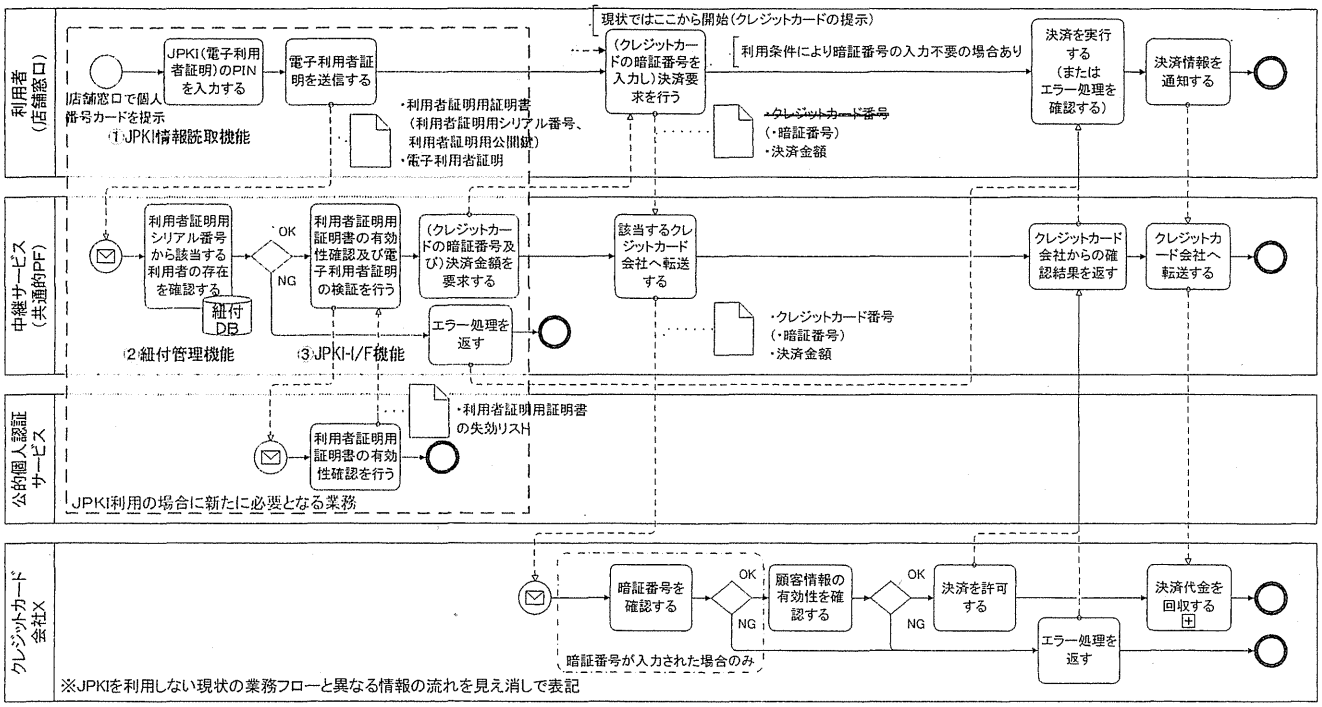


図 2　クレジットカード機能の実現の一例

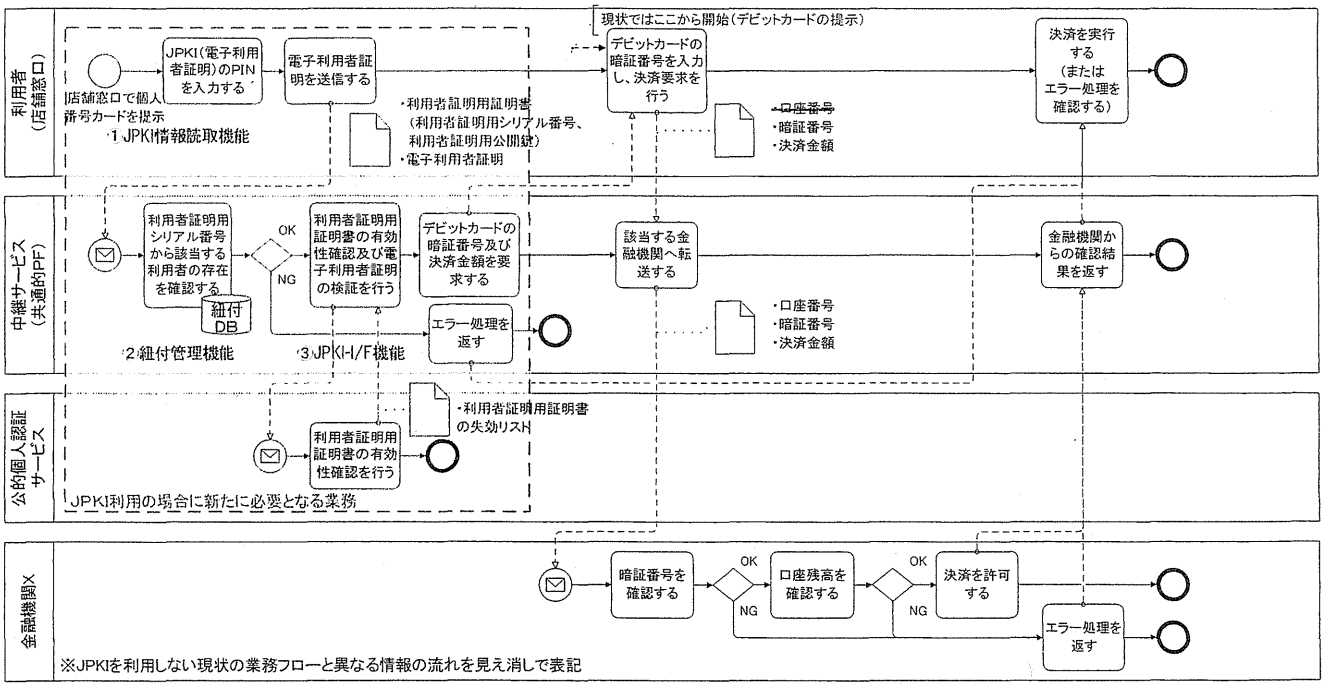


図 3　デビットカード機能の実現の一例

2.4. キャッシュカード機能の実現可能性

個人番号カードでキャッシュカード機能（ATM における現金引き出し）を実現する場合の業務フローの一例を図 4 に示す.

各金融機関の ATM は，専用の中継サービス（㈱NTT データが提供する「統合 ATM スイッチングサービス」[7]など）により相互接続されている.

JPKI の活用にあたり，まず，「JPKI 情報読取機能」を各金融機関の ATM 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」であるが，クレジットカードやデビットカードの場合と異なり，個々の ATM は一度自行のオンラインシステムに接続された後，中継サービスを介して他行に接続されるネットワーク構成となっているので，当該 2 つの機能をどのように構築するかについては，いくつかのバリエーションがあり得るものと考えられる.

図 4 では，現状のネットワーク構成を前提として，まず，金融機関が自行の ATM から送信されてきた利用者証明用シリアル番号をもとに ATM 利用者が自行の利用者かどうかを確認し，自行の利用者の場合には必要な確認を行った上で希望金額の引き出しを許可し，自行の利用者でない場合には中継サービスへ転送し，中継サービスにおいて利用者証明用シリアル番号をもとに該当する金融機関を判断して転送し，該当金融機関において必要な確認を行った上で希望金額の引き出しを許可する，という業務フローとしている．すなわち，「紐付管理機能」は各金融機関と中継サービスの双方が構築し，「JPKI インタフェース機能」は各金融機関が構築するという構成になっている．

このほかにも，例えば，サービス提供の初期段階などにおいては，自行の利用者にのみ JPKI を使ったサービスを提供し，他行の利用者には対応しない方法（この場合には中継サービス側のシステム改修は不要）や，サービスが十分に普及した段階などにおいては，JPKI を使ったトランザクションについては一旦全て中継サービスまたはその他の外部機関へ転送し，「紐付管理機能」及び「JPKI インタフェース機能」をそちら側に集約するといった方法なども想定され得ると考えられる．

