中間サーバを介して接続される。

ここでインターフェイスシステムは、コアシステムから提供される電子的な許可証を用いた情報提供に関するプロトコルを実行する（透明性の確保に不可欠）とともに、情報提供に関するログを記録する等の機能を有している。また中間サーバは、情報保有機関が用いている基幹システムに代わって、他機関との情報提供を可能とするために設置されるものであり、システムの安全性、可用性等の理由から、法定されている個人情報の写しが記録・管理されることになる。このことを言い換えると、情報保有機関の基幹システムが管理する個人情報が正本であるのに対して、中間サーバに記録されるのは副本になることを意味している。そして中間サーバが保持する副本は、他機関へ提供されることから、その記録フォーマットは必然的に標準化されることになる。次節以降で述べるように、この標準化されたフォーマットで記述される副本が利用可能になることは、電子自治体の加速にとって極めて重要な環境の整備につながると考えられる。

3．これまでの取り組みと新たなサービス提供

我が国の政府は、情報システムに係る政府調達について、自由で公正な競争を促し、より一層の透明性・公平性の確保を図り、もって情報システムの開発・運用経費の削減等を目指した取り組みを、平成12年頃から開始した。当初は、CMMI（Capability Maturity Model Integration）の調査研究には始まり、その後、EVM（Earned Value Management）、EA（Enterprise Architecture）等を用いた諸外国の事例等を参考にして、平成19年に「情報システムに係る政府調達の基本指針」を決定し、同指針に沿って、情報システムに係る政府調達を実施している。そして、具体的な取り組みとして、各府省において業務と情報システムを最適化するための計画（最適化計画）を策定し、情報システムの運用コスト等の削減や業務処理時間の削減を図ってきた。これまでの取り組みにより、レガシーシステムのオープンシステ

ムへの置き換えや分離調達等が実施され、1000億円／年を超える経費が削減されてきた。一方、地方自治体の情報システム調達については、中央政府と同様の取り組みを進めることを目的として、平成19年６月に「自治体EA業務システム刷新化の手引き」を公表し、多くの自治体により刷新化の取り組みがなされてきた。

発注側が行うこのような情報システムの調達改革に加えて、受注側によるサービス提供の形態も大きく変化してきた。その代表例は、SaaS（Software as a Service）やASP（Application Service Provider）さらにはその発展形となるクラウド等である。これらの新しいサービス提供形態は、民間分野等での事例を見ると、ハードウエアの共有や基本的なパッケージソフトの利用等による経費削減、さらにはサービス・インまでの時間短縮等の様々な利点があるといえる。他方、これらのサービスを利用することにより、サービス提供者に依存する割合が増える傾向がみられることから、新たなベンダーロックインに陥る危険性にも留意すべきと思われる。そこで次節では、これらの課題を避けるための手法について解説する。

4．本質的な課題

自治体を含めた行政による情報システムの調達には、WTOによる政府調達ルールや会計法等による制約、さらにはシステム部門の職員数及び専門性の不足等、金融機関に代表される民間による情報システムの開発・調達が持つ課題にアドオンされる様々な制約や課題が存在する。そのため、これらの制約等を回避するための工夫がなされ、結果として受注側がこれらのリスクをヘッジする事例が多くなったと思われる。よく知られている典型的な事例としては、旧社会保険庁が契約していたデータ通信役務サービスがあげられ、その問題点として、情報システム調達の競争性の喪失、及びその結果としての経費の高止まり等があげられた。クラウドサービスの究極が、ハードウエアおよびソフトウエアに加えて保守・運用を含む情報システムの利用に必要

となる全てのサービスを、受注者から提供してもらうことを考えると、そのサービス提供形態はデータ通信役務サービスと似ることになる。

このような問題の解決につながる有効な要件は、システム調達の競争性の確保であると思われ、そのためにはベンダーロックインの解消あるいは防止が不可欠となる。事実、前者はこれまで中央政府が取り組んできた業務・システム刷新化の目標の一つになっていることからも、ベンダーロックインの防止がクラウドサービスを採用する際の重要な留意点であることを示している。これまでの事例をみると、ベンダーロックインになる主たる要因は、①発注側のITおよび業務のガバナンスが不十分であること、②ユーザデータ等の新システムへの移行作業にかかわる問題の2つに大別される。ここで①の要因となるITガバナンスの不足に関しては、CIOの設置に代表されるIT部門の強化等による対策がとられてきた。この対策は、確かに功を奏し始めていると認められることから、未対応の団体等においては、適切に対処することが望まれる。他方、情報システムの構築・運用等を長期に渡りアウトソースしてきた機関や組織においては、残念ながらその効果が小さい事例が見受けられる。このような事例について、諸外国及び民間等の例を参考にして検討したところ、共通した問題点として業務そのもののガバナンスが不足しているのではないかと思われた。このような経緯から今回の指針には、業務とITのガバナンスの確保に有効（具体的には業務に対する受発注両者の共通認識の確保と責任分界点の明確化による競争性の確保）と思われるBPM（Business Process Management）と業務フローの見える化に有効なBPMN（Business Process Model and Notation）を参考資料として追加している。これらの手法および具体的な取り組みについては、次章以降において紹介されているので、参考にしていただきたい。

上記②は、発注側にとって最も重要な業務関連情報（多くの場合はDBとして記録されるユーザデータ）を新システムに移行する際に発生する問題である。行政等が用いている現有の情報システムの多くは、それぞれ独自のフォーマット（受注側の知財になる場合もあり）でユー

ザデータを記録・管理している。システム内でのデータの記録・管理手法は、データベースのパフォーマンスに影響するとともに、各ベンダーの創意工夫の範囲であることから、これらに制約を設けるべきではないと思われる。しかしながら、当該システムと他システムがこれらのデータを用いた連携を行うには、共通フォーマットの制定が必要になり、その汎用性を重視すれば、記述形式を標準化することが不可欠となる。このことを言い換えると、既存のシステムに標準形式によるユーザデータの入出力ポートを設けることは、全てのITベンダーが、スムースかつ廉価にユーザデータを正確に移行できるようになることから、②の問題の有効な解決策になると予想される。

5．番号制度の導入を機として

図2で示したように、番号制度の実施に合わせてコアシステムと接続される行政機関等は、各機関が記録・管理する行政情報（前節で述べたユーザデータ）を中間サーバに副本として記録することになる。そしてこの副本に当たるデータは、情報提供ネットワークシステムを介して他の機関と送受信されるため、その記述形式は標準化されたものになる。このことは、前節で触れた②の問題の解決策になる。もちろん、今回の情報提供の対象となるユーザデータは移行対象となるデータの一部ではあるが、今後、情報提供されるデータの種別が拡張されること、および副本の重要性が明確になること等の理由により、副本を用いるアプローチの有効性が高まっていくと期待される。これらの事がまさしく、番号制度の導入を機として地方公共団体等が有する情報システムの刷新あるいはクラウド技術の導入に資すると考える根拠である。

6．終わりに

電子自治体の構築は、行政業務の正確性・透明性の確保、効率およ

び住民サービスの向上等を実現する現実的なアプローチである。もちろんその構築に相当額の経費を要することは、誰の目にも明らかである。逼迫している地方自治体の財政状況を考えれば、さらなる支出が困難ことも理解される。だからこそ、既存の情報システムの経費を削減し、その削減分を電子自治体の構築に振り向けることが極めて重要と思われる。今回の番号制度の導入が、システムの刷新化やクラウドへの移行等を実現する好機になることから、電子自治体の実現に向けて、着実に歩みが加速されることを期待する。

SPECIAL INTERVIEW

東京工業大学
像情報工学研究所
教授 工学博士

大山 永昭氏

中間サーバーはデータ移行に有用 業務フロー可視化で調達改革を

おおやま ながあき
大山 永昭

1982年東京工業大学総合理工学科物理情報工学専攻博士課程修了。米アリゾナ大学研究員などを経て1993年東京工業大学教授。専門は情報セキュリティ、画像再構成、医用画像解析など。番号制度に関わる政府の「情報連携基盤技術ワーキンググループ」構成員、厚生労働省の個人情報保護に関する検討会の座長代理、総務省の電子自治体加速検討会の座長などを歴任。現在、地方公共団体情報システム機構（J-LIS）の経営審議委員会委員長、厚生労働省の参与および医療等分野での番号制度活用研究会の構成員などを務める。

