このとき，ユーザから市民 X の 2009 年の健康記録について読み取り要求があった場合，読み取り要求ユーザの属性情報に含まれるロールが医師となっており，かつ，読み取り要求データの範囲が 2008 年 1 月 1 日から 2011 年 12 月 31 日に収まっているかを判定する．判定結果が全て真となる場合，更に読み取り要求ユーザが市民 X の「かかりつけ」という関係にあるか否かを判定するために，市民 X のユーザ関係情報（表 2）を参照する．表 2 の例の場合，かかりつけとして，P 医師と Q 医師が登録されているため，要求ユーザが P 医師あるいは Q 医師ならば，要求範囲の健康記録を閲覧させる．ルール 2 は，アクセス要求ユーザが A 病院という組織に所属しており，かつ,「かかりつけ」という人間関係に登録されているかを確認し，診療記録の読み取り書き込みの可否判定を行うことを示している．このルールに基づくと，表 2 における P 医師はアクセスが許可されるが，B 診療所に所属している Q 医師はアクセス許可されない．ルール 3 は，組織やロールに関する指定がなく，「かかりつけ」という人間関係にあるユーザである Q 医師，J 保健師（表 3）に対し診療記録の読み書きが許可される例である．

ルール 4 は，ルール 3 を含む，市民 Y の ACL の編集許可ルールである．ルール 3 等市民 Y の ACL の編集要求があった場合，編集要求ユーザが市民 Y の家族であるかを判定し，家族である場合（編集要求ユーザが表 3 の通り，市民 X である場合）にのみ，ACL の編集を許可する．

データへのアクセス制御をより厳密に実施するために，例えば，表 1 に「認証種別」という項目を具備し，医療・健康情報へのアクセスを許可する認証手段を設定できるようにしたり，ACL の「有効期間」を設定できるようにしたりすることも有用だと思われる．例えばルール 1 では，IC カードで認証された場合のみ健康記録の読み取りを許可している．また，ルール 5 では市民 Z に対し，2009 年 10 月 1 日から 3 ヶ月間のみ健康記録の読み取りを許可している．

4. システムへの適用

ここでは，3 章までに述べた，データへのアクセス制御方法を医療・健康情報活用サービスに適用することを検討する．

4.1 前提条件

適用する医療・健康情報活用サービスおよびユーザは以下の通りとする．

【サービス】

医療・健康情報活用サービスはさまざまな形態が想定されうるが，既にフィールドでの実証事業[3]が行われている EHR サービスを電子公共サービスの典型例として取り上げる．EHR サービスについて，筆者らは既にそのサービスモデルを提案している[4]．このモデルでは，サービスを運営する事業者として次の 3 者を想定している（図 3）．本稿でも同様の構成を想定することとする．

- データプロバイダ：
  エンドユーザの医療・健康情報を保持するプロバイダ．
- サービスプロバイダ：
  データプロバイダから集めた医療・健康情報を用いて，エンドユーザに対して具体的なサービスを提供するプロバイダ．
- 情報連携基盤：
  データプロバイダ，サービスプロバイダ間での情報連携を実現する共通基盤．

【ユーザ】

他ユーザの情報へのアクセスに関連するユーザとして，図 3 のサービスモデルに従って以下を想定する．

- 一般ユーザ：
  医療・健康情報を有するシステム利用者．
- 代理ユーザ：
  親・保護者等，一般ユーザの代理人としてふるまうシステム利用者．
- プロユーザ：
  医者，保健指導師，インストラクタ等，具体的な医療・ヘルスケアサービスを提供するシステム利用者．ユーザ属性として，所属する組織の情報やロール（例えば国家資格等）の情報を有する．

