特集論文

医療認証基盤

村上耕平*
長浜隆次*

Healthcare Public Key Infrastructure Authentication Service

Kohei Murakami, Ryuji Nagahama

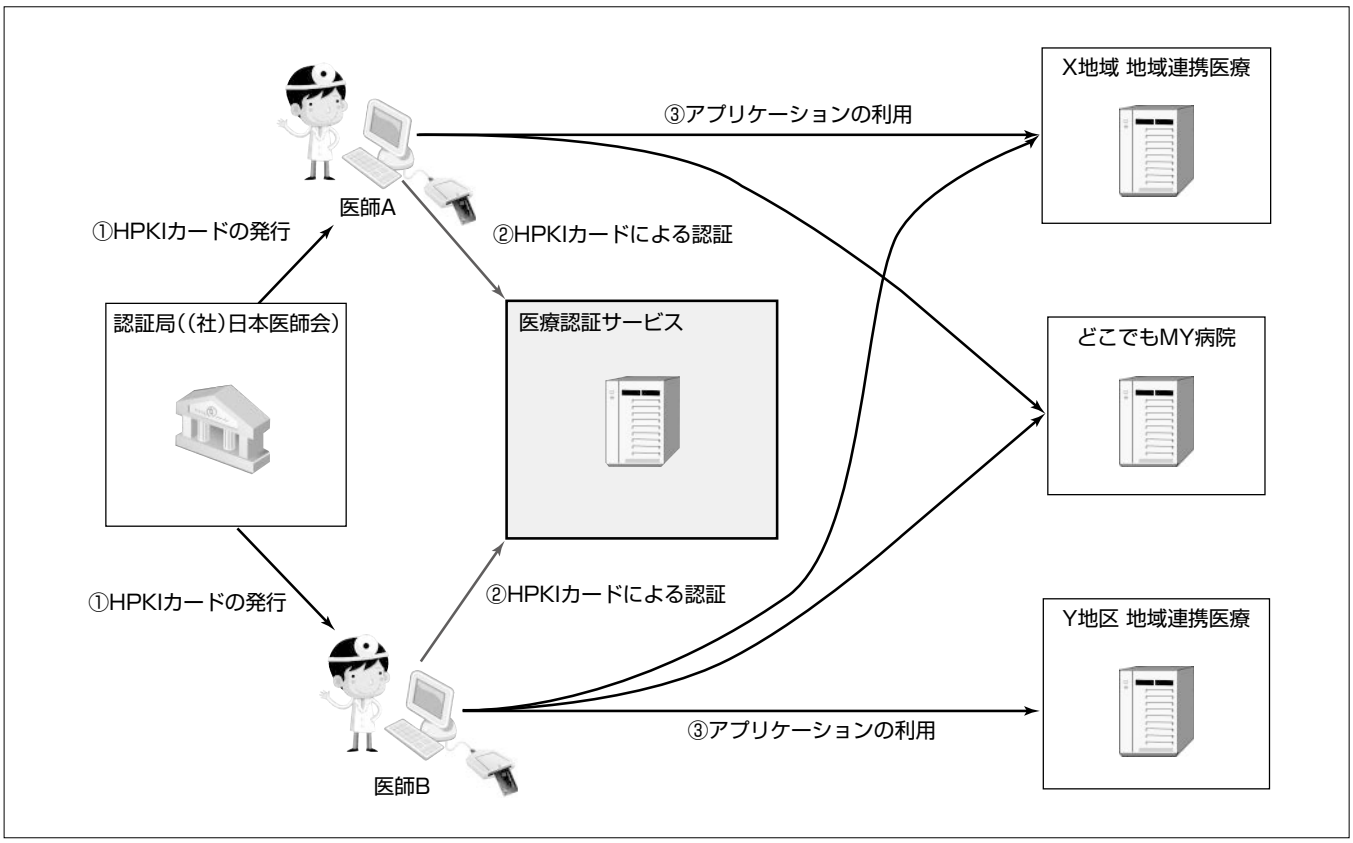
要　旨

我が国では，高齢化の進展，医師の偏在化等が顕著になっており，現場のニーズに適合した医療システムの構築が重要となる。一方，セキュリティのポリシー設計や実装に当たっては，医療情報を取り扱うための注意が必要であり，署名・認証における標準化技術として厚生労働省が進める“保健医療福祉分野における公開鍵暗号基盤”(Healthcare Public Key Infrastructure：HPKI)の幅広い活用が求められている。

