M-064

医療分野における個人情報保護に対応したアクセス制御方法の提案

The proposal of the access control method corresponding to the protection of personal information in a medical field

丸山剛1　鈴木裕之1　喜多紘一1　小尾高史2　谷内田益義1　山口雅浩1　大山永昭3
Tsuyoshi Maruyama　Hiroyuki Suzuki　Koichi Kita　Takashi Obi　Masuyoshi Yachida　Masahiro Yamaguchi　Nagaaki Ohyama

１．はじめに

近年医療分野において医療情報を電子化・共有化して利用する動きが進んでおり、それに伴い個人情報保護の重要性に対する意識も高まっている。これまでの個人情報保護における議論の中心は主に守秘義務や責任問題であったが電子化した医療情報を共有化して利用するようになった昨今では、利用者の意図しない利用の危険性が存在するため各ユーザが自分の情報を自分でコントロールすること（自己情報コントロール）が強調されている。

現段階の電子情報の共有化技術では、管理者が一括してアクセス制御を行っているケースが多く、自己情報コントロールに対応したアクセス制御方法が確立しているとは言えない。

そこで本研究では、医療分野における自己情報コントロールが必要なシーンを想定し、アクセス制御用許可書を利用することで自己情報コントロール可能なアクセス制御手法を提案する。

２．想定する利用形態

本稿では、アクセス制御が必要なアプリケーションの一つとして、健康手帳を電子化・共有化して保存や閲覧を行うシステムの検討を行う。電子化・共有化によるメリットとしてはネットワークでの利用が可能になること、データの二次利用が可能になること等があげられる。現在の健康手帳は、健康の管理・維持を目的として、健康状態を紙の文書に記録し、健康診断、健康相談、医療行為等に利用している。また、健康手帳の管理は各個人に任されており、医者等の第三者への情報提供も個人の意思によって決定される。よって、健康手帳を電子化・共有化する際にも健康手帳利用者が自分のデータを自己情報コントロールできることが望ましい。特に健康手帳の電子化・共有化を有効に活用できるサービスの一つとして遠隔医療を考えた場合、医師と健康手帳利用者が地理的に離れた場所にいるため、ネットワーク経由で電子的にアクセス権を設定する仕組みを提供する必要がある。よって本稿では、健康手帳利用者が遠隔地の医療施設の医師に対し、健康手帳データへの閲覧許可権を設定する方法について検討を進める。

図１に本稿で想定する電子健康手帳システムに登場するプレイヤとその役割を示す。このシステムでのプレイヤとしては、医者・健康手帳利用者のほかに、健康手帳データの管理やサービスの提供を行う「健康手帳サービス提供機関」を設置することを想定する。また、医者や利用者の認証には公開鍵認証基盤の仕組みを用いた個人認証、資格認証[1,2]を行う。

３．アクセス権設定における要件

本稿で想定するシーンにおけるアクセス権設定の要件としては、以下の４つが挙げられる。

■健康手帳利用者のみがアクセス権の設定を行えること

アクセス権の設定における脅威としては利用者以外の人がアクセス権を設定する事が考えられる。この脅威に対しては利用者のみがアクセス権の設定を行える仕組みを施すことで脅威を防止することができる。

