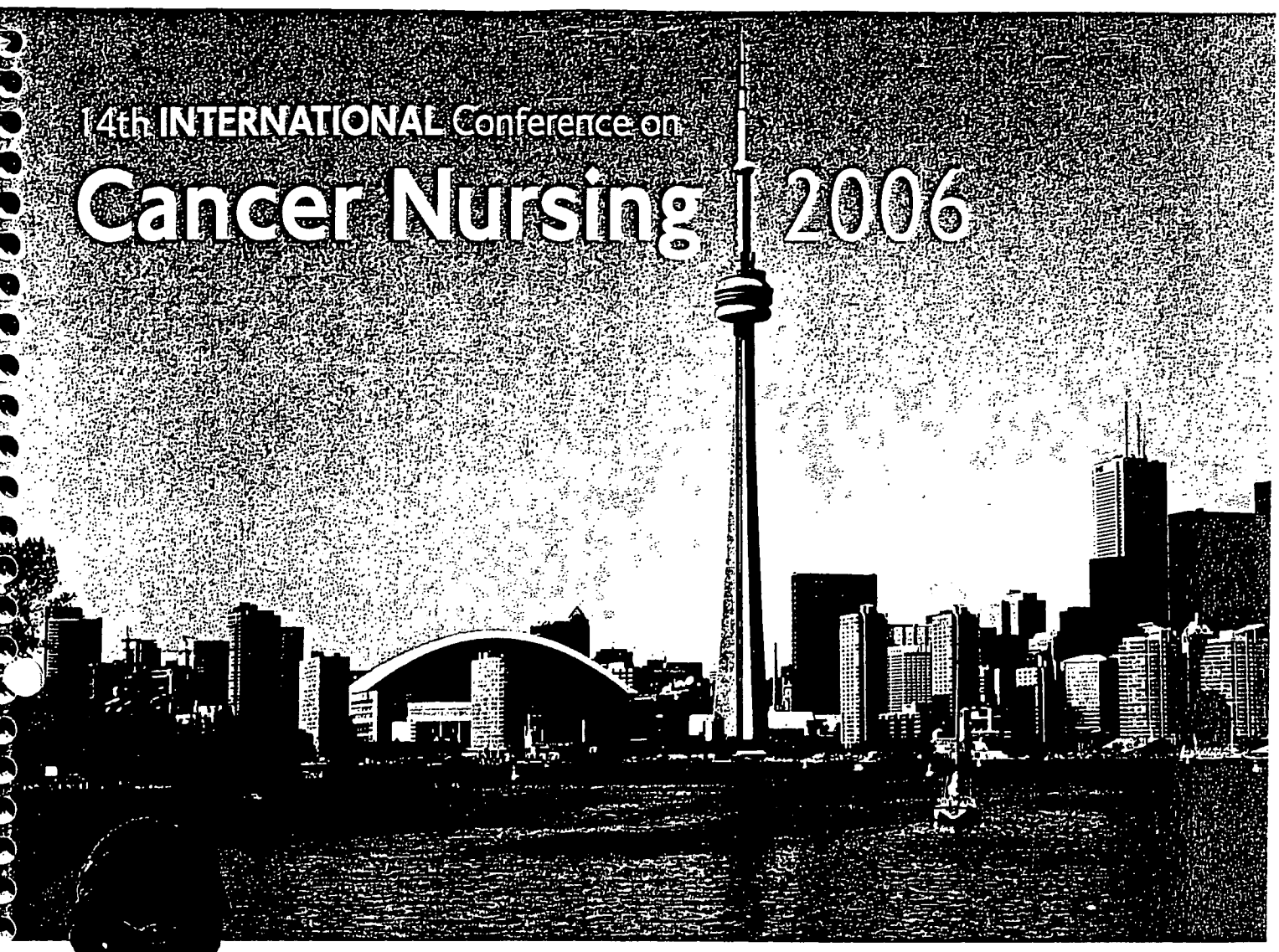
14th INTERNATIONAL Conference on

Cancer Nursing | 2006



September 27th –
1st October 2006
Sheraton Centre
Toronto
Canada

International
Society of Nurses
in Cancer Care

CANO
ICO

SUPPORTIVE CARE: INNOVATIVE APPROACHES TO CARE DELIVERY

A STUDY ON THE FEASIBILITY OF HAVING NURSES EVALUATE PATIENTS FOR CHEMOTHERAPY-INDUCED NEUTROPENIC COMPLICATIONS USING A RISK ASSESSMENT TOOL 306

Kelley Moore, Vice President, Clinical Projects, Supportive Oncology Services, Inc., Barry Fortner, MD, USA

Statement: Chemotherapy-induced neutropenia (CIN) may result in febrile neutropenia and other complications. A risk assessment tool was developed to help evaluate patients' risk for CIN complications, and the feasibility of nurses implementing this tool into clinical practice was also assessed.

Description: Nurses in 15 community oncology practices used the tool to evaluate patients' risk of CIN complications before starting chemotherapy.

Nurses completed an evaluation form each time the tool was used and then a survey assessing the tool's utility.