三菱電機インフォメーションシステムズ㈱(MDIS)が参加した医療分野共通認証基盤整備コンソーシアムでは，経済産業省の平成22年度“医療情報化促進事業”で共通に利用可能なHPKIを活用した認証基盤の整備を行った。これまで，個々のシステムで認証情報の管理を行っていたが，この認証基盤によって一元的な認証を行うことが可能となり，個々のシステムでの認証情報の管理は不要となる。また，医師の資格確認も容易に実施できる。

認証の一元化のために，HPKIの証明書を使った個人認証を行う医療認証サービスシステムを構築した。また，医療認証サービスシステムで認証した認証情報を取得できるモジュールの開発を行い，他の医療情報化促進事業に提供し，利用できるようにした。

今後，医療情報化促進事業以外でも医療機関連携に幅広く活用してもらえるように，普及啓発活動を進めていくことが課題となる。また，開発したモジュールを応用することで，様々な国家資格(薬剤師，歯科医師，看護師等)に対応した利用者認証を実現することができるので，医師のみならず，医療全体の基盤となるシステムとして普及拡大に努める。



医療認証サービス

これまでは，個々のシステムで認証システムを構築し認証情報の管理を行っていた。今回の基盤整備事業では，HPKIカードを使って医療認証サービスで医師の認証を行い，その認証情報を提供することで個々のシステムで医師の認証情報の管理は不要となる。医師は，一度の認証で複数のアプリケーションを利用できるため利便性が向上する。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

我が国では，高齢化の進展，医師の偏在化等が顕著になっており，質の高い医療サービスなどを受けるための環境整備が急務となっている。

医療情報化では，現場のニーズに適合したシステム，現場の実情を反映したシステムの構築が重要である。しかし，相互運用性の確保やセキュリティ対策については，現場で個々に対策を立てるのではなく，我が国として標準的な対応が求められている。標準化の必要性，統一されたセキュリティのあり方については，過去の事業の検証も踏まえ，例えば厚生労働省の“医療情報システムの安全管理に関するガイドライン”[(1)]などにまとめられている。ところが，そのような指針が存在しても，現場の実情としては各種の解釈が存在し，必ずしも統一された標準形式やセキュリティ対策が取られているとは言えない。

一方，署名・認証における標準化技術として，厚生労働省が進める保健医療福祉分野における公開鍵暗号基盤(Healthcare Public Key Infrastructure：HPKI)が存在しており，広く活用することが求められている。

本稿では，HPKIを活用した医師向けの認証サービスを通して，医師の利便性向上を実現した医療認証基盤について述べる。

2. 医療認証基盤整備事業

経済産業省の平成22年度“医療情報化促進事業”で，“どこでもMY病院構想”(以下“MY病院”という。)の実現に向けた実証事業，シームレスな地域連携医療(以下“地域連携医療”という。)の実現に向けた実証事業，及び共通項目の開発に向けた実証事業が実施された。共通項目では，実証事業の多くのフィールドでの活用が見込まれる機能の整備を行うが，MDISが参加する医療分野共通認証基盤整備コンソーシアムでは，医師の認証と資格確認を共通化する医療認証基盤整備事業を推進した。

MY病院や地域連携医療では，患者(国民)の医療・健康情報を取り扱うため，この基盤整備事業では次の実現を目的とした。

(1) 患者(国民)の情報にアクセスしてよい資格者の確実な認証
(2) 認証の一元化(一度の認証で複数のアプリケーションが利用できる)による利用者(医師)の利便性向上
(3) 個々の医療アプリケーションで医師の認証情報管理や資格確認を行う必要がなくなることによるシステム構築・運用費用の抑制

この基盤整備事業では，㈳日本医師会(以下“日本医師会”という。)から発行された医師向けの証明書で個人認証を行う医療認証サービスシステムを構築した。また，医療認証サービスシステムの認証情報を取得できるモジュールの開発を行い，他の医療情報化促進事業に提供し，認証情報を活用できるようにした。

3. 開発したシステム

3.1 システムの概要

医師の認証はHPKIカードを使って行う。HPKIカードは日本医師会から発行される証明書を収めたICカードであり，証明書に医師の登録番号となる医籍番号及びHPKIで定義されている保健医療福祉分野の国家資格情報であるhcRole(health care Role)が記載されている。医師の場合，hcRoleには“Medical Doctor”が入る。

