付帯情報を含んだ JPEG 画像の秘匿性確保のために steganography 技術を用いてダミー画像に JPEG 画像を埋込む。これらの操作を本研究で開発したソフトウェアで一括処理する。

②埋込み方法

本研究では埋込み法としてビット置換法を用いた（図 2）。本処理においては、画素が持つ濃度値に僅かな変化を与えることで情報の埋込みを可能とする。

まず、デジタル画像の RGB 成分画像より画素を 8 画素単位で取り出して、それぞれの濃度値を読み込む。それに平行して、埋込み対象となる情報を順次 1 バイトづつ取り出していく。次に取得した埋込み対象情報を濃度値の最低位ビット（LSB: Least Significant Bit）に 1 ビットづつ上書きする。これにより 8 画素を用いて 1 バイトのデータを画像内部に書き込むことができる [4,5,6]。この上書きによって、一部の画素において濃度値が変化する事になるが、それは±1 の範囲にすぎないので、人の目では色の違いを判別できない。よって、画像に情報が隠されていることを気づかれる恐れが無い。

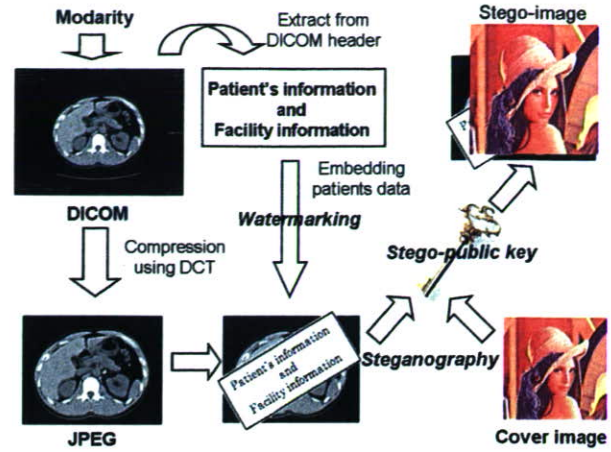

図 1　The integration security system

Example
Hiding Message : 01000001
Change with 3pixels(Cover Image)

Original	Red	Green	Blue
pixel 1	11111000	11001001	00000011
pixel 2	11111000	11001001	00000011
pixel 3	11111000	11001001	00000011

Message embedding to LSB : 01000001

New	Red	Green	Blue
pixel 1	1111100**0**	1100100**1**	0000001**0**
pixel 2	1111100**0**	1100100**0**	0000001**0**
pixel 3	1111100**0**	1100100**0**	0000001**1**

図 2　Embedding Algorithm

Abdominal CT　Vertebrae MRI　Chest CR

図 3 Medical images used in the experiment

③対象画像

本研究では、512×512 画素の腹部 CT 画像、256×256 画素の頭部 MR 画像、および 1024×1024 画素の胸部 X 線画像の 3 種類のモダリティについて検討を行った（図 3）。また、施設情報を埋込んだ医用画像を埋込むためのダミー画像として 512×512 画素の SIDBA（Standard Image Data-BAse）標準試験画像 Lena を用いた。

④埋込み後の画質評価－客観的－

埋込み前後の画像の評価として PSNR を用いた。PSNR は映像品質の客観的な画像評価指数であり、原画と処理後の画像の平均二乗誤差（MSE）で表される（図 4）。両画像の相違が大きければこの値は小さくなる。一般的に、PSNR=40dB 以上で原画との見分けが難しく、20dB 以下になると見るに耐えない画質と言われている [7]。

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \, dB$$

$$MSE = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left(f(x,y) - f'(x,y) \right)^2$$

図 4　The definition of PSNR

⑤埋込み後の画質評価－診断医による主観的画質評価－

モダリティごとに原画像 1 枚と、これに透かし埋込強度 t を変化させて得られた透かし埋込画像 4 枚を加えて計 5 枚とした。さらに、同一画像を読影した結果が一致するか否かの再現性を評価するために、読影する枚数を 2 倍にし、ランダムな順序で計 10 枚の番号付けを行った。

読影は、1名の10年以上の読影経験を有する放射線科医1名が3Mピクセルの LCD モニタを用いて時間制限無しでおこなった。はじめに、透かしの埋め込まれていない画像を LCD モニタ上に表示し、次にビット置換法にて最も強く透かしが埋め込まれたサンプル画像を表示することにより、透かし位置・パターンを例示した。その後、モダリティごとに番号順に10枚の読影を行った。画像に対する評価は、下記基準の3段階とした。

(1) 原画像と見分けがつかない (○)

(2) この画像が診断できる最低限度である (△)

(3) 劣化が激しく、診断への利用不可 (×)

C．研究結果：

埋込み後の画像の視覚的な劣化が見られないことがまず、必要である。加えて、埋込み前後の画像の容量変化がないことが必要となる。これらによって、医用画像が隠されていることを隠すことができ、秘匿性をうち破る意欲が湧かないと予想できる。これにより、異なる施設間で医用画像の送受信時など、万が一、画像が流出した場合でも医用画像の秘匿性・安全性が確保できると考えられる。

本研究により作成したソフトウェアは二つの処理から成り立つ。まず、一つ目は DICOM 画像のヘッダー情報から患者情報・施設情報を抽出し、JPEG に圧縮する際に、電子透かしとしてその情報を埋込む。その際、圧縮率は75%とした。また、二つ目は電子透かしを含んだ JPEG 画像をおとり画像に埋込む処理である。

そのソフトウェアを用いる事で埋込み許容容量であればモダリティ画像に関わらず電子透かしとして患者情報埋込み可能であり、その付帯情報を含んだ医用画像をおとり画像に埋込みが可能であった。それぞれの埋込み前後の画像を図5に示す。

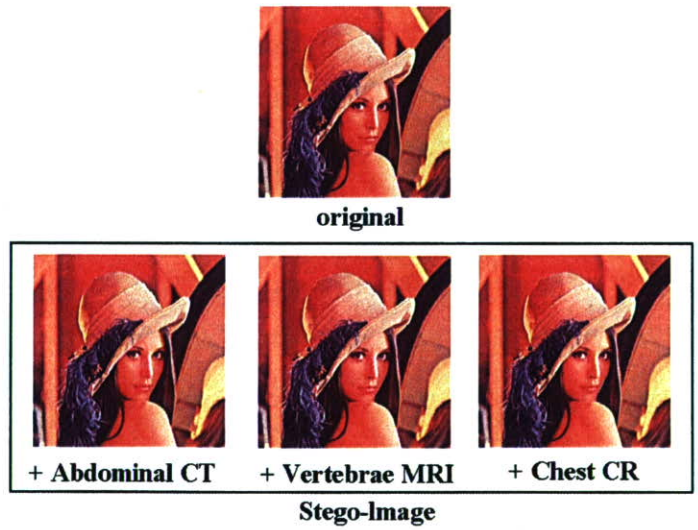

図 5 Different embedding in the Stego-image

埋込み前後の画像間に視覚的変化がほとんど無いことが確認できる。埋込み方法として画素の濃度値を僅かに変更することにより埋込みを行っているので、画像容量が変化しないことが確認できた。また、埋込み前後の画像劣化を客観的に示すために行った PSNR の値を表1に示す。どのモダリティの種類に関わらず、PSNR が 40dB を超えていることから画像が劣化せず、埋込み対象の容量のみに依存することが確認できた。

表 1 処理後画像の PSNR (dB)

Modarity	Watermark Embedding Intensity, t			
	2	4	8	16
Chest X-p	42.3	41.2	40.6	37.6
Abdominal CT	48.4	43.5	40.3	38.0
Head MRI	45.9	41.4	38.5	36.2

表 1 の値を見ると、電子透かし強度が 4 以下の場合、基準値と言われている 40dB を超えているので、各モダリティから出力される画像の種類に関わらず、本研究で提案した電子透かし埋込による画像劣化を抑えていると言える。

しかし、モダリティの種類によって、診断に影響を与えない透かし埋込強度は異なった。なお、40dB を超えているが CR の値は他の MR、CR と比較して画質が劣化しているという結果になった。これは、画素値の数による違いになると考えられる。

専門医の肉眼による主観評価の結果を表 2 に示す。

表 2 処理後画像の肉眼的主観評価結果

Modarity	Watermark Embedding Intensity, t			
	2	4	8	16
Chest X-p	○	○	△	×
Abdominal CT	○	○	○	△
Head MRI	○	○	○	○