写真：佐藤 久

ここ数年、マイナンバー（社会保障と税の共通番号）の制度化、政府CIO主導による行政システムの最適化、自治体クラウドの推進など、IT活用による行政サービス/事務の高度化・効率化の取り組みが急速に広がっている。セキュリティなどのIT技術の専門家として政府の電子行政政策に深く関わってきた大山永昭東京工業大学教授に、現状の評価を聞いた。（聞き手は本誌編集長、井出 一仁）

——3月に総務省の検討会の座長として、「電子自治体の取組みを加速するための10の指針[注1]」を取りまとめました。

大山　自治体だけでなく国のシステムもそうですが、行政システムで最も大きな課題はシステムの刷新とそれに関わる調達の改革です。そこでの最大の問題は、競争が働く開かれた市場になっていないことです。

自治体システムがこうした状況になっている原因は2つあります。

一つは自治体が持つ住民情報の移植性が十分に確保されていないことです。例えばA社のシステムからB社のシステムへ情報を移す際にはデータの記述形式などが変わる可能性があります。しかし従来の調達方法では移植はB社の役割になるので、B社はA社にデータの仕様などを詳しく聞かないと作業ができません。このためベンダーの切り替えが難しくなっていました。

全国地域情報化推進協会（APPLIC）が「地域情報プラットフォーム[注2]」の標準仕様を作成・公開しており、その普及が望まれますが、使うかどうかは任意なので強力な推進力が必要です。

——データ移植性の問題は当面、解決の見込みがないのでしょうか。

大山　実はマイナンバー制度で各自治体に導入される「中間サーバー[注3]」に注目しています。

中間サーバーには、国の機関やほかの自治体との間で住民情報を連携させるために、各自治体の各種業務システムの住民データが、副本として標準化されたフォーマットで保存されます。つまり、各自治体は業務システムを更新する際に、業務システムにある原本のデータは捨てて、中間サーバーにある副本を使って原本を再生できるはずです。これを実現すれば、データの移植性の問題は解決できるでしょう。

——自治体システムでベンダー間の競争が働かない2番目の要因は。

大山　ソフトウエアの切り替えが難しいことです。なぜ自治体のシステ

注1）電子自治体の取組みを加速するための10の指針
総務省の「電子自治体の取組みを加速するための検討会」が2014年3月に公表した指針。電子自治体推進指針としては7年ぶりの改訂版。

注2）地域情報プラットフォーム
自治体の様々な業務システムを連携させるための業務面や技術面の標準仕様。データ項目やデータ形式、インタフェース、通信手順などを規定。

注3）中間サーバー
マイナンバー制度で自治体が他団体との間で符号を用いた住民情報の連携を実現するために新規導入するサーバー。ハードウエア費用は総務省が負担。『中間サーバー・プラットフォーム（仮称）』として東日本・西日本の2カ所に集約・設置する。

注4）WFA
Work Flow Architectureの略。業務流れ図ともいう。

注5）BPMN
Business Process Model and Notationの略。ISO19510。

「公的個人認証サービスとの連携で個人番号カードの可能性が広がる」

ムでは独自開発が多く、切り替えが容易なパッケージソフトが広がらないのでしょうか。パッケージを利用している自治体でも、結局カスタマイズが多くなっています。

ようやくわかってきたのは、自治体を含む行政機関ではシステム化の前提となる業務フローの可視化が十分ではないということです。行政機関のシステム調達では、業務フローの記法として政府独自の「WFA[注3]」を用いることが多いのですが、はたして現場のどのくらいの職員が理解しているでしょうか。

WFAでは、システム化された業務の流れを中心に記述します。しかし大切なのは、業務全体のフローを基にパッケージの機能を分析していくことです。カスタマイズを抑えるには、パッケージに合わせて業務フローを見直すことも重要です。

そこで、業務全体のフローを可視化するために提唱したのが、国際標準にもなっている「BPMN[注4]」です。「10の指針」では、「指針5」の中で取り組み手法の例として挙げました。

BPMNは、作業の内容を「～を～する」という形で記述します。システムの操作フローを中心に記述するWFAと比べて、システムの専門家でなくても利用しやすくなっています。また、プロトタイプの自動生成ツールなどもそろってきています。

――業務フローを正しく記述できればパッケージ導入も進みますか。

大山　自治体の人は業務はわかっているわけですから、パッケージベンダー側も業務フローを示したカタログを作るなど、工夫をするべきでしょう。そうすれば少なくとも今よりは競争性が増すはずです。

BPMNで業務フローを可視化することには、もう一つ大きな利点があります。組織的・継続的な業務改善の手法である「ビジネスプロセスマネジメント(BPM)」を進めやすくなることです。

BPMNでは、システム向けのWFAと異なり、手作業を含めた業務全体を記述できます。このため、首長や幹部は「システム部門の問題だから」と逃げることができなくなります。同様に現場の職員も巻き込みやすくなります。BPMによって、今の業務フローに無駄があるのかないのか、業務の棚卸しや標準化を検討しやすくなるわけです。

――「10の指針」では、指針1から指針6まで半分以上を自治体クラウドの導入加速策が占めています。

大山　検討会を通じて感じたのは、自治体でのクラウド導入の最大の障害は、自庁舎内にシステムがなくなることへの不安だということです。複数の自治体と組むとき、経費が下がることはわかっていても、どこがリーダーシップを取るのかとなると、根深い問題も出てきます。クラウドへの移行に伴い、クラウドベンダーにロックインされないようにすることも考えないといけません。

――医療分野でのマイナンバー活用についての展望は。

大山　税や社会保障よりも機微性の度合いが高い医療情報にはマイナンバーを使うべきではないという意見があります。しかし、だからといって別の視認性のある番号を割り当てるのは、かえって危ないかもしれません。誤ってほかの人の情報とひも付けてしまったら、生命にかかわる問題になる場合もあります。

提案しているのは、「個人番号カー

注6）公的個人認証サービス（JPKI）
申請・届け出のような行政手続きなどの際に、なりすましやデータ改ざんを防ぐために用いられる本人確認サービス。現在は住民基本台帳カードのICに内蔵された署名用電子証明書を使って、国税電子申告・納税システム（e-Tax）などで利用されている。マイナンバー制度の個人番号カードには、利用者証明用の電子証明書（基本4情報を含まない）も格納されるほか、民間企業も署名検証者として認証業務が可能になる。JPKIはJapanese Public Key Infrastructureの略。

注7）地方公共団体情報システム機構
2014年4月に設立された地方共同法人。略称はJ-LIS。住民基本台帳ネットワークや総合行政ネットワーク（LGWAN）の運営など、地方自治情報センター（LASDEC）の業務を引き継ぐとともに、マイナンバー制度での個人番号カード発行業務や公的個人認証サービスの運営も担う。

ド」に内蔵される公的個人認証サービス（JPKI）[注6]の利用者証明用電子証明書を使って、医療情報とひも付ける方法です。医療用に別の番号を割り当てて別のカードを発行するのは、コスト面から選択肢にはなりえないでしょう。

公的個人認証サービスを健康保険証の資格確認サービスと連携させれば、通院時に個人番号カードさえ持っていけば健康保険証は不要になります。個人番号カードの交付が始まる2016年1月以降は、総務大臣が認める民間事業者にも署名検証者の業務が認められるので、クレジットカード決済などにも使えるようになると期待します。インターネット上のカード決済では利用者証明用の電子証明書を送るだけなので、カード番号が漏えいする心配もなくなります。

――カード決済との連携は総務省も実証を計画しているようです。

大山　総務省の「ICT街づくり推進事業」の放送・ID融合サービスプラットフォーム実証実験では、2014年度に1枚のカードが健康保険証にもクレジットカードにもなる事業を計画しています。16年1月以降は、カード決済の機能は実サービスに移行する可能性が高そうです。

個人番号カードの電子申請を簡単に行うための共同研究を、東京工業大学と大日本印刷で進めています。

2015年10月以降に住民に郵送される紙製の「番号通知カード」には、事務処理用の番号がバーコードで印刷される見込みです。証明写真用ボックスに付加したリーダーでバーコードを読み取らせてから顔写真を撮り、申請ボタンを押すと、個人番号カードの発行元となる地方公共団体情報システム機構[注7]へ暗号化してデータを送り、交付申請が済むという仕組みを考えています。

すでに実験をしていて、今後は証明写真用ボックスのベンダーとも協議していきます。総務省とも話をしていますが、ボックスを自治体の窓口などに置いてもらえれば、個人番号カードの普及促進に大いに貢献できるでしょう。

病院情報システムにおける紙情報の現状と変化の方向性

八幡 勝也[*1] 武田 裕[*2] 松村 泰志[*3] 中川 肇[*4] 木村 映善[*5] 村田 晃一郎[*6] 瀬戸 遼馬[*7]