医師は医療認証サービスシステムにアクセスして個人の認証を行う。その認証情報はSAML(Security Assertion Markup Language)と呼ばれる認証情報をデータ交換するための技術を使ってMY病院や地域連携医療等の医療アプリケーションに提供される。医療アプリケーションは医療認証サービスシステムから取得した認証情報を基にアプリケーションのサービス提供を行う。

MDISは医師の認証を行う医療認証サービスシステムの構築と，医療アプリケーション側で認証情報を取得できるSAML連携モジュールの開発を行った。この基盤整備事業におけるシステムの概要を**図1**に示す。

3.2 資格者の確実な認証

医師個人の確実な認証のために，医療認証サービスシステムではIDパスワードではなくHPKIカードを使った認証を行う。HPKIカードを使用することで，カードを持っていることと，利用するためPIN(Personal Identification Number)が必要なことの2要素認証となり，セキュリティの高い個人認証が実現できる。

医療認証サービスシステムでは，HPKIカードの証明書の検証及び失効確認を行う。その上で証明書内に記載されている医籍番号を取得し，個人の認証を行う。証明書のシリアルナンバーではなく，格納してある情報で確認が行えるため，証明書の再発行や更新に伴う認証情報の再登録作業を必要としない。また，証明書のどの情報で個人を確認するかは設定ファイルで指定することが可能であり，HPKIに限らず通常のPKIでもそのまま利用可能で医療系以外のシステムにも適用可能である。

医師の資格確認では，証明書に記載されているhcRoleを取得して医療アプリケーションに提供する。医療アプリケーションでは，hcRoleを確認することで医師であることが確認でき，また，証明書記載のhcRoleを使用しているため，医師以外のhcRoleにも容易に対応できる。証明書に記載されているhcRoleの取得は通常のPKIモジュールで対応することは難しく，追加でhcRoleを取得するモジュールを作成する必要があるが，MDISは既にhcRoleを取得するモジュ

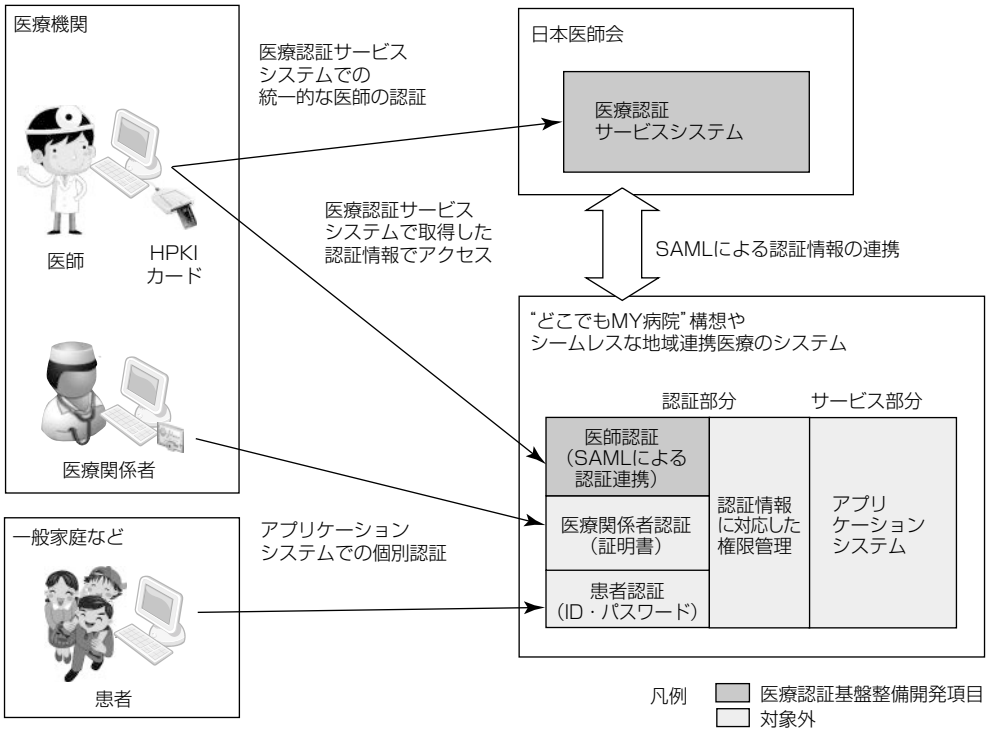


図1．システムの概要

ールを開発していたため，容易に取得することができた。

3.3　認証の一元化と認証情報の提供

従来，医療アプリケーションを利用する際には，アプリケーションごとに認証が必要であった。例えば，アプリケーションAで認証を行った後，アプリケーションBを利用する場合，Bでも認証が必要となり，利用者(医師)にとっての利便性を欠いていた。今回，HPKIカードで統一的に認証を行う医療認証サービスシステムを構築し，その上で認証を行うことによってアプリケーションごとの認証を不要とすることができた。