PSNR の結果と同様に、モダリティの種類によって、診断に影響を与えない透かし埋込強度は異なった。しかし、埋込強度が 4 以下の場合はいずれのモダリティでも診断に影響を与えないという結果になった。これにより、画素値の変化が 4 以下にした場合は医用画像に対して電子透かしを埋め込んだ場合でも、診断に影響を与えないと言うことを示唆できた。

また、PSNR の結果と主観的評価を比較した場合、MRI と CR に違いが見られた。PSNR の結果では、MRI は劣化しているという結果がでたにもかかわらず、主観評価においては、ほとんど劣化していない結果になった。それに対し、CR では PSNR では画像の劣化が見られなかったのに対し、主観的評価においては診断に影響を与えやすいという結果になった。これは、それぞれの画像の画素数の違いが影響していると考えられる。CR は MRI に比べて、画素数が多いためにノイズに対して敏感であるために、電子透かしを含むことで視覚的に変化をとらえやすい。一方、MRI は画素が小さいために画素に変化を与えても視覚的には変化を人の目では見えにくいと考えられる。

D. 考察：

本研究で構築したシステムは、モダリティに依存せず、埋込み許容容量内であればいずれの画像でも埋込可能であった。埋込み法として、ビット置換法により画素の濃度値を僅かに変化させることにより埋込みを行っているので、埋込み前後で画像容量の変化はなかった。また、本システムでは Steganography を用いたので、人間の視覚的に医用画像埋め込み前後での画質変化を知覚できないのに加えて、PSNR の結果から画像の統計的性質などにおいても不自然さを検出されないことが確認できた。よって、ダミー画像を閲覧されても、医用画像が埋込まれていることを推測されないと考えられる。　したがって、異なる施設間で医用画像の送受信・保管時など、万が一、画像が流出した場合でも医用画像の秘匿性は十分確保できると考えられる。

E．結論：

電子透かしの著作権の保障、Steganography の高い秘匿性という利点を統合することにより医用画像の伝送前後に関わらず著作権保護と秘匿性確保とが同時に得られる。また、本研究で構築したシス

テムは、フリーウェアのツールを使用しているため、医用画像伝送の際に各施設の初期投資及び運用コストを少なくでき廉価なシステムとなり、全ての処理を自動で行えるので簡便なシステムとなる。

今後、埋込み許容容量が増加することにより、遠隔画像診断など医用画像を施設外に持ち出す際にも、VPN など特別な暗号化は必要としなくても、一般のネットワークを利用した画像伝送・保管も可能になると考えられる。

【参考文献】

1) 赤木信裕、稲本一夫、芦田信之、他：位置情報付画像所見を利用した人間ドッグのデータ提供、医療情報学、22(Suppl.)、 610-611, 2002

2) Umeda T, Yuminaka Y, Haneda K, Harauchi H, Inamura K, Iwata Y：Development of Digital Images Communication and Archieve System using Watermarked Image、MEDICAL IMAGING TECHNOLOGY、Vol18、No4、507-508、2000

3) 佐々木良一、吉浦裕、手塚悟、他：インターネット時代の情報セキュリティ　暗号と電子透かし、共立出版、2000

4) 小野東：電子透かしとコンテンツ保護、(株) オーム社、2001

5) 真嶋由貴恵、後藤大輔、島田恭宏、橋本禮治、塩屋充：施設間ネットワークにおける看護情報の保護　ステガノグラフィ技術の応用、医療情報学、Vol20、No2、135-142、2000

6) 山野辺裕二：医療分野へのステガノグラフィ技術の応用について、医療情報学、Vol20、No.6、539-541、2000

7) 八幡勝也、波田哲郎、國武惠明、宮野章、伊勢田司、小池淳、東敏昭：JPEG/JPEG2000 方式による内視鏡画像の評価、医療情報学、Vol24、No2、291-296、2004

Ⅲ. 研究成果の刊行に関する一覧表レイアウト

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
丸山剛,喜多紘一,鈴木裕之,小尾高史,谷内田益義,山口雅浩,大山永昭	医療分野における自己情報コントロールを目的としたアクセス制御方法に関する研究	電子情報通信学会論文誌	J90-D(12)	3170-3180	2007
鈴木裕之,喜多紘一,谷内田益義,小尾高史,山口雅浩,大山永昭	HPKIによる電子署名を利用した健康管理データ提供・参照システム	ワイヤレス・テクノロジーパーク2007講演予稿集		56-57	2007
喜多紘一,平井正明,鈴木裕之,谷内田益義,山口雅浩,小尾高史,大山永昭	CDA R2に準拠した個人提供用健康診断結果報告書を利用した個人健康診断結果管理システム	第27回医療情報学連合大会(第8回日本医療情報学連合大会)予稿集		P7-4	2007
喜多紘一,鈴木裕之,竹田忠雄,猪俣彰浩,島田宏,有馬一閣	HPKIとダイナミック・オンデマンドVPNとの連携によるセキュアな医療ドメインネットワーク	第27回医療情報学連合大会(第8回日本医療情報学連合大会)予稿集		1-H-3-2	2007
喜多紘一,鈴木裕之,竹田忠雄,猪俣彰浩,島田宏,有馬一閣	VPN接続許可をポリシー制御可能なダイナミック・オンデマンドVPN	SCI2008(暗号と情報セキュリティシンポジウム)予稿集		4C2-2	2008
岡野翔,鈴木裕之,小尾高史,山口雅浩,谷内田益義,大山永昭,喜多紘一	個人情報の利活用を可能とするサービス基盤に関する研究	電子情報通信学会2008年総合大会講演予稿集		520	2008
大山永昭	電子政府・電子自治体の実現について	月刊 日本行政	412	10-18	2007
大山永昭	政府が掲げるIT戦略は、“正しい方向”を向いているか “国家IT戦略”から“変化の時代”を正しく読み解く	CIO Magazine	83	20-28	2007
大山永昭	医療情報システムのネットワーク環境と基盤の整備を推進します	月刊 新医療	Vol.34 No.390	152-155	2007

大山永昭	住基カードの今後の展開～利便性を実感できるカードとして活用の幅が広がる～	月刊LASDEC	Vol.37 No.8	6-7	2007
八幡勝也 他	特定健診制度に対して産業保健が抱える問題点と解決策、これでわかる特定健診制度	じほう		233-247	2007
八幡勝也	3.特集1『健康情報シリーズ第２回』生涯健康管理の重要な要件となる健康情報システムについて	Report of the Society of HDS	Vol.11 No.2	18-22	2007
八幡勝也	特定健診制度と産業保健の問題点と解決策	第27回医療情報学連合大会	S11-2-C	140-141	2007
山本隆一	医療情報の安全管理	医学のあゆみ	Vol.222 No.8	571-575	2007
Katsuya Tanaka, Mayumi Yoshida, Ryuichi Yamamoto	Secure Remote Access for Web Based Clinical Information System Using Policy Control of PCs and Healthcare PKI Authentication	MEDINFO 2007		1480	2007
Omatsu M., Umeda T., Tachibana H., Okawa A.	Development of Narratine Based Medicine(NBM) Automatic Medical Comminication System	The Kitasato Medical Journal	Vol.37 No.2	65-75	2007
Kenta Miwa, Tokuo Umeda, Nao Fukuchi, Shuji Yamamoto, Akio Okawa, Hidenobu Tachibana, Masahiro Omatsu	A Novel Security Model for Hiding in Medical images using High-Capacity Digital Watermark And Steganography Technique	93th Scientific Assembly and Annual Meeting Rediologi-cal Society of North America2007		841	2007
三輪健太, 梅田徳男, 阿見年典, 福地奈緒, 山本修司, 大川明子, 橘英伸,	電子透かし技術を用いた医用画像の秘匿性確保･著作権保護システムの構築	医療情報学会秋季大会予稿集		1-3	2007

大松将彦					
Okawa A., Umeda T., Fukuchi M., Miwa K., Hashiguchi N.	Development of a tele-support system for cancer outpatients	The Kitasato Medical Journal	Vol. 38 No. 1	1-8	2008

論　文

医療分野における自己情報コントロールを目的としたアクセス制御方法に関する研究

丸山　剛[†*a)]　喜多　紘一[†b)]　鈴木　裕之[†c)]　小尾　高史[††]
谷内田益義[†]　山口　雅浩[†]　大山　永昭[†]

The Research of the Access Control Method for Self-Information Control in a Medical Field

Tsuyoshi MARUYAMA[†*a)], Koichi KITA[†b)], Hiroyuki SUZUKI[†c)], Takashi OBI[††], Masuyoshi YACHIDA[†], Masahiro YAMAGUCHI[†], and Nagaaki OHYAMA[†]

