IT ヘルスケア 第 2 巻 1 号, May 27, 2007: 32-35

A-8

個人健康データの管理とその応用

中村 泰明　　尾崎 博嗣　　水島 洋　　田中 博
特定非営利活動法人 日本情報通信研究開発機構

Management and Application of Personal Health Data

Nakamura Yasuaki, Ozaki Hirotsugu, Mizushima Hiroshi, Tanaka Hiroshi
NPO Japan Data and Communication Research Institute

1. はじめに

厚生労働省は，平成20年4月1日から施行される「高齢者の医療の確保に関する法律」[1]において、「医療保険者は、特定健康診査及び特定保健指導を40歳以上の加入者に対し、計画を定め実施する」ことと定めた．この法律に基づき，被扶養者を含めた加入者を対象として、健康診断の義務化，保健指導の徹底、医療費適正化効果の検証を医療保険者に課されることとなった．一方，個人情報の保護の観点から，健康保険法等により守秘義務が規定されており，検診データにおいても当然，個人情報として保護する必要がある．したがって，健康診断データや個人の病歴などのヘルスケアデータの収集，管理，利用においては，効果的な利用と相まって，個人情報と言う観点からは利用の制限が課せられることになる．本稿では，健康診断データなどの個人の健康データを安全，かつ機密性を保って蓄積，管理，利用するための健康データ管理システムについて述べる．

2. 個人健康データの管理

医療保険者は，被扶養者を含めた加入者の健康診断を収集し，適切に管理するとともに，収集データを基に保健指導や医療費の適正化を実施する必要がある．健康診断データを収集する場合，現在のIT社会においてはインターネット経由でのデータ入力が実施されると考えられる．この場合，通信時のデータの盗聴，漏洩，データベース管理サイトにおけるデータ漏洩や改竄を防ぎ，かつ災害や事故からデータを保全する必要がある．本研究では，個人健康データ管理のために，図1のような構成のデータセンタ，利用者端末を含むシステムを構築した．

健康データの管理を行うデータサイトは，地理的に分散した3箇所のサイトで複製を保存する．これは，万一何らかの天災や事故により一箇所のサイトが故障や破損した場合でも他の2箇所に同一のデータが保管されていることから，データの安全性を確保することができる．特に地理的に離れた場所のサイトを構築していることから，同時に3箇所が破損や故障する確率は非常に低いことから，データ保全の観点からは十分な安全性を確保できると考える．また，各サイトではデータは2重化されており，ハードウェア故障などへの対処をしている．

データの漏洩，流出や盗聴，改竄などに対する対処として，データサイトに保存するデータは暗号化することができる．利用者端末もしくは，データ入力

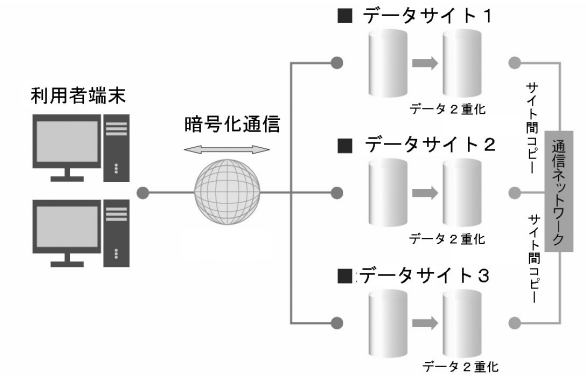

図 1　健康データ管理システム構成

Fig.1 System Configuration of Health Data

端末からデータセンタにデータを送る際，データを共通鍵暗号[2]により暗号化することで，データセンタ内のデータは，暗号化した共通鍵（暗号鍵）によってのみ復号が可能である．すなわち，データセンタ内のデータがたとえ漏洩，流出した場合でも，そのデータを復号することはできないため，個人の健康情報は保護されることになる．さらに，通信路においてデータが盗聴された場合でも，データは暗号化されているため，情報の漏洩を防げる．