医師の認証を一元的に行うための医療認証サービスシステムは，医療アプリケーションとは独立したサイトに構築した。認証のための情報に関しては，日本医師会の認証局と連携し，認証局が発行した証明書の情報一覧を取得する。また，証明書の失効情報に関しては，定期的にリポジトリから取得する。この基盤整備事業では，日本医師会内に医療認証サービスシステムを構築し，運営は日本医師会が行っている。

利用者サイトには，利用者が使用する参照クライアント及びMY病院や地域連携医療の医療アプリケーションが存在する。医療情報を扱うため，利用者サイト内は“医療情報システムの安全管理に関するガイドライン”に沿ったネットワークで構築している。

利用者サイトと医療認証サービスサイトはインターネットで接続されている。そのため，利用者サイトからはプロキシなどを使った代理接続を行い，セキュリティを確保する。各サービスサイトの構成を**図2**に示す。

認証情報の提供に当たっては，この整備事業以外でも幅広く利用できるように規格を制定する必要がある。SAMLはインターネット上のIDやパスワードを交換するためのXML(Extensible Markup Language)仕様であり，シングルサインオンを行う際に主に使われる技術である。この基盤整備事業ではSAML2.0の規約[2]に沿って認証情報を提供するための仕様を策定し，SAML実装仕様書[3]を作成した。この実装仕様書に従うことで，様々な医療アプリケーションから認証連携を行うことが可能である。SAMLを使った認証情報提供の流れを**図3**に示す。

利用者(参照クライアント)は医療アプリケーションにサービス利用の要求を行う(①)。医療アプリケーションでは，利用者がまだ認証されていない場合，参照クライアントを経由して医療認証サービスシステムに認証要求を行う(②)。医療認証サービスシステムではHPKIカードによる個人認証を行う(③，④)。認証情報は直接参照クライアントには提供せず，アーティファクトと呼ばれる認証したことを識別するための情報を参照クライアント経由で医療アプリケーションに提供する(⑤)。医療アプリケーションは取得したアーティファクトの情報に基づき，医療認証サービスシステムから認証情報として医籍番号とhcRoleを取得する(⑥，⑦)。参照クライアントを経由せず，直接医療認証サービスから医療アプリケーションに認証情報を提供するため，セキュリティ強度が高い。医療アプリケーションは取得した医籍番号とhcRoleを基に利用者へサービスの提供を行う(⑧)。また，既に利用者の認証が行われている場合は，②～⑦の処理は省略される。