あらまし　本論文では自己情報コントロールが必要な場面を想定し，アクセス制御用の閲覧許可書を用いたアクセス制御方法を提案する．提案手法では医療データの情報主体者が閲覧許可者に対して許可書を発行し，閲覧許可者は閲覧時それをサーバに送り，サーバ側でデータにアクセスする人及び/または資格の認証を行うことにより情報主体者が閲覧を同意した閲覧者のみがその医療データにアクセス可能となる．また実証システムの構築及び動作実証を行い提案手法の実現可能性を示した．

キーワード　個人情報保護，自己情報コントロール，資格認証，アクセス制御

1. まえがき

近年，医療分野において医療情報を電子化・データベース化・ネットワーク化して利用する動きが進んできている．医療情報を電子化・データベース化・ネットワーク化することのメリットとしては，ネットワーク通信によって，高速で低コストな情報伝達が可能になること，データを共有できること，また計算機を利用することで情報解析などのデータの二次利用が容易に行えることなどが考えられる．

その結果として医療サービスの質の向上[1]，コスト削減，今まで行えなかった新たな医療サービスの展開が期待できる．その反面，医療情報は極めてセンシティブな個人情報であるため，医療情報の盗聴・漏えいや不正なアクセスなどの危険を防止するための対策が必要になる．

また，情報の電子化・共有化が進むのに伴い，個人情報保護[2]に対する要求も高まっている．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，電子化した情報を共有化して利用するようになった場合，利用者の意図しない利用の危険性が存在するため，各情報主体者が自分の情報を自分でコントロールする権利（自己情報コントロール権）を保護することに移ってきている．2005年4月に全面施行された「個人情報保護法」はその保護を「個人情報取扱事業者の義務」として取り入れられている．

自己情報コントロール権をより具体的にいえば「情報主体者の同意に基づいた利用目的にのみ被提供者が利用するように自分に関する情報をコントロールする権利」である．

現段階の電子情報の共有化技術では，管理者が一括して各施設のアクセスポリシーに従って各個人のデータへのアクセス制御管理を行っているケースが多く，各個人が自分の情報に対するアクセス制御を提供情報ごとあるいは状況に応じてそのつど機敏に行うという

† 東京工業大学像情報工学研究施設，横浜市
Tokyo Inst. of Tech. Imaging Sci. & Eng. Lab., 4259 Nagatsuta-cho, Midori-ku, Yokohama-shi, 226-8503 Japan
†† 東京工業大学総合理工学研究科，横浜市
Tokyo Inst. of Tech. Interdisciplinary Grad. School of Sci. & Eng., 4259 Nagatsuta-cho, Midori-ku, Yokohama-shi, 226-8503 Japan
* 現在，NEC ソフト株式会社
a) E-mail: maruyama-tsuyoshi@mxp.nes.nec.co.jp
b) E-mail: k.kita@gakushikai.jp
c) E-mail: hiroyuki@isl.titech.ac.jp

自己情報コントロール権に対応したアクセス制御方法が確立しているとはいえない．医療情報の場合のアクセス制御は収集時に利用目的や提供先の指定の同意をとり，その後はあまり変更させない静的なコントロールよりは，病状に応じてそのつどこまめにコントロールできる動的なコントロールに対応できる方式が望まれる．そこで本論文では，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，想定した利用形態での自己情報コントロールに対応したアクセス制御方法の提案を行う．

2. 想定する利用形態

本論文では，自己情報コントロールに対応したアクセス制御が要求される利用シーンとして，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を想定する．

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，医療行為等に利用されている．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．

将来的には，電子化され，データも健康診断データ，お薬手帳，介護ノートや母子手帳の内容のみでなく，診断書や退院サマリー等の診療情報も個人に提供され，個人の管理でデータベース化されることが予想される．こうした患者，被介護者や健康人に提供されたデータの集合である電子化されたデータベースをここでは健康手帳といっている．今後，各種医療施設，介護施設及び健康増進施設等のデータベースとリンクを取り合いながら健康管理を行うことが考えられる．

そうした場合，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，現在，制約付で一部実施されているネットワークを通じた遠隔医療やセカンドオピニオンにおける患者健康情報の提示が挙げられる．遠隔医療では，医師と健康手帳利用者が地理的に離れた場所に存在するため，遠隔の医師がデータにアクセスできるためには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．また，生命の危機が生じた場合などの緊急時には，健康手帳利用者が閲覧許可を与えていない医師に対しても，必要に応じてデータを閲覧できる仕組みが要求される．

よって本論文では，遠隔地の医療施設の特定の医師あるいはその施設に勤務している不特定の医師に対し，健康手帳利用者の自己情報コントロールによって健康手帳データへの閲覧許可権を設定する方法を例に挙げ，検討を進める．

図 1 に本論文で想定する電子健康手帳システムに登場するプレイヤを示す．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．健康手帳利用者が，ある医者に遠隔診察を依頼し，その診察において健康手帳の内容を提示することを行う．その場合，閲覧する医者は，患者の許可を得ることと，自分自身の身分の証明（個人認証及び資格認証）を要件とする．また，医者や利用者の認証には医師等の国家資格を証明するヘルスケア公開鍵基盤 (HPKI) [3] の仕組みを用いた個人認証，資格認証 [4], [5] を利用する．なお，健康手帳サービス機関へのアクセスは患者が選択した医師の属する不特定な医療機関からのアクセスとなり，あらかじめ健康手帳サービス機関と契約した特定の固定した医療機関へのサービスを行うものではない．

この証明書形式は医療用の PKI の ISO 規格である TS17090 [6] に準拠している．更に，厚労省のネットワーク基盤検討会で検討されている「保健医療福祉分野 PKI 認証局証明書ポリシー」[7] にも準拠している．

このポリシーでは証明書の拡張領域の「subjectDirectoryAttributes」に hcRole という項目をもうけ国家資格を認証し証明することができる．

[7] は現在では署名用の証明書を発行するための証明書ポリシーのみとなっているが，同様な形式（以下認証用 HPKI と称す）で認証用証明書の発行が可能であり，こうした証明書は（財）医療情報システム開発

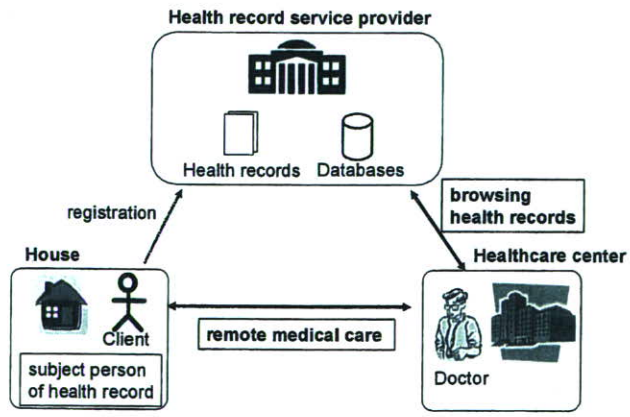

図 1 想定する利用形態
Fig. 1 Usage pattern.

センターから入手することができる．本論文では情報主体者へは署名用の証明書，医師に対しては認証用の証明書を発行して実証試験システムを構築する．

3. アクセス権設定における要件

本論文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，以下の四つが挙げられる．

（1） 健康手帳利用者のみがアクセス権の設定を行えること

健康手帳利用者以外の第三者が，アクセス権を不正に設定するという脅威が考えられる．この脅威に対しては，健康手帳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が必要になる．

（2） 利用者の意図した人のみが閲覧可能なこと

健康手帳の閲覧を許可されていない人が，不正に閲覧するという脅威が考えられる．この脅威に対しては，健康手帳閲覧者が健康手帳利用者の許可を受けていることを健康手帳サーバに証明できる仕組みが必要になる．また，健康手帳データを閲覧する人は，医師に限定されるため，閲覧許可を受ける人が医師であることを証明する必要がある．

ただし緊急時において可用性を確保するため，閲覧するのに適当であると判断できる人ならば，利用者の閲覧許可証がなくてもアクセス可能になるよう，前もって健康手帳利用者に「どのような資格者にどのデータを閲覧してもよいか」同意をとっておく必要がある．

（3） アクセス権の設定を細かく行えること

健康手帳利用者が医師に提示する健康データは医師が診断に必要とし医師により要求されたデータ以上は見せる必要はないため，TPO によって提示項目が変化する．よって健康手帳利用者の意図するデータのみを医師に閲覧させるために，アクセスを許可するデータ項目を細かく指定可能な仕組みが必要になる．

（4） 閲覧許可の取消しが可能なこと

医師に健康手帳データへのアクセスを許可した後でも，一定期間経過後あるいは何らかの理由で許可を取り消す場合があるので，許可の取消しを行う仕組みが必要になる．

4. 提案手法

4.1 アクセス権設定方法

本論文では，閲覧する権限や資格を証明する機能を有し，また個人レベルで発行可能な電子証明書として「閲覧許可書」を定義し，閲覧許可書を用いたアクセス権の設定手法を提案する．

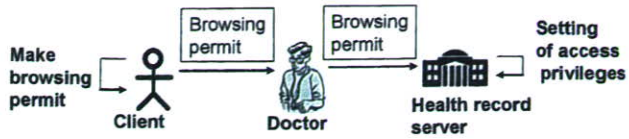

図 2 提案するアクセス制御方法
Fig. 2 Access control method.