■アクセス権の設定を細かく行えること

利用者がアクセス権を設定する際には、医師にアクセスを許可するデータをファイル単位で細かく指定できる必要がある。

■許可の取り消しが可能なこと

医師に健康手帳データへのアクセスを許可した後でも、何らかの理由で許可を取り消す必要がある場合には、許可の取り消しが行える必要がある。

■利用者と医師が直接コネクションを張らなくてもアクセス権の設定が行えること

運用面を考慮した場合、利用者と医師が直接コネクションを張れない場合も考えられるため、そのような場合でもアクセス権の設定を行える必要がある。

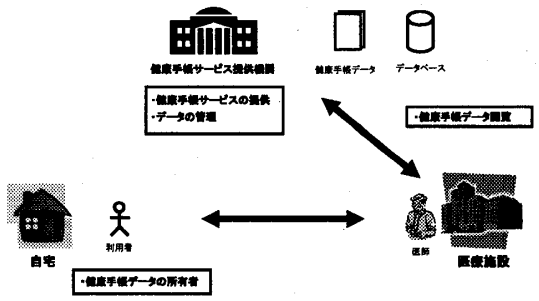

図１：想定する利用形態

４．提案手法

４．１．アクセス権設定方法

前節で述べた要件を満たすために、権利や属性を証明する機能を有し個人レベルで発行できる電子証明書として「閲覧許可書」を定義し、それを用いてアクセス権の設定を行う。閲覧許可書は、利用者が自身のポリシーに従って利用者自身が発行し、健康手帳の閲覧許可を与える医師に渡す。医師は閲覧許可証を健康手帳サービス提供機関内に設置された健康手帳サーバに送付し、健康手帳サーバでは閲覧許可書の検証後に閲覧許可書の内容に従ってアクセス権の設定が行われる。

このように閲覧許可書を用いることにより、利用者が自分のポリシーに従ってアクセス権を設定することが可能となり、自己情報コントロール可能なアクセス制御が実現できる。

４．２．閲覧許可書

以下に示す内容を閲覧許可書に記載する。

①利用者番号　②医師の情報
③権限の詳細　④閲覧許可書の有効期限
⑤利用者の電子署名

「利用者番号」には利用者が健康手帳サービス機関に登録した時に発行された利用者番号、「医師の情報」には医師

１．東京工業大学像情報工学研究施設
２．東京工業大学総合理工学研究科
３．東京工業大学フロンティア創造共同研究センター

の公開鍵証明書の識別名、「権限詳細」には閲覧を許可するデータの範囲を記載、「閲覧許可書の有効期限」には閲覧許可書の有効期限をそれぞれ記載する。そして閲覧許可書の完全性の保証及び閲覧許可の意思表示のために利用者の電子署名を記載する。また利用者は、署名の検証を行うための準備として、予め健康手帳サービス機関に公開鍵証明書を登録しておくこと、また閲覧許可証に記載する医師の公開鍵証明書を前もって入手することが必要になる。

健康手帳サーバが医師から送付された閲覧許可書を検証する方法は、まず医師と健康手帳サーバ間で相互認証、資格認証を行い、次に健康手帳サービス提供機関に予め登録してある利用者の公開鍵証明書を用いて閲覧許可書に記載してある「利用者の電子署名」を検証する。そして相互認証時に利用した医師の公開鍵証明書を用いて「医師の情報」を検証し、閲覧許可証の検証が完了する。

４．３．アクセス権設定のシーケンス

利用者がある医師へ健康手帳データの閲覧許可を設定するシーケンスは、次のようになる。

●利用者と医師間の通信

①利用者が医師の公開鍵証明書を取得②利用者が閲覧許可書を作成③医師に閲覧許可書を送信

●医師と健康手帳サーバ間の通信

④医師が健康手帳サーバにアクセス⑤医師と健康手帳サーバ間で相互認証、資格認証⑥セキュア通信の開始⑦医師が健康手帳サーバに閲覧許可書を送信⑧健康手帳サーバで閲覧許可書の検証⑨健康手帳サーバが閲覧許可書の内容に従ってアクセス権を設定⑩健康手帳サーバから医師に利用者の健康手帳データを送信、医師が閲覧

