Vol.2009-DPS-141 No.14
Vol.2009-GN-73 No.14
Vol.2009-EIP-46 No.14
2009/11/26

医療・健康情報の流通・活用に向けた情報連携基盤の提案

爰川知宏[†]　宮島麻美[†]　大野浩[†]　中村亨[†]　前田裕二[†]

公共分野における，ネットワークサービス基盤が持つべき要件について，EHR に代表される医療・健康情報を扱うサービスを対象に整理を行った．サービスモデルを定義し，情報開示，情報流通，公共サービスの観点から要件を抽出した．それに基づき，SAML.および ID-WSF 技術をベースとした情報連携基盤を提案し，そのアーキテクチャについて述べる．

A Proposal of Information Delivery Platform for Medical and Healthcare Information Services

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

The evolution of public services improved by broadband network technology is expected. As a case study, we discussed the requirements the network service platform for medical or healthcare services such as EHR. We defined a service model, and extract the requirements to integrate services using variety of medical or healthcare information, focused on information access policy, information delivery, and specific issues of public services. After that we proposed a information delivery platform and described its architecture based on SAML and ID-WSF technology.

1. はじめに

近年，インターネット技術の発展により，FTTH/ADSL を中心としたブロードバンドネットワーク環境の一般家庭への急速な普及が進んできており，今やネットワークは，重要な社会インフラの一部として認知されつつある．民間サービスの発展とともに，国や自治体が中心に担ってきた行政分野や，医療・健康・介護・福祉といった公共性の高い分野においても，ネットワークサービスの発展への期待が高まっている．

わが国におけるネットワークサービス関連施策は，2001 年に IT 戦略本部が策定した e-Japan 戦略[1]より本格的に始まった．e-Japan 戦略においては，ブロードバンドネットワークの普及促進とともに，公共系サービスに対する施策としては，電子政府・電子自治体の推進が謳われており，医療分野についても先導的分野の一つとして後に追加された．e-Japan 戦略の施策は，国あるいは自治体における，従来は紙ベースで行われてきた膨大な行政業務の電子化が主点であり，国民・自治体住民の視点から見れば，一部の申請業務を自宅からインターネット経由で行える程度にとどまっていた．

しかし，本格的なブロードバンド社会の到来にあわせ，ネットワークを介した情報の本格活用について議論や，実証実験等の具体的な施策が動き始めた．2009 年に策定された i-Japan 戦略 2015[2]においては，エンドユーザである国民・住民に向けた具体的なサービスイメージとして，国民電子私書箱(仮称)，および日本版 EHR(仮称)について言及されており，これまでの電子政府・電子自治体の戦略から一歩踏み込んだ内容となっている．国民電子私書箱(仮称)は，「希望する国民・企業等に提供される，電子空間上で安心して年金記録等の情報を入手し，管理できる専用の口座であり，社会保障分野のみならず幅広い分野でワンストップの行政サービスを提供するもの」，と定義されている．また，日本版 EHR(仮称)は，(1) 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，(2) 処方せんの電子交付及び調剤情報の電子化，(3) 匿名化された健康情報を全国規模で集積し，疫学的に活用，の３点を基本構想として挙げている．両サービスに共通するのは，単なる従来業務の電子化にとどまらず，公共機関が保有する情報をエンドユーザ(国民・住民)の視点で積極的に活用した公共サービスを実現しようという試みである．具体的なサービスイメージが提示されることで，公共系分野におけるネットワーク活用に関する議論が活発化し，今後様々なサービスが検討されていくものと考えられる．

このような，国あるいは地方自治体が主体として実施すると思われる，公共性の高い情報を扱う本格的なネットワークサービスの実現が現実化しつつある中で，そのためのサービスインフラとしてどのような基盤が必要であるかについて検討するのが本稿の目的である．既存の民間サービスとは大きく異なるサービス要件が存在すると思

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

Vol.2009-DPS-141 No.14
Vol.2009-GN-73 No.14
Vol.2009-EIP-46 No.14
2009/11/26

われるため，本稿においては，まずは典型的な公共サービスとして，医療情報あるいは健康情報を扱うサービスを対象として，要件を整理した上で，サービス基盤のあり方について提案を行う．