本論文で想定した健康手帳システムにおいて，健康手帳利用者は，健康手帳データの閲覧を許可する人に対して閲覧許可書を発行・送付する．健康手帳データの閲覧を許可された人は，閲覧許可書を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内容に従ってアクセス制御が行われる（図 2）．

このように閲覧許可書を用いてアクセス制御を行うことにより，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

提案手法で使用する閲覧許可書の記載内容は，アクセス権設定における要件を満たすために以下のようになる．

- 利用者の情報
- 医師の情報
- 権限の詳細
- 閲覧許可書の有効期限
- 利用者の電子署名

「利用者の情報」は，健康手帳サーバに登録されている利用者を識別するための情報として，健康手帳サービス機関に登録するときに発行される利用者登録番号を記載する．

「医師の情報」は，健康手帳データを閲覧する人を特定するための情報として，特定の医師を指定する場合は医師の公開鍵証明書の識別名あるいは医師であればだれでもよいとするのであれば医師資格を記載する．

「権限詳細」は，健康手帳利用者が健康手帳データ閲覧者に閲覧を許可する項目を記載する．設定する項目としては，検査データ（検診データ，画像データ，問診データ）や病歴等であり，それぞれ検査期間を指定してアクセス許可を設定する．例えば「1990 年から 2000 年までの体重と血圧のデータを閲覧許可」といった具合になる．

「閲覧許可書の有効期限」は，健康手帳データ閲覧

者に閲覧を許可する期間を限定するための有効期限を記載する．

「利用者の電子署名」は，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．

また利用者は閲覧許可書の作成及び署名の検証を行うための準備として，特定の医師を指定する場合は「医師の情報」の欄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，及び利用者が電子署名を作成するための秘密鍵に対応する公開鍵の公開鍵証明書を健康手帳サービス機関に登録しておくことが必要となる．

また，閲覧許可の取消しについては，利用者が健康手帳サービス提供機関へ取消しを申請し，サービス提供者側で閲覧許可証の失効リストを管理する運用を行うか，有効期限を短くすることにより閲覧許可書の取消しを行わなくとも実質的な効果を上げることができ，不必要な閲覧を防ぐことが可能になる．

医師から健康手帳サーバに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，資格認証を行う．次に健康手帳サービス提供機関にあらかじ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」の検証を行う．そして電子署名の検証結果が正しければ閲覧許可書に記載してある有効期限の検証を行う．最後に医師の公開鍵証明書に記載されている識別名あるいは資格と閲覧許可証の「医師の情報」の比較を行い，両者が同じならば，閲覧許可証に指定されている健康手帳データの項目について閲覧が許可される．医師資格の確認は，医師の公開鍵証明書の国家資格を示す hcRole の項目を評価して行う．

なお，緊急時におけるアクセス許可の方法については，利用者が信頼する第三者に対して健康手帳データを臨時に閲覧する権利を与えられるような仕組みが必要になるが，そのための具体的方法については今後の課題であり，本論文の「むすび」にその１ソリューションを示した．

4.3 アクセス権設定のシーケンス

まず，利用者が閲覧許可書を作成し閲覧を許可する医師に閲覧許可書を送付するまでのシーケンスを説明すると，以下のようになる（図 3）．

① 利用者が医師の公開鍵証明書を取得する．

② 利用者が閲覧許可書を作成する．

③ 利用者が医師に閲覧許可書を送信する．

次に，閲覧許可書を受け取った医師が閲覧許可書を健康手帳サーバに送付して健康手帳データを閲覧するまでの流れは以下のようになる（図 4）．

④ 医師が健康手帳サーバにアクセスする．

⑤ 医師と健康手帳サーバ間で相互認証，資格認証を行う．

⑥ セキュア通信を開始する．

⑦ 医師が健康手帳サーバに閲覧許可書を送信する．

⑧ 健康手帳サーバで閲覧許可書の検証を行う．

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する．

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，医師が閲覧する．

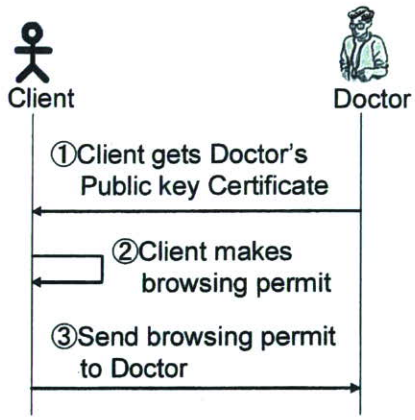

図 3 利用者が閲覧許可書を作成する場面
Fig. 3 Stage of making browsing permit.

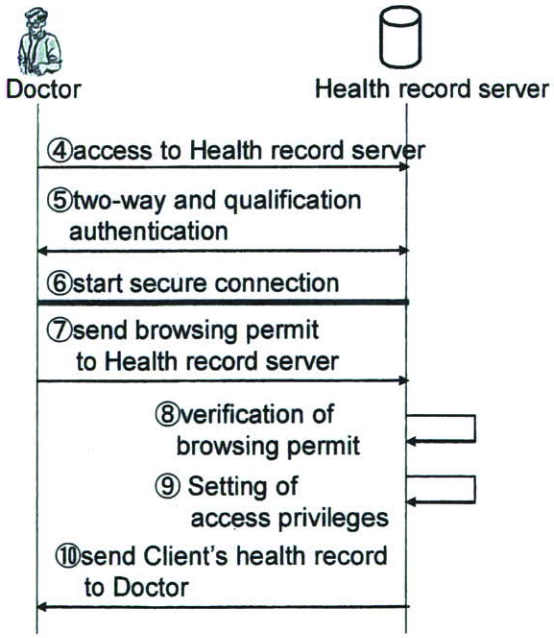

図 4 医師が健康手帳データを閲覧する場面
Fig. 4 Stage of browsing health record.

4.4 提案手法と関連研究との比較

本節では，代表的な従来のアクセスコントロール技術との比較を行い，本手法の特徴を述べる．

文献[8]で提案されている手法は，共有データベース上のデータに対するアクセス制御という点で本研究の提案手法と類似しているが，情報主体者（履修者）とシステム（大学）がどのように閲覧者（第三者）を認証しているのかが不明確である．これに対し本提案手法は，情報を閲覧する人の認証をPKIの仕組みを利用して実現している．

また文献[9]では，信頼性の連鎖を用いてアクセスコントロールを行っており，本論文と同じように情報主体者が属するコミュニティ以外の人に関してもアクセス権の付与が行える仕組みとなっている．しかしあるエンティティを信頼するためには二つ以上の信頼点が必要となり，この方法は確実な信頼点一つが定まらない場合には有効であるが，医療分野におけるHPKIのような確実な信頼点がある場合には本提案のようなシンプルな仕組みの方が信頼性が高いと考えられる．

また医療分野におけるアクセス制御を考えた場合，健康手帳の閲覧を許可する医療機関や医師は医療法上，患者の行き先を限定してはならないこと，つまりフリーアクセスが原則なため，患者がある特定の「健康手帳サービス機関」に対して行きつけの医療機関や閲覧する医師をあらかじめ登録しておくことはできない．そこで患者が発行する閲覧許可証により，「健康手帳サービス機関」のサーバがアクセスする相手をアクセスのつど，判断して閲覧を許可することを特徴としている．こうしたフリーアクセスを原則としたシステム要件は医療分野で要求される特徴であり，文献[8],[9]を含む従来研究では今のところ議論されておらず，医療で一番ニーズが高い課題である．

更に提案したシステムでは，サーバは閲覧許可証に記載された患者の署名によりアクセスの正当性を判断し，閲覧許可証の中には医師個人の公開鍵証明書，あるいは医師資格，あるいは医療機関名が記入されているので，これとサーバへアクセスしたときの認証結果をマッチさせ許可している．この際用いる公開鍵証明書は他分野ではまだ使用されていない証明書形式である本人確認と属性証明である医師などの国家資格や医療機関の管理者を署名できる証明書を利用している．これは医療分野での標準に準じた認証用HPKIを用いて初めて解決できるので医療分野に特化した新規性のある技術である．