Findings: The nurses successfully used the tool in all patients, evaluating each for 14 patient risk factors and the chemotherapy risk factor (a regimen associated with a moderate to high risk of neutropenic complications). The most frequently identified risk factors were chemotherapy (55%) and advanced cancer (31%). Nurses reported that the tool helped "identify neutropenia risk" in 69% of patients and "determine the degree or severity of neutropenia risk" in 57%. Nurses reported initiating an action because of the tool in 141 (94%) patients. The actions most frequently reported were "closer monitoring for neutropenia" (64%) and "use of prophylactic G-CSF" (27%). Five (33%) nurses reported that their practices planned to adopt the tool, while 6 (40%) planned to modify it to meet their practices' needs.

Conclusions: Clinical risk assessment tools can quickly and effectively assist oncology nurses in evaluating patients for risk factors of CIN complications. These tools may assist in identifying patients who would benefit from intervention intended to prevent or decrease the severity of CIN complications.

ESTABLISHMENT OF MEDICAL/NURSING SUPPORT NETWORK FOR CANCER PATIENTS AT UNIVERSITIES 307

Tamae Futawatari, Professor, Gunma University School of Health Science, Taro Kano, Yukiko Isobe, Junko Ishida, Kiyoko Kanda, Kazuko Ishida, Japan

Aim: We are working to establish a medical/nursing support network to improve the QOL of local cancer patients. Here we report our university's actual work on the issue in the year of 2005.

Activity details:

1 Gunma Cancer Nursing Research Society

It has held academic meetings patients and their families can participate.

Also, as a training to improve the skills of its members, discussions were made after nurses, pharmacists, and hospital executives gave lectures on "team approach in outpatient chemotherapy" from their side of view.

Comments collected from the participants were generally satisfactory: "The direct voice of the patients touched my heart"; "The opinions of people from other occupations were interesting".

2 Trainings to improve the practical ability of nurses (university's contributive project to the local community).

First, lectures on chemotherapy knowledge and role of nurses were held, and exercises to acquire skills needed in practice were performed. Also, participants were given opportunities to look back on their nursing methods through case examinations. There were comments saying this was a precious opportunity to know the situations of other facilities.

3 Support of cancer patients and their families Cancer nursing consultation was held once a week in cooperation with Gunma University Hospital and dealt with various complicated problems of patients and their families concerning their mental and physical health.

Conclusion: The participants evaluated activities generally satisfactory, and we intend to strengthen the ties of the cancer patients and the nursing professionals.

DEVELOPING TEACHING MATERIALS TO IMPROVE QUALITY OF LIFE FOR PATIENTS WHO HAVE UNDERGONE GASTRECTOMY 308

Hizuru Amijima, Associate Professor, PhD RN, Prefectural University of Hiroshima, Michiyo Yamanaka, MSc RN, Yoshie Sugimoto, PhD RN, Japan

The purpose of this study is to develop and evaluate teaching materials for guidance for living to raise QOL (Quality of Life) for patients who have undergone gastrectomy. To clarify the problems that they had, twenty patients who had undergone gastrectomy, were interviewed after informed consent was obtained. The data were analyzed using Content Analysis.

The data indicated that the patients had four types of problems: physical problems, dietary problems, psychological problems, and support problems.

In more detail the problems, they indicated included: body weight does not increase, anemia, constipation and diarrhea, quantity of meal, meal time is short, anxious about a recurrence, lack of confidence about self-care, lack of support.

These results suggest that important components of guidance for living should include information about post-operative physical problems and how to cope with them, dietary information, points to keep in mind about everyday life, information about medication, and encouragement to have regular health checks.

In order to teach this content effectively, we developed a leaflet, a booklet, and an Internet homepage. We carried out guidance for living for twenty patients who had undergone gastrectomy using the teaching materials which we developed, and conducted a questionnaire survey.

The results of the questionnaire survey showed that the teaching materials we developed were effective, particularly with regard to confidence about self-care and dietary management, and could be used more extensively to provide guidance for living and to raise QOL (Quality of Life).

VISIT NURSING STATION SYSTEM WITH SECURED INTERNET COMMUNICATION USING WATERMARKING TECHNIQUE: TELE-NURSING SYSTEM EXPERIMENTS 309

Tokuo Umeda, Medical Information, School of Allied Health Sciences Kitasato University, Akiko Okawa, Toshiaki Ikeda, Hareaki Yamaoto, Hajime Harauchi, Japan

This paper describes our developed home health care support system. Our system can input vital data automatically.

The tele-nursing system was composing two modules. One is patient house system and the other is the visit nursing station system. The vital data measurement equipment in the patient house was made the blood pressure, the pulse, the blood sugar

SUPPORTIVE CARE: INNOVATIVE APPROACHES TO CARE DELIVERY

value measurement machine, weight, the body fat meter, and a clinical thermometer. Moreover, every day vital data can be transmitted to the visit nursing station by using the network and the telephone line, and the developed systems can be connected with the individual hospitals automatically. Hiding patient information secretly was secured by using the electronic watermark technology when transmitting.

Consequently, the system was able to acquire individual patient's vital data from the vital data measurement equipment automatically. Moreover, it was possible to glance at these vital data and glance at a change with the lapse of time because the chart was made to be displayed automatically. In addition, it was possible to glance at the evaluation of a normal range or an abnormal range the vital data of every day. The cooperation physician can evaluate and examine patient's vital data, and the physician can tell the result to the patient using the developed system.

As a result, the patient is able to consult about patient's health cares with visit nurse and physician while staying at home.