2. 関連動向

EHR(Electronic Health Record)は，医療情報のネットワーク化，情報共有のためのツールとして，近年議論が進んでいる．EHR において扱われる情報としては，医療機関が保有する患者のカルテ，処方せん，調剤記録といった医療行為そのものに直接関係する情報がまず考えられるが，健康情報の記録という観点からは，医療機関が必ずしも保持していない日々の健康情報，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，血圧等の記録も重要度の高い情報である．後者の情報を扱うサービスは PHR(Personal Health Record)として，(狭義の) EHR とは別物として扱う動きもあれば, 両者の密接な関連を考慮して広義に EHR と呼称する動きもあり，統一的な定義は存在しない．本稿においては，医療機関が持つ情報と個人あるいはフィットネスクラブ等が保有する健康情報を区別せず，まとめて医療・健康情報と呼称し，広義の EHR として検討を行う．

EHR の動向としては，日本国内においては前述の通り，日本版 EHR(仮称)が i-Japan 戦略にて謳われており，文献[3]をはじめ幾つかの取り組みが進められている．一方，海外に目を向けると，それぞれの国の事情に合わせた形で幾つかの取り組みが行われている．

米国では, オバマ政権の新 IT 政策の中で, EHR の構築と有意な利用(電子処方せん，地域医療連携など)に対して財政支援を積極的に進めている．また，2009 年 1 月に医療 IT ネットワークを開発・促進する非営利組織 NeHC (National eHealth Collaborative)[4]が，官民の協力により発足した．NeHC は，全米ネットワークで EHR を共有・更新するために必要な標準の策定や, 医療組織・医療関係者・市民による EHR の利用を促進するための教育・指針・奨励策の提供，安全かつ相互運用可能なネットワークの構築，組織間の協力体制などをミッションとしている．

カナダでは，Canada Health Infoway [5]が中心となり，州単位に構築された EHR システムの国レベルでの相互運用および普及活動を進めており，医療従事者に適切な患者情報と意思決定支援ツールの提供を目指している．

欧州においては, 医療費適正化・医療事務効率化等を目的として医療情報を一元化・統合化する観点から, 国家プロジェクトとして EHR システムの整備が進み, その拡張機能として，統合された医療情報を個人に開示する仕組みの整備が公的に進められている．例えば英国では，「Connecting for Health」[6]を推進し，2020 年までに 3 万人の「かかりつけ医」と 300 の病院を結び，5,000 万人の患者情報を管理・共用するシステムの構築，電子処方せんの実現，オンラインによる病院予約システムや患者によるアクセス権及び開示範囲の管理を目指している．

3. 医療・健康情報の活用に向けた要件整理

3.1 サービスモデル

本稿にて想定するサービスモデルを図 1 に示す. エンドユーザの医療・健康情報は，診療や健康診断を受けた病院等の医療機関や，日常的に利用するスポーツジム・フィットネスクラブなどの健康施設など複数の組織に分散して保管されているものと考える．一方で，診療や健康指導といった具体的な医療や健康管理に関するサービスを提供する側では，例えば大病院で行った検査結果をもとにかかりつけの病院で診療を受けるとか，スポーツジムでの運動記録などをもとに健康指導を行うなど，自身の組織に保管された情報だけでなく，異なる組織に保管された情報を活用できる仕組みが求められる．すなわち，サービスを実現するにあたり，ユーザの医療・健康情報を保持し，提供する側(データプロバイダ)と，その情報を入手し，エンドユーザに提示する側(サービスプロバイダ)の 2 種類の事業者が存在する．それぞれの事業者は複数存在することから，両者の間での情報流通を支援するための共通基盤(情報連携基盤）を提供する事業者が必要となる．それぞれの事業者の概要は以下の通りである．

- 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．病院等の医療機関やフィットネスクラブのような健康関連企業などが想定される．

- 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．他の医療機関での検査情報を入手して診察を行うかかりつけの病院や, 健康指導や運動指導を行う組織などが想定される．

- 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．プロトコル，データフォーマット等を規定するとともに，認証や通信処理など共通的な機能を提供する．国や自治体，あるいはそこから委託を受けた、中立的な立場の事業者が運営することを想定する．