5. 実装方法

5.1 システム構成

医師が利用者の健康手帳データを閲覧する場合を想定し，実証システムを構築した．このシステムは，閲覧許可書を作成する利用者システム，健康手帳データを閲覧するWebブラウザ，健康手帳データを保存しアクセス制御を行う健康手帳サーバから構成される．

医師の健康手帳サーバへのアクセスには，汎用のWebブラウザ(InternetExproler6.0)を用いた．また今回のシステムでは医師が健康手帳サーバにアクセスする際にはSSL通信を用いて暗号化通信を行った．

5.2 利用者システム

利用者システムは閲覧許可書を作成するシステムである．本システムではXML形式の閲覧許可書を作成した．また利用者システムはPC上のアプリケーションとICカード内のアプリケーションから構成され次のような機能を有する．

- 医師の公開鍵証明書から医師の識別名を取得する機能
- 利用者が決定した閲覧許可の権限詳細を閲覧許可書に記載する機能
- 権限詳細をもとにXML形式の閲覧許可書を作成する機能
- 利用者のICカード内に保存してある秘密鍵を用いて電子署名を作成する機能

利用したICカードは，マルチアプリケーション対応型（複数のアプリケーションがインストール可能）のG&D社製カードを用い，JAVAアプリケーションでの開発を行った．

利用者システムで閲覧許可書を作成する際の流れは次のようになる（図5）．

① 利用者がアクセス制御情報（健康手帳データの閲覧を許可する医師と閲覧を許可するデータの範囲）の内容を決定する．

② アクセス制御情報をICカードに送信する．

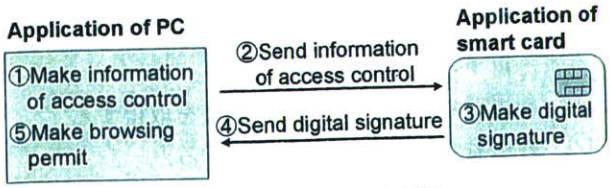

図5 閲覧許可書作成手順
Fig. 5 Procedure of browsing permit.

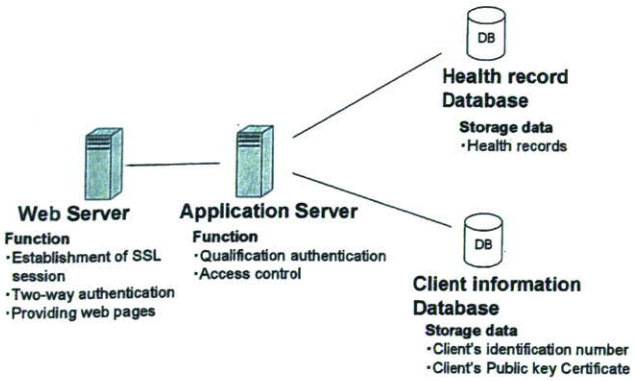

図 6　健康手帳サーバの構成
Fig. 6　Health record server structure.

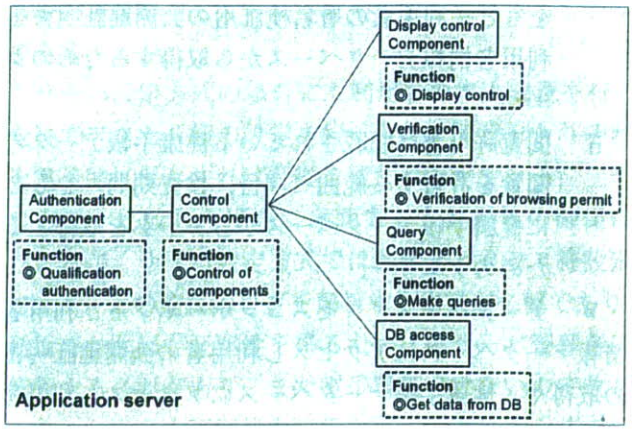

図 7　アプリケーションサーバ内のコンポーネント
Fig. 7　Components of application server.

③　IC カード内では，送られてきたアクセス制御情報からハッシュ値を求め，秘密鍵で暗号化して電子署名を作成する．

④　電子署名データを PC 上のアプリケーションに送信する．

⑤　PC 上のアプリケーションでは，IC カードから送られてきた電子署名データを用いて閲覧許可書を作成する．

5.3　健康手帳サーバ

本システムでは提案したアクセス制御手法を実現するために健康手帳サーバを以下の三つの要素から構成する（図 6）．

- Web サーバ
- アプリケーションサーバ
- データベース

Web サーバは Web ページの提供と医師との相互認証を行う機能を，アプリケーションサーバは医師の資格認証や閲覧許可書の内容に従ってアクセス制御を行う機能を，データベースは利用者の登録情報と健康手帳データの保存を行う機能を有する．

5.3.1　Web サーバ

本システムでの Web サーバの機能としては

- 医師と SSL 通信を行う
- 医師と相互認証を行う
- Web ページを提供する

である．

Web サーバとしては汎用的な Web サーバである Apache2.05 を使用した．また Apache のクライアント認証機能を用いて医師との相互認証を行い，医師との SSL 通信も Apache に SSL モジュールを組み込んで行った．

5.3.2　データベース

本システムでは利用者の登録情報を保存するデータベース（利用者情報データベース）と健康手帳データを保存するデータベース（健康手帳データベース）の二つのデータベースを用いる．また DBMS（Database Management System：データベース管理システム）としては実証試験用として利用が容易な MySQL4.0.13 を使用する．

利用者情報データベースには利用者の登録番号と電子署名検証用の公開鍵証明書を保存し，健康手帳データベースには利用者の健康手帳データを保存する．

5.3.3　アプリケーションサーバ

アプリケーションサーバを以下のコンポーネントから構成する（図 7）．

- 認証コンポーネント：医師の資格認証を行う
- 制御コンポーネント：各コンポーネントの制御を行う
- 許可書検証コンポーネント：閲覧許可書の正当性の検証を行う．検証項目は次のようになる

i.　閲覧許可書に記載されている電子署名の正当性の検証

ii.　閲覧許可書の有効期限の正当性の検証

iii　閲覧許可書に記載されている医師の識別名と健康手帳サーバにアクセスしてきた医師の識別名の検証

- クエリー作成コンポーネント：クエリー作成コンポーネントは各データベースからデータを取得するためのクエリーを作成するコンポーネントであり次に述べるような 2 種類のクエリーを作成する．

i.　閲覧許可書に記載されている利用者の登録番号

をもとに利用者の署名検証用の公開鍵証明書を利用者情報データベースから取得するためのクエリー．

ii. 閲覧許可書に記載されている健康手帳データの閲覧を許可する範囲（項目，検査期間）をもとに健康手帳データベースからデータを取得するためのクエリー．

- データベースアクセスコンポーネント：利用者情報データベースにアクセスし利用者の公開鍵証明書の取得や，健康手帳データベースにアクセスし利用者の健康手帳データの取得を行う．
- 表示制御コンポーネント：健康手帳データの表示を制御する．

6. 動作実験

提案手法の実現可能性の検証を行うために実際に実証システムを構築し動作実験を行った．

今回の動作実験での動作手順は次のようになる．

① 健康手帳サーバの起動
② 閲覧許可書の作成
③ 医師が健康手帳サーバにアクセス
④ 医師・健康手帳サーバ間で相互認証，資格認証
⑤ 閲覧許可書の送受信
⑥ 閲覧許可書の検証
⑦ アクセス権の設定
⑧ 健康手帳データ閲覧

動作実験の結果，健康手帳データの情報主体者である利用者のみが閲覧の許可を行えることを確認した．そして閲覧許可を与える際には利用者の意図したデータのみを閲覧者に閲覧させることができた．

また適切な資格を有していない人が閲覧を行おうとした場合，閲覧許可書を改ざんした場合，有効期限の切れた閲覧許可書を使用した場合，第三者が利用者から閲覧を許可された医師になりすました場合等の利用者の意図しない不適切なアクセスの場合には健康手帳データの閲覧が行われず，利用者のデータが守られることが確認された．

7. システム評価

7.1 比較対象とするサーバ設定方式

提案手法と「サーバ設定方式」とを比較する．サーバ設定方式のうち，現在多く行われている方式はサーバ管理者が利用者のシステム加入時の同意に基づき，アクセス者によるアクセス権限を設定する方式が主流であり，この方式ではサーバ管理者へ何らかの形でその意思を書面等で伝える必要がある．そのため，そのつど利用者の意思を反映して，臨機応変に設定をコントロールすることは難しい．

