- 機関認証 JPKI 利用時には、端末利用開始時に PKI を用いた端末認証（クライアント認証）の実施を行うこと。但し、機器固有 ID 確認のみ等の暗号アルゴリズムを利用しない機器の識別は認めない
- 認定認証機関と利用端末間で IP-Sec などを利用した安全な通信路を確保すること
- 利用者端末内に保持した機関認証用公開鍵証明書を容易に外部から読み取れないようにすること
- 番号カード（JPKI-AP）と端末内アプリケーション間の通信情報等を容易に読み取れないようにすること
- 機関認証 JPKI 利用のためのアプリケーションの実行環境を保護すること
- 同一端末からの機関認証による同一利用者認証利用回数を制限すること
- カード所有者の明示的な同意の下で利用すること。（機関認証 JPKI 利用時には、カード所有者に“OK”ボタンを押させるなど、機関認証 JPKI 利用を意識させるユーザインターフェースを利用する）

図１にこのような安全対策を満足する端末のシステム構成案を示す。このシステムでは、機関認証用の秘密鍵を端末内に保持している UIM などの耐タンパな Secure Element に格納し、端末の電源投入時にこの秘密鍵を利用可能な状態にするための外部認証鍵を保険資格確認機関であるサービス事業者が保持している。そして、端末の NFC 機能を介してマイナンバーカードや HPKI カードと接続することで、保険資格のオンライン確認を可能とする。

具体的な処理シーケンスは、図２に示す通りであり、従来は図３のように機関認証に必要となる外部認証処理をマイナンバーカードに格納されている JPKI-AP とサービス提供者の設置する