Vol.2009-DPS-141 No.14
Vol.2009-GN-73 No.14
Vol.2009-EIP-46 No.14
2009/11/26

・ エンドユーザ
サービスを享受するユーザ．医療・健康情報を持つ一般ユーザだけでなく，それらの情報をもとに医療行為等を行う医師，インストラクタ，健康指導士なども含まれる．

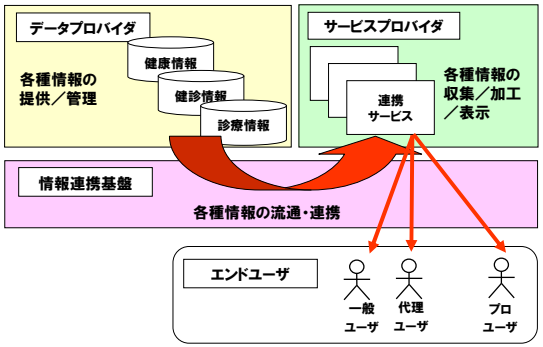

図 1 サービスモデル

3.2 情報開示に関する要件

本サービスモデルにおいて，医療・健康情報に対する操作として求められるのは，以下の 2 点である．

・ 一般ユーザの許諾に基づき，データプロバイダが保持する，対象ユーザの医療・健康情報をサービスプロバイダへ提供することで，対象ユーザ自身の権限により，該当する医療・健康情報へサービスプロバイダ経由でアクセスできること
・ 一般ユーザの許諾に基づき，上記サービスプロバイダに提供された医療・健康情報について，本人以外に対してアクセス権限を与えること．アクセス権限を与える対象としては，そのユーザの代理人としてふるまうユーザ(代理ユーザ：親・保護者など)と，具体的なサービス行為を提供するユーザ(プロユーザ：医者，保健指導士，インストラクタなど)がある．前者(代理ユーザ)と後者(プロユーザ)ではアクセス権限に対する考え方が異なる．前者は一般ユーザの操作を代行する立場であることから，アクセス権限は対象となる一般ユーザと同等，あるいはそのサブセットとなる。一方，後者については，一般ユーザ本人でも行えない操作をプロユーザに対しては認めるケースも存在しうる．例えば医療行為の記録については，その行為者である医療従事者(プロユーザ)には作成権限が与えられるが，患者自身(一般ユーザ)には閲覧のみが許される．

情報開示パターンの例を表 1 に示す．表 1 において，ユーザ(B)はユーザ(A)の保護者として操作を代行する立場から、ユーザ(A)と同等のアクセス権限を持つ代理ユーザとなる．(A)の教師であるユーザ(C)は，生活指導の立場から閲覧権限のみを特別に許可された代理ユーザとしてふるまう。主治医であるユーザ(D)は，ユーザ(A)に対する医療行為の記録として情報の変更権限を持つが、ユーザ(A)本人にはその情報に対する変更権限は与えられない．

表 1 情報開示パターンの例

	ユーザ(A) 本人	ユーザ(B) (A)の保護者	ユーザ(C) (A)の教師	ユーザ(D) (A)の主治医
ユーザ種別	一般ユーザ	代理ユーザ	代理ユーザ	プロユーザ
一般ユーザ(A)の情報閲覧	○	○	○	○
一般ユーザ(A)の情報変更	×	×	×	○
一般ユーザ(A)の情報アクセス権変更	○	○	×	×

3.3 情報連携基盤に求められる要件

本サービスモデルに基づいて情報連携を行うにあたり，情報連携基盤として求められる要件を整理すると，以下の通りとなる．

・ 複数の事業者(データ／サービスプロバイダ)のサーバをまたがってユーザの医療・健康情報を流通させることから，シングルサインオン(SSO)によりそれぞれのサーバにアクセスするための共通的な認証機能が必要．
・ 上記 SSO を行った条件の元で，データプロバイダからサービスプロバイダに対して安全な情報流通を行う仕組みが必要．

3.4 公共サービス特有の要件

本稿の対象である，医療・健康情報を活用する公共サービスに限らず，一般の民間サービスにおいても，前述のサービスモデルが適用できるケースは数多く存在する．しかし，公共サービスと民間サービスには，幾つかの点で，サービス要件に影響する