そこで比較にあたり，従来方式より進んだものとして慶応義塾大学の内山らにより提案されている文献[8]による方式と比較した．このサーバ設定方式ではアクセス権設定の際には情報主体者はアクセス許可者（情報主体者からデータへのアクセスを許可される人）や閲覧を許可するデータなどの情報をサーバに対して直接設定を行う．この際には情報主体者はサーバで管理者によって管理されているアクセスコントロールリストの自分の情報に関する部分の変更を行う．またアクセス許可者はあらかじめサーバに登録されており，情報主体者がアクセス権の設定を行う際には，サーバに登録されている人の中から自分のデータへのアクセスを許可する人を選択する．

サーバ設定方式での情報主体者及びアクセス許可者のサーバへのユーザ登録の際には，サーバを管理するサーバ管理者が情報主体者及びアクセス許可者の本人確認を行う．

7.2 評価項目

手法の評価は次に述べる評価項目に従って行う．

- 利用者へのなりすましの脅威に対応しているか

この項目はアクセス制御を行う際に利用者へのなりすましに対応しているかどうかを評価する．

- 医師へのなりすましの脅威に対応しているか

この項目はアクセス制御を行う際に医師へのなりすましに対応しているかどうかを評価する．

- 許可取消しの迅速性

この項目は利用者が医師に対してデータ閲覧の許可を出した後で許可を取り消す場合の迅速性を評価する．

- 同意の証拠性の確保

この項目は利用者が医師にデータ閲覧の許可を行ったという同意の証拠性の確保が容易に行えるかを評価する．

- 利用者がアクセス許可を行える医師の範囲

この項目は利用者が医師にアクセス許可をする際に医師にどのような条件があるのかを評価する．なお前提条件として医師は相互認証，資格認証用の公開鍵証明書を有しているものとする．

- アクセスコントロール管理の容易性・安全性

アクセスコントロールの方式について容易にシステムを構築できるか，操作が簡単化，外部からの不正ア

クセスに対する安全性を評価する．

- アクセス制御の細かさ

アクセスコントロールを行う際にどの程度詳細なアクセス権の設定が行えるかを評価する．

7.3 評価結果

7.3.1 利用者へのなりすましの脅威に対応しているか

提案手法における利用者の本人確認は，利用者によって閲覧許可書に記載された電子署名を利用して行っており，一定の安全性を担保している．

一方，サーバ設定方式の場合にはIDとパスワードを用いた認証，生体認証，ICカードを用いた認証などが考えられる．IDとパスワードを用いた認証の場合には知識認証のみなので提案手法に比べて本人認証の安全性は劣るが，生体認証やICカード内の秘密鍵とサーバの秘密鍵による相互認証の場合には，提案手法と同様に一定の安全性を担保している．

7.3.2 医師へのなりすましの脅威に対応しているか

提案手法では医師の本人確認はICカードを用いた相互認証を用いて行う．

サーバ設定方式の場合にはIDとパスワードを用いた認証，生体認証，ICカードを用いた認証などが考えられる．IDとパスワードを用いた認証の場合には知識認証のみなので提案手法に比べて本人認証の安全性は劣るが，ICカードによる相互認証の場合には，提案手法と同様に一定の安全性を担保している．

7.3.3 許可取消しの迅速性

提案手法では利用者がサーバ管理者に取消しを申請するか，あるいは有効期限の短い閲覧許可書を発行し，短い期間で閲覧許可書を失効させる方法で許可の取消しに対応している．

一方，サーバ設定方式では利用者が医師に対して閲覧許可を行った後で許可を取り消す場合には，利用者が再度サーバにアクセスしてアクセス権の再設定を行うことで許可の取消しが可能となる．提案手法では閲覧許可書が失効するのを待つのに対してサーバ設定方式では利用者が許可を取り消したいと思ったときにサーバにアクセスすることで迅速に許可の取消しが可能である．このため提案手法に比べて迅速に許可の取消しが行える．

7.3.4 同意の証拠性の確保

提案手法では利用者の同意を示すために電子署名付きの閲覧許可書を用いる．この電子署名によって利用者が閲覧を許可したという証拠性を容易に得ることができる．

サーバ設定方式の場合にも利用者の本人確認を行った後でアクセス権の設定を行った後，同意をとりそれを電子的に保存すれば証拠を残すことができる．二つの方法を比較した場合には両方とも証拠性の確保は行えるが，サーバ設定方式では同意とアクセス権設定ファイルとの連結のログを解析する作業が必要であり，利用者や医師が証拠性を得るためにはサーバ管理者に依頼する必要があり，また電子署名ではないので改ざんされた場合の証拠能力に乏しい．一方提案手法では閲覧許可書の電子署名により利用者，医師ともに容易に証拠性が得られる．

7.3.5 利用者がアクセス許可を行える医師の範囲

提案手法では，医師が相互認証，資格認証用の公開鍵証明書を有していれば，前もってサーバにユーザ登録を行わなくても利用者は医師にアクセス許可を行える．このため提案手法では，サーバのコミュニティの系にあらかじめ属さないが，認証用HPKIの証明書[4]を保有する系には属している閲覧者に対するアクセス制御が可能となる．

一方サーバ設定方式では，利用者がアクセス許可を行う医師は前もってサーバに登録されている必要がある．つまり同一のサーバのコミュニティに属している医師に限られる．

また提案手法で，閲覧許可証の「医師の情報」を医師資格とし，医療機関の窓口に閲覧許可書を送付することで，特定しない医師へ閲覧許可を与えるシステムへと発展させることが可能である．また，閲覧許可証の「医師の情報」に医療機関と医師資格を記入できるように改良し，サーバに医療機関を認証する仕組みを組み込めば（例えば医療機関の管理者を認証する証明書の利用），患者の選択した医療機関のある医師からのアクセスかどうか検証することができ，患者の選択した医療機関の医師の閲覧機能が実現できる．よって提案手法の方がアクセス許可を与えることのできる医師の範囲は広く柔軟性があると考えられる．

7.3.6 アクセスコントロール管理の容易性·安全性

提案手法の場合は，送られてきた閲覧許可書を用いてアクセス制御をサーバのソフトウェアで行うため，サーバ管理者はアクセスコントロールリスト（ACL：Access Control List）の設定を行う等の管理を行う必要がない．サーバで管理する必要があるのは本人確認のための利用者の公開鍵証明書の登録のみである．

一方サーバ設定方式では，アクセス制御をサーバで管理しているACLを用いて行うため，サーバ管理者は利用者や医師の本人確認を行うための情報のほかにACLの管理及び利用者のアクセス権設定を行う必要がある．このためアクセスコントロールの容易性の点では提案手法の方が優れている．

また，提案手法は閲覧許可証の作成は個々の利用者のPC上で行うのに対してサーバ設定方式は利用者にサーバにアクセスさせるので，それだけサーバに対する攻撃の窓口が増えることになる．

また，サーバ設定方式は利用者がサーバでの操作で誤操作により意図しない人や条件に対して許可を設定する可能性があるが，本方式では許可証を意図した人に送るという過程が入るため安全性が高くなる．以上の点を総合すると安全性の点からも提案手法が優れている．

7.3.7 アクセス制御の細かさ

従来手法は，アクセス設定の変更や取消しの迅速性に優れるため，アクセス設定内容を随時変更する可能性のあるような項目に対しては設定がしやすいといえる．一方提案手法では，アクセス設定の証拠性に優れるため，非常に細かい設定を行っても履歴管理は容易であり，安全性に優れているといえる．よって，それぞれの手法のアクセス制御の細かさに関する評価としては，それぞれ一長一短あるが同程度であると考える．

7.3.8 評価結果のまとめ

システム評価の結果を表1に示す．

評価の結果，一部の項目でサーバ設定方式の方が優れている場合もあるが総合的に見た場合には提案手法の方が今回想定した利用形態において，想定した評価項目では優れているという結果となった．想定した利用形態により評価は異なるので実際の応用にあたっては，それぞれの手法のメリット・デメリットを評価して採用すべきである．

表1 評価結果
Table 1 Result of assessment.