[*1]医療法人 住田病院 [*2]滋慶医療科学大学院大学
[*3]大阪大学大学院医学系研究科医療情報学 [*4]富山大学附属病院経営企画情報部
[*5]愛媛大学大学院医学系研究科博士課程医学専攻 社会・健康領域医療情報学講座
[*6]北里大学メディカルセンター [*7]東京医療保健大学医療保健学部医療情報学科

Current state of paper documentation in hospital information system and directionality of change

Yahata Katsuya[*1] TAKEDA Hiroshi[*2] MATSUMURA Yasushi[*3]
NAKAGAWA Hajime[*4] KIMURA Eizen[*5] MURATA Kouichirou[*6] SETO Ryoma[*7]

[*1]Sumida Hospital [*2]Graduate School of Health Care Science, Jikei Institute
[*3]Medical Informatics, Osaka University Graduate School of Medicine
[*4]Division of Medical Planning, Management and Informatics, Toyama University Hospital
[*5]Dept. Medical Informatics of Medical School of Ehime Univ.
[*6]Kitasato University Medical Center
[*7]Division of Healthcare Informatics, Faculty of Healthcare, Tokyo Healthcare University

The hospital information system spread, and paperless of the hospital work advanced. However, in medical institutions that use computer system, the handling of the paper documents, inpatient care plan and the paper of the release form etc. is a problem, too. How is a paper document and an electronic system combined and is the use management done? Technical and legal examination is necessary.

In "The 4.2th edition of Security Guidelines for Health Information Systems", it is described about the handling of the scanned medical documents.

The management of the document of paper is practiced in shape of "Document Archiving and Communication System" and computer system operation is practiced in Osaka University Hospital. Various examinations were done through this development.

This workshop, discuss about various problems (scanning, originality, and long preservation, etc.) caused between the document and the information system of paper. In addition, the use-cases with the community health, nursing, and health care, etc. the profit use of the paper medium in the information system is examined.

Keywords: paper document, scanning, Document Archiving and Communication System, long-term preservation of medical documents

1. はじめに

病院情報システムが普及し、院内のペーパーレス化が進んでいる医療機関でも、紙で作成された診療情報提供書、検査結果、入院診療計画書、承諾書、熱型表、指示記録などの書類の取扱いに課題がある事が多い。紙の記録と電子的システムをどのように組み合わせて利用管理するか。技術的・法的な検討が必要となっている。

「医療情報システムの安全管理に関するガイドライン 第4.2版」の「9 診療録等をスキャナ等により電子化して保存する場合について」では、次のようにケースを想定している。

1)電子化された医療機関において、他院からの診療情報提供書や調剤済み処方

2)電子保存を施行したが、施行前の紙の診療録等が残り一貫した運用ができない場合、及びオーダエントリシステムのみの運用で紙等の保管に窮している場合。

大阪大学病院においては診療記録統合管理システムという形で、紙の書類の管理を電子的な運用を実践している。この開発を通じて様々な検討が行われた。

今回は、本事例を通じて紙の書類と情報システム間で生じる諸課題(スキャン、原本性、長期保存、など)について検討する。さらに、ユースケースを検討し、情報システムにおける紙媒体の利活用について検討する。

2. 統合文書管理システムの開発・運用における経験

大阪大学大学院医学系研究科医療情報学
松村泰志

電子カルテシステムは、基幹システムだけでなく、いくつかのサブシステムを統合して構成されている。例えば、大阪大学医学部附属病院(阪大病院)では、画像レポートや病理レポートシステムなどは、基幹システムとは別ベンダーのものを利用しており、実体データは、サブシステム側のサーバに保存されている。これらのシステムでは、レポートシステムはWebシステムとなっており、基幹システムの患者を指定して開くカルテ画面から、その患者のIDをURLに組み込んで問い合わせすることで、その患者の画面が開く仕組みとなっている。これにより、ユーザには、サブシステムを意識させずに、一体の電子カルテシステムかのように見せることができる。

しかし、この構成の電子カルテシステムには致命的な欠点を持つ。第一に、基幹システム、サブシステムを含め、将来ベンダーを変更した際には、過去のデータが閲覧できなくなる危険性が高い点である。基幹システムを提供するベンダーとは、永久に契約し続ける覚悟があったとしても、サブシステムも含めてのつもりではないのが通常である。しかし、サブシステムを別ベンダーに変更した場合、過去データを閲覧する方法が無くなってしまうことになる。

第二は、同じ文書種であっても、別システムで作成された文書は、別のビューアから閲覧することになる点である。例えば、阪大病院では、手術レポートは、電子カルテシステム内の文書システムを利用する診療科と、自分たちがこれまで作成してきたファイルメーカのシステムを継続して使い、電子カルテシステムには、スキャンしたファイルを保存する診療科がある。手術レポートを閲覧する場合、閲覧者は、作成者がどちらのシステムで作成したかを知らないので、どちらにあるかを探さなければならなくなる。慣れていない他科のユーザは、片一方を探して無い場合に、手術レポートが無いと勘違いする危険性がある。

第三は、それぞれのビューアを立ち上げなければ、この患者がどのような情報を持っているかを知ることができない点である。入院、手術、心臓カテーテル検査等の重要検査などの重要イベントですら、ユーザがその有無を調べようとしなければ確認することができない。結果的に、当該患者がどのような疾患で、どのようなヒストリをとってきたかを大まかに把握することができない。

以上の三つの欠点は、診療録として容認できるものではなく、それが解決されていない電子カルテシステムでは、ペーパレス電子カルテ運用はすべきでない。

我々は、統合文書管理システムを開発することで、この問題の解決を図った。統合文書管理システムは、電子カルテ記録を文書の集合とみなし、基幹システム、サブシステムで作成される文書をPDF等に変換して、中央のサーバに保存する仕組みである。これにより、第一の問題は解決される。文書を統合的に管理する際に、文書種コードを振り、文書種コードのグループで統合的に閲覧できるビューアを開発すれば、ソースとなるシステムが異なっていても、同じ文書種を同じところから閲覧できることになる、これにより、第二の問題が解決される。更に、この文書種と文書内容の発生日(イベント日)で各文書をマトリックス上に表示するだけで、当該患者の重要な情報を一覧できるようになり、ユーザは、その画面から当該患者がどのような情報を持っているかを知ることができる。いつどの科で入院し、いつ何の手術をし、いつどのような検査をしたかが一つの画面上に表現されることになる。これにより紙カルテよりもはるかに全体の病歴が把握しやすくなり、第三の問題が解決される。

このシステムをリリースして4年半が過ぎたが、データが蓄積されるにつれ、その真価が明らかになってきている。上記三つの課題が解決されていることに加え、以下の点にもメリットがあることが明らかになってきた。

一つ目に、カルテ開示請求があった際の処理が迅速である点である。全ての文書が統合管理されていることで、これらを当初設定された順番で一度の操作で出力することができる。このシステムが無ければ、全てのサブシステムを確認し、文書があれば出力し、最終的に意味のある順番に人が並び替えて患者に渡す作業となり、大変な手間となる。二つ目は、あるべき文書が無いことが直ぐに分かる点である。例えば、手術をした場合に取得しておくべき同意書が無いとか、手術レポートが作成されていないなどのことが、直ぐに把握できる。この原理を使って、診療録監査システムが構築できる。従来の紙カルテでは、退院してからチェックをすることになり、問題が見つかった時には遅すぎることもあったが、このシステムを利用することにより、リアルタイムに問題が把握でき、対処しやすくなった。

統合文書管理のコンセプトとは別件にはなるが、それ以外にも、スキャン文書が見やすく管理される点、しかも、署名、タイムスタンプを押して保存しているために原紙を破棄できる点、同意書をスキャンするだけで説明文書も電子カルテに保存される点など、導入したスキャンシステムの機能により、紙文書を電子化して管理することで運用しやすくなった。また、文書内の重要データを収集する仕組みがあり、そのデータが、データ共有データベースおよびデータウェアハウスに保存されるため、他の文書へのデータの流用やデータの集計が可能になるなどの良い点もある。

以上の通り、ペーパレス電子カルテを運用するためには、何らかの統合文書管理システムが必須と思われる。逆に、統合文書管理システムを導入することにより、ペーパレス電子カルテ運用に比較的容易に移行しやすくなる。