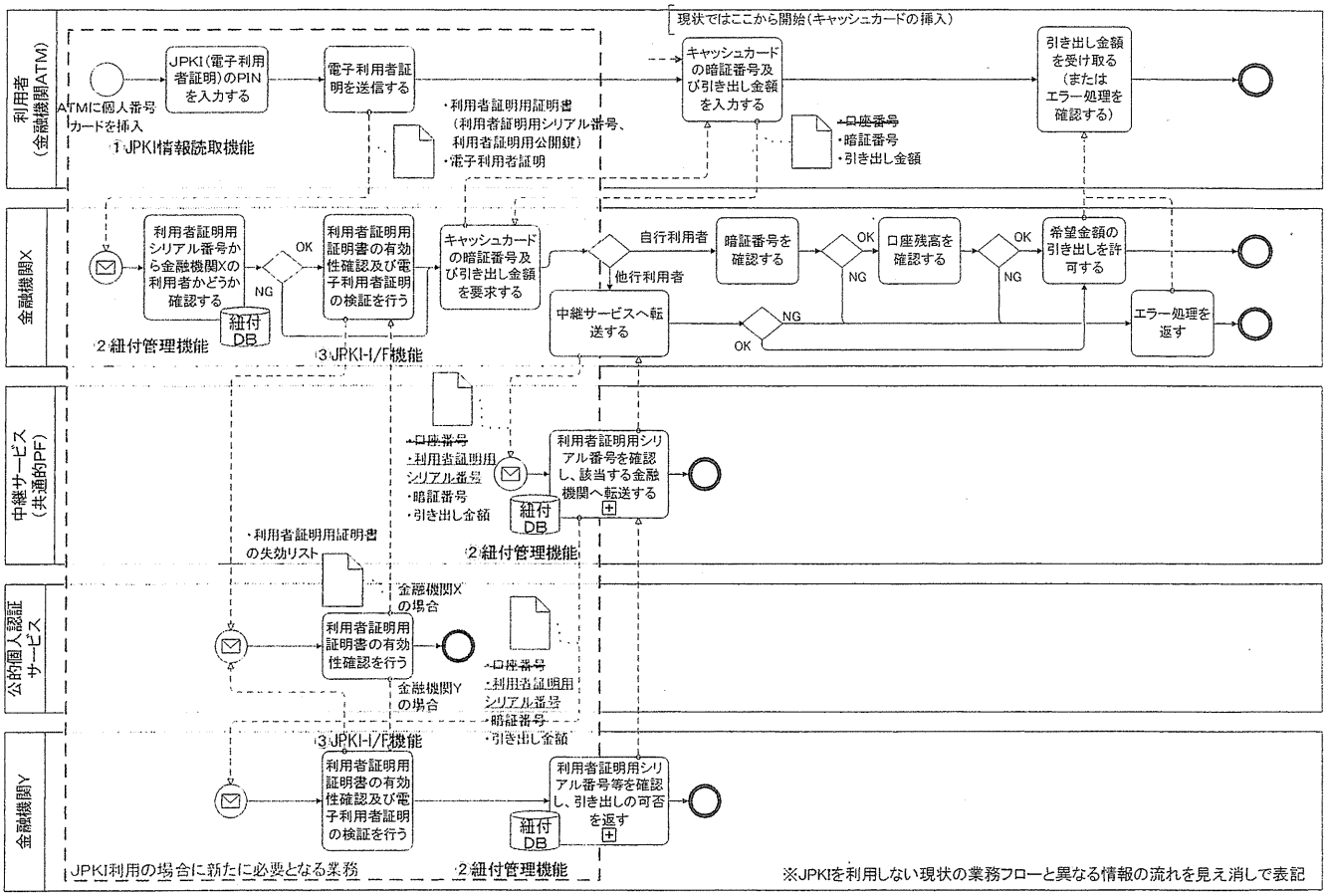


図 4　キャッシュカード機能の実現の一例

2.5. 留意事項

クレジットカード，デビットカード，キャッシュカードの各機能の実現にあたり，共通する事項として次の点に留意する必要があると考えられる．

「紐付管理機能」に関して，利用者証明用シリアル番号との紐付けを行う「顧客情報」の範囲についてさらに検討する必要がある．図 2 または図 3 を例に考えた場合，中継サービス側に構築する「紐付管理機能」において，クレジットカード番号や口座番号そのものをデータベース化して管理することに関し，サービス提供者の顧客情報管理ポリシー等の観点で問題がないかどうかに留意する必要がある．もし何らかの問題がある場合には，例えば，利用者証明用シリアル番号とクレジットカード番号または口座番号そのもののデータベースはサービス提供者側で管理することとし，中継サービス側では情報の転送先の特定のために最低限必要な情報（サービス提供者の識別番号等）のみを紐付けて管理するといった方法をとることなども考えられる．また，図 2，図 3，図 4 はいずれも，1 つの利用者証明用シリアル番号に紐付けられる顧客情報（クレジットカード番号または口座番号）は 1 つであることを前提としている．もし，複数のカードの情報が紐付

けられる場合は，中継サービス側，あるいは，各加盟店のカード決済端末または各金融機関の ATM において，利用者がどのカードの利用を希望しているのか，選択させるための機能の提供も必要となる．

JPKI の PIN（Personal Identification Number）や，クレジットカードまたはキャッシュカードの暗証番号の入力に関しても，利用者の利便性と必要なセキュリティ確保の両面からさらに検討する必要がある．新しい JPKI の電子利用者証明においては，カードを活性化させるための PIN 入力を必要としない手法も検討されている[8]．また，クレジットカードの場合，利用条件によっては暗証番号の入力が不要なケースもある一方，デビットカードやキャッシュカードの場合は，暗証番号の入力は必須となっている．こうした状況を踏まえ，JPKI の PIN，あるいはクレジットカードの暗証番号を省略することの是非についてさらなる検討が必要である．なお，我々が以前に提案した JPKI の PIN 入力を不要とする仕組み [4][9]においては，サービス提供者側において，当該サービス提供者が JPKI の発行機関によってあらかじめ認められた機関であることを確認するための機能を構築する必要がある．このように，JPKI の PIN 入力を不要とする際には何らかの代替の機能が追加で必要となることに留意が必要である．また，その機能を，個々のサービス提供者または中継サービスのいずれが構築するのかについても検討が必要である．

3. 署名検証者及び利用者証明検証者の制度的位置付け

3.1. 検証者に関する制度の概要

冒頭にも述べたとおり，新しい JPKI においては，今後，政令で定める基準に基づいて総務大臣が認定する民間事業者が署名検証者及び利用者証明検証者となることができる（改正公的個人認証法第 17 条及び第 36 条）．また，他に提供されることを予定して署名用シリアル番号や利用者証明用シリアル番号が記録されたデータベースを構成することは法律上禁じられているが，これら検証者は例外とされており（改正公的個人認証法第 63 条），2.1 で述べた「紐付管理機能」等の構築が許されている．

他方，検証者は，上述の総務大臣による認定の基準を満たす必要があるほか，電子証明書に記録された公開鍵の目的外利用の禁止，電子証明書の失効情報の安全確保及び目的外利用の禁止などに加え，電子証明書の失効情報提供の対価の負担が求められる．

2.で説明した基本システム構成及び業務フローを基に，サービス提供者や中継サービス（共通的 PF）がこうした制度上どのように位置付けられるのかについて，以下に考察する．

3.2. 想定される検証者の制度的位置付け

例えば，図 2 及び図 3 の業務フローにおいて，「紐付管理機能」及び「JPKI インタフェース機能」は共通的 PF に置かれ，サービス提供者側にはこのような機能はないことから，一見，共通的 PF が検証者であるようにも考えられるが，ここで，各利用者の利用者証明用シリアル番号とカード番号とを確実に紐付けする責任を最終的に負うのは誰なのか，また，利用者証明用証明書の有効性確認及び電子利用者証明の検証の結果を最終的に利用するのは誰なのか，という点に着目する必要がある．

これらがいずれも個々のサービス提供者である場合には，あくまでサービス提供者が検証行為の主体であって，その業務を共通的 PF に「委託」していると解するのが自然であり，この場合は，個々のサービス提供者と共通的 PF（が有する「紐付管理機能」及び「JPKI インタフェース機能」）がセットで検証者としての認定を受けることになるものと想定される．

一方で，サービス提供者と共通的 PF との間の契約関係において，サービス提供者の検証行為を共通的 PF が「代行」する，すなわち，共通的 PF 側が上述の紐付けの最終的な責任を負うとともに，電子証明書の有効性確認や電子利用者証明の検証結果を最終的に利用（サービス提供者はあくまで間接的に利用）しているとの整理ができる場合には，共通的 PF だけが検証者としての認定を受けるという解釈もあり得るものと想定される．技術的にも，例えば，共通的 PF が利用者証明用シリアル番号と一対一で対応する別の ID を発番することで，サービス提供者との全ての情報のやりとりを当該 ID を介して行う（すなわち，サービス提供者は利用者証明用シリアル番号に一切触れない）というような運用形態も実現可能と考えられる．但し，「代行」の場合には，サービス提供者は検証行為の主体ではなく，一般的なシングルサインオンにおける ID 連携のように，あくまで契約関係によって JPKI の認証結果を利用しているだけであることから，自らが検証者となる場合と比較して，認証のセキュリティレベルは必然的に下がるという点に留意が必要である．また，2.1 で述べた初期の紐付け作業に関し，サービス提供者は，検証者ではないので，電子署名の検証や，両シリアル番号が記録されたデータベースの構成ができないことから，利用者からの申し込みを受けた後，顧客情報等の個人データを検証者たる共通的 PF に渡し，共通的 PF の責任で紐付けの作業を実施してもらうこととなる．個人情報保護法では，個人情報取扱事業者に対し，個人情報の利用目的を本人に通知することや，