DEVELOPMENT OF THE REMOTE NURSING SUPPORT SYSTEM IN AN OUTPATIENT'S CHEMOTHERAPY 310

Akiko Okawa, Adult Nursing, Nagoya City University School of Nursing, Tokuo Umeda, Kazuko Onishi, Japan

In recent years, the chemotherapy in outpatients are increasing. It is very important to grasp the recuperation-at-home patients' condition. In this study, we develop a remote nursing system for supporting outpatients' chemotherapy in order to gain the Quality of Life (QOL) for the patients and their family.

Our remote nursing support system possesses a digital automated sphygmomanometer, so that it may be transmitted and displayed in our system. Also, out system can record the grade of a recuperation-at-home person's pain. We build automated pain measurement system to carry out the Web input of 13 items of the pain condition scale Symptom Distress Scale (SDS).

Moreover, the recuperation-at-home person side system was considered as the panel touch, and carried out simple of the operation. It is necessary to clarify individuality, such as a side-effect of chemotherapy, so that this system supports a better QOL for a patient and its family. Moreover, we are now planning to expand this system to construction of the cooperation system connecting several hospital and patients' homes.

A part of this research received assistance of the Ministry of Education, Culture, Sports, Science and Technology grants-in-aid for scientific research (No.16791382) in the last year.

MEETING THE NEEDS OF ADOLESCENTS POST AUTOLOGUS STEM CELL TRANSPLANT: A PEDIATRIC CENTRE'S EXPERIENCE 311

Josee St-Denis-Murphy, Registered Nurse, IWK Health Centre, Christa McGuirk, Canada

Where we Were: Our health centre has a small pediatric population who require SCT and therefore are referred to other centers that specialize in SCT. The age, maturity and disease protocol of the recipient is taken into consideration when choosing either an adult (local) versus pediatric (out of province) facility. Adolescents who are 14 to 18yrs are possible candidates for SCT in the local facility. The adult facility identified an absence of specific services required to provide holistic care to adolescents and their families.

Benefit of Change: Recognizing that we can meet the needs of the adolescent. Both centers decided that autologus SCT recipients would be cared for by our pediatric facility day +1 post autologus SCT until engraftment.

How We Did It: Both institutions set up medical criteria that adolescents were required to meet prior to transfer. The pediatric bone marrow transplant coordinator and other disciplines met to develop evidence based guidelines. Staff were educated.

Outcome: We plan to evaluate this change through focus groups that would include the adolescents, families and staff. Health care professionals working in adult or pediatric oncology could gain from our experience.

THE DEVELOPMENT OF A STANDARDIZED APPROACH FOR LYMPHEDEMA MANAGEMENT 312

Christine Ransom, Registered Nurse, BC Cancer Agency – Centre for the Southern Interior, Maureen Ryan, Allison Filewich, Canada

Lymphedema of the upper or lower extremities is a potentially devastating sequel to tumor invasion, surgery and/or radiotherapy. It can occur to varying degrees and at any point in the oncology patient's life span. Nurses at our center have been challenged to provide evidence-based, standardized care for patients at risk or exhibiting signs and symptoms of lymphedema.

There has been recognition that care providers differ in their level of expertise in its management. As well, there is variation in accessibility of services among the many communities within our vast region. This presentation will outline the results of a literature search, a nursing survey and the manner in which an algorithm and resource manual were developed. Future goals for the provision of consistent, seamless care delivery will be discussed.

PSYCHO SEXUAL THERAPY IN CANCER CARE 313

Janet Ellen Jones, Lecturer and Psycho Sexual Therapist, School Of Health Science, University Of Wales, UK

I am running workshops for women with Breast Cancer during their rehabilitation 35–70 years. We are discussing loss of sex drive, clitoral shrinkage, relationship failure since diagnosis and treatment.

My workshop involves coaching the women to get back to being sexual for themselves and their partners. How to talk to their partners, clothes to wear and self-esteem.

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

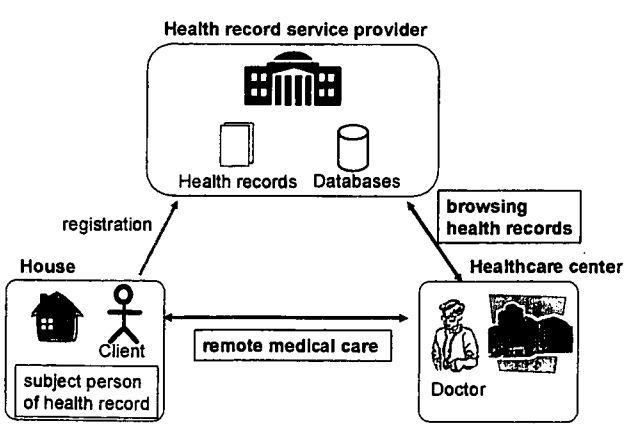


図 1　想定する利用形態
Fig. 1　Usage pattern.

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．

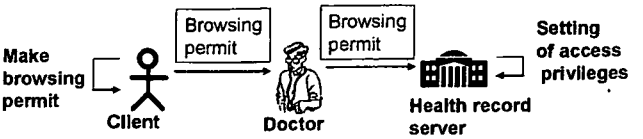


図 2 提案するアクセス制御方法
Fig. 2 Access control method.