3. 紙医療文書の電子化長期保管システムの運用経験

富山大学附属病院経営企画情報部
中川　肇

3.1 はじめに

多くの病院では、未だインフォームドコンセント(IC)などの患者への説明文書、生理・自家検査結果レポートなど多くの紙媒体での記録が残っておりその処理にそれぞれ工夫されている。臨床現場では、紙をスキャンして電子カルテで参照できればいいという声も聞かれるが、情報管理側としては、医療記録として、諸法令、ガイドラインを遵守する必要があり、そのためのシステムを構築していることを周知する必要がある。

3.2 電子化保存の根拠となる法令とガイドライン

電子署名および認証業務に関する法律(平成12年法律第102号)、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」(平成16年法律第149号)、厚生労働省医療情報システムの安全管理第4.2版の遵守が必要になる。

3.3 本院での長期保管システムの概要と運用

本院では、病棟で発生したICなどの書類を診療情報管理室でスキャナ処理をし、出電子署名、タイムスタンプを付与している。その稼働状況を表にしめす。デジタル署名は電子署名が失効しないうちに、有効なタイムスタンプを付与しなければ文書の信憑性が失われるため、検証情報も含めたPDFとし、長期保管に対応している。

表1 稼働状況

平成26年	処理枚数	一日平均処理枚数	稼働日数
1月	5,246	276.1	19
2月	5,196	273.5	19
3月	5,881	294.1	20
4月	5,248	249.9	21
5月	6,079	301.0	20
6月	4,673	222.5	21
7月	5,537	251.7	22
合計	37,860	266.6	142

3.4 今後の方向について

平成27年1月からの電子カルテのリプレースに伴って、統合文書管理システムについて提案を募り本原稿執筆時点で調達中である。長期保存のフォーマットについてはPAdESとXAdESの2種類の提案がなされている。機能的には①文書発生から処理までの迅速性、正確性を目的として電子カルテから出力される文書にバーコードを入れて文書メタファイルを付与し仕切紙を使わない処理　②他の診療行為との関係性が分かるように電カル上で密に連携すること　③既存の文書の再利用を可能にすること　④時系列的表示　を目指している。また運用面では診療情報管理士の監督の下に処理要因を増員させ迅速な処理を図っている。

4. 印鑑に代わるコピー防止つきQRの運用の提案

愛媛大学大学院医学系研究科博士課程医学専攻
木村　映善

4.1 背景

当院は、ペーパーレス化による業務効率化を目指して、スキャンと文書管理システムの導入[3]、問診票の電子化[4,2]、そして紙媒体由来のデータと電子情報を統合するための医療におけるECM(Enterprise Content Management) [6,7,3]について提唱してきた。いわゆる、院内に発生を起源とする紙文書の大半は電子化もしくはスキャン文書に移行することができたのであるが、院外の医療機関や施設、患者に持たせるものについては、未だ手つかずのものが多い。2012年に同意書・問診システムを発表した時以来の質疑から浮かび上がってきた課題と方向性を紹介する。

a.同意書に患者の印鑑が必要であるか？

同意書は民法上の同意書は民法上の契約書面というよりは、説明をしたことの確認の記録という位置づけでしかない。その解釈に立てば、患者の署名のみでよい。

b.筆跡認証に必要なデジタルデータを採取すべきか？

筆圧も含めた筆跡データを採取できるタブレットでデータ取得することにより、本人の認証をすべきではないかという意見については、患者の筆跡情報を別途に採取する必要があること、筆跡鑑定が正しくできるというエビデンスが存在しないこと、利用できる場面が限られるという制約があることから積極的な採用を検討しない。

c.同意書は契約書類ではないか。

医療サービスは治療プロセスに対する準委任契約であり、包括的なものである。一つ一つの行為に対する請負契約を結んでいる訳ではないと理解している。同意書は治療プロセスにおける善管注意義務を果たしている一つの書証に過ぎないと考える。

d.医師の押印がなくなると、その医師が実際に記載したとする証拠をどうするか。

電子カルテ上でのログイン認証による医師の同定と、同意書の文書オーダ履歴より確認ができるので、押印が無くてもその医師が記載したことが確認できると考える。また文書管理システムなどワークフローを管理できるシステムでは、最終的な文書の発行に医師の承認を要求することとし、それを医師の意思確認とすることができるものとする。

e.患者が同意をしていないと反論するリスクがある。

同意書を紙文書で取っていたとしても、同意書に記載されていない部分で反論されるケースが多い。つまり、同意書への同意記載の真贋についての議論より、説明内容が適切であったかどうかが争点になりやすい。

仮に同意書の真贋が問題になった場合は、患者がその同意書が偽造されたという立証責任があり、その点において防衛的な患者が改めての書面への押印を求めるということは考えられる。

上記の議論を積み重ねても残るのは、結局紙文書になった時に、その紙文書の証拠能力をどう担保するのかというところである。

4.2 記名と押印の位置づけ

契約書(契約書ではないものでも、法的背景がある書類も含めるものとする)において、署名捺印、署名、記名押印が法的な証拠能力として認められており、記名のみでは正式な効力とは認められていない。プリンタによる印影の印刷は記名同様、証拠能力として認められていない。

言い換えれば、印刷した時に証拠能力を持たせられるものが開発できればよいわけである。上記で印刷ができるのは、記名と押印に代わる印影である。すなわち、押印に相当する印刷物が証拠能力を有するというコンセンサスを成立させれば、PCによる印刷物でも記名押印相当の証拠能力を持たせることができると考える。

4.3 証拠能力を持つ印刷物

印刷物が証拠能力を持つには、(1)複製ができないこと、(2)改竄ができないこと。加えて、デジタル時代の特長として、(3)違反の事実を即時に検出できること、が必要である。

a. 複製防止機能

機密文書のセキュリティ対策のために、文書の背景

に隠し文字・複製制限文字を埋め込んだ地紋パターンを合成して印刷する技術が開発されている。隠し文字とはコピーすることで浮き出る文字列であり、原本とコピーの区別ができるものである。高精細な印刷が可能になったプリンタが普及したこと、プリンタドライバに内蔵されたことにより、汎用的に使える仕組みとなってきている。

b. 改竄防止機能

押印の証拠能力は印影の形状と、印鑑をつきあわせて検証できることに由来する。また印鑑の法的位置づけは印鑑・実印登録した印鑑証明書が担保する。

これを印刷物で実現するためには、印影の印刷ではなく、検証をするためのコードでもって代える。例えば、QRコードは動的に生成することが可能である。医療機関名、印刷日時、入力者、情報を埋め込む。同時にQRコードをクラウドにアップロードすることで、検証が必要な場合は、QRコードを読み込み、クラウドに問い合わせる。

c.QRコードの複製禁止・抑止

QRコードは四角の形状をとっているため、(a)の複製防止の対策をとっていても、切り抜いて他の文書に貼り付けることも可能かもしれないし、アルゴリズムがわかれば偽造も容易である。公開部と非公開部が混在するSQRC(セキュリティ機能搭載QRコード)、複製防止の対策技術を組み合わせた2次元コードの印刷、特殊なインクを塗布することによるコードの複製を防止する等の対策が施されている。

また、前項で述べたクラウドへの照会機能を使うことで、一度照会されたQRコードは無効化し、次回以降の問い合わせには無効の結果を返すことで再利用を防ぐことも可能である。

4.4 提案

処方箋、診断書、紹介状等については、記名押印に代えてプリンタによる出力を認める。条件として、文書に複製禁止機能が施されていること、埋め込んだコードの内容について問い合わせることができるWebサービスを提供することとする。文書には有効期限を設けて、規定日以降は無効とする。

文書の真正性については、文書そのものよりも、文書を発行したところに問い合わせ、速やかにその真贋に回答できる体制を整える。そのために、文書管理システムを導入することが望ましい。

4.5 対費用効果への考察

いかなる対策を取っても管理の隙間をつき、また偽造を防ぐことは不可能である。それは従来の署名押印などでも同じ事である。署名押印の方がより証拠能力を有することは否めないが、その不備を利用されることの不利益と、ワークフローが電子化されることによる経済効果・医療の効率化を天秤にかけてはいかがだろう。いずれは地域医療連携システムを使って、すべてはそこから参照して頂くという時代の到来を期待して10年以上経つが、紙との共存も当面続くであろうことも見えてきた現在、紙を伴うワークフローの良さも利用しつつ、便益とリスクのバランスを取って電子化のメリットも享受していく運用を率先して検討していく時期に来ているのではないかと考える。

5. 終わりに

紙は情報の参照・保持に電気や機器が不要という利点がある。代わりに、物理的な場所を必要とし、管理や検索に手間を必要とし、コピーや転送に際しては情報機器を要する、という欠点がある。