個人データの第三者提供に際してあらかじめ本人同意を得ることなどを義務付けている．後者に関しては，個人データの取扱いを委託する場合は適用除外となっているが，ここで述べている「代行」の場合には，この規定を踏まえ，サービス提供者として適切な形で利用者の事前同意を得ることが必要になるものと想定される．

4. 今後の検討課題

金融・決済分野におけるいくつかの具体的なユースケースにおいて，JPKIの電子利用者証明の仕組みが技術的に活用可能であることを説明してきたが，今後の実サービスに繋げていくためには，個別のユースケースごとに，適切なシステム構成や，具体的な費用対効果について更に詳しく検討することが必要である．

また，単に個人番号カードがクレジットカードやキャッシュカードの機能を代替するだけでは，利用者にとってのメリットは必ずしも十分とは言えず，例えば，医療保険資格のリアルタイム確認の機能なども相乗りさせることで，医療機関における受付から支払い，さらには薬局での薬の受け取りまでが個人番号カードだけで済むというように，1枚のカードに複数の機能が集約されること（ワンカード化）によって，利用者側の利便性が飛躍的に向上することが期待される．そのためには，業種を越えた様々な関係者の理解増進や連携促進のための環境づくりも重要である．

このほか，本論文では触れなかったが，JPKIの民間活用に関して，「変更確認」のユースケースも有効と考えられている．これは，JPKIの署名用証明書に基本4情報（氏名・住所・生年月日・性別）が記録されており，これらのいずれかが変更された場合に証明書が失効することを利用し，証明書の失効をトリガーとして，利用者に住所変更等の手続を促すというものである．利用者が引越をした場合の住所変更の届出が必ずしも十分に行われていないような業種における活用が期待されており，金融・決済分野における活用可能性についても，あわせて検討していくことが有効と考えられる．

5. おわりに

本論文では，社会保障・税番号制度の下で導入される新たな公的個人認証サービスの金融・決済分野での活用について検討した．新たな公的個人認証サービスは，金融・決済分野での利用にとどまらず，保健医療分野など他の民間分野での利用も期待されており，今後は安全性やプライバシーに配慮しつつ，更なるユースケースの検討や，実際のサービス導入に際した費用対効果等の検証等を行っていくことが必要である．

文　献

[1] 行政手続における特定の個人を識別するための番号の利用等に関する法律，http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/260717bangouhou.pdf

[2] 行政手続における特定の個人を識別するための番号の利用等に関する法律の施行に伴う関係法律の整備等に関する法律，http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/seibihou.pdf

[3] 藤田和重，小尾高史，御代川知加大，谷内田益義，李中淳，夏目哲也，平良奈緒子，庭野栄一，熊倉誠，岩丸良明，大山永昭，“公的個人認証サービスを用いた官民連携の可能性について”，信学技報，vol.113,no.381,pp.29-34,Jan.2014

[4] 小尾高史，藤田和重，大山永昭，“新たな公的個人認証サービスとその医療分野での利用に関する検討”，2014年暗号と情報セキュリティシンポジウム（SCIS2014），SCIS2014論文集，4B1-3，Jan. 2014.

[5] Information technology — Object Management Group Business Process Model and Notation, ISO/IEC 19510, Jul.2013

[6] CAFIS (Credit And Finance Information System), http://www.nttdata.com/jp/ja/lineup/cafis/

[7] 統合ATMスイッチングサービス，http://www.nttdata.com/jp/ja/lineup/integration_atm_switching/index.html

[8] ICT街づくり推進会議 共通ID利活用サブワーキンググループ（第2回）議事要旨（総務省），http://www.soumu.go.jp/main_content/000287016.pdf

[9] 小尾高史，本間祐次，大山永昭，“公的ICカードを利用した医療機関からの保険資格確認方法の検討”，コンピュータセキュリティシンポジウム2010，2F22-1，2010年10月

MEDINFO 2015: eHealth-enabled Health
I.N. Sarkar et al. (Eds.)

doi:10.3233/978-1-61499-564-7-933

Development of Clinical Database System Specialized for Heavy Particle Therapy

Masami Mukai[a], Yutaka Ando[b], Yuki Yokooka[a], Yasuo Okuda[a], Masayoshi Seki[c], Masahiro Kimura[d], Hiroshi Tsuji[b], Tadashi Kamada[b]

[a] Medical Informatics Section, National Institute of Radiological Sciences (NIRS), Chiba, Japan
[b] Research Center for Charged Particle Therapy, NIRS, Chiba, Japan
[c] Global-for Co., Tokyo, Japan, [d] Fujitsu Systems East Limited, Saitama, Japan

Abstract

We have developed a data archiving system for study of charged particle therapy. We required a data-relation mechanism between electronic medical record system (EMR) and database system, because it needs to ensure the information consistency. This paper presents the investigation results of these techniques. The standards in the medical informatics field that we focus on are Integrating the Healthcare Enterprise (IHE) and 2) Health Level-7 (HL7) to archive the data. As a main cooperation function, we adapt 2 integration profiles of IHE as follows, 1) Patient Administration Management (PAM) Profile of IHE-ITI domain for patient demographic information reconciliation, 2) Enterprise Schedule Integration(ESI) profile of IHE-Radiation Oncology domain for order management between EMR and treatment management system(TMS). We also use HL7 Ver2.5 messages for exchanging the follow-up data and result of laboratory test. In the future, by implementation of this system cooperation, we will be able to ensure interoperability in the event of the EMR update.

Keywords:

Radiotherapy, Database, Strandards, IHE, HL7.

Introduction/Purpose

Our hospital has a mission of clinical research for radiotherapy. Charged particle therapy (carbon ion) was started in 1994, and over 9,500 cases have been treated by November, 2014. To accomplish this mission, we managed multi-system such as electronic medical record systems (EMR) and charged particle therapy treatment management system (TMS).

In 2000, we started to operate the Advanced Medical Information Database System (AMIDAS) for archiving the radiotherapy information. With the starting of EMR, we allocated a role to information systems as follows, EMR: input data related radiotherapy, AMIDAS: make report and summary of radiotherapy. So the AMIDAS is required to construct a mechanism to collect the data which is input by end-user on EMR.

Methods

The data targeted for the cooperation are following: (1) patient demographic information, (2) tumor related information, (3) radiation plan information, (4) follow-up information (tumor effect, advance reaction, mortality, etc.), (5) laboratory results, (6) treatment delivery information. We divided the implementation process into two stages and examined it as two steps: (1) investigated the availability of IHE [1]. (2) investigated the use of HL7 messages.

Results

This cooperation function was realized by two IHE integration profiles as follows, (1) Patient demographics and visit information: PAM Integration Profile, (2) Radiotherapy order and delivery information: ESI Integration Profile. For communication of treatment follow-up information and laboratory test we defined context and used HL7 messages.

Discussion

We show the comparison results using standard with original sysytem-interface in Table 1.

Table 1– The Comparison of Standard with original messages

Comparisonpoint	Standard-IHE	Standard-HL7	Orignal interface
Meeting number of times	little	few	much
The use of the library	possible	possible	impossible
Time to make specifications	short	middle	long

Conclusion

In comparison with original message system interface, it may be said that the system which was developed using a standardization technology has interoperability. From the standpoint of system-operation by using standards, when we will renew the EMR, AMIDAS can receive the data from EMR without software modification.

References

[1] IHE(Integrating the Healthcare Enterprise) http://www.ihe.net/Technical_Frameworks/

Address for correspondence

MUKAI Masami E-mail:m_mukai@nirs.go.jp

潮流

「マイナンバー制度と医療保険の資格確認」

東京工業大学
像情報工学研究所
教授
大山　永昭

1．はじめに

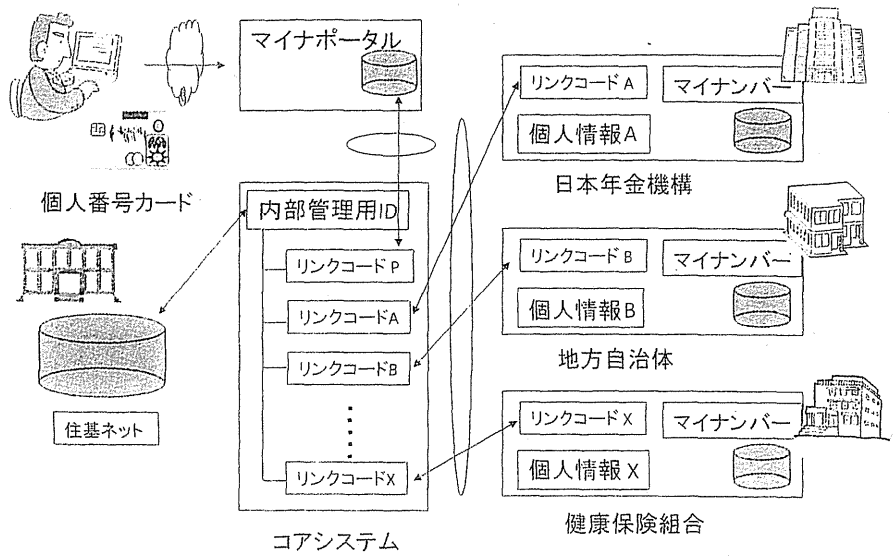
平成28年1月、いよいよマイナンバー制度が実施される。よく知られているように、本法の施行目的は、社会保障制度のきめ細やかかつ的確な実施、行政業務の正確性および効率の向上、国民の利便性向上等とされている。本制度については、すでに多数の解説記事等があることから、ここではマイナンバーの利用範囲と個人情報保護について述べ、次に制度実施に伴う変化について解説する。そして、医療保険業務への影響に触れ、最後に医療保険の資格確認と更なる展開について紹介する。