Vol.2009-DPS-141 No.14
Vol.2009-GN-73 No.14
Vol.2009-EIP-46 No.14
2009/11/26

差異が存在すると考えられる．

・ サービスの加入要件が異なる
民間サービスの場合は，基本的にサービスの加入はエンドユーザの自由意志であり，利用登録を行ったエンドユーザだけを対象にサービスが提供される．エンドユーザの特定については基本的にサービス依存であり，システム上でユーザの一意性が確保できれば，必ずしも実利用者を特定する必要はない．一方で，公共サービスの場合は，利用者は国民あるいは住民全体を対象とするものとなることから，サービス加入にあたっては厳密な本人確認が必要となる．

・ 扱う個人情報の特性が異なる
民間サービスの場合は，利用登録を行ったエンドユーザから直接入手した個人情報をもとにサービスが提供される．一方で，公共サービスの場合は，国や自治体が直接行った場合，対象ユーザである全国民・住民の，本人特定に直接繋がる基礎データが予め揃っている状態で運営される可能性が高い．そのため，万が一情報漏えい等が起きた場合の影響ははかりしれない．また，本稿で対象とするような医療・健康情報は，個人情報の中でも非常にセンシティブな内容が含まれており，民間サービス以上に慎重な個人情報の取扱いが求められる．

・ 標準技術・ガイドラインへの準拠が強く求められる
公共サービスにおいては，相互接続性，ベンダ中立性，さらにサービスの安全性を担保するために，各種標準技術やガイドラインへの準拠が，法令に準ずるものとして，民間サービス以上に強く求められる．医療・健康情報を扱うシステムに対しては，関連省庁より複数のガイドラインが出されており，例えば厚生労働省が策定している「医療情報システムの安全管理に関するガイドライン」[7]などがある．これらのガイドラインにおいては，通信路の暗号化・署名や，操作状況のログ監査に至るまで様々なレベルの規定が存在し，その準拠がシステムに求められる．

4. 要素技術

4.1 シングルサインオン

SSO に関する代表的な技術として，OpenID[8]と SAML (Security Assertion Markup Language)[9]が存在する．

OpenID は，OpenID Foundation が中心となって定める，URI ないしは XRI 形式のユーザ識別子を用いて，ユーザに関するアイデンティティサービスを提供する規格であり，一つのグローバルにユニークな ID を OpenID として，複数の OpenID 対応サイトを利用することができる．OpenID においては，サービス提供者 (RP: Relying Party)は，使用する OpenID を持つユーザに対し，その ID を払いだした認証主体(OP: OpenID Provider)における認証結果を流通させることで SSO を実現する．

SAML は，標準化団体 OASIS および Liberty Alliance(現 Kantara Initiative)によって策定された，ID やパスワードなどの認証情報を安全に交換するための XML 仕様である．グローバルな ID を流通させる OpenID とは異なり，SAML はサイト間の信頼関係(トラストサークル)を前提とし，匿名化された中間 ID(仮名)を用いて認証サーバ(IdP: Identity Provider)とサービス提供者(SP: Service Provider)の間で認証結果の流通を行う．

公共サービスという観点で見た場合，OpenID は既に民間サービスで払い出された ID を活用して，事前の事業者間契約の必要なく簡易にシステム構築ができるというメリットがある反面，特定企業(群)の払い出す ID にシステムの動作を委ねることから抵抗感が強まることが予想される．さらには，ログイン情報の漏洩によるサービス全体への影響の波及というセキュリティリスクの観点でも懸念がある．一方，SAML を適用した場合は，対象サイト間で PKI に基づくトラストサークルを構築することによるセキュリティ上の優位性がある．また，中間 ID を介した認証情報の流通により，サイト毎に保持するユーザ ID の漏洩リスクは少ないと考えられる．一方でトラストサークル構築を前提とすることから，事業者間の契約も含め，接続にかかる手順が複雑である点が導入の障壁となる．なお，最近では Kantara Initiative を中心に OpenID と SAML の相互運用についても議論が進みつつあることから，将来的には両者は共存し，実質的な違いは既存の ID を用いるか否かという観点にとどまるものと考えられる．