デジタル機器・メディアばかりでなくソフト環境は違いや変化が激しく、利用に際して普遍性に課題がある。それに対し紙は、予測できない不特定の場面や利用者に情報を提供できるという特徴を持つ。両者の特徴を利用して医療情報の利活用すべきと考えられる。

参考文献

[1] 武田 理宏, 真鍋 史朗, 三原 直樹, 松村 泰志, 他. DACSによる診療記録統合管理と文書閲覧における効果. 第33回医療情報学連合大会論文集 33rd JCMI(Nov.,2013) P852-P855.
[2] 中川肇. 長期署名フォーマット(PAdES)を採用した院内紙文書電子保存システム. 新医療, 2011年4月号, P100-P103.
[3] 赤堀 澄子, 木村 映善, 小林 慎治, et al. 紹介状の電子化運用を想定したドキュメントスキャンシステムの開発. 第29回医療情報学連合大会論文集; 2009; 2009. p. 1159-60.
[4] 片上 敦詞, 木村 映善, 西岡 里枝, et al. クラウドを利用した問診システムの開発. 医療情報学. 2010;30(Suppl.):1380-1.
[5] 森脇 留美子, 天野 利江, 矢野 みゆき, et al. 内視鏡看護記録の改善への取り組み～iPad看護記録の開発および導入を試みて～. 第66・67回日本消化器内視鏡技師学会; 2011; 2011. p. 2859.
[6] Association for Information and Image Management. What is Enterprise Content Management ?. http://www.aiim.org/What-is-ECM-Enterprise-Content-Management.aspx.
[7] 木村 映善. 文書スキャンシステムと電子カルテの連携～IHE XDSプロファイル準拠のリポジトリを用いた院内診療文書管理の着想～. 第29回医療情報学連合大会論文集. 2009:50-1.
[8] 木村 映善. 医療ECM視座での電子化紙文書と電子文書統合に向けた課題. 新医療. 2011 2011 April;38(4):92-5.
[9] 八幡勝也. 紙による電子的診療情報連携の検討. IT ヘルスケア, 2013, 第8 巻1 号: 14−15.

プライバシーを考慮した医療情報の活用とその実現に向けた課題

Practical Use of the Medical Information in Consideration of Privacy and Future Subjects

小尾高史　鈴木裕之　李　中淳　平良奈緒子　大山永昭

Abstract

近年，地域医療情報連携基盤構築の進展や全国規模での医療情報ネットワーク基盤の構築など，医療情報の連携を目指す取組みが進められている．このような取組みにより個人の医療情報や健康情報の連携が進み，生涯にわたる経年的な健康医療情報を利用することで，よりきめ細かな医療サービス実現への期待が高まっている．しかしながら，医療等の分野で取り扱われる情報の多くは，生命・身体等に関わる機微性の高い情報であるため，患者のプライバシーには十分な配慮が不可欠である．このような条件の下で，患者への直接的な医療サービス等を提供することはもちろんのこと，医学の進歩等の公益目的のためにも，許容される範囲で共有・活用されるべきものと考えられる．本稿では，構築されつつある地域や全国規模での医療情報連携基盤と，医療等分野におけるICT化の現状を概説する．そして，医療情報の利用に関する課題とその解決の方向性について解説する．

キーワード：医療情報，プライバシー保護，二次利用，匿名化

1. はじめに

2014年6月にIT総合戦略本部から「パーソナルデータの利活用に関する制度改正大綱」[1]が発表され，パーソナルデータの利活用に対する期待が高まっている．医療分野においても，様々な場面で医療情報を利用できる基盤が整備され，情報の利活用や分析の高度化が推進されることによって，医療の質の向上や医学研究の進展が期待されている．一方で，医療・介護等の分野で取り扱われる情報は生命・身体等に関わる機微性の高い情報が多く，その保護のために厳格な取扱いを要する分野である．そのため，患者のプライバシーに十分配慮しつつ，患者本人への医療サービスの質的向上を図るとともに，医学の進歩等の公益目的のために活用できる仕組みを構築することが重要である．

本稿では，はじめに，構築されつつある地域や全国規模での医療情報連携基盤と医療等分野におけるICT化の現状を概説する．次に，医療情報の利用に関する課題を明らかにし，カナダの取組みと課題解決の方向性について解説する

2. 医療等分野におけるICT化の現状

2.1 医療情報連携基盤の現状

我が国の医療制度では，患者は医療機関を自由に選択でき，患者の診療情報は，受診した各医療機関に個別に保存されている．そのため従来は，自らの意思で医師から提供された検査データを管理するなど，患者が本人の診療情報の収集に対する積極的な関与を示さない限り，経年的な医療データであっても，その管理・蓄積は困難であった．

このような状況に対して，地域全体でより効率的な医療提供を実現することや，地域の医療機関が連携して急性期診療から社会復帰までの診療に当たることなどを目

小尾高史　正員　東京工業大学像情報工学研究所
E-mail obi@isl.titech.ac.jp
鈴木裕之　正員　東京工業大学像情報工学研究所
E-mail hiroyuki@isl.titech.ac.jp
李　中淳　東京工業大学像情報工学研究所
E-mail j-lee@isl.titech.ac.jp
平良奈緒子　東京工業大学像情報工学研究所
E-mail taira@iri.titech.ac.jp
大山永昭　正員　東京工業大学像情報工学研究所
E-mail yama@isl.titech.ac.jp
Takashi OBI, Hiroyuki SUZUKI, Nagaaki OHYAMA, Members, Joong-Sun LEE, and Naoko TAIRA, Nonmembers (Imaging Science and Engineering Laboratory, Tokyo Institute of Technology, Yokohama-shi, 226-8503 Japan).
電子情報通信学会誌　Vol.98 No.3 pp.207-211 2015年3月
©電子情報通信学会 2015

的として，地域内の医療機関が医療情報を交換あるいは共用するために医療情報基盤の整備が進められている．そして例えば日医総研の調査[2]では，既に150以上もの地域・地区において地域医療連携ネットワークが稼動している旨が報告されている．

このように地域医療ネットワークは整備されつつあるが，患者は一地域にとどまらないことから，全国どこの医療機関においても患者の医療情報が参照できる仕組みの構築も検討されている．具体的には2014年6月に改訂された政府の「世界最先端IT国家創造宣言」[3]には，「地域を超えた国民への医療サービス提供等を可能とする医療情報利活用基盤の構築を目指し，医療情報連携ネットワークについて，データやシステム仕様の標準化，運用ルールの検討やシステム関連コストの大幅な低廉化等による費用対効果の向上を図りつつ，2018年度までに全国への普及・展開を図る」とあり，その早期実現を目指す旨が明記されている．

このような取組みを通して個人単位の医療情報が連携可能になれば，その分析・解析等を通して，個々の患者に対する身体情報の経年変化への注意喚起や疾病の早期発見，更には医療の質の向上等が期待される．

2.2 医療等分野における個人番号制度に関する検討

2.1で述べた地域や全国規模での医療情報連携の推進に見られるように，医療等分野における情報連携へのニーズは高く，運用面やコストの観点から，同一の番号を用いて患者を特定し，患者本人の診療・治療に限定した医療情報連携を可能とする基盤整備が求められている．しかし，医療分野では，年金分野における基礎年金番号のような本人を特定する生涯不変な番号は導入されておらず，一般的な医療機関等では，診察券番号などの医療機関独自の番号を利用して診療情報等を管理している．また現在，医療等分野における代表的な番号としては，健康保険証に記載されている記号・番号・保険者番号（被保険者番号）があるが，これらは被保険者とその扶養者で同じ番号が用いられていること，転職等により保険者が変わると変更が生じることから，被保険者番号により患者を一意に特定することは難しい．

このため，厚生労働省は現在，「医療等分野における番号制度の活用等に関する研究会」[4]において，医療情報を連携する医師等が，相互に一意の人物を特定でき，かつ漏れや重複のない（唯一無二性と悉皆性を満たす）医療分野独自の番号（以下，医療等ID）の導入を検討している．現在検討されている医療等IDは，原則として，取り扱われる医療情報を一元的に管理するためのIDではなく，医療等分野内で散在する個人の健康医療情報を生涯にわたり，確実にひも付けるために用いられるものである．医療等IDの導入は，直接的には，後で述べる医療情報の一次利用の促進を目的にしており，個人を特定した安全な情報連携を実現することにより，生涯にわたる連続性を持った医療情報（既往歴や服薬歴など）の活用を可能とし，各個人に即した，より確実性の高い医療の提供を目指すものである．そのため，ひも付けされた医療情報の分析や利活用を推進するには，医療等IDの導入を踏まえた，更なる検討が必要になると考えられている[5]．