2．マイナンバー法の概要

マイナンバー法に先立って策定された「社会保障・税番号大綱」では、個人番号の利用範囲をA：税、B-1：税＋社会保障分野での現金給付、B-2：B-1＋社会保障分野の現物給付、C：民間利用の4つに分類し、社会の受容性や導入効果等を勘案した方向性が示されている。ここで、現物給付は医療等分野で提供されるサービスに伴う一連の情報で、カルテや処方箋、投薬情報等のいわゆる医療情報が具体例として挙げられる。これらの情報は、一般的に極めて高い機微性を有するため、現物給付に関する個人情報の管理にはマイナンバーを用いないとし、別途、医療等IDを用いることとしている。さらに、Cは平成30年を目途として別途検討するとしている。医療保険に関する事務は、基本的に医療費等の決済に関することであるから、上記の分類ではB-1に入る。

マイナンバー法の策定作業では、当初から個人情報保護に十分配慮することが念頭に置かれていた。そのため、前述の大綱に先立って、マイナンバーが導入されることに起因する個人情報保護に対する脅威が分析され、その抑止に有効な技術的及び制度的な対策が検討された。技術

図1　情報提供ネットワークシステムの概念図
コアシステムには、個人別のリンクコード連携テーブルを例示している



内部犯罪防止を図っている。また、制度的な対策としては、マイナンバーが付いた個人情報を特定個人情報と定義し、第三者委員会を設置するとともに、情報漏えいに対する直接罰の導入があげられる。したがって、特定個人情報の保護は、既存の個人情報保護法に比して、制度的にも強化されていると言える。

3．制度の実施に伴う変化

マイナンバー法の施行に伴い、我々の生活に直接関係する主な変化として、①番号の導入、②添付書類の削減、③マイナポータルの実現、④マイナンバーカードの配布の4つを取り上げ、それぞれの概要を紹介する。

①は個人及び法人向けの固有番号の導入を意味している。法人番号は、法務省の商業登記番号を基本として、国税庁が発番するものである。他方、個人番号は乱数を用いて、外国人を含む全ての住民（住民基本台帳に登録されている）に対して新たに付番するものであり、番号通知カードとして、本年10月から世帯単位に簡易書留で郵送される予定である。この番号通知カードは紙製になることから、紙幣等で用いられている偽変造防止技術が施される。そして源泉徴収業務等では、顔写真付きの公的証明書と組み合わせて本人確認を行い、正しい個人番号を取得することが規定されている。このことから、現在の税や社会保障に関する各制度の確実かつ効率的な運用が実現されると期待されている。

②は、マイナンバー法の別表第一に記載されている情報保有機関（自治体、日本年金機構等）をＫＷＡＮ（霞が関 Wide Area Network）やＬＧＷＡＮ（Local Government WAN）等を用いてネットワーク化し、別表第二に記されている120の法定業務に必要な情報提供を可能とすることにより実現するものである。提供されるこれらの情報は、年収や年金種別等の個人情報であるため、ネットワーク化に起因する情報漏えい等の脅威を抑えることが必須である。そのため、情報提供の正当性を全数チェックするコアシステムを新たに構築し、不当な個人情報の取得を技術的にもできない仕掛けとしている。さらに、提供される個人情報については、その全ての履歴（日時、機関名、

的対策の代表例は、図1に示されるコアシステム等で用いるリンクコードであり、これにより、情報漏えいの影響を局所化することを可能にするとともに、コアシステムを運用する職員等の

業務名、情報種別等）と提供される情報そのものを、本人が確認できるようになる。これらのことから、別表第二の法定業務における添付書類が削減され、国民の利便性が向上するとともに、個人情報のコントロール権の一部が実現されると期待される。

③は、前述の情報提供に関する本人の情報実体と提供履歴を確認するために構築されるものであり、既存のウェブサービスでの個人アカウントに相当する。このアカウントを介して確認できる個人情報等には、機微性の高いものが含まれるため、安全確実なアクセスに有効なマイナンバーカードの利用が想定されている。

④は、現在の住基カードに代わって平成28年1月から希望者に発行されるICカードであり、その役割は、裏面にマイナンバーが記載された顔写真付きの公的身分証明書である。そのため、源泉徴収業務等でのマイナンバーの取得には、マイナンバーカードのみで行うことが可能になる。もちろん、このカードには券面およびICチップに記録される情報の偽変造対策が施される。さらに、現在e-TAX等で用いられている電子署名に加えて、安全確実なログイン等を可能とする利用者証明が付加される。これら2つの機能は、JPKI（Japan Public Key Infrastructureの略）サービス〔1〕と呼ばれ、改正された公的個人認証法（平成28年1月施行予定）に依拠している。このことからわかるように、JPKIはマイナンバーとは全く別であり、JPKIは総務大臣の認定を得た民間事業者での利用が可能であるのに対して、マイナンバーは法定された業務以外での利用は禁止されている点に、留意することが必要である。

4. 医療保険業務への影響

既に知られているように、マイナンバー法の実施に伴い、医療保険組合は被保険者全員のマイナンバーを取得することが必要になる。これにより、例えば被扶養者認定に必要となる所得証明書の提出が不要となり、マイナンバー法の制定目的の一つである国民の利便性向上等に資すると期待されている。具体的には、生計を同一とする家族全員のマイナンバーを用いて、リンクコードの発番を依頼することにより、マイナンバーを提供した者の被保険者の情報提供が実現される。その結果、必要となる各人の年収を、情報提供ネットワーク経由で居住自治体から受け取ることが可能になる。具体的には、各自治体が記録・管理する年収等の個人情報は、中間サーバーと呼ばれる機器に副本として記録され、コアシステムの許可により個人情報のやり取りが行われる。そして自治体向けの中間サーバーは、費用対効果の観点から東西2か所のクラウドサービスとして構築される。同様の観点から、各保険組合向けの中間サーバーは、審査支払基金に集約される予定である。

マイナンバーの利用範囲は、法に記載されている業務に限定されるため、既にマイナンバー法の改正案が国会に提出されている。追加される予定の利用シーンは、特定健診情報の管理および予防接種履歴の情報提供等である。さらに、本年6月30日に閣議決定された日本再興戦略の改訂版には、医療保険のオンライン資格確認を平成29年度の7月以降早期に実現する旨が述べられている。そこで次節では、想定されている個人番号カードを用いた実施例を紹介す

る。

5. 医療保険の資格確認と更なる展開

平成29年度からの実施が予定されているオンライン資格確認は、平成26年度に総務省により実施された実証実験〔2〕が基になっている。紙面の関係で詳しく説明することはできないが、その基本原理は以下の通りである。すなわち、平成28年1月から発行される個人番号カードには、前述したように2組のPKI（電子署名と利用者証明）が標準で実装される。健康保険のオンライン資格確認は、このPKIを用いて行うもので、具体的には利用者証明書のシリアル番号と医療保険の記号・番号等をサーバー上で紐づけることにより実現される。現実の資格確認は、番号カードのICチップ内のコンピュータとサーバーが相互認証を行った後に、利用者証明書のシリアルナンバーから被保険者を特定し、必要な保険情報を返信することにより実施される。ここで、カードとカード保持者の一致は、一般的にはPIN（Personal Identification Numberで、チップ内に記録された4桁のパスワード）を入力して行われるが、医療機関等での混雑を避ける等の要望に応えるために、PIN入力を省略することも可能になっている。総務省の実証実験では、国民健康保険を対象として、大分県別府市および山形県酒田市の医療機関において、番号カードの模擬版を用いて東京のサーバーに記録した保険資格情報をオンラインで取得した。さらにこの実証実験では、クレジットによる支払いも試みられ、同じような手法で実現できることを実験的に確認している。これらのことから、番号カードに医療保険証とクレジットカードの機能を紐付ければ、一枚のカードで医療サービスを受けることが可能になると思われる。