Vol.2010-GN-74 No.5
2010/1/21

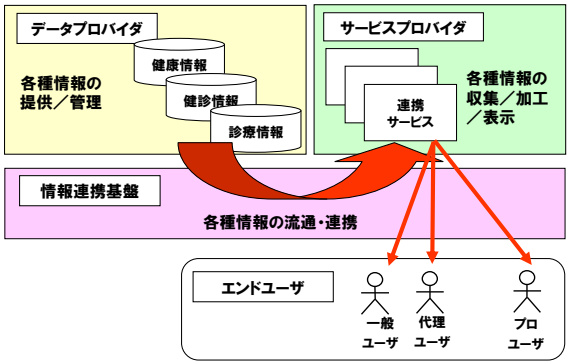

図 3　前提とする医療・健康情報活用サービスイメージ（[4]より引用）

4.2　データアクセス制御に関わる基本機能とシステムにおける機能配置

前節にて提示した医療・健康情報活用サービスにおいて，3 章までに述べた，データへのアクセス制御方法を実現するために必要な基本機能を以下の通り整理した．

表 4 データへのアクセス制御方法を実現するための基本機能

機能	概要
ユーザ関係管理機能	要求に基づき，関係名の検索・参照，登録，更新，削除処理および，ユーザ関係情報の検索・参照，登録，更新，削除処理を実行する．
ACL 管理機能	アクセス制御ルールリスト（ACL）の検索・参照，登録，更新，削除処理を実行する．
アクセス制御機能	医療・健康情報へのアクセス要求に対し，ACL を参照し，アクセス制御（アクセス可否判定）を行う． ※ACL の「対象関係」項目が設定されている場合には，ユーザ関係管理機能に対し，関係確認のための問い合わせも行う．

データへのアクセス制御方法を実装する，[4]にて提案されている EHR サービスの情報連携基盤では，認証連携（シングルサインオン）およびそれに基づく情報連携を実現するための要素技術として，SAML/ID-WSF に基づく通信処理を採用している．表 4 に示した本手法の基本機能は，図 4 に示す通り，[4]の情報連携基盤内の機能として配置する．

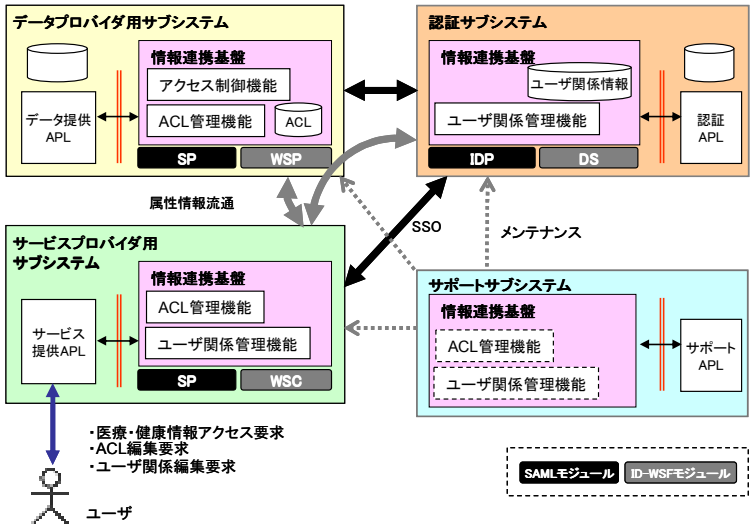

図 4 システム構成と機能配置

ユーザ関係情報およびユーザ関係管理機能は，システム上のユーザ管理を統括している認証サブシステムに配置する．ユーザ関係の管理はユーザ管理の一つとして，サービス利用時に共通的に利用する機能と考えられるためである．ユーザインタフェースを持つサービスプロバイダ用サブシステムにも，認証サブシステム上のユーザ関係情報の編集を行えるよう，ユーザ関係管理機能を配置する．ユーザの登録やシステム利用を支援するサポートセンタを設置する場合には，サポートサブシステムにおいてユーザ関係の初期登録作業を実施できるよう，ユーザ関係管理機能を配置する．

ACL および ACL 管理機能は各データプロバイダ用サブシステムに配置する．ACL を認証サブシステムなどに統括管理させることも可能であるが，現状と同様に，データを管理している事業者が，そのデータに対するアクセス制御の管理を実施するものと考えた．そのため，アクセス制御機能についても同様に各データプロバイダサブシステムに配置する．

ユーザ自らが ACL を編集できるよう，ユーザインタフェースを持つサービスプロバイダ用サブシステムにも ACL 管理機能を配置する．また，ACL の初期登録作業の実施を想定して，サポートサブシステムに ACL 管理機能を配置することも考えられる．

4.3 処理の流れ

以上のようなシステム構成・基本機能配置において，ユーザが医療・健康情報へのアクセスを要求してから，医療・健康情報を取得するまでのシーケンスとしては図 5 のようなものが考えられる．