3. 医療情報の活用に向けた課題

3.1 医療情報とは

一般的に，医療情報とは，患者が医療機関において，診査や治療を受ける過程で発生した患者個別の診療情報等のことであり，以下の情報が含まれる．

- 氏名，性別，年齢などの患者の基本情報
- 血液検査の結果，X線画像など，患者の身体状態に関する客観的な検査情報
- 診療録に記載される医師の所見や患者の疾病等に関する各種の情報

現在，これらの情報については，通常必要と考えられる個人情報の利用範囲を医療機関内に掲示し，患者側から特段明確な反対・留保の意思表示がない場合には，利用について同意が得られているものとして扱われる場合が多い．もちろんこの同意は，医療機関での通常の業務，すなわち患者に適切な医療サービスを提供する目的の範囲内であり，保険会社や勤務先からの健康状態の照会などの場合には，明示的な本人の同意を得ることが不可欠とされている．また，一般的に診療録（カルテ）は，医師の判断や主観的評価等が記載されていることから，医師等の管理下にあるものとされてきたが，患者の自己情報コントロール権を尊重する（個人情報保護の概念として一般化しつつある）観点から，現在は，患者からの要求があれば，原則，診療録等の診療記録の開示を行うこととされている．

表1 医療情報の一次利用と二次利用の例

利用区分	一次利用	二次利用
利用目的	患者本人の診療・治療	・医学研究等を目的とした利用 ・教育，論文作成や学会発表のための使用 ・行政機関での統計作成 ・医療資源の最適配置等，医療政策の立案
関連機関	医療機関	・医学研究機関 ・行政機関 ・教育機関
使用される情報	患者本人の医療情報	・個人を特定できない情報 ・一般的に匿名化された情報を使用

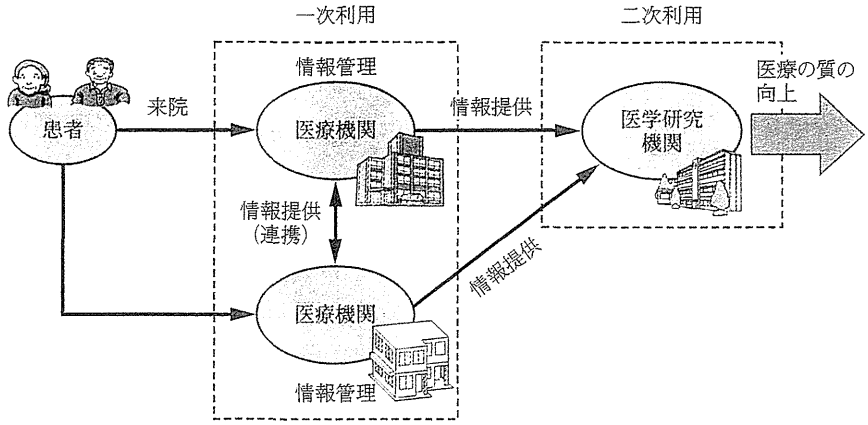

図1　医療情報二次利用のフロー

3.2　医療情報の利用について

医療情報の利用には，大きく分けて一次利用と二次利用がある．表1に示されるように，医療情報の一次利用が，収集された患者の情報を，医療本来の目的である患者本人の診断・治療に利用することを指すのに対し，二次利用は患者本人の診断・治療ではない目的で利用すること，例えば「医学研究のための統計分析」や「論文作成や学会発表」，更には「医療政策の立案」等に利用することを意味する．

図1に示すように，通常，患者が来院し，診療を受けることにより，患者本人の医療情報は当該医療機関で管理される．そして管理された患者の医療情報は，当該病院での診察や治療の目的で「一次利用」されている．また，地域医療情報連携基盤などがある場合には，患者の移動やより専門性の高い医師のアドバイスを得る等の理由により，他の医療機関から患者情報が参照されることもある．このような利用については，先に述べた「第三者への情報提供のうち，患者の傷病の回復等を含めた患者への医療の提供に必要であり，利用目的を院内掲示等により明示している場合には，原則として黙示の同意が得られているものと考えられる」場合に相当することから，「一次利用」と分類される．

これに対して，例えば大学等の医学研究機関が正当な目的で医療機関に医療情報の提供を依頼した場合を考えると，医療機関はその依頼が妥当であると判断し，医療情報に適切な匿名化処置を行った上であれば，医学研究機関に情報を提供できるとすることが望まれる．これが正しく医療情報の「二次利用」にあたる．

3.3　医療情報の二次利用とその課題

3.2で述べたように，情報の取得や活用が，専ら患者本人に対する一次的利用を目的とする場合には，本人に対して掲示等によりその旨及び情報の管理責任者等を明らかにすることで同意を得たとみなせるが，二次利用を目的とする場合には，法的な根拠のあるものを除き，現状では，原則，本人の同意を取る運用がなされている．しかしながら，既に蓄積されている医療情報の多くは二次利用の同意を得ておらず，例えば，地域の医療情報連携基盤等に蓄積されている膨大なデータの二次利用を進めるにあたっては，改めて本人同意を取る必要が生じる．また，今後，二次利用にあたり，いかなる場合も同意を原則とした場合には，ある特定の疾病の情報のみが欠落したデータベースが構成される恐れがあるなど，疫学研究やサーベイランスが成り立たなくなることが想定され，結果として本来患者が享受すべき恩恵を十分に受けられない可能性がある．このため，今後は，個人が特定される可能性を低減する匿名化技術を利用するなど，一定のルールに従って医療情報を取り扱えるようにする（明示的な本人同意を必須としない）ことが望まれている．そこで以降では，プライバシー保護に有益な k-匿名性の概念を用いた医療情報の利用とその課題を紹介する．

個人情報を匿名化して利用する際に用いられる手法としては，k-匿名化という技術が知られている[6]．この技術は，個人を特定できる確率を $1/k$ にする匿名化するという概念に基づいていることから，k の値は匿名化レベルの指標として利用されている．具体的には，k-匿名化で匿名化された個人情報は，k を大きくすることにより個人が特定される危険性を小さくすることができることから，プライバシーはより安全に保護されると言える．他方，図2に示されるように，情報の有用性も低下すると言える．医療情報の二次利用では，医学的に重要な情報を保持しつつ，個人が特定できないレベルまでデータを適切に加工することが重要となることから，匿名化の指標となる k 値と k-匿名化の技術は有用と考えられている．ただし，匿名化レベルを k に加工したデータであっても，データが持つ属性情報に多様性が欠けている場合（l-diversity の問題）[7]や属性の分布が

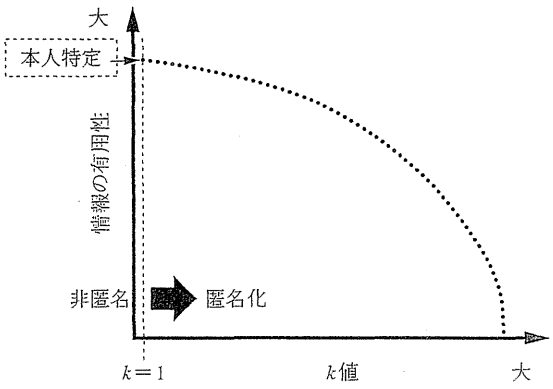

図2　匿名化レベルと情報有用性の関連性

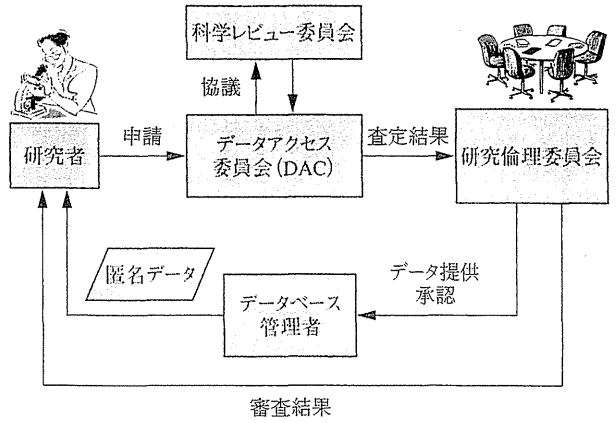

図3　CHEO による匿名化データ提供の流れ

偏っている場合（t-closeness の問題）[8]は，個人を特定できる確率が $1/k$ 以下であるとは保証できないことにも留意しなければならない．また，情報の収集は時間経過に伴ってダイナミックであるため，データが追加，変更，削除された後に匿名化されたデータを公開する場合や，同じ元データから異なる匿名化を施した別のデータを公開する場合に，以前の匿名化データと照合することで k-匿名性が崩れ，個人を特定できる場合が生じることにも留意しなければならない．そのため，医療現場で k-匿名化手法を用いる際には，データの利用状況を綿密に検討した上で，あり得る様々なぜい弱性を分析することが必要であり，このことは医療情報の二次利用を推進する観点から，極めて重要な課題であると言える．