わが国の医療保険制度は、国民皆保険になっていることから、本質的には、何時、誰が、どこの医療サービスを受けたかを電子的に記録することで、医療保険業務の手間、医療費の未収金やレセプトの返戻の削減等を実現することが望まれる。番号カードは、現実および電子空間での身分証明書であることから、上記要求の〝誰が〟に関する正確な情報を提供することが可能になる。さらに、PKIによる資格確認であることから、カードとの相互認証プロセスはエビデンスとしての証明力を有すると期待される。このことからも、生涯に渡る健康管理等に不可欠となる個人情報の紐づけに、JPKIの利用は極めて有効と言える。

6. おわりに

わが国が世界に誇る国民皆保険制度は、少子高齢化等に起因する財源不足等の問題から、持続的な安定運用が困難になっている。このような状況での番号制度の導入は、社会的な課題解決に大いに資すると期待されている。今後は、具体的なユースケースを明確にするとともに、社会保障・税分野における現制度の着実かつ効率的な実施を図ることが重要である。

参考文献等

1. 地方公共団体情報システム機構のホームページ参照：https://www.j-lis.go.jp
2. 総務省「ICT街づくり推進会議」第9次回会合、配布資料9-1参照：http://www.soumu.go.jp/main_sosiki/kenkyu/ict-town/02tsushin01_03000305.html

識者コメント

ハード・ソフト・データの市場性こそ大事

東京工業大学教授
大山　永昭氏

コンピューターを使う自治体から見れば、安全かつ確実、しかも廉価というのは当然の要求だ。今の時代、自治体がICT（情報通信技術）をまったく使わないで住民サービスをすることはあり得ない。安全対策に加え、専門知識を持つ人材不足の問題が重なって、外部資源活用のニーズが高まってくる。

先進的にクラウドに取り組んだ自治体の多くは、システム経費を下げなければならない、やむにやまれぬ財政事情が強力に作用した。実際、取り組んでみるとコスト削減の点で大きな効果があった。大規模自治体でクラウド化が進んでいないことは、財政状況の違いが大きな要因なのだろうか。

ベンダーロックインに代表される競争性の欠如は、クラウド化した後も起こり得る。競争性の維持によるコスト削減のポイントは２つある。１つは新システムに行政の住民情報を移す際の移植性の確保だ。これは北九州市の事例が参考になる。同市はデータ移行時に、新旧それぞれのシステムのベンダーの間にデータ移植を専門とする第３のベンダーを入れて、役割分担と責任分解点を明確化した。

今後、始まる国の番号制にも関連する重要な点がある。それは自治体の持つ住民情報を原本とすると、国が東西に設置する２つの中間サーバーに副本として同じ情報をアップロードすることである。番号制度の対象情報は、中間サーバーから副本を読み出せるので、自治体はシステムを更新しやすくなる。

２つ目は業務フローの可視化だ。競争的な市場を作るには、新規のベンダーが自治体の仕事の流れを容易かつ確実に理解できることが重要であり、そのためには業務フローの可視化が極めて有効である。ISO19510として国際標準化されているBPMN（ビジネス・プロセス・モデル・アンド・ノーテーション）はシステムに詳しくない人でも容易に理解でき、作成支援ツールも多い。さらに、自身の業務になるべく合ったパッケージを選ぶのにも役立つ。クラウド化はあくまで通過点。自治体にとってハード（＝オープン化）、ソフト（＝業務フローの可視化）、データ（＝移植性の確保）の３つにおいて市場競争性を確保することが、コスト削減に必要不可欠だ。自治体の担当者は中長期にわたったシナリオを練る必要がある。

大規模自治体、PaaS型が主流に

富士通　東京支社第二営業部長
野坂　浩史氏

大規模自治体のクラウド化が今後どのように進んでいくかを見通すのは難しい。東京23区の中でもクラウドサービスの共同利用に踏み出した世田谷、豊島、練馬、中央区のような例がある一方、ホストコンピューターを継続使用している自治体もある。富士通の顧客である新宿区もその一つだ。クラウド化を含めた様々な提案の中から最終的には機器の入れ替えを選択し、昨年１月にホストコンピューターを更新したばかりだ。

事務手続きの煩雑さが相対的に少ない地方の中小規模の自治体の方が、クラウドサービスの共同利用を進めやすいだろう。当社では和歌山県橋本市と奈良県大和郡山市における住民情報の共同利用にクラウド型サービスを提供している。大規模自治体では費用だけでなく、業務に携わる人員の問題など総合的に勘案しなければならない要素が多い。大規模自治体間のクラウドサービスの共同利用は、現場の職員や主管部門が混乱しないよう事務をどこまで統合できるかが最大のカギとなる。帳票まで一緒にするとなると大変な労力だ。その点からすると、大規模自治体では各自治体が独自のアプリケーションを使えるPaaS型クラウドが主流になるのではないか。今後、災害対策などを念頭に遠隔地にある大規模自治体が連携を模索する可能性もある。コスト削減など双方の思惑が一致すれば、支援していきたい。

富士通の東京23区向け住民情報システムのパッケージ製品「MICJET（ミックジェット）23」は、都への報告資料の作成機能や、転出・転入に伴う大量のデータを夜間に一括処理するバッジ機能を標準装備する。自治体クラウド化に踏み出した４区以外で、同製品を使っている港、品川、葛飾区にも、データセンターの安全性や月額利用料方式などの特徴を示しながらクラウドサービスの利用を提案している。

ただ、番号制度の開始を控えたこの１～２年は、各自治体ともシステム更新に動きづらいのが実情だ。クラウドサービスを前面に出した営業は、３年後を目標に積極展開していきたい。

New Japan e-ID Card toward Infrastructure of e-Health and e-Business

Takashi Obi

Imaging Science and Engineering Laboratory,
Advanced Research Center for Social Information Science and Technology,
Tokyo Institute of Technology

New ID Number

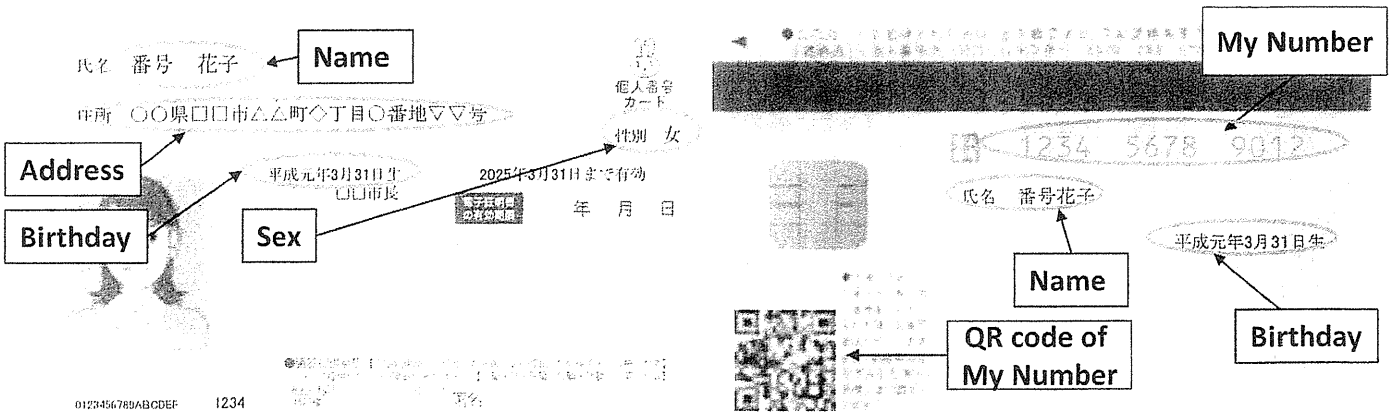
- The Number Use act (Act on the User of Number to Identify a Specific Individual in the Administrative Procedure) promulgated on May 31th 2013.
- Based on this act, every resident, Japanese or foreign, will receive his/her 12 digits ID number on Oct 1st 2015 and a Individual Number (called "My Number") will be effective in Jan. 1st 2016.
- The new ID number can be only used in the tax and social security area excluding health, medical and aging care information.
- New e-ID card will be issued from Jan 1st 2016.