3．健康データの共有と利用

図1のシステムでは，通常，データセンタに保存される個人健康データはデータを保存した利用者（所有者）のみが知る暗号鍵により暗号化されているため，所有者のみが復号化が可能である．したがって，所有者のみが個人の健康データにアクセスでき，利用することが可能である．逆に，所有者以外はそのデータを復号化することができないため，健診期間や健康保険組合などは，個人の健康データを保健指導や健康指導などに利用することができない．そこで，他の個人や病院などの組織が個人健康データを利用できる方式として，共通暗号鍵配布によるデータ共有，公開鍵暗号化[2]によるデータ共有，機密レベル設定によるデータ公開の3方式を用意した．

3．1 共通暗号鍵配布によるデータ共有

データの所有者がそのデータの利用を許可する利用者に対して，暗号鍵を配布することで，データへのアクセスと復号化を許可する．この方式では，暗号鍵の配布を受けた利用者は，データ保有者に対する健康指導資料等を配布された暗号鍵により暗号化することで，安全にこのような資料を送付（共有）することができる．

3．2 公開鍵暗号化によるデータ共有

病院や診断機関などに健康データの利用を許可し，そういった機関で多人数の健康データを統計処理するあるいは，自動処理すると言った場合には，（1）の方式のデータ共有では,個人個人のデータに対して，個別の暗号鍵で復号化する処理は効率的でない．一方，病院や機関の方から暗号化鍵を個人に配布する方式も考えられるが，その場合，病院から配布された鍵を多数の人が持つことになり，その鍵により暗号化されたデータを他の人が復号化可能となってしまうため，この方式は現実てきでない．

共通鍵暗号は，公開鍵と秘密鍵のペアから構成され暗号化方式である．暗号鍵は，暗号化データの受け取り側が作成し，公開鍵をデータの送り手に配布する．この公開鍵は一般に公開しても構わない．データの送り手は公開鍵を用いてデータを暗号化し，受け取り手に送信する．このデータは，秘密鍵により復号化可能であり，かつ秘密鍵は作成者しか知らないので，安全な情報の受け取りが可能となる．図2に公開鍵暗号を用いたデータ共有方式を示す．病院や診療所などの診療機関での診断を受けたい利用者は，診療期間に申し込むとともに，公開されている公開鍵を利用して健診データを暗号化し，病院や診療所が開設しているデータセンタの指定領域に転送する．診療機関は，秘密鍵によりデータを復号化することで，診断に利用できる．