次に，匿名化された医療情報を二次利用している参考実例として，カナダの The Children's Hospital of Eastern Ontario（CHEO）[9]の取組みを紹介する．CHEO は，カナダ・オンタリオ州オタワにある小児科の医療と研究を行う機構であり，オンタリオ州法により定められた，同州の新生児と産婦の健康状態などに関する情報を集めるプログラムである BORN（Better Outcomes Registry & Network）の公認レジストリとして認定されている．BORN には，新生児とその母親の出産前後の健康状態などに関する情報が蓄積されており，情報自体には識別情報（名前，医療保険番号など）は含まず，別体系の ID で管理されている．

CHEO は，患者情報を二次利用するため，高速かつ情報損失を最小に抑えるように工夫された k-匿名化手法の一つである Optimal Lattice Anonymization（最適格子構造匿名化）[10]を取り入れた PARAT（Privacy Analytic Re-identification Risk Assessment and De-identification Tool，プライバシー分析による再識別リスクの評価と非識別化を行うツール）[11]を用いて情報管理システムを構築しており，外部から情報提供の要請があれば，提供先を審査し，BORN からデータを匿名化して提供している．

具体的には，審査は図3に示すように3段階で行われる．まず，データを利用したい申請者が，CHEO に対して利用申請を提出する．申請を受理した CHEO 内のデータアクセス委員会（DAC）は，第一審査として，利用申請の内容について，研究の妥当性（実現可能性，科学的妥当性，要求データ項目の妥当性）を審査する．この際必要に応じて，科学レビュー委員会との協議を行う．第一審査を通ると，第二審査では，申請者の所属組織のセキュリティやプライバシーの保護状況や提供されるデータと取り扱われ方，想定される攻撃者の種類，匿名化のレベルを PARAT に入力し，プライバシーのリスクを定量的に評価する．ここで，リスク評価の結果が，設定されたしきい値内に収まれば，データの提供が行われるが，リスクがしきい値を超えた場合には，しきい値内に収まるまで，再度，匿名化レベルの選択が行われる．そして，第三審査では，最終的な意思決定を行う組織である研究倫理委員会が DAC から提出された第二審査の結果を用いて，提供リスクや倫理面の問題について審査を実施し，承認された場合には，申請者に対して匿名化データが提供されることになる．

また，データ利用者と CHEO 間はデータ利用に関する契約を交わし，CHEO は，その契約の範囲内でのみの利用を許可している．このことは言い換えると，CHEO は契約を前提としているため，k の値を大きくした匿名化データをいわゆるオープンデータとして提供していないということである．この事例は，実際に匿名された医療情報を二次利用する実例として興味深いものであり，我が国において医療情報の二次利用を進める際にも参考にすべきものと考える．

さて，医療情報の二次利用が進まない理由の一つには，個人情報漏えいに対する潜在的な不安もあると考えられる．このため，たとえ匿名化技術を利用した場合でも，情報保有機関である医療機関は，個人情報の漏えいを恐れるために上記の例で挙げた k 値を大きく設定し，それによって医療情報が元来有している有益な情報は失

われ，適切な情報解析が行えなくなる可能性も想定される．医療機関と医学研究機関の双方の立場に立つと，医療情報の有用性とプライバシー保護のバランスが取れた適切な医療情報利用の促進が望ましい姿であり，匿名化技術の改善のような技術的な方策だけでなく，制度や組織的な運用などを組み合わせ，皆が安心して医療情報の二次利用を推進できる仕組みを構築することが重要である．例えば，その一案として，CHEOの取組みのように，信頼される第三者機関が客観性を持って医学研究機関の安全性を評価し，その結果をもって，医療機関が研究の目的とデータ自体の取り扱われ方，データを分析・解析した成果の活用目的などを判断した上で，情報提供の可否の決定を行い，利用範囲等を契約により定める仕組みの構築が考えられる．しかしながら，二次利用本来の目的を達成する観点からは，この対応で十分かどうかは不明と言わざるを得ない．

4. ま　と　め

本稿では，医療情報利用における課題とその解決の方向性について述べた．医療・健康情報を本人や医療従事者等の関係者間で共有する仕組みの導入は，患者・医療機関等への直接的なメリットを与えるだけでなく，その利活用を通して，医療の質の向上，更には医療費の適正化にも寄与するものである．今後は，先に述べた医療等分野における番号制度の活用等に関する研究会などを通して，より議論が深まり，国民に分かりやすい制度が整備されるためにも，プライバシー保護を考慮した新たな技術開発が強く望まれる．

文　献

（1） パーソナルデータの利活用に関する制度改正大綱，http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20140624/siryou5.pdf
（2） 上野智明，ITを利用した全国地域医療連携の概況（2012年度版），日医総研ワーキングペーパー，http://www.jmari.med.or.jp/download/WP289.pdf
（3） 世界最先端IT国家創造宣言，http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20140624/siryou1.pdf
（4） 医療等分野における番号制度の活用等に関する研究会，http://www.mhlw.go.jp/stf/shingi/other-jyouhouseisaku.html/?tid=26
（5） 平良奈緒子，小尾高史，李　中淳，鈴木裕之，大山永昭，“生涯にわたる個人健康管理システムの実現，”日本がん検診・診断学会誌，vol. 21, no. 2, pp. 114-120, 2013.
（6） L. Sweeney, “k-anonymity : A model for protecting privacy,” Int. J. Uncertain. Fuzziness Knowl.-Based Syst., vol. 10, no. 5, pp. 557-570, 2002.
（7） A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, “l-diversity : Privacy beyond k-anonymity,” Proc. Int'l Conf. Data Eng. (ICDE), pp. 3-7, April 2006.
（8） N. Li, T. Li, and S. Venkatasubramanian, “t-Closeness : Privacy beyond k-anonymity and l-diversity,” Proc. Int'l Conf. Data Eng. (ICDE), pp. 106-115, 2007.
（9） The Children's Hospital of Eastern Ontario. http://www.cheo.on.ca/
（10） K. El Emam, F.K. Dankar, R. Issa, E. Jonker, D. Amyot, E. Cogo, J.P. Corriveau, M. Walker, S. Chowdhury, R. Vaillancourt, T. Roffey, and J. Bottomley, “A globally optimal k-anonymity method for the de-identification of health data,” J. Am. Med. Inform. Assoc., vol. 16, no. 5, pp. 670-682, 2009.
（11） De-identification Software, Privacy Analytics Inc.. http://www.privacyanalytics.ca/software/de-identification/

（平成26年9月30日受付　平成26年10月29日最終受付）

小尾　高史（正員）

平元東工大・理・物理卒，平6東工大大学院総合理工学研究科物理情報工学博士課程単位取得満期退学．博士（工学）．同年東工大像情報教務職員，平9同助手，平15東工大大学院総合理工学研究科助教授，平24東工大像情報准教授，現在に至る．医療情報，医用画像，社会情報システムに関する研究に従事．日本医用画像工学会奨励賞受賞．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．

鈴木　裕之（正員）

平10東工大・工・電気電子卒，平15東工大大学院総合理工学研究科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，日本光学会，レーザー学会，日本医療情報学会各会員．

李　中淳

昭61韓国延世大大学院物理卒．同年LG電子研究所入社．平7東工大大学院総合理工学研究科物理情報工学博士課程了．博士（工学）．韓国健康保険管理公団，日立コンピューター機器，インフィニトテクノロジ，NTTコミュニケーションズ，平20東工大像情報特任准教授，現在に至る．社会情報，医療情報セキュリティに関する研究に従事．

平良　奈緒子

平17国際医療福祉大・医療福祉・医療経営管理卒．平19国際医療福祉大大学院医療福祉学研究科修士課程了，修士（医療福祉経営）．同年（株）医療福祉総合研究所入社．平20東工大統合研究院ソリューション研究機構研究員，像情報工学研究所研究員，現在に至る．医療情報システムに関する研究に従事．日本医療病院管理学会，日本がん・健診診断学会各会員．

大山　永昭（正員）

昭52東工大・理・物理卒，昭57東工大大学院総合理工学研究科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各受賞．日本医学放射線学会，日本産業衛生技術学会，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．

一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

金融・決済分野における公的個人認証サービスの活用に関する考察

藤田 和重† 小尾 高史† 谷内田 益義† 李 中淳† 平良 奈緒子† 奥 信人†
庭野 栄一† 則武 智† 福田 賢一† 岩丸 良明† 大山 永昭†

†東京工業大学 〒226-8503 神奈川県横浜市緑区長津田町 4259
E-mail: †fujita@ssr.titech.ac.jp

あらまし 社会保障・税番号制度の導入に伴い，公的個人認証サービスにおいて，マイ・ポータルの利用等に活用できる「電子利用者証明」の仕組みが創設されるとともに，行政機関等に限定されていた検証者の範囲が拡大されて総務大臣が認定する民間事業者が追加されることとなった．これらを踏まえ，ID・パスワード方式よりも高いセキュリティレベルが要求されると考えられる金融・決済分野においてこれらの仕組みを活用するためのシステム構成を例示するとともに，関連する技術面・制度面での課題等について考察した．

キーワード 認証，電子署名，ネットワークセキュリティ，社会情報システム，ビジネス支援

A study on the possibility of utilizing the Public Certification Service for Individuals in the field of finance or credit settlement.