4.2 安全な情報流通

SSO 結果に紐づいて安全に情報流通を行う技術としては，SAML，OpenID それぞれについて属性情報の流通という観点で方式が規定されている．

SAML に対応する属性情報流通技術として，Liberty Alliance では ID-WSF(Identity Web Services Framework) [10]の標準化を行っている．ID-WSF は，認証機能付き Web サービスを展開するためのオープン標準仕様ベースの手法を規定しており，パーミッション・ベースの属性共有，認証ディレクトリ・サービス，相互運用サービスなどを扱っている．基本的な動作としては，要求元(WSC: Web Service Client)は，DS(Discovery Service)に対して属性情報の保有元(WSP: Web Service Provider)の場所を問い合わせ，その応答に基づいて，該当 WSP に対して属性情報の要求・取得を行う流れである．

OpenID の場合は，属性流通に対する明示的な規格は存在しない．属性情報は基本的に SSO 時に OP から各 RP へ配布する形となっており，ID-WSF に比べて属性情報の流通に関する制約は大きい．SAML/ID-WSF ベースおよび OpenID ベースでの SSO および属性情報の流通における動作の差異について図 2 に示す．

Vol.2009-DPS-141 No.14
Vol.2009-GN-73 No.14
Vol.2009-EIP-46 No.14
2009/11/26

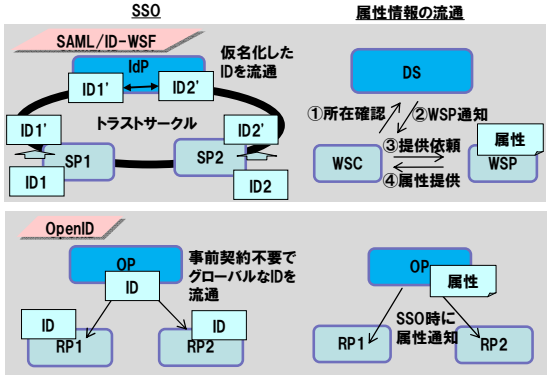

図 2 SAML/ID-WSF と OpenID の関係

5. 情報連携基盤の提案

以上を踏まえ，医療・健康情報の流通・活用に向けた情報連携基盤のコンセプトについて提案する．

5.1 アーキテクチャ

提案する情報連携基盤のアーキテクチャを図 3 に，システム全体のアーキテクチャを図 4 に示す．

情報連携基盤の基本構成要素は以下の通りである．

- SSO および属性情報流通を実現する通信モジュール
- 上位アプリケーション(APL)に提供する共通機能(基盤モジュール)
- APL に対して公開するインタフェース(API)

主要な要件である，SSO およびそれに基づく情報流通を実現するため，SAML/ID-WSF に基づく通信処理を情報連携基盤に採用する．但し，OpenID 等の他標準の存在も考慮し，上位 APL に対しては，SAML/ID-WSF 処理への依存性を低減するために，通信処理は抽象化した形で提供することとした．

図 3 情報連携基盤のアーキテクチャ

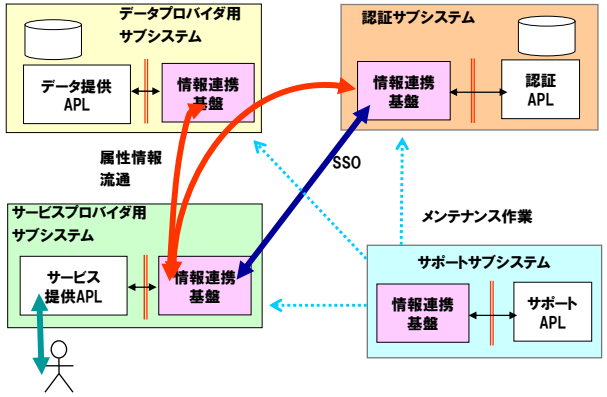

図 4 全体アーキテクチャ

APL とのインタフェースの形態としては，Java API などのプログラムインタフェースを提供する方法と，SOAP あるいは REST に基づく Web サービスベースのプロトコルインタフェースを提供する方法が考えられるが，本アーキテクチャにおいては，通信周りは基本的に SAML/ID-WSF に基づく SOAP ベースの処理を規定しており，Web サービスベースのインタフェース提供では通信周りのオーバーヘッドが大きくなることから，Java ベースの API を提供する方針とした．