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．

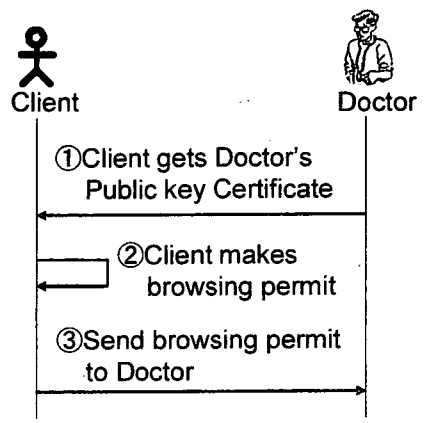


図 3 利用者が閲覧許可書を作成する場面
Fig. 3 Stage of making browsing permit.

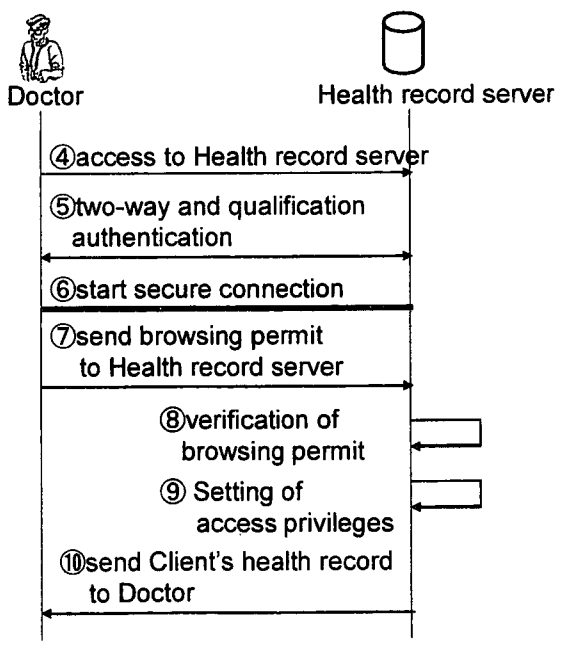


図 4 医師が健康手帳データを閲覧する場面
Fig. 4 Stage of browsing health record.

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．

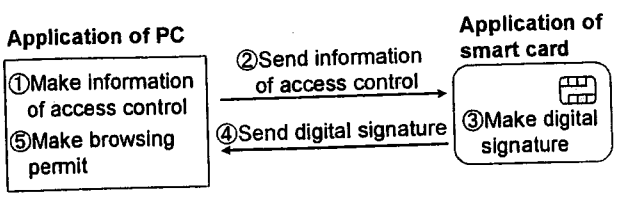


図5 閲覧許可書作成手順
Fig. 5 Procedure of browsing permit.

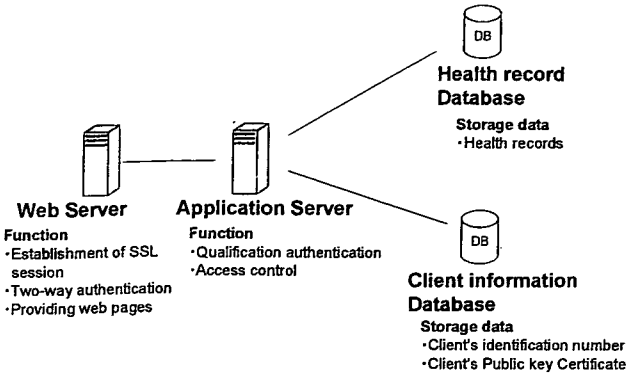


図 6　健康手帳サーバの構成
Fig. 6　Health record server structure.

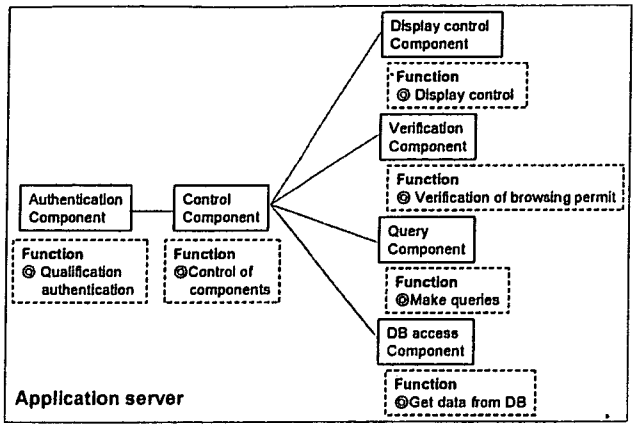


図 7　アプリケーションサーバ内のコンポーネント
Fig. 7　Components of application server.