評価項目	提案手法	サーバ設定方式
利用者へのなりすましの脅威に対応しているか	◎	◎
医師へのなりすましの脅威に対応しているか	◎	◎
許可取り消しの迅速性	○	◎
同意の証拠性の確保	◎	○
利用者がアクセス許可を行える医師の範囲	◎	○
アクセスコントロール管理の簡易性・安全性	◎	○
アクセス制御の細かさ	○	○

8. むすび

本論文では医療分野において自己情報コントロールが必要な場面として健康手帳システムにおける遠隔医療での健康手帳データの利用を想定し，自己情報コントロール可能なアクセス制御方法を提案した．この手法における医療分野に独特な特徴としては，診断の場面に対応した動的自己情報コントロールを可能とした点，医療分野の公開鍵証証明の特徴である資格付き公開鍵証明書により資格認証を行う点，あらかじめサーバに登録されていなくても患者が選択した全国の医師が閲覧できる，すなわち医療としての特徴である患者のフリーアクセスに対応した点，及び緊急時のデータアクセス対応の可能性を示した点が挙げられる．

提案したアクセス制御手法では，アクセス制御用の許可書を情報主体者がデータ閲覧を同意する人に対して発行し，データ閲覧者及び/または資格をサーバで認証することで情報主体者が同意した正しい公的資格をもった特定の公的資格者（医師）あるいはその施設に属する公的資格をもった不特定の公的資格者（医師）のみに対してデータのアクセスを可能にした．この場合，公的資格者は従来のアクセス制御のように前もってサーバに登録しておく必要がない．つまり閲覧者は，認証用HPKIというドメインに属していれば（認証用HPKIにより発行された証明書があれば），情報主体者と提供者からなるドメインにあらかじめ属している必要はなく，必要に応じ情報主体者の同意によりそのドメインに参加できることになる．

またアクセス項目も，情報主体者のコントロールによって選択できた．サーバ管理者はこの閲覧許可証を同意書相当に取り扱うことができる．

緊急時におけるアクセス制御については，厚生労働省「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」[9]においても「生命，身体又は財産の保護のために必要がある場合であって，本人の同意を得ることが困難であるときには，情報の第三者提供が情報主体者本人の同意なしに行える」と述べられているように，生命を救うための緊急避難措置は，自己情報コントロール権の保護よりも優先すべきであると考えられるため，今後は緊急時におけるア

クセス制御方法の検討が必要である．1ソリューションとして次のような方式が考えられる．まず，健康手帳サービス提供機関のサーバにデータを登録する際に，緊急時に閲覧を許可するデータ，例えば常用薬や注意すべき既往症等をどの資格保有者まで許可するかの同意に基づき設定を行っておく．緊急時に健康手帳サービス機関にデータがあることが分かった場合は，医師は医療機関の認証できるシステムあるいは，認証用 HPKI から発行された医療機関管理者用の公開鍵証明書に対応する秘密鍵で緊急モードの切換申請を行う．意識不明等患者が直接許可証を発行できない場合は，その利用者の IC カードを借用し，医師カードと併せてアクセスすることにより緊急時に必要なデータを閲覧する．あるいは利用者のカードがない場合も多いので，2名の医師の IC カードによってアクセス可能とするシステムも有効である．すなわち健康手帳サービス提供者の緊急時のアクセス許可ポリシーと事前の患者の同意による設定の組合せによりアクセス可能とする．以上の方策は1ソリューションに過ぎず，こうした可用性の確保は今後の検討課題である．

提案手法の実現可能性を示すために実証システムの構築を行った．実証システムの構築においては実証システムの実現形態やシステムにおいて必要な機能の検討を行い実証システムを構築した．また構築した実証システムの動作実験を行い提案手法の実現可能性を示した．

サーバ設定方式との比較で評価を行い想定している利用形態及び提案した評価項目の範囲では，提案手法が優れていることを示した．

本論文では健康手帳を対象とし，閲覧者は主に医師を対象に評価を行ったが，本提案の手法は何らかの個人情報を含むデータベースを他の人に閲覧を許可し指導を仰ぐシステムに応用可能である．

なお，本論文では健康手帳データにアクセスすることを「閲覧」としたが，現状の医療情報システムでは「参照」というのが一般的であるが，現状のアクセスコントロール方式との混同を防ぐためにこの用語のままとした．

文　献

[1] M. Bruun-Rasmussena, K. Bernsteinb, and C. Chronaki, "Collaboration-a new IT-service in the next generation of regional health care networks," Int. J. Medical Informatics, vol.70, pp.205–214, 2003.

[2] "個人情報保護法（個人情報の保護に関する法律)," 内閣府. http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html

[3] 青木隆一，稲田　龍，PKI と電子社会のセキュリティ，共立出版，東京，2001.

[4] (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

[5] 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，" 2002 信学総大，D-9-11，2002.

[6] ISO/TS 17090–2, "Health informatics—Public key Infrastructure Part 2: Certificate profile," 2002.

[7] 保健医療福祉分野 PKI 認証局，証明書ポリシ（案）Version 1.1 厚生労働省，http://www.mhlw.go.jp/shingi/2006/03/dl/s0330-8a.pdf, 2006.

[8] 村上陽子，小川浩司，大川恵子，村井　純，"電子証明書を用いたインターネット成績通知証明システムの設計と実装，" インターネットコンファレンス'99 論文集，1999.

[9] A. Herzberg, Y. Mass, J. Michael, D. Naor, and Y. Ravid, "Access control meets public key infrastructure or: Assigning roles tostrangers," IEEE Symposium on Security and Privacy, pp.2–14, 2000.

[10] 内山映子，宮川祥子，太田喜久子，村井　純，吉野肇一，"サービス利用者のプライバシポリシーに基づくインターネットを利用した在宅ケア情報共有システム，" 信学論（D-I)，vol.J87-D-I, no.12, pp.1098–1109, Dec. 2004.

[11] 厚生労働省，"医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン，" http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805-11a.pdf, 2006.

（平成 17 年 3 月 31 日受付，18 年 8 月 14 日再受付）

丸山　剛

平 14 千葉大・工・電子機械卒，平 17 東工大総理工物理情報工学修士課程了．同年 NEC ソフト（株)，現在に至る．医療情報管理システム等の開発に従事．

喜多　紘一　（正員）

昭 42 東大・工・電子卒．同年（株）東芝，平 8 国際医療福祉大学特任教授（併任），平 9 東工大客員教授（併任），平 12（財）医療情報システム開発センター審議役，平 16 東工大特任教授，現在に至る．ヘルスケア情報工学，個人情報保護，公開鍵基盤，電子保存，医療情報セキュリティ，個人健康・医療情報管理システムに関する研究に従事．RSNA (Radiology Society of North America) Award (Certificate of Merit)．日本生体医工学会，日本医療情報学会，放射線技術学会，日本医用画像工学会各会員．

鈴木　裕之　（正員）

平 10 東工大・工・電気電子卒，平 15 同大大学院総理工物理情報工学博士課程単位取得退学．博士（工学）．同年東工大フロンティア創造共同研究センター産学官連携研究員，平 16 東工大像情報助手，平 19 東工大像情報助教，現在に至る．光情報処理，生体認証，医療情報セキュリティに関する研究に従事．応用物理学会会員．

小尾　高史　（正員）

平元東工大・理・物理卒，平 6 同大大学院総理工物理情報工学博士課程単位取得満期退学．博士（工学）．同年東工大工学部教務職員，平 9 東工大像情報助手，平 15 東工大総理工助教授，平 19 東工大総理工准教授，現在に至る．医用画像処理，画像処理，情報セキュリティに関する研究に従事．日本医用画像工学会奨励賞．医用画像工学会，応用物理学会，日本医学放射線物理学会，日本核医学会，IEEE 各会員．

谷内田益義　（正員）

昭 59 国際基督教大・教養卒，平元東工大総理工物理情報工学博士課程了．博士（工学）．同年高知医大助手，平 3（株）リコー，平 13 東工大 IT 都市創造工学寄附研究部門客員助教授（併任），平 19 東工大 IT 都市創造工学寄附研究部門客員准教授（併任），現在に至る．セキュリティ応用システム（文書管理システム，医用情報システムなど）に関する研究に従事．応用物理学会，医学放射線学会，放射線技術学会各会員．

山口　雅浩　（正員）

昭 62 東工大・理・応物卒，平元同大大学院総理工物理情報工学修士課程了．博士（工学）．同年東工大助手，平 8 東工大助教授，平 19 東工大准教授，現在に至る．応用光学，画像工学に関する研究に従事．映像情報メディア学会，応用物理学会，日本医用画像工学会，日本光学会，OSA，SPIE 各会員．

大山　永昭

昭 52 東工大・理・物理卒，昭 57 同大大学院総理工物理情報工学博士課程了．工博．同年東工大助手，昭 61 アリゾナ大学研究員，昭 63 東工大助教授，平 4 同教授，現在に至る．光情報処理，医用画像工学，画像システムに関する研究に従事．科学技術庁長官賞，情報化促進貢献個人表彰（郵政大臣表彰），日本医学物理学会第 7 回論文賞，情報通信月間個人表彰．(社) 日本医学放射線学会，(社) 日本産業衛生技術学会，(社) 日本放射線技術学会，応用物理学会，日本医学物理学会，日本医用画像工学会，日本核医学会各会員．