New e-ID card -My number card-

- Replacement of the resident registration card
- My number is printed on the backside of the e-ID card
- New e-ID card have facial photo
- New e-ID card and revised JPKI act will come into reality on Jan 1st 2016
- Revised JPKI will support both digital signature and digital authentication services

- My number card will be issued on request up to 87M per 3 years (2/3 of Japanese population)

My Number card



Card Applications	Usages
Card Face AP	Store the card face image for tamper detection Use Basic Access Control for read-out
JPKI AP	Digital Signature Pass Code : 6 to 16 alphanumeric characters Authentication PIN1 : 4 digits
My Number AP	Store My Number, Name, Birthday, Sex, Address Need to enter PIN2 (may be same as PIN1) for read-out
Resident Record AP	Store Resident Record code (To ensure compatibility with old card) Need to enter PIN3 (may be same as PIN1) for read-out

vs. Basic Resident Registration Card

	Basic Resident Registration Card	My Number Card
Card Issuer	Local Government (Issued individually)	Local Government (Issued by JAPAN Agency for Local Authority Information Systems)
Card face	Facial photo, address, birthday, sex are optionally	Facial photo, name, address, birthday, sex are mandatory
JPKI function	Digital Signature (Option)	Digital Signature (over 15 yr. old) Authentication (Mandatory)
Fee	1000 Japanese Yen (7.1 euro)	Free (estimation is several thousand yen)
Valid period	10 yrs. (Card), 3 yrs. (JPKI)	10 yrs. (Card), 5 yrs. (JPKI)
Scope	Limited to the public sector	Expand into the private sector
Number of cards issued	8.8M (2003-2014)	15M (2016), 86M (-2019) (scheduled)

New JAPAN e-ID card toward infrastructure of e-Gov, e-Health, e-Business

- National e-ID card is difficult to be widely used
  - Lack of applications
  - Require specialized hardware
  - No need for high level authentication in the private sector
- Now we ready to provide "real deal" for citizens
  - Realize multi functions with one e-ID card using New JPKI
  - Plan to support multi-devices, CATV STB, smartphone, etc.
  - JPKI will be accepted by Banks, Credit card issuers, etc.

AS/ST WORLD e-ID AND CYBERSECURITY
Copyright Takashi Obi, Tokyo Tech. 2015
TOKYO TECH TOKYO INSTITUTE OF TECHNOLOGY

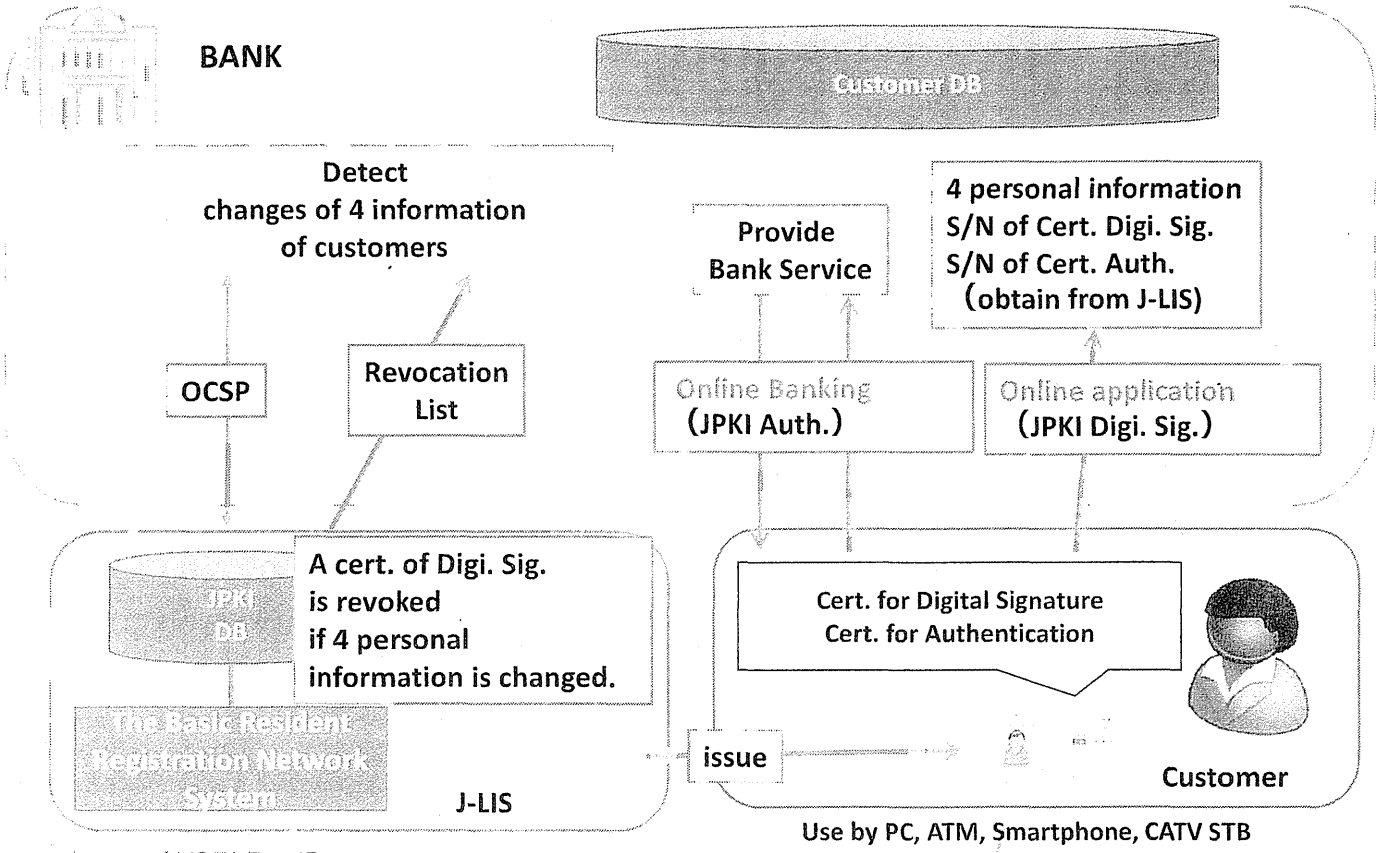
New JAPAN e-ID card toward infrastructure of e-Gov, e-Health, e-Business

- National e-ID card is difficult to be widely used
  - Lack of applications
  - Require specialized hardware
  - No need for high level authentication in the private sector
- Now we ready to provide "real deal" for citizens
  - Realize multi functions with one e-ID card using New JPKI
  - Plan to support multi-devices, CATV STB, smartphone, etc.
  - JPKI will be accepted by Banks, Credit card issuers, etc.

New JPKI

- Certificates are issued by JAPAN Agency for Local Authority Information Systems (J-LIS)
- Certificate of digital signature must include 4 personal information (Name, Address, Birthday, Sex)
- Certificate of authentication service does not include any personal information
- Linkage information of the Certificates of digital signature and authentication is provided by J-LIS
- CRL and OCSP will be disclosed to private sector under permission of minister of ministry of internal affairs and communication
  - Current JPKI is limited to the public sector in order to avoid a potential depression of private business of PKI

BANK-Use case



Reason of Revocation

Certificate of Digital signature and Authentication will expire when entries in the Basic Resident Register are changed.

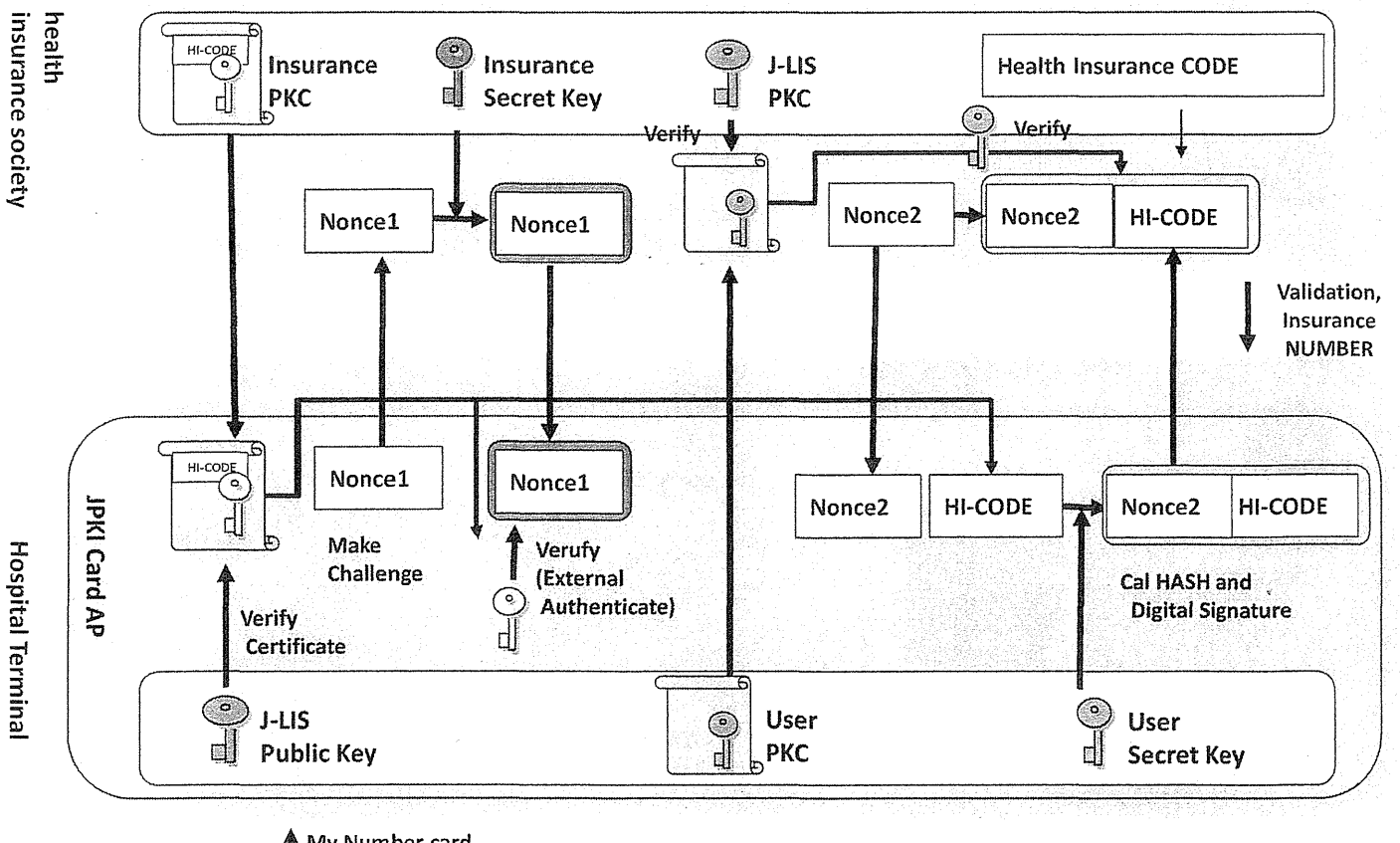
Verifiers of JPKI Certificate can recognize a change of registration information.