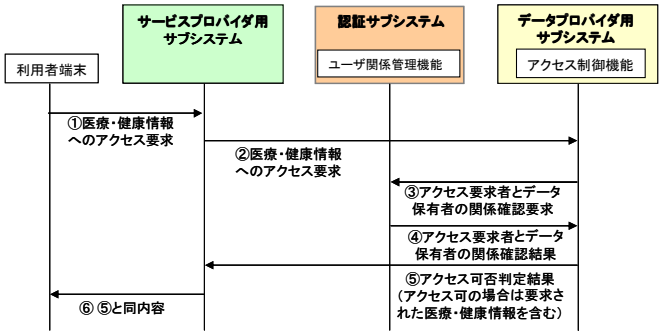

図 5 医療・健康情報アクセス時のシーケンスの例

例えば，表 3 における市民 Y が，「かかりつけ」として登録している Q 医師の診察を受ける場面を考える．表 1 のルール 3 により，「かかりつけ」には診療記録の読み書きが許可されている．市民 Y の診察を始める際に，Q 医師はシステムにログインし，サービスプロバイダのユーザインタフェースより，市民 Y を指定し，診療記録の閲覧メニューに進む．市民 Y を指定するように，システム上で登録済みのユーザを指定する手法の実現については，別途技術課題となるため，[5]において議論されている．システム上では，Q 医師の利用者端末からサービスプロバイダ用サブシステムに対し，市民 Y の診療記録へのアクセス要求が送られ（①），診療記録を管理するデータプロバイダ用サブシステムに対し，アクセス要求が送られる（②）．データプロバイダ用サブシステムでは，市民 Y の ACL を参照し，認証サブシステムに対し，アクセス要求者である Q 医師が市民 Y の「かかりつけ」として登録されているかを問い合わせる（③）．認証サブシステムでは市民 Y のユーザ関係情報を参照し，データプロバイダ用サブシステムに関係確認結果（OK）を返却する（④）．データプロバイダ用サブシステムでは，関係確認結果を受けて，市民 Y の診療記録の読み書きを許可すると判定し，その判定結果（診療記録を含む）をサービスプロバイダ用サブシステムを介して，利用者端末に送る（⑤, ⑥）．

5. まとめと今後の課題

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，データへのアクセス制御の実現方法について，要件を整理しながら，システムへの適用例までを示した．

今後は，本手法を適用した実システムの利用実験などにより，想定したユースケースが実態に合致する妥当なものであるか，ACL に含ませた設定項目が市民や医療関係者の要望に十分に応えるものであるか，について評価を進める必要がある．

本手法の中では，ユーザの「人間関係」を活用することによって，ACL の編集負荷を低減させることを試みているが，誤った開示を防止するには，更に ACL 編集用のユーザインタフェースの整備が必須である．その上で，たとえ誤ったアクセス制御設定をしてしまった場合にも，その設定をシステム上で有効化してしまう前に，誤りに気づくことができるようなしくみ作りも必要である．

参考文献

1) IT 戦略本部, i-Japan 戦略 2015（平成 21 年 7 月）,
http://www.kantei.go.jp/jp/singi/it2/kettei/090706honbun.pdf
2) 前田樹海, 太田勝正, 井口弘子, 新實夕香理, 中村惠, 浅沼優子, 山内一史, 唐澤由美子, 門井貴子, 鈴木千智, 藤井徹也, 松田正巳: 職種および関係性の違いによるカルテ情報の共有範囲:入院患者を対象とした全国調査より，医療情報学 29(Suppl.), 2009
3) 総務省・厚生労働省・経済産業省: 健康情報活用基盤実証事業について（平成 20 年 9 月 5 日）,
http://www.kantei.go.jp/jp/singi/it2/iryou/kaisai_h20/dai2/siryou4.pdf
4) 爰川知宏, 宮島麻美, 大野浩, 中村亨, 前田裕二: 医療・健康情報の流通・活用に向けた情報連携基盤の提案, 情報処理学会研究報告, Vol.2009-GN-73, No.14, pp.1-6, 2009
5) 宮島麻美, 中村亨, 爰川知宏, 大野浩, 前田裕二: 個人情報保護を重視するシステムにおける他ユーザ指定手法の提案, 情報処理学会研究報告, Vol.2009-GN-74, 2009