Kazushige FUJITA† Takashi OBI† Masuyoshi YACHIDA† Joong Sun LEE†
Naoko TAIRA† Makoto OKU† Eikazu NIWANO† Satoshi NORITAKE†
Kenichi FUKUDA† Yoshiaki IWAMARU† and Nagaaki OHYAMA†

† Tokyo Institute of Technology 4259 Nagatsuta-cho, Midori-ku, Yokohama, 226-8503 Japan
E-mail: †fujita@ssr.titech.ac.jp

Abstract With the introduction of the Social Security and Tax Number System, electronic authentication function, which is required to login to the My Portal that helps people to confirm the access records for their personal information associated with the Numbers, is added to the Public Certification Service for Individuals, and the function can be used by not only administrative bodies but private companies which are authorized by the Minister of Internal Affairs and Communications. Taking into account this situation, we presented the possible system architecture for the use of this new function in the field of finance or credit settlement, which is thought to require higher security level than other fields using ID and password, and studied some related subjects on the technical and regulatory aspects.

Keyword Authentication, Digital signature, Network security, Social information system, Business support

1. はじめに

社会保障・税番号制度の導入[1][2]に伴い，平成 27 年 10 月から国民に対する個人番号の通知が開始されるとともに，平成 28 年 1 月から個人番号カードの交付が開始される予定となっている．

同制度の導入に関連し，e-Tax 等のオンライン申請の安全性確保のために利用されている「公的個人認証サービス（JPKI）」について，従来の「電子署名」の機能に加えて，国民が自己の個人番号に係る個人情報が行政機関等においてやりとりされた記録を自宅のパソコン等から確認できる仕組みである情報提供等記録開示システム（マイ・ポータル）への安全なログイン手段として「電子利用者証明」の機能が追加される．また，従来は「電子署名」の検証は行政機関等に限定されていたが，今後は「電子署名」及び「電子利用者証明」の検証は，総務大臣が認定する民間事業者も可能となる．そして，JPKI の機能は現在，住民基本台帳カードに（国民の選択に基づき）搭載されているが，上述の新しい JPKI の機能は平成 28 年 1 月以降，個人番号カードに標準搭載される．

今回新たに導入される「電子利用者証明」の機能は，マイ・ポータルへのログイン手段としての利用だけでなく，民間における金融・決済分野や保健医療分野など ID・パスワード方式よりも高いセキュリティレベルが要求される各種サービスへのアクセス手段としての応用も期待される．

我々は以前にそのような応用を具体的に実現する方策について検討し報告[3][4]している．本論文では，

This article is a technical report without peer review, and its polished and/or extended version may be published elsewhere.
Copyright ©2014 by IEICE

それらの検討をさらに進め，特に金融・決済分野において「電子利用者証明」の機能を活用するための具体的なシステム構成や，関連する技術面・制度面での課題等について考察したので，その結果を一案として提示する．

2. 金融・決済分野における公的個人認証サービスの活用

2.1. 金融・決済分野での活用の概要

我々が以前に報告[3]したとおり，民間等のサービス提供者（金融・決済分野の場合はクレジットカード会社や金融機関等）は，利用者の個人番号カードに記録される利用者証明用証明書の発行の番号（利用者証明用シリアル番号）と，各種サービスの顧客情報（クレジットカード番号や口座番号）等とをあらかじめ紐付けて管理しておくことにより，個人番号カードをクレジットカードやデビットカード，キャッシュカード等の代替として利用可能とすることが期待できる．

JPKIの活用にあたり，サービス提供者は，主に次の機能を新たに構築する必要がある．

①店舗窓口等において個人番号カードからJPKIに関連する情報の読取を可能とする機能（JPKI情報読取機能）

②利用者証明用シリアル番号と各種サービスの顧客情報とを紐付けして管理する機能（紐付管理機能）

③JPKIの電子証明書の有効性を確認するとともに電子署名及び電子利用者証明の検証を行う機能（JPKIインタフェース機能）

特に②の紐付管理機能に関し，初期の紐付け作業の具体的手法については，我々が以前に報告[3]したとおり，あらかじめ利用者がサービス提供者に対し，電子署名を付して，JPKIを活用したサービスの提供開始を申し込む方法が効果的である．署名検証者は，利用者から受け取った署名用証明書の発行の番号（署名用シリアル番号）を基に，JPKIの運営主体である地方公共団体情報システム機構から，当該利用者に係る利用者証明用シリアル番号の提供を受けることができる（改正公的個人認証法第18条第3項）ので，申込書に記載された顧客情報等と照合することにより，両シリアル番号と顧客情報の紐付けを行うことができる．

これらの機能を個々のサービス提供者がそれぞれ個別に用意することが非効率であるような場合，それらを複数のサービス提供者で共有するための「共通的プラットフォーム（共通的PF）」を構築するケースも想定される．

以上の前提を踏まえたJPKIの活用における基本システム構成を図1に示す．

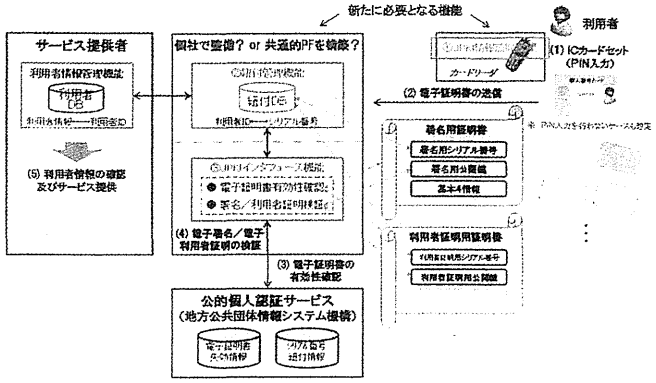

図1　JPKIの活用における基本システム構成

2.2以降では，この基本システム構成をベースとして，金融・決済分野におけるJPKIの活用を実現する場合の業務フローを示す．業務フローの記述には，その手法の国際標準であるBPMN（Business Process Model and Notation）[5]を使用した．なお，それらの業務フローは，基本的な仕組みをできるだけシンプルに可視化する観点から粗めの粒度で記述しているが，具体的なシステム実装の検討においては更なる詳細化が必要である．

2.2. クレジットカード機能の実現可能性

個人番号カードでクレジットカード機能を実現する場合の業務フローの一例を図2に示す．

クレジットカード加盟店に設置されているカード決済端末とクレジットカード会社の間は，専用の中継サービス（㈱NTTデータが提供する「CAFIS（Credit And Finance Information System）」[6]など）を介して接続されている．

JPKIの活用にあたり，まず，「JPKI情報読取機能」を各加盟店のカード決済端末に付加する必要がある．次に，「紐付管理機能」及び「JPKIインタフェース機能」については，この中継サービスを共通的PFと位置付け，そこに構築することが一案として考えられる．このようなシステム構成とすることにより，中継サービス側で利用者の利用者証明用シリアル番号とクレジットカード番号の変換が行われるので，個々のクレジットカード会社側では大きなシステム改修を行うことなくJPKIへの対応が可能となる．

2.3. デビットカード機能の実現可能性

個人番号カードでデビットカード機能を実現する場合の業務フローの一例を図3に示す．

2.1で述べた各機能構築の考え方は，2.2で示したクレジットカードの場合とほぼ同様である．