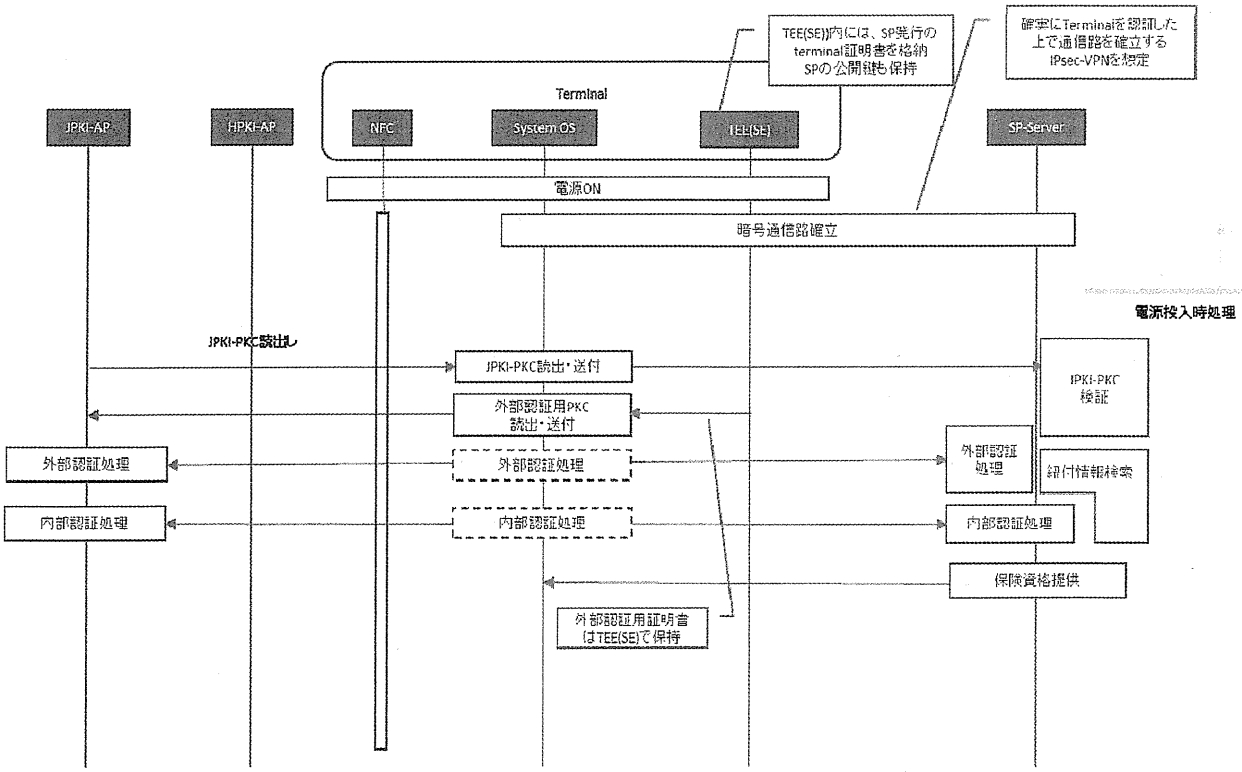


図３　機関認証鍵をサーバで保持する場合の想定処理フロー

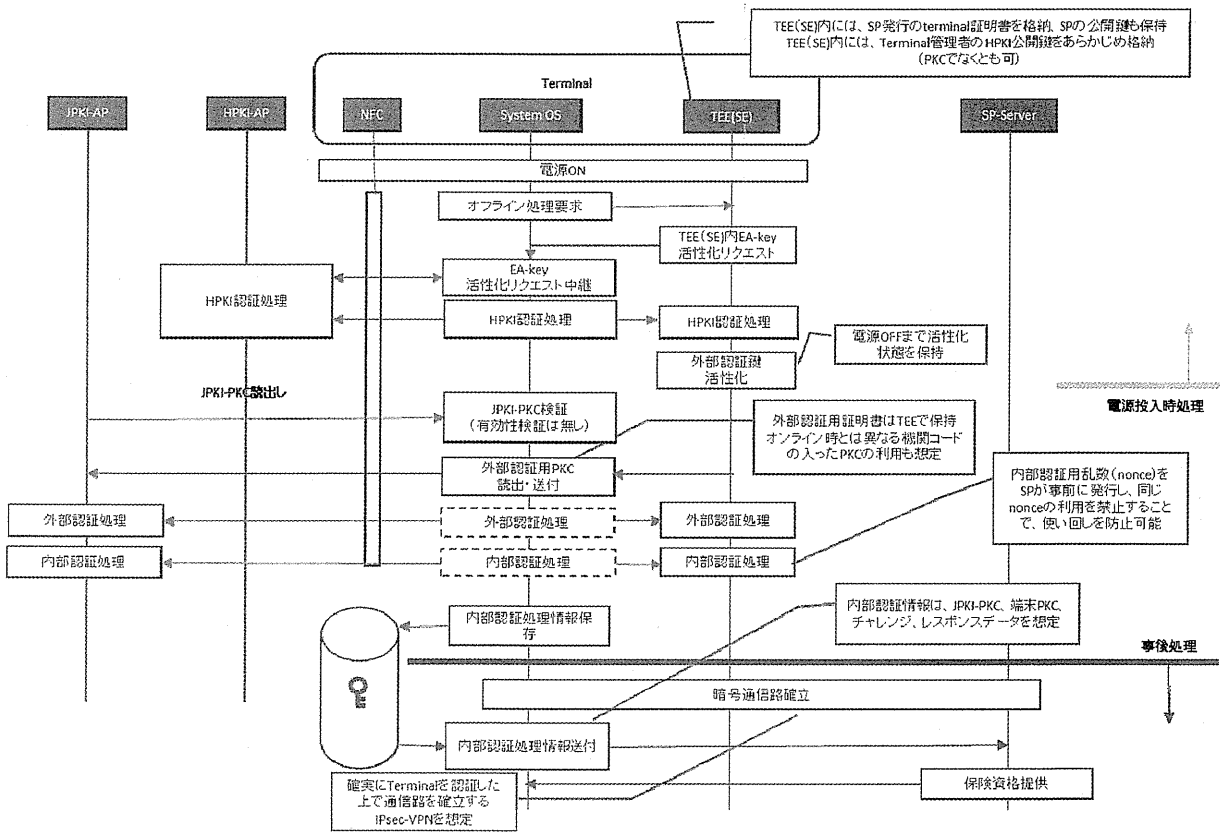


図４　機関認証鍵を端末で保持する場合のオフライン処理時想定フロー

サーバ間で行っていたのに対して、同様の処理を JPKI-AP と端末間で実施することにより、通信にかかる時間を短縮し、処理全体にかかる時間を短縮することを可能としている。

また、先に述べたように、医療機関と保険資格確認機関間のネットワーク障害等が発生した場合には、オンラインでの保険資格確認を実施できないが、レセプト請求のための情報取得を行うためにマイナンバーカードを所持する患者の来院の履歴を端末で管理し、事後に保険資格の確認を実施することが必要となる。また、この際には、図２で示した、機関認証用秘密鍵を利用可能な状態にするための処理を行うことができない。これに対しては、我々は、端末内の Secure Element 内に端末利用医療機関の医師等の HPKI 公開鍵を格納し、HPKI 認証を行うことで、機関認証用秘密鍵を利用可能な状態とする仕組みを提案した（図 4)。