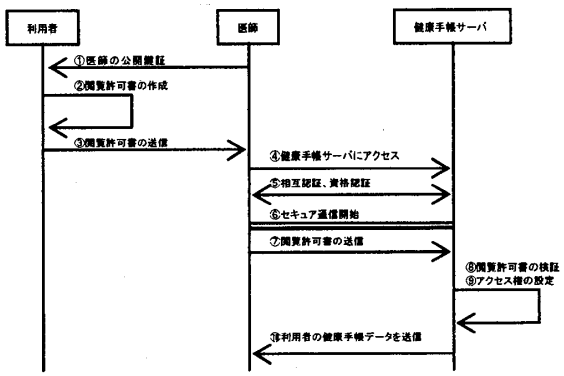

図２：アクセス権設定のシーケンス

５．実装方法

５．１．各プレイヤに必要な機能

図２のシーケンスを実装するために各プレイヤのアプリケーション（AP）に必要な機能は以下のようになる。

●利用者 AP に必要な機能

・閲覧許可書を作成する機能

・閲覧許可書送信機能

●医師 AP に必要な主な機能

・健康手帳サーバと相互認証、資格認証を行う機能

・通信機能

　閲覧許可書送信機能

　セキュア通信機能

　データ送信機能

●健康手帳サーバ AP に必要な機能

・医師の個人認証と資格認証を行う機能

・閲覧許可書を受信、検証する機能

・閲覧許可書に従ってアクセス権を設定する機能

５．２．システム構成

●利用者 AP

安全に秘密鍵を保存するために IC カード内に秘密鍵を保存し閲覧許可書の署名を IC カード内のアプリケーションで行う。また閲覧許可書の送信は PC 上のアプリケーションを用いて行う。

●医師 AP

PC 上のアプリケーションに通信機能を実装し、IC カード内に秘密鍵を保存し IC カード内のアプリケーションを用いて相互認証、資格認証を行う。

●健康手帳サーバ AP（図３）

健康手帳サーバ AP は以下の３つの要素から構成する。

・Web-アプリケーションサーバ（Web サーバ＋アプリケーションサーバ）

・健康手帳データベース

・利用者情報データベース

「Web-アプリケーションサーバ」は、医師の個人認証と資格認証を行う機能、閲覧許可書を受信して検証する機能、閲覧許可書に従ってアクセス権を設定する機能をもつ。「健康手帳データベース」と「利用者情報データベース」はそれぞれ健康手帳データ及び利用者の登録情報と公開鍵証明書を保存するデータベースである。

健康手帳サーバでは、医師の相互認証後に医師の公開鍵証明書と利用者情報データベースに保存してある利用者の公開鍵証明書を用いて閲覧許可書の検証を行う。検証成功した場合、閲覧許可書からクエリーを作成し、そのクエリーを用いて健康手帳データベースから健康手帳データを取り出す。

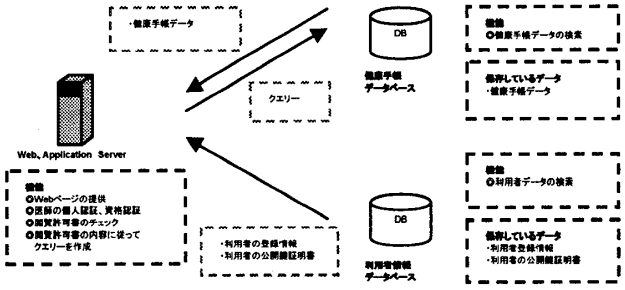

図３：健康手帳サーバ AP の構造

６．まとめ

本研究では自己情報コントロールが必要な医療アプリケーションとして健康手帳システムを想定し、閲覧許可書を用いる事により自己情報コントロール可能なアクセス制御手法の一例を提案した。また手法を実現するために各プレイヤに必要な機能を明らかにし、実装方法をしめした。

今後モデルシステムの実証およびシステム評価を行い、手法の有効性を示す。

参考文献

[1]（財）医療情報開発センター、医療用ＰＫＩシステムの開発　http://www.medis.or.jp/6_pki/hpki.html

[2] 高橋裕樹, 鈴木裕之, 小尾高史, 山口雅浩, 大山永昭, 角田貢, 喜多紘一, "属性証明書を利用した保健医療分野における資格認証システム", 電子情報通信学会総合大会 D-9-11, (2002)