上位 APL に対する共通機能として想定される機能例を以下に示す．

- ユーザ認証機能
- 各プロバイダの組織情報や，プロユーザの役割定義等の共通データ(マスタ情報)提供機能

Vol.2009-DPS-141 No.14
Vol.2009-GN-73 No.14
Vol.2009-EIP-46 No.14
2009/11/26

- エンドユーザの許諾に基づくアクセス制御機能
- HL7(Health Level Seven)[11]など標準に基づく医療関連データを扱う機能
- 各種ガイドラインに基づく通信路の暗号化，署名付与機能
- 各種ガイドラインに基づく監査用ログ出力機能
- システムのメンテナンスを行うためのサポート系機能(ユーザ管理など)

5.2 機能配備

本アーキテクチャに基づく機能配備としては以下の通りとする．

- 情報連携基盤は，データプロバイダ，サービスプロバイダそれぞれを実装するサブシステムにおいて, APL に対して API を提供するモジュールとして配置`する．
- 共通機能のうち，認証機能やサポート系機能については，サービス要件によって必要な機能が異なると想定されるため，それぞれ専用のサブシステムを設け，上記同様に，情報連携基盤の提供する API を介して，必要となる機能をアプリケーションとして個別実装できる形態とする．
- 医療・健康情報の管理主体は APL 側になると規定し，情報連携基盤においては，エンドユーザの個人情報の扱いは，認証に必要な情報など最小限に留め，極力保持しない方針とする．共通機能として具備する暗号化，署名，監査用ログ出力など，通信路としての安全性の担保を APL に対して提供する．

6. まとめと今後の課題

本稿では，ブロードバンド時代の公共向けネットワークサービスにおけるサービス基盤の要件とアーキテクチャについて，医療・健康情報を扱うケースを中心に検討を行い，情報連携基盤の提案を行った．

現在，本提案に基づく情報連携基盤についてプロトタイピングを進めている．具体的な評価や機能追加については今後の検討課題であるが，以下の観点で行う必要があると考えている．

- ユースケースの洗い出しと，それに基づくサービスのプロトタイピング
  医療情報の取扱いについては，ステークホルダや情報特性毎に要件が異なるため[12], より具体的なサービス(上位 APL)や事業者を想定したユースケースの洗い出しが必要である．ユースケースや業務フローについて整理した上で，基盤として持つべき共通機能の抽出を行い，サービスのプロトタイピングにより機能性を評価する．

- スケーラビリティ・運用性
  サービスで想定される規模(市町村レベル／県レベル／全国レベル)に応じたシステム構成や，スケールアップの方式について検討するとともに，プロトタイプを用いた性能評価を実施する．また，監査業務など運用上の課題についても，評価と課題抽出を進める．

本稿では，主として医療・健康情報を扱うサービスに特化して検討を進めたが，ここで述べた要件の本質的な部分は，公共向けサービス全般に広く適用可能であると考えている．その観点から，より汎用的な公共向けサービス基盤の構築に向けた検討を今後進めていく予定である．

参考文献

1) IT 戦略本部, e-Japan 戦略(平成 13 年 1 月), http://www.kantei.go.jp/jp/it/network/dai1/pdfs/s5_2.pdf
2) 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
3) 原量宏ほか, かがわ遠隔医療ネットワークから日本版 EHR の実現へ, 新医療(0910-7991)35 巻 2 号 Page48-53(2008).
4) NeHC, http://www.nationalehealth.org/
5) Canada Health Infoway, http://www.infoway-inforoute.ca/
6) NHS Connecting for Health, http://www.connectingforhealth.nhs.uk/
7) 厚生労働省, 医療情報システムの安全管理に関するガイドライン第 4 版, http://www.mhlw.go.jp/shingi/2009/03/s0301-4.html
8) OpenID 1.1, http://www.openid.net/
9) SAML 2.0, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
10) ID-WSF 2.0, http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates
11) HL7, http://www.hl7.org/
12) 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, 情報処理学会研究報告, Vol.2009-EIP-45 No.5, p.1-6 (2009).