Reason of change of registration information or card status	Reason code for the Certificate of Digital Signature	Reason code for the Certificate of Authentication
Move, Marriage, etc.	affiliationChanged	Not expire
Removed from the Basic Resident Register (Death, move to foreign country,)	affiliationChanged	affiliationChanged
Lost card	certificateHold	certificateHold
Renewal of certificates	Superseded	Superseded
Return card	cessationOfOperation	cessationOfOperation

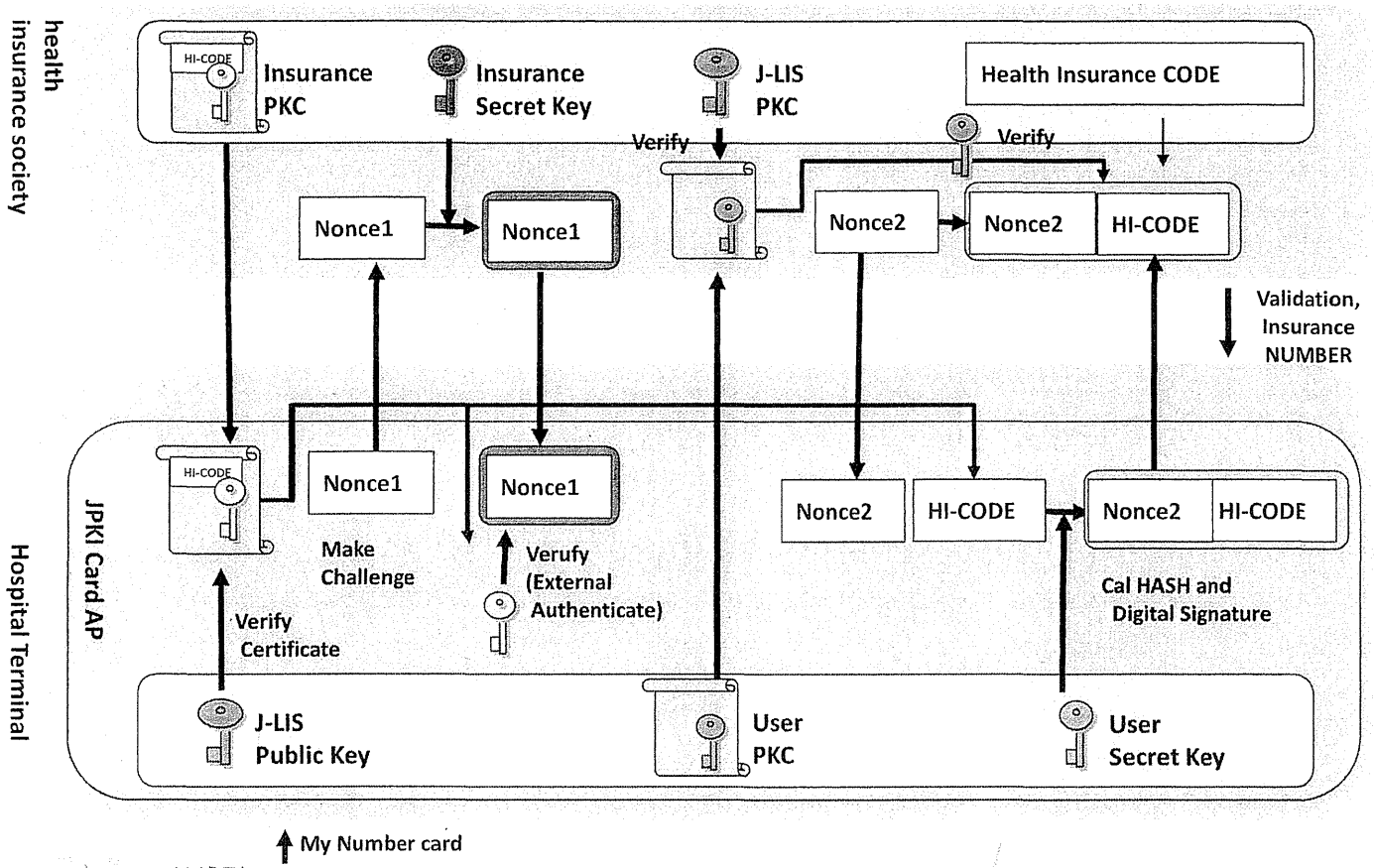
Enrichment of JPKI services

- Services could be securely linked to my number card through the on-line authentication
  - Attributes such as license and qualification
    - Validation of the health insurance through linking to the insurers
  - Payment services under plan
    - Functions of an internet banking card and a credit card (secondary card), etc.
  - External Auth. scheme is supported by New JPKI
    - Useful for Validation of the health insurance and micro payment just like sign-less
    - Especially statistics tells us that Monday morning, we have 15 M transactions for the validation of health insurance