ＨＰＫＩによる電子署名を利用した健康管理データ提供・参照システム

Management system for Electronic Health Record based on HPKI

○鈴木裕之　喜多紘一　谷内田益義　小尾高史　山口雅浩　大山永昭

(Hiroyuki Suzuki　Kouichi Kita　Masuyoshi Yachida　Takashi Obi　Masahiro Yamaguchi
Nagaaki Ohyama)

東京工業大学(Tokyo Institute of Technology)・

像情報工学研究施設 (Imaging Science and Engineering Laboratory)

〒226-8503・横浜市緑区長津田町 4259-R2-55・電話 045-924-5197／FAX 045-924-5177

Yokohama MidorikuNagatsutacho 4259-G2-2 226-8503
E-mail:hiroyuki@isl.titech.ac.jp

1. はじめに

近年の少子高齢化社会の流れにおいて豊かで創造的な生活を安心しておくる為には、個人ごとに適切な医療サービスを提供することが必要になる。ＩＴ新改革戦略では、2010 年度までに個人の健康情報を「生涯を通じて」把握できる基盤を作り、国民が自らの健康情報を活用し、健康増進に努めることや保険者による高度な保健指導の実現を支援する予定となっている。また、医療制度改革大綱では、医療機能の分化・連携の推進により、地域単位で切れ目のない質の高い医療の提供を行うことが要求されている。上記のような社会を実現するためには、健康診断情報、診療情報、薬歴情報等（以下、健康管理情報とする）をより有効に活用することが重要である。これまでの健康管理情報の活用方法としては、病院や企業などの組織内にデータベースを構築し、その組織内で登録情報を利用するといったクローズな形態が大半であったが、最近では地域ごとに医療サービス提供者側が主体となって共有データベースを構築し、そこから各医療機関や個人が必要な情報を参照できるような地域連携システムが利用され始めている。このシステムでは迅速、簡便にデータを管理、提供することは可能であるが、個人情報保護の観点から言うと、情報提供の同意などの実現で満足の行くシステムを構築するには制約が多いため、患者自身が情報コントロール可能な診療情報データベースの構築が必要になると考えられている。

このような動向に対し我々は、個人の経年的な健康管理データを簡便に管理することができ、また携帯端末などによる医師へのデータ提供や、医師、国家資格保有者あるいは医療機関が責任をもって提供したデータであることを検証可能なシステムについて研究を行っている。今回、医療従事者の電子署名を付与した健康管理データをデジタル媒体へ出力・提供し、またデジタル媒体に格納した健康管理データの参照や署名の検証を行うシステムの開発を行ったので報告する。

2. 健康管理データを有効活用するためのシステム

2.1. 健康管理データの電子化に求められる要件

電子化された健康管理データを個人が責任もって管理するためには、データの安全性、真正性を保つことが必要になる。データを共有データベースに保管する場合、安全性を保つためにはそのアクセス制御方法が重要になるが、今回はデータを携帯可能な媒体（CD-R）に暗号化して保存することで安全性を保証する。またデータの真正性を保証するためには、電子署名を付与することが一般的であるが、医療情報の提供では、誰が、という人の保証だけでなく、医療業務を行う資格を有している人や組織であることを保証する技術が求められる。そこで本研究では、ヘルスケア PKI（HPKI）を利用した電子署

名によってデータの真正性を保証する。

2.2. HPKI を利用した電子署名

医療における診療情報提供者や診断書等の記名押印にかわる署名に使うものとして HPKI の構築が厚生労働省を中心に進められている[1]。HPKI では、X509 証明書形式を用い、証明書内に医療関連の国家資格あるいは施設管理責任者情報を格納しているので通常の PKI 証明書のような自然人の確認だけではなく国家資格保有者や施設管理責任者を確認することができる。

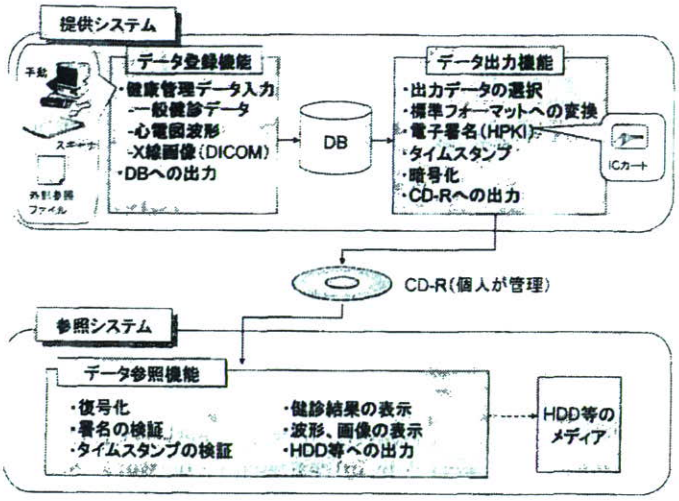

図１．検証システムの概略図

3. 検証システム

前章で述べた仕組みを検証する実験システムの構築を行った。このシステムでは、健康管理データの登録及び CD-R への書き込みを行うソフトウェアと、CD-R 内へ書き込まれたデータの参照を行うソフトウェアで構成され（図１）、検体検査結果、心電図の波形、X 線等の画像結果を管理することが可能である。またそれぞれのデータは標準的なフォーマットで記述され、例えば検体検査結果データについては、HL7CDA に準拠した XML 形式、画像結果は DICOM に準拠した形式で保存される。これらの検査結果データに電子署名およびタイムスタンプを施し、暗号化した上で CD-R へ出力する。提供されたデータは、CD-R 内に格納されている専用のビューワーで参照し、単に検査結果データを閲覧する機能だけでなく、どのような電子署名が施されているかを簡単に確認する機能を有している。検証システムの動作確認を行ったところ、正しく動作することを確認した（図２-３）。

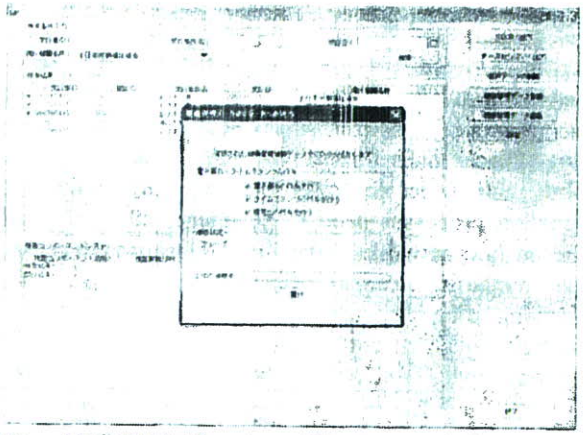

図２．健康管理データの CD-R への書き込み

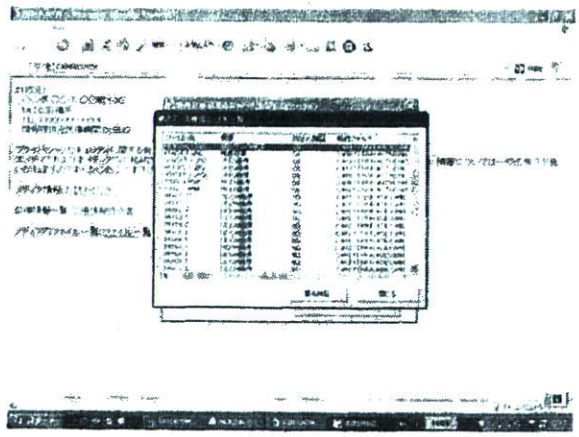

図 3. 健康管理データ参照時における電子署名の検証

4. まとめ

本研究では、健康管理データの提供、参照を行う実験システムを構築し、個人での簡便なデータ管理が行えること、また HPKI に基づく電子署名によって正当な医療業務の有資格者が提供したデータであることを確認できることを示した。今後は健康管理データをネットワーク上の共有データベースに保管し、個人や医療従事者がインターネットや携帯端末でデータを参照できるシステムや、医療情報だけでなく他の公的サービスを総合的に管理できるポータルサイトの構築について検討を行う予定である。

本研究は、（独）情報通信研究機構の委託研究「ネットワーク認証型コンテンツアクセス制御技術の研究開発」により行われた。

参考文献

[1] 財団法人医療情報システム開発センターホームページ「医療用 PKI システムの開発」 http://www.medis.or.jp/6_pki/hpki.html