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。

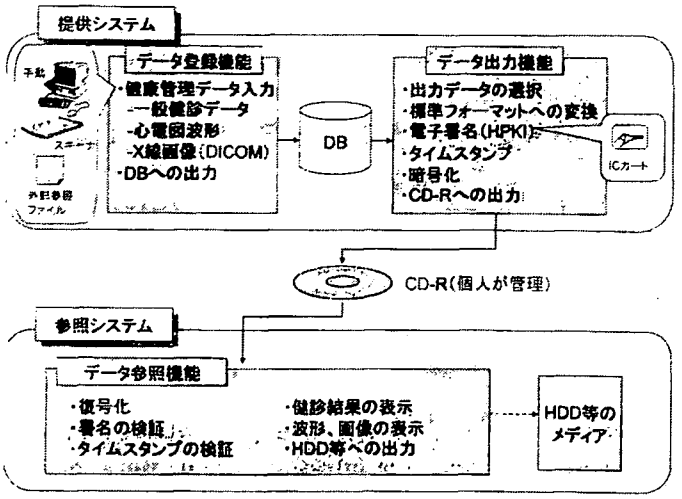


図１．検証システムの概略図

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）。

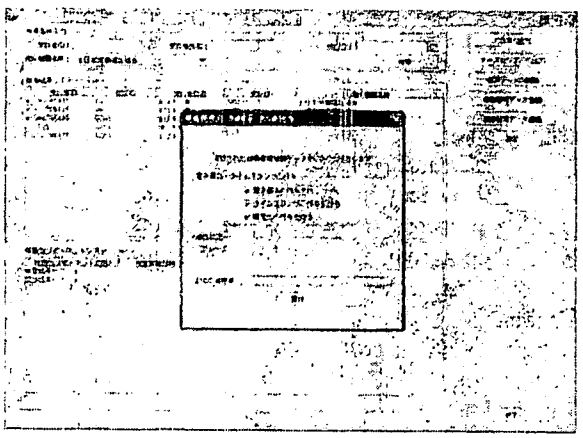


図２．健康管理データの CD-R への書き込み

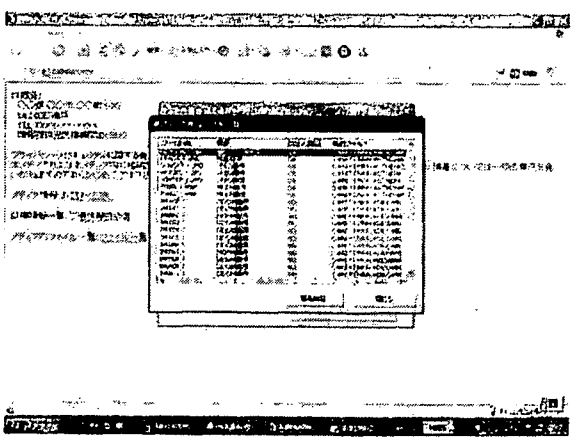


図 3. 健康管理データ参照時における電子署名の検証

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

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情報管理システム

喜多 紘一[1)] 平井 正明[2)] 鈴木 裕之[1)] 谷内田 益義[1)] 山口 雅浩[1)]
小尾 高史[1)] 大山 永昭[1)]
東京工業大学[1)] HL7 Japan CDA SIG WG1 Leader[2)]

The personal health data referring system conforming to a health checkup report standard for personal use based on CDA R2

Kita Kouichi[1)] Hirai Masaki[2)] Suzuki Hiroyuki[1)] Yachida Masuyoshi[1)]
Yamaguchi Masahiro[1)] Obi Takafumi[1)] Ohyama Nagaaki[1)]
Tokyo Institute of Technology[1)] HL7 Japan CDA SIG WG1 Leader[2)]

Medical examination result reports with image data such as chest films and a wave pattern or of the electrocardiogram could be provided electronically to an individual using an "electronic post-office box" mechanism. These reports will be proposed in the case of medical treatment at a hospital. The standard formats were proposed. A card with PKI for the certification as an access card to the system is effective and dynamic on-demand VPN is useful as a secure network for this purpose.

Keywords: CDA R2, Medical helth examination, Electronic POB, Health checkup report

1. はじめに

1.1 個人提供用健康診断結果報告書の電子的提供

日本HL7協会のCDA SIGでは患者診療情報提供書のCDA R2準拠フォーマットでの標準化を行い、Helics規格としても採用された[1]。一方、特定健診による生活指導が2008年より始まり、健診データの保険者による保管と健診機関からの電子データの送付が計画され、そのフォーマットの規格化が進められている[2]。特定健診でのフォーマットは波形や画像をデジタルで提供することを目的としていない。また、健康保険組合等が健康指導を行う為のもので、個人へ提供し、個人が健康管理や診療に活用することを直接の目的としていない。そこで、特定健診のフォーマットと互換性があり、必要により波形や画像もデジタルで提供可能で且つ、個人に提供することを目的としたフォーマットを提供することを目的とした。

1.2 重点計画-2007

一方、IT戦略本部でまとめられた[重点計画ー2007]では「個人が自ら健康情報を管理し健康管理等に活用するための仕組みの確立」および「国民視点の社会保障サービスの実現に向けての電子私書箱(仮称)の創設」が歌われている[3]。前者は「個人が健康情報を電子的に入手し、自ら健康管理や診療時における提示等に活用できるよう、健康情報入手及び管理に関するルール等の仕組みについて、2008 年度までに方針を示す。」となっている。具体的な動きとして「静岡県版電子カルテシステム」[.4]や「厚生労働省の電子的診療情報交換辞表(SS-MIX)では診療情報をCD-Rに書き出して提供することを始めている。また、経済産業省では相互運用性実証事業の中の「電子診療情報システムの実証事業」で診療情報提供書を電子的に患者に渡す実証事業を行った。電子私書箱は「医療機関や保険者等に個別管理されている情報を、希望する国民が自ら入手・管理できる「電子私書箱(仮称)」を検討し、2010 年頃のサービス開始を目指す。」となっていて検討が始まった段階である。

1.3 ヘルス情報共有データベース基盤としての4つの観点

ヘルスケア分野で情報を共有することがはじまっているが、図1に示すように4つの観点に整理される。即ち「地域連携クリティカルパスのための野情報共有」、「かかりつけ医のための情報共有」、「行政、研究、経営管理のための情報共有」および「個人の自己健康管理のための情報共有」である。前者の3つは今まで議論がなされ実際に実現しつつあるが、最後の観点のものは検討が始まった段階である。