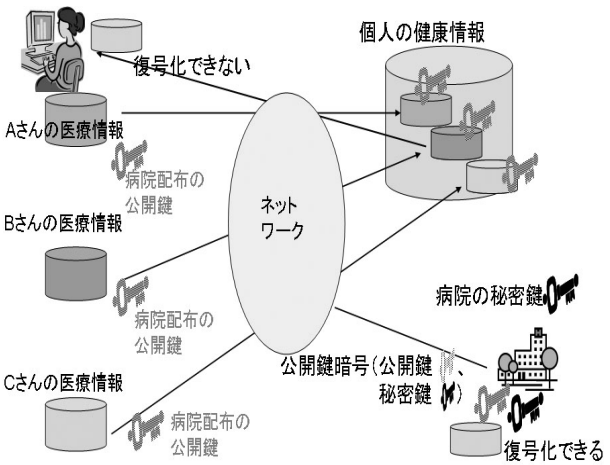

図 2 共通鍵を用いた健康データの共有

Fig.2 Data Sharing With Public Key Encryption

3．3 機密レベルに応じた暗号化

健康診断データには，個人の氏名，生年月日な

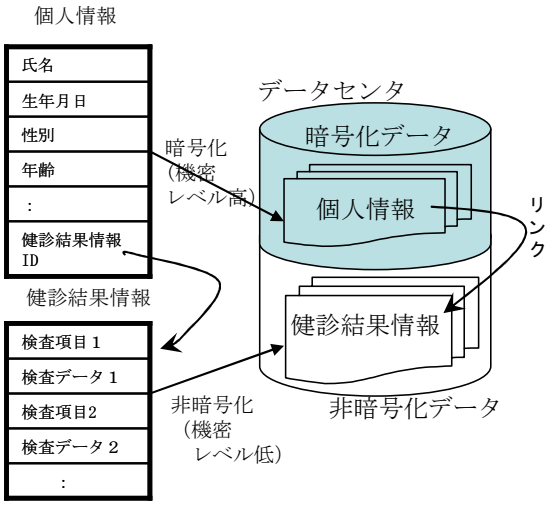

図 3 暗号化レベル設定によるデータ共有

Fig. 3 Data Sharing by Encryption Levels

どのいわゆる個人情報も多く含まれるが，検査結果の数値自体は，個人情報と組み合わせなければデータに過ぎない．そこで，個人に係わる情報は機密にし，検査結果データは機密レベルを低く設定することで，検診データ等への保健機関からのアクセスを可能とする．すなわち，保護したい個人情報に対しては，機密レベルを高く設定し暗号化する．一方，健診結果データは機密レベルを低く設定し公開する．図 3 に示すように健診データを例に個人情報と検診結果データの機密レベルを設定することで，センタでは，個人情報のみ暗号化され，健診結果データは暗号化されずに保存される．データの保有者がアクセスする場合には機密情報と公開データを合成することで，通常の検診データとしてアクセス可能とする．一方，何らかの統計処理をする場合や個人を特定する必要のない検診結果の評価，診断は機密レベルの低い（公開）データにのみアクセスし，結果をフィードバックする場合には，フィードバックデータを公開データに添付することで，データの所有者に渡すことができる．

4. 健診・健康データの入力と自動診断

4．1 データ入力画面の設計機能

体重，体脂肪率，血圧などの健康データを計測し，保存・転送・交換できる健康機器が多く開発されている．また，付属の診療機関を有し，健診情報システムなどを持つ大企業や団体健診データを電子的に健診実施期間から入手可能な健康保険組合増加している．しかし，特に被扶養者の健康診断は民間の病院や健診機関で実施され，健診結果は多くの場合，専用の用紙にプリントされ個人に配布される．装置から電子的に健康データが入手できる場合や健診実施機関からネットワーク経由で個人の健診データが入手できる場合以外は，手作業で健診結果データを入力しデータセンタに送付することになる.そのためのデータ入力ソフトウェアが必要となるが，本システムでは，データ入力部を対話的に設計する機能を提供している．

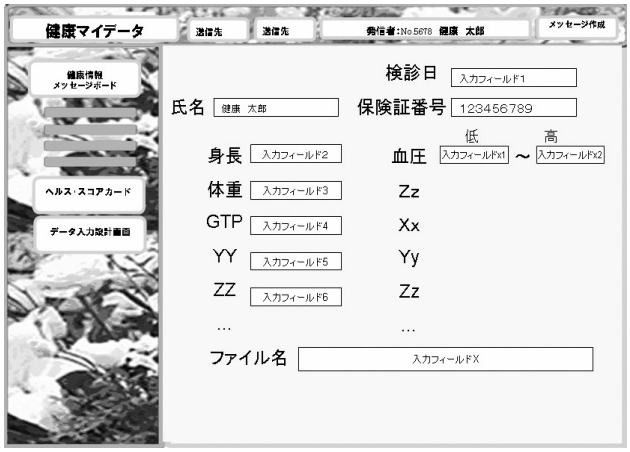

図 4 データ入力画面設計例

Fig. 4 Design Example of Data Entry GUI

図4のように，データ項目と入力フィールを画面上に設定することで，自動的に指定したフォームでのデータ入力画面（プログラム）が作成される．入力フィールドには，数値，文字入力やファイルデータの読み込み指定が可能である．各入力フィールには，データ属性として，実数，整数，文字列，ファイルが指定できる．ファイルデータと指定されたデータフィールドは，ファイルからデータが入力されるので，レントゲン画像，CTやMRI画像などが指定可能である．入力されたデータは，XML形式で保存されるため，入力データのHDML（Health Data Markup Language）形式[3]や他の形式への変換も容易である．