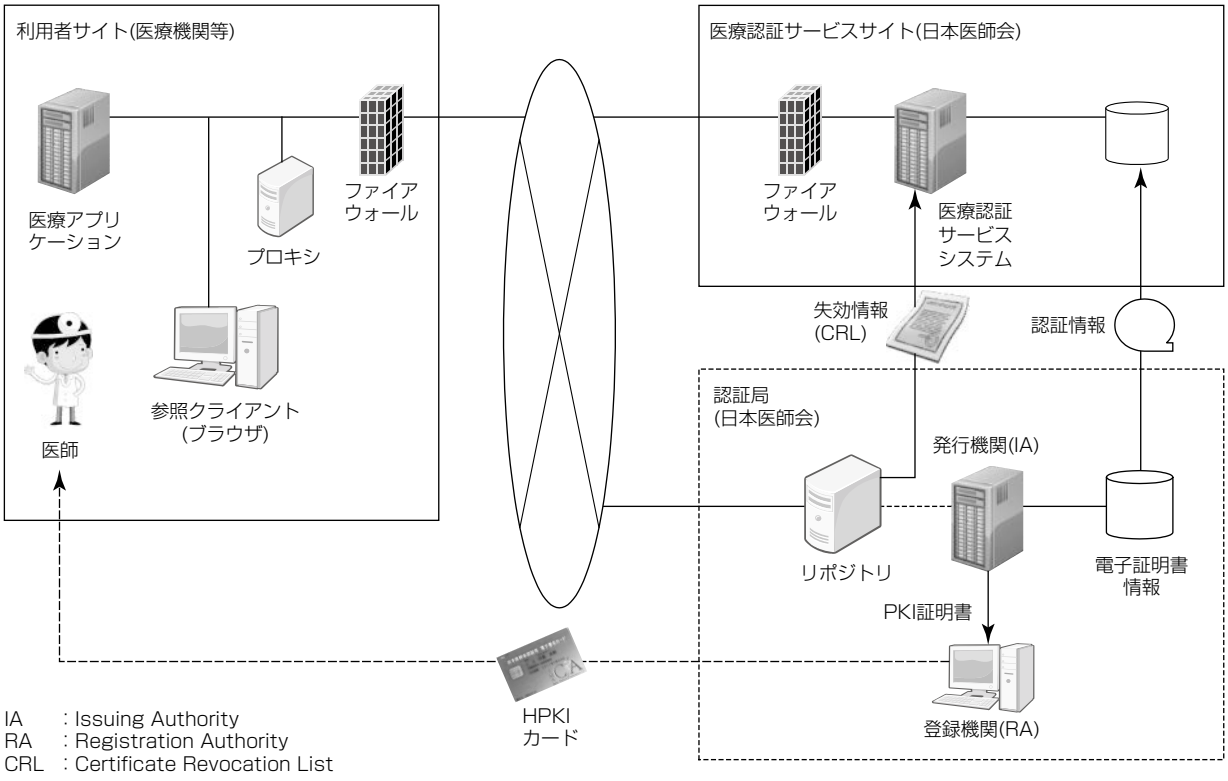


図2．サービスサイト

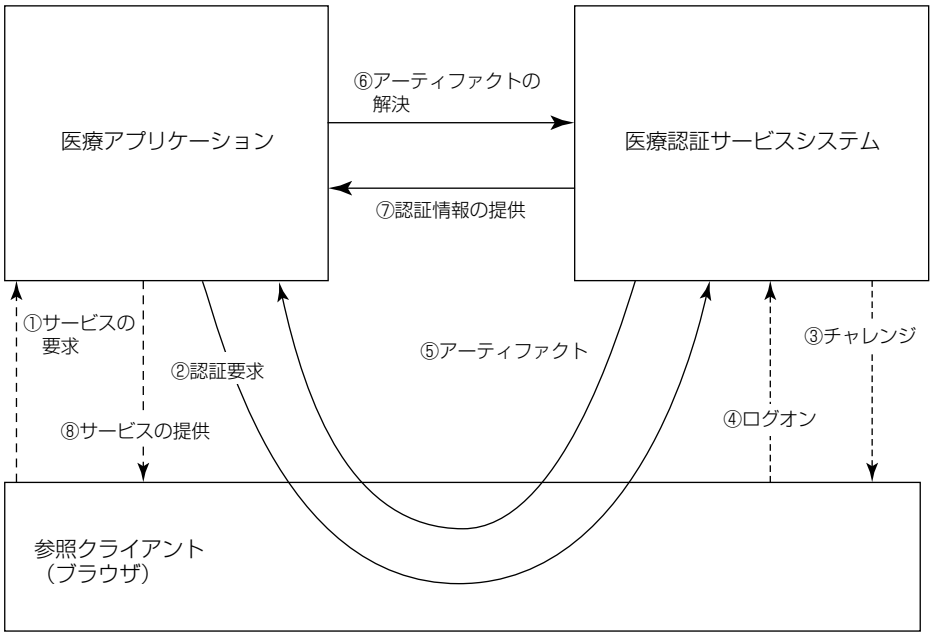


図3．認証情報提供の流れ

3.4　医療アプリケーションの構築・運用負荷抑制

医療アプリケーション側でのシステム構築・運用負荷を抑制するため，医療認証サービスシステムに連携して認証情報を容易に取得できるSAML連携モジュールと呼ばれるモジュールの開発を行った。このモジュールは，参照クライアントと医療アプリケーションの間に入るサーバである。医療認証サービスシステムから取得した医師の認証情報を確認した上で，医療アプリケーションに対してリクエストを中継する。医療アプリケーションに対しては，認証情報をHTTP(Hypertext Transfer Protocol)におけるヘッダ情報で提供する。その内容を**図4**に示す。

SAML連携モジュールを導入することで，HTTPのヘッダで提供される認証情報を処理すればよく，個別にHPKIカードの認証やhcRoleを取得する機能を開発する必要がない。そのため，医療アプリケーション側の開発負荷が軽減される。