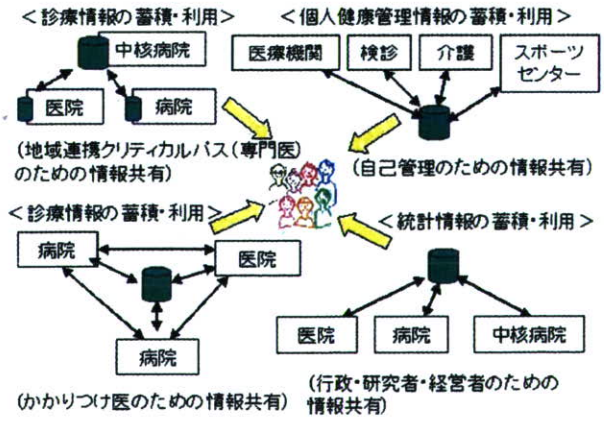


図1 ヘルス情報共有のための4つの基盤の観点

健康情報の個人の自己健康管理を電子的に配送し、受診者がダウンロードしたり、サーバに登録し、診療や健康維持のために必要なものだけを整理して医療機

関や自宅で参照することが可能である。こうした「個人健康情報管理システム」の電子私書箱による構想も合わせて提案する。

2. 方法

個人提供用健康診断結果報告書フォーマットは特定健診フォーマットの規格との整合をもたせた。波形や画像も提供できるようにCDAの外部参照ファイルとした。受診者情報、報告書作成機関情報、検査結果コンポーネント、問診結果コンポーネント及び判定結果コンポーネントは特定健診のフォーマットと同様とした。

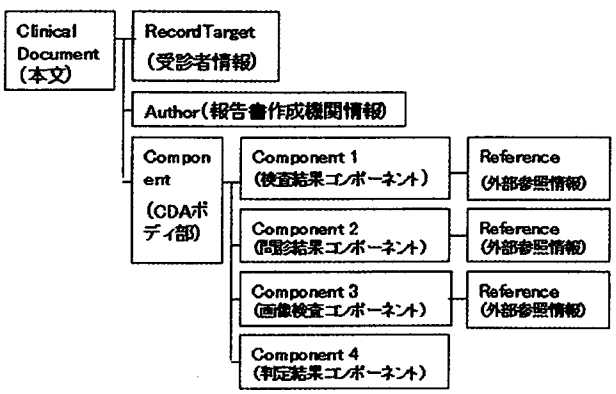


図2 個人提供用健康診断結果報告書フォーマット

本規格はHL7 CDA R2に基づいて規定し、且つHelicsで採用されたている患者診療情報提供書の署名、タイムスタンプ、暗号化方式に準じた。電子私書箱は重点計画等の発表資料を参考に調査した。

3. 結果

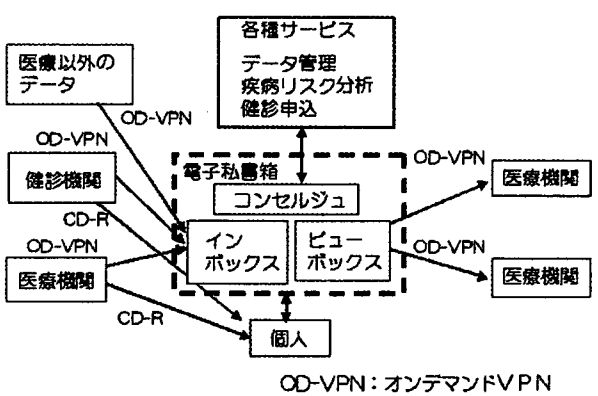


図3 電子私書箱構想による実現

個人提供用健康診断結果報告書はCD-Rへ書き込み付属のViewerで表示を行った。検体検査の表示は数値データだけでなく経年変化がグラフで確認でき、心電図やDICOM画像は専用のビューワーでそれぞれ確認することができた。「個人健康情報管理システム」は図3に示すように健康診断結果を受取るところ（インボックス）、及び病院で個人が参照し（ビューボックス）、結果から疾患リスクの評価や健診申込等のサービスを行う部分（コンセルジュ）に電子私書箱構想を利用した。健診機関等から健康・医療情報を電子私書箱へ提供するネットワークはHPKIを利用してVPN機器の所属する機関の属性を確認可能とするためダイナミック・オンデマンドVPNに機能追加[5]を行うこととした。電子私書箱のデータを医療機関側で参照する場合もアクセスするネットワークは同様のネットワークを使用することとした。

4. 考察

CDAフォーは日本HL7 CDA-SIGに提案を行いスキーマとの整合性のチェックを行っている。特定健診とのハーモナイゼーションを行うために全体を「HL7CDA健診情報規格群」として一体化した以下のような規格体系で検討している。Part1が本研究のフォーマット、Part2が特定健診のフォーマットにあたる。

1) Part1－通則－
2) Part2－個人提供用健康診断結果報告書－
3) Part3－健診情報ファイル仕様規格－

HPKI署名や署名検証画面がわかりにくいので印鑑の押印や検証の感覚で使えるためには今後の検討が必要である。個人健康情報管理システムは電子私書箱で暗号化されたデータを復号する場合の安全性確保の検討が必要である。