4．2 データ処理プログラムの組み込み

医療・健康データには，数値，文字，画像，信号など様々な形態のデータが存在する．また，データの保存形式や管理形式もことなるため，データ処理を行うためには，統一のフォーマットに変換するか，各形式のデータを扱えるようにソフトウェアを対応させることが必要となる．本システムでは，XML 形式でデータを保存していることから，タグ情報を元にある程度の汎用性を持った形でのデータ処理プログラムの設計が可能であるがすべての形式のデータを扱うことは難しい．そこで，本システムでは，図 4，5のような GUI 画面を利用したプログラム開発ができるインタフェースを公開し，そのインタフェースを利用したプログラムをシステムに組み込むことができるようにした．さらに，センタにデータだけでなく特定の形式のデータを閲覧するソフトウェアも関連付けて保存することで，本システムが提供しないデータ表示機能（例えば，CT や MRI 画像の 3 次元表示など）などを補完することができる．図5

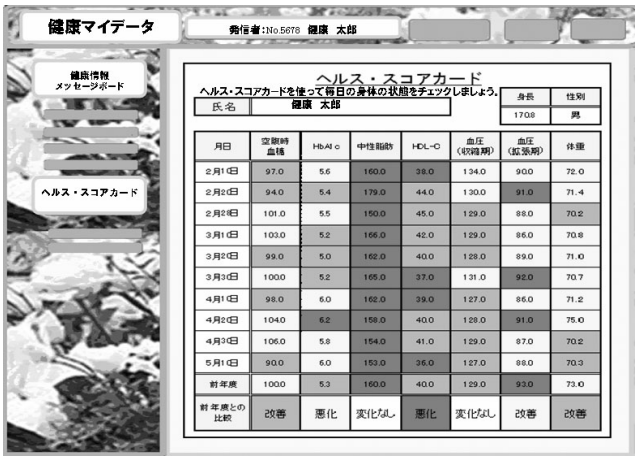

図 5 健康データ評価・表示機能の組み込み
Fig. 5 Evaluation and Display Function of Health Data

は，入力して日々の健康データを表形式で表示し，生活習慣病評価指標に基づき色分け表示するプログラムを組み込んだ例である．

データ入力画面設計やデータ処理プログラムを作成することでシステムの機能拡張が可能であり，このような拡張機能もセンタに登録することで他の利用者も利用可能となる．同様に診療機関が診断結果データを閲覧ソフトとともに健診データや健康データの所有者に暗号化して送付することで，所有者のみが閲覧することができ機密保護が可能である．

5. おわりに

個人の健康・健診データは，個人情報として保護される対象であるため，このようなデータを診断や健康指導に利用する場合にも情報の管理・処理においては厳重なセキュリティが要求される．一方，効果的な健康指導や分析においては，データ収集や統計処理等が必要であり，個人情報として保護しながら，診療機関や健康保険組合が健診データを利用可能に刷る必要がある．本論文では，健診・健康データを暗号化し，センタに保存しつつ，共通鍵，あるいは公開鍵暗号化方式を利用した共有化方式を提案した．さらに，一般利用者が健診データを入力する画面を自由に設計できる機能を提供することで，自由な形式でのデータ入力を可能とした．

参考文献

(1)「高齢者の医療の確保に関する法律」，http://www.mhlw.go.jp/bunya/shakaihosho/iryouseido01/pdf/hoken83b.pdf

(2) 辻井重男,笠原正雄「情報セキュリティ―暗号、認証、倫理まで」，昭晃堂

(3) 保健医療福祉情報 システム工業会:「JAHIS 健診データ交換規約 Ver1.3」，http://www.jahis.jp/standard/seitei/st005/005-00.PDF