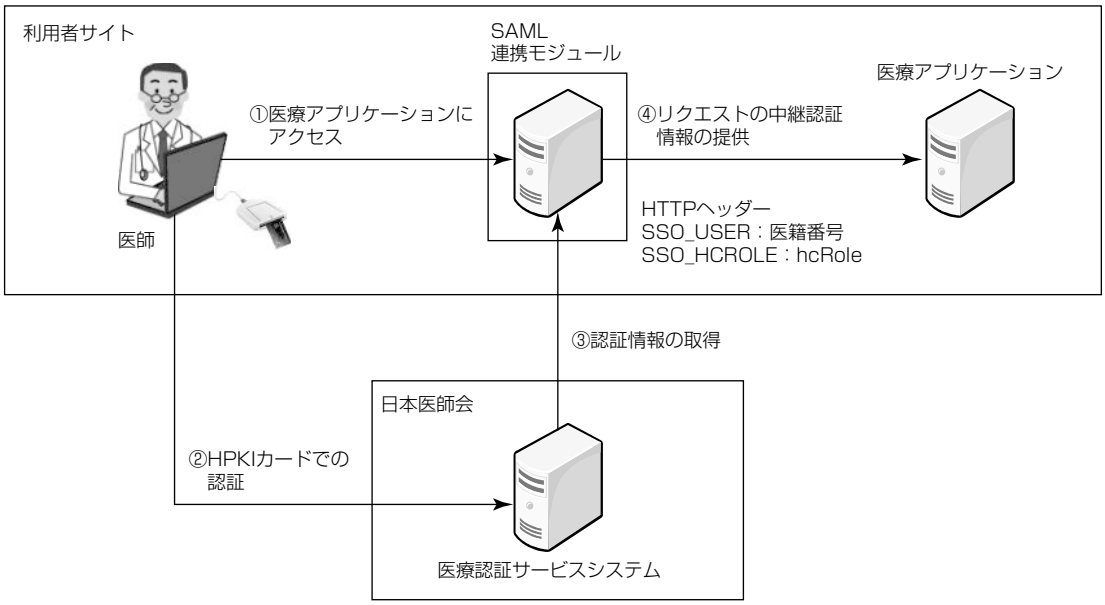


図4．SAML連携モジュール

また，医師に新規のHPKIカードが発行された場合や，医師の資格に問題が発生し証明書が失効した場合，SAML連携モジュールが医療認証サービスに問い合わせて確認するため，医療アプリケーション側での医師の認証情報の追加削除が不要となり運用負荷を下げることが可能となる。

4. むすび

この基盤整備事業で構築した医療認証サービスシステムの運用が開始され，“医療情報化促進事業”の，MY病院及び地域連携医療の事業に提供され，実際に医療認証サービスシステムと連携した認証を行っている[(4)(5)]。そのため，基盤整備事業における目的を十分に果たすことができたと考えている。

医療認証サービスは日本医師会が公益事業として運用することによって，全国規模での展開が容易である。

今後は，医療情報化促進事業以外にも医療機関を連携するシステムに幅広く活用してもらえるように，普及啓発活動を進めていく。

また，今回のシステムを応用することで，医師以外の様々な国家資格(薬剤師，歯科医師，看護師等)に対応した利用者認証や，医療分野以外でもWebアプリケーションにおける認証システムとして提供していきたい。

参考文献

(1) 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4.1版（2010）
http://www.mhlw.go.jp/shingi/2010/02/dl/s0202-4a.pdf

(2) Scott Cantor，et al：Assertions and Protocols for the OASIS Security Assertion Markup Language（SAML）V2.0，OASIS Standard（2005）
http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

(3) 医療分野共通認証基盤整備コンソーシアム：SAML実装仕様書第1.0版（2012）
http://www.keieiken.co.jp/medit/pdf/240423/7-data.pdf

(4) 医療分野共通認証基盤整備コンソーシアム：平成22年度医療情報化促進事業(医療認証基盤整備事業)―どこでもMY病院構想及びシームレスな地域連携医療の実現に向けた実証事業―成果報告書（2012）
http://www.keieiken.co.jp/medit/pdf/240423/7-report.pdf

(5) ㈱NTTデータ経営研究所：平成22年度医療情報化促進事業最終報告会（2012）
http://www.keieiken.co.jp/medit/pdf/report_20120214.pdf