5. まとめ

重点計画-2007で示されている「健康情報の入手及び管理システム」の一つとして「電子私書箱」構想を利用して健康診断結果報告書を電子的に提供し、さらに希望者には心電図の波形や胸部写真等の画像データも入手し、診療の際に病院で提示できることを示した。また、システムへのアクセスカードとして認証用のPKI入りカードが有効であり、セキュアなネットワークとしてダイナミック・オンデマンドVPNを利用できることを示した。今回は個人提供用健康診断結果報告書を電子化するためのフォーマットを利用してその実現性の評価をおこなった。今後はさらにフォーマットのスキーマとの整合性の精査を行っていくとともに、健診以外のデータも提供可能となるよう検討を行う。

6. 謝辞

「個人提供用健康診断結果報告書フォーマット」の提案およびCD-Rへの書込等の基礎技術開発は情報通信研究機構委託研究：「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」において行われた。また、電子私書箱の調査は文部科学省科学技術振興調整費支援を受けている。

参考文献

[1] 制定済標準規格.http://www.hl7.jp/intro/index.html.
[2] 健診データの電子的管理の整備に関するホームページ.http://tokuteikenshin.jp/.
[3] 重点計画－2007.http://www.kantei.go.jp/jp/singi/it2/kettei/070726honbun.pdf.
[4] 静岡県版電子カルテシステム.http://www.mi.hama-med.ac.jp/emr/.
[5] 喜多紘一他5名.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.

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

喜多 紘一[1)] 鈴木 裕之[1)] 竹田 忠雄[2)] 猪俣 彰浩[3)] 島田 宏[4)] 有馬 一閣[5)]
東京工業大学[1)] (株)NTTPCコミュニケーションズ[2)] 富士通(株)[3)]
Heasnt 技術委員会 主査[4)] (株)NTTデータ[5)]

A secure health domain network by cooperation with HPKI and dynamic on-demand VPN

Kita Kouichi[1)] Suzuki Hiroyuki[1)] Takeda Tadao[2)] Inomata Akihiro[3)]
Shimada Hiroshi[4)] Arima Kuniharu[5)]
Tokyo Institute of Technology[1)] NTTPC Comunications[2)] Fujitsu Limited[3)]
Heasnet Technical Committee chairman[4)] NTT DATA CORPORATION[5)]

The VPN service provider judges it whether it is connection application from the VPN equipment which is administrated by a medical institution with HPKI certificate and admits connection to medical database. By this method, secure network environment of the free access for the medical institution by the patient that is a infrastructure between medical associated institutions are realized.

Keywords: HPKI, Dynamic on-demand VPN, XACML, SAML, Secure network

1. はじめに

1.1 ダイナミック・オンデマンドVPNのねらい

医療情報システムの安全管理に関するガイドライン第2版」では、「外部と個人情報を含む医療情報を交換する場合の安全管理に対する最低限のガイドライン」として以下の8項目をあげている。

1) セキュアなネットワーク経路を確保
2) データ送受信の拠点の出入口、使用機器で利用者の必要な単位で相手確認
3) 正規利用者、許可機器への成りすまし防止
4) ルータ機器は安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶVPN間で送受信が不可となる経路設定
5) 送信元と相手先当事者間で当該情報そのものに対する暗号化などのセキュリティ対策を実施
6) 医療機関等、通信事業者、システムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社などの組織間で責任分界点、責任の所在を契約書等で明確化
7) リモートメンテナンスを実施する場合は不必要なログインの防止
8) 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認

また、「外部との医療情報の交換」に関して、以下の5通りの接続形態が記述されている。

1) クローズドなネットワークで接続する場合
   a) 専用線で接続されている場合
   b) 公衆網で接続されている場合
   c) 閉域IP通信網で接続されている場合
2) オープンなネットワークで接続されている場合
   a) 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保した形態でサービス提供する場合
   b) 医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合

ダイナミック・オンデマンドVPNはこの中の2aにあたる形態のネットワークであり、通信経路上の脅威の対策のための管理責任の大部分をこれらのVPNサービス提供者に委託できる。最低限のガイドラインの1番目に対しIKEとIPSecによるVPN方式により対応している。これにより、以下にあげる医療分野におけるネットワーク要件を満たし、ガイドラインに適合したネットワークの提供を目指している。

1) 安全な通信
2) 大容量データの高速通信
3) メッシュ型ネットワークの実現と拡張性
4) 参加メンバ(利用者、組織、機器)の真正性保証
5) セキュアネットワーク接続に関するコスト削減

1.2 ダイナミック・オンデマンドVPNの手続き

1.2.1 VPNサービス利用申請

VPNサービス利用申請は電話で言えば電話番号を入手することに当たる。サービス利用者は、機器証明書が搭載されたVPN機器を購入(入手)し、ダイナミック・オンデマンドVPNサービス提供者(以降サービス提供者)に、VPNサービス利用申請をする。サービス提供者は一階層目のPKIで機器証明書により機器の正当性を認証し、VPNサービスの為のサービス証明書をネットワーク経由でVPN機器にダウンロードする。

1.2.2 接続許可申請

接続許可申請は電話で言えば相手の電話番号の入手や、相手に自分の電話番号を連絡することにあたる。ダイナミック・オンデマンドVPNの場合、双方から接続をしたい機器を申請、両方から申請(許可)されて