このように、オンライン保険資格確認については、昨年度の研究で抽出した課題の解決を行ったが、さらに、我々は、オンライン保険資格確認の仕組みを利用することで、医療等ＩＤの発番管理が可能であることを明らかにした。

現在厚生労働省においては、医療等ＩＤの検討が進められているが、医療等分野の情報連携に用いる識別子（ＩＤ）は、安全かつ効率的な情報連携の基盤を整備する上で欠かせない仕組みであり、診療情報等のデータの電子化とネットワークの整備を併せて推進することで、①地域内や複数地域をまたがる医療機関・介護事業者等の連携や地域包括ケアの提供、②健康・医療の研究分野での大規模な分析研究、③国民自らが健康・医療の履歴や記録を確認し、健康増進に活用する仕組み（ポータルサービス）など

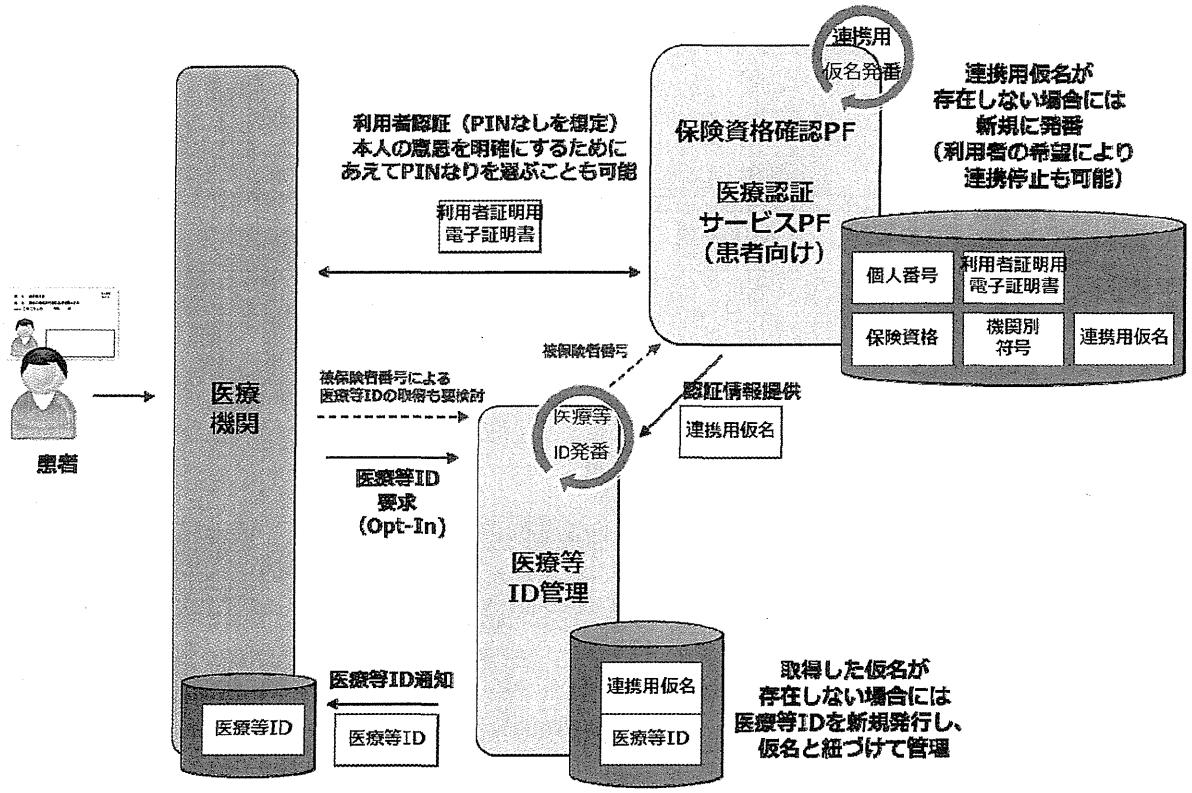


図５　医療等 ID 発行・運用（案）

が、飛躍的に進むことが期待されている。

そこで、我々は、医療等ＩＤの有する性質として、以下の三点を考慮して、システム検討を行った。

- 一意の人物を特定できる唯一無二性と漏れや重複のない悉皆性を満たすこと
- 本人の同意のもとで希望する患者が番号を持つことができる仕組みであること
- 本人の希望により番号の使い分けができる仕組みであること