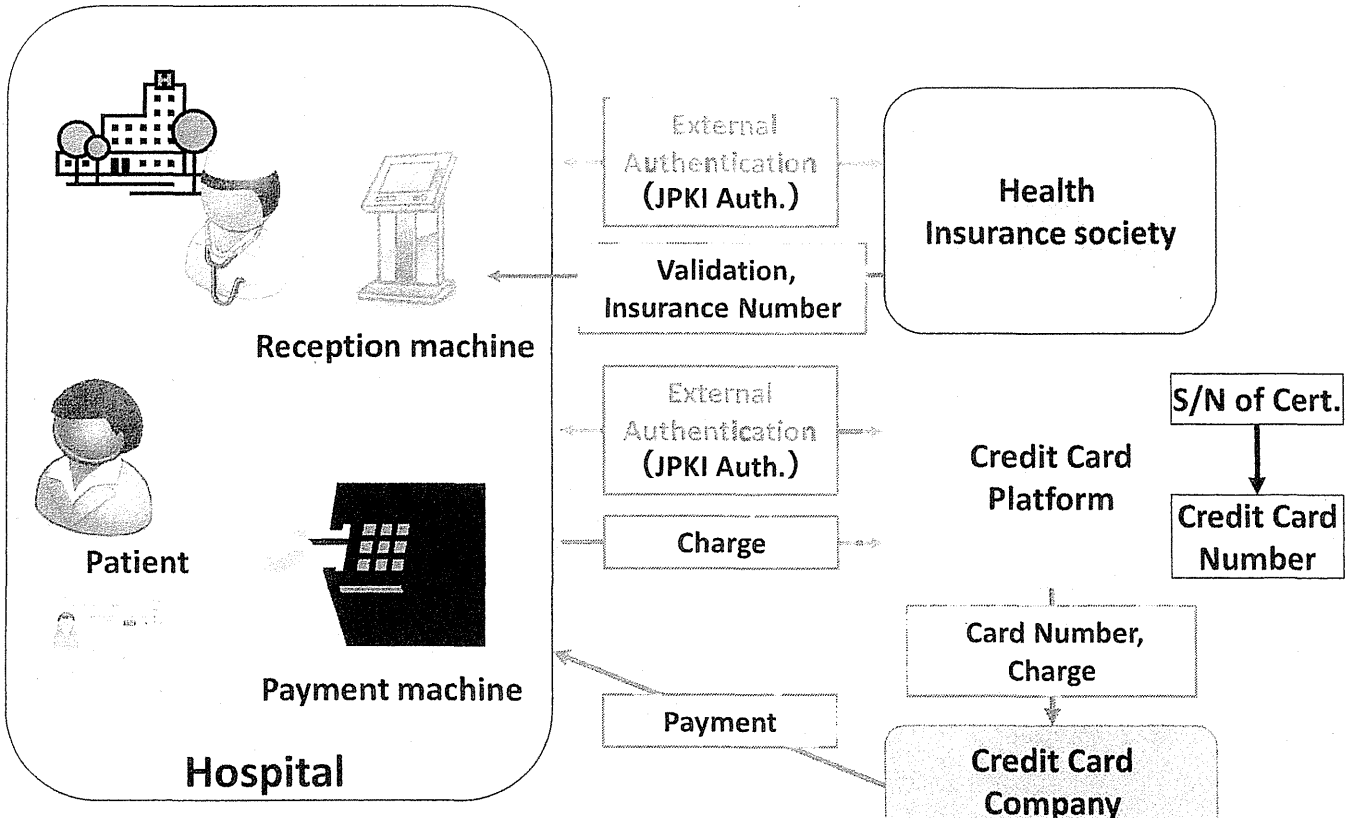
External Auth. Scheme



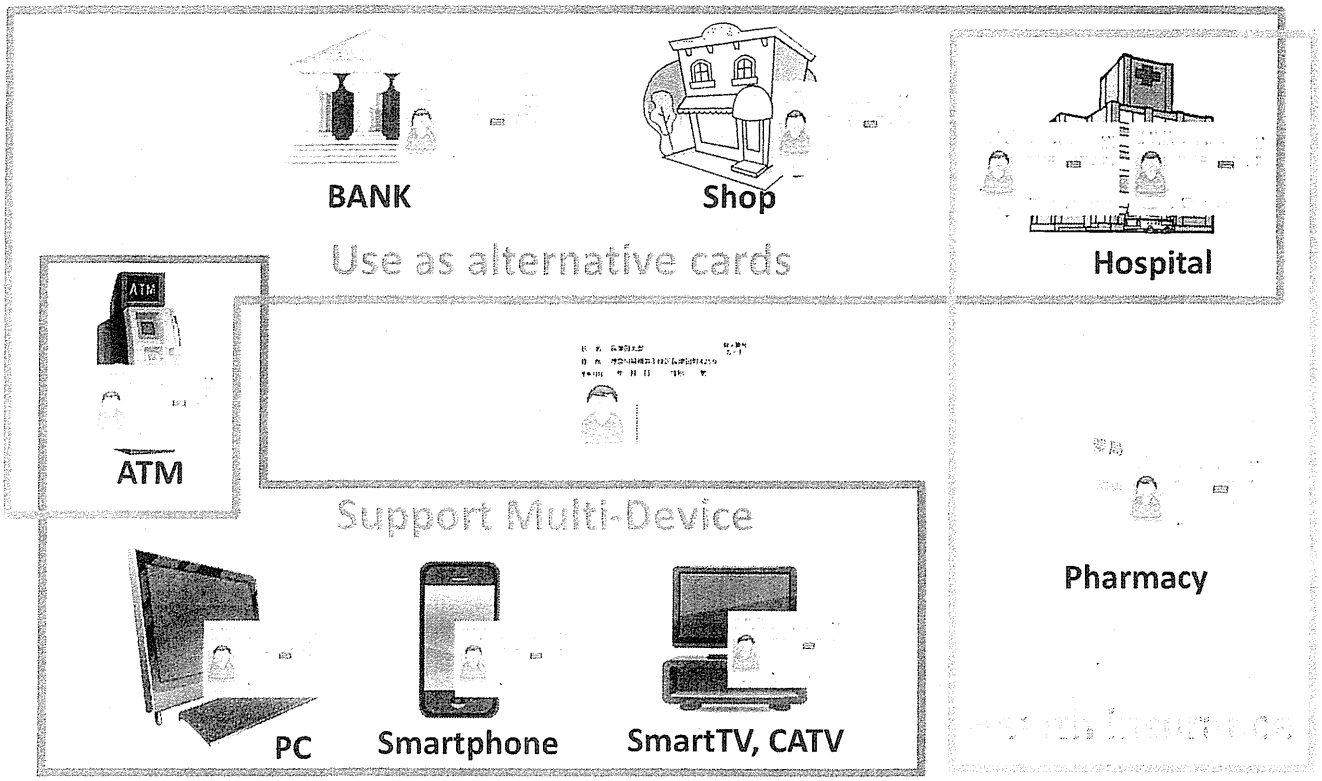
External Auth. Scheme



Hospital-Use case



Don't leave home without my number card



Thank you

A part of this work was supported by Health Labour Sciences Research Grant, Research on Region Medical H26-Iryo-Shitei-034.

An Access Control System for Home Based Healthcare Information Sharing using Smart Gateway

Daniel Agbesi Dzissah*[1] Hiroyuki Suzuki*[2] Joong-Sun Lee*[3] Obi Takashi*[2] Nagaaki Ohyama*[2]

[1]Interdisciplinary Graduate School of Science and Engineering, [2]Imaging Science & Engineering Tokyo Institute of Technology, [3]ASIST

1. Introduction

As a result of the graying population, home-based healthcare services has seen a rapid demand over the past decade. Home based care and nursing services are a joint service involving a broad range of healthcare services provided by several other individuals and organizations. Mobile computing devices such as smartphones and tablets have been widely recognized as a means for integrating disparate data and computing resources in the pervasive mobile healthcare field. Moreover, mobile devices provide a platform to develop applications on wireless infrastructure to execute healthcare process that in turn can provide remote access to healthcare information exchange services. Such an environment provides ubiquitous and universal access to resources at the point of care, thus improving healthcare quality. In such conditions the ability to provide effective access control environment to ensure the security and privacy of healthcare information are essential [1]. However, traditional authentication scheme adopted in mobile devices such as passwords, digital certificates, secure tokens and biometrics. mainly focus at only user entry-point authentication, which may not suit dynamic healthcare environments. We propose an experimental design of a certificate based context-aware access control method to be used by caregivers and physicians with mobile devices in home-based healthcare environments. In our proposed system, whenever a user visits a patient's home, a gateway authenticates the user's device using certificates and collects context data used for authorizing access to preliminary services using the PKI-based smart card. For accurate context evaluation, the gateway service collects context data and generates certificate credential based on the received context data such as GPS data and user device MAC address for verification and trust assessment of the authenticated user's device.

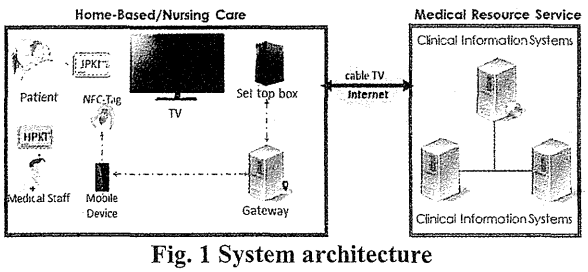


Fig. 1 System architecture

2. Design methods

There are three main elements of the proposed model. First is the application processes running on the mobile device. Second is the gateway, processing authentication requests between remote services and the mobile device.Third is the remote medical resource service, performing duties like authenticating of Japanese-PKI cards and Healthcare-PKI and handle's parsing H-Role privileges of medical staff. When a medical staff requests to access a medical resource service via his/her mobile device, a connection is established with the gateway via a secure NFC-tag as

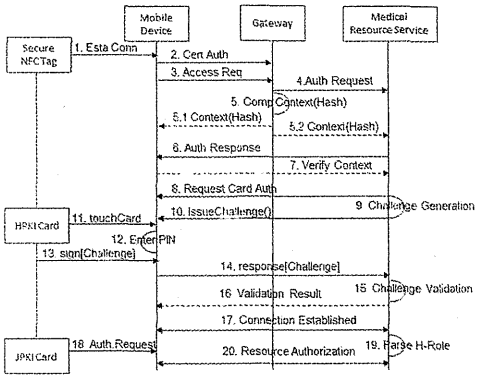


Fig. 2 Activity flow

Shown in Fig [2]. By using the application running on the mobile device, a user selects their profile and the resource type. Profile selection allows the mobile application to fetch device's certificate automatically. The application generates a request envelope containing the certificate, the little context data and sends it to the gateway. The gateway receives the request envelope and parses the certificate and returns the generated context. A copy of the context is sent with an authentication request to the medical resource service. A user smart card authentication is required to the medical resource service after authentication between gateway and mobile is confirmed. Context verifies transactions between the medical server and the mobile device, after this verification can the transaction be validated and continue. During this process, a medical staff uses his/her HPKI card to sign a challenge response and enters a PIN code for authenticating card transactions on the mobile phone. According to the validation of the context and the HPKI authentication, the resource authenticates the H-Role of the user. The service is allowed or denied by the system. For a medical staff to access the patient's information, authorization is performed using the JPKI card to sign a challenge response from the medical resource server.

3. Discussion

The proposed model uses certificates and context as add-ons with PKI-smart cards the aim of providing healthcare resource access to legitimate medical staff. Since relying on a single point, entry authentication cannot be relied on in such setting.

References

[1] He D, Naveed M, Gunter CA, Nahrstedt K. Security Concerns in Android mHealth Apps. *AMIA Annual Symposium Proceedings*. 2014;2014:645-654.