いるものに対してサービス提供者はVPN接続に必要な「接続情報」をVPN機器にダウンロードする。

1.2.3 通信の開始

サービス利用者は通信開始時、通信相手を選択しIKEを行い相手とIPトンネルを形成し、通信を開始する。ダイナミック・オンデマンドVPNは2階層PKIによりルータの接続パラメータをオンラインでダウンロードする。接続相手を変える場合もパラメータをダウンロードすれば良いのでN:NのVPN接続が可能となる。

1.2.4 HPKI連携の目指すもの

現状のダイナミック・オンデマンドVPNは安全性の観点から、接続元および接続先の双方から接続許可が出されるまで、接続を許可しない。従って患者データが保存された医療関連データベース(以降MDB)に患者が診療を受けにきた医療機関からアクセスする場合を想定すると、あらかじめ事前にMDBから接続許可のあった医療機関しかMDBと通信できないことになる。いいかえれば、患者はあらかじめMDBとの接続を許可された医療機関へ行かざるをえずフリーアクセスの原則がみたせなくなる。本研究ではHPKIを利用して課題を解決できる方式を提案する。

2. 方法

2.1 HPKI署名付サービス利用申請書

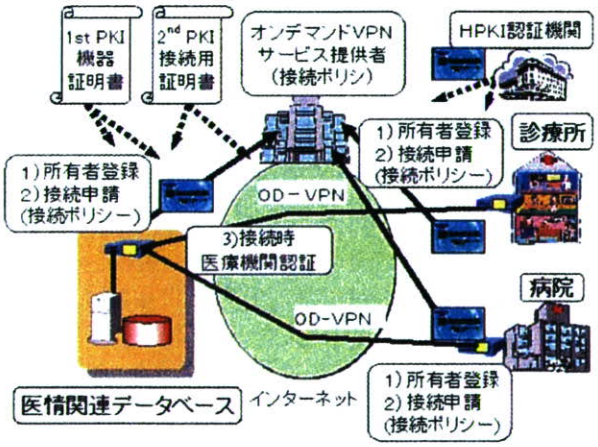


図1 HPKIを利用したダイナミック・オンデマンドVPNの概要

医療機関がVPNサービス利用申請としてVPN機器の登録情報をVPNサービス提供者に送付する際、申請書に医療機関の責任者用のHPKIで署名する。MDBは接続申請時に接続申請する機器がHPKI付申請のものであれば接続を許可することをVPNサービス提供者に申請する。VPNサービス提供者はあらかじめHPKI署名付申請で医療機関であることを登録したVPN機器からの接続申請かを判定し、MDBへの接続を許可する。この場合、接続の合意はMDBのポリシーと一致することにより事前確認が双方で取られているものとみなす。このポリシー制御の考え方はXACMLの概念に類似している。

2.2 XACMLおよびSAMLの概念の利用

XACMLはPDP(Policy Decision Point)、PEP(Policy Enforcement Point)およびPAP(Policy Administration Point)のキープレーヤを定義している。[1]

ダイナミック・オンデマンドVPNではPEPは接続許可申請に対し接続情報のVPN機器への配布点にあたる。PDPはポリシーに基づく接続許可の判断す点にあたる。PDPはPAPのポリシーに基づき判断を行う。

XACMLは3つのContextを定めている。PAPからPDPに示すルールやポリシーを記述するための「XMLスキーマ」、PEPがアクセス要求者の属性情報を記述してPDPに提示する「要求Context」およびPDPがPEPに返す認可決定の「応答Contextのスキーマ」である。

「ポリシーを記述するスキーマ」はMDBの接続許可申請時に「MDBに対して接続許可申請するVPN機器がHPKI付申請のものであれば接続を許可する」ポリシーをVPNサービス提供者に申請するときの構文の考え方に使用できる。

また、SAMLでは「認証オーソリティ」と「属性オーソリティ」がAssersionをResponseとして応答するときにオーソリティの署名つきで応答する。これは「VPNサービス利用申請時、申請書に医療機関の責任者用のHPKIで署名する」時の構文の考え方に利用できる。ただし、PDPが署名の属性も利用するところが異なっている。

3. 結果

本方式により、医療機関からのアクセスであれば、事前のサーバ側からの個別接続許可がなくても、接続を可能とすることができ、患者の医療機関に対するフリーアクセスの環境を実現でき、医療関連施設間のネットワーク基盤すなわち医療ドメインネットワークを形成することができる。

4. 考察

医療機関というだけでMDB側が接続を許可するのはダイナミック・オンデマンドVPNのセキュリティポリシーの制御としてものたりないとの考え方もある。その為にはhcRoleを使って、例えば薬局、病院、その他を区別したり、他の方法で確認した属性を利用したポリシー制御が出来る方式を検討する必要がある。

5. まとめ

サービス提供者にXACMLで定義するPDPに相当するものをおくことによりMDBのポリシーやVPN機器の属性を配慮した接続ができ、またサービス利用申請時にHPKIで署名することにより、hcRoleの属性を利用できることを示した。標準化を配慮しXACMLやSAMLのようなXML形式の申請書やポリシーマッチングの標準的形式を検討する必要がある。

6. 謝辞

本研究は情報通信研究機構委託研究:「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」において行われた。

参考文献

[1] 第5回 PKIとPMIを融合させる次世代言語XACML.http://www.atmarkit.co.jp/fsecurity/rensai/webserv05/webserv01.html.