図５に、医療等ＩＤの発行・運用を行うシステム構成案を示す。提案システムでは、患者は医療機関にマイナンバーカード１枚を持っていくことで、保険資格確認の実施と医療等ＩＤの医療機関への通知を一度に行うことが可能となっている。また、図６に示す様に、医療等ＩＤの管理を行う組織において、医療機関と医療等ＩＤの紐づけ情報を保持することで、本人の希望により複数の医療等ＩＤの使い分けを行うことも可能である。

特定個人情報保護評価指針において、個人番号を扱うことのできる者が個人番号と紐づけてアクセスできる情報は、特定個人情報ファイルと定義されるため、医療等 ID を利用する業務において、特定個人情報ファイルを作成しないために、提案システムにおいては、医療等 ID を利用するシステムと個人番号を扱うシステムを分離しており、患者確認のために保険資格確認ＰＦの一部機能を利用するが、特定個人情報保護評価の対象となるシステムを限定するために、保険資格情報とは論理的、物理的に分離したデータベースを作成することとしている。

C．研究結果

本研究で提案するシステムを利用することで、医療機関は患者の個人番号カードを利用し

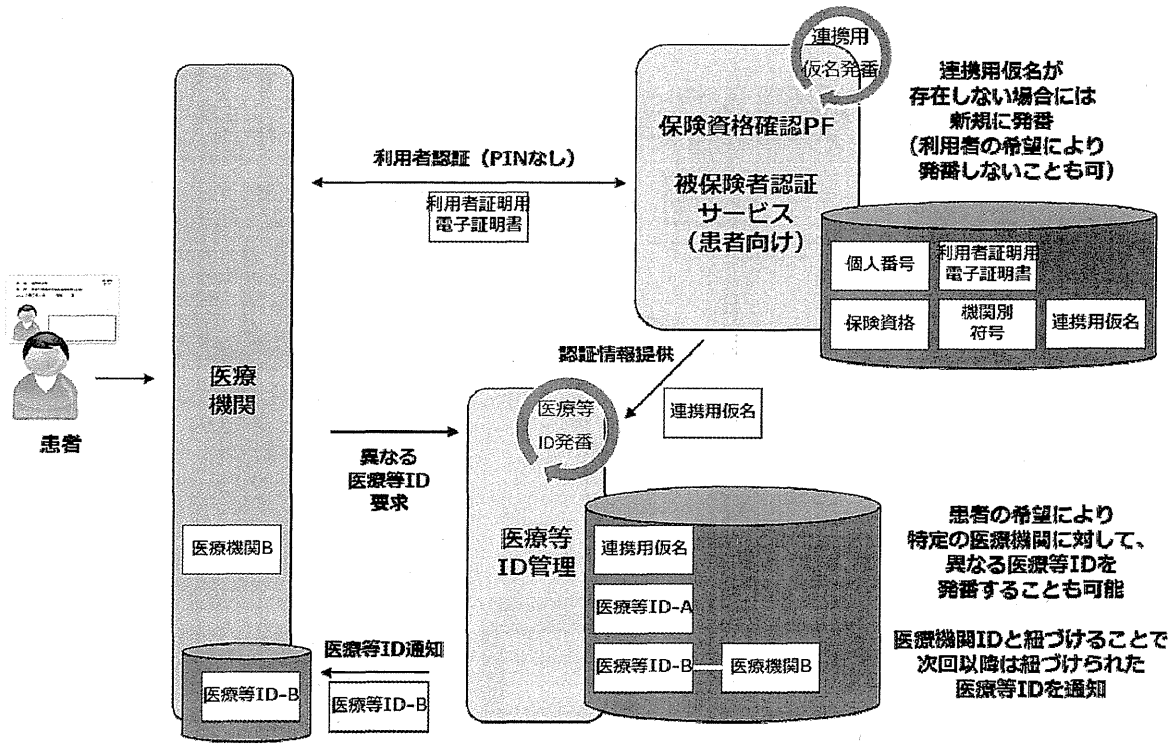


図６　複数の医療等 ID 発行・運用（案）

て、PIN の入力を求めずに保険資格の確認を行うことが可能となる。オンライン資格確認では、本人を一意的に識別する必要があるが、例えば保険資格確認番号などの利用では、本人を一意的に識別する方法の安全性確保が難しいと考えられるため、安全性の観点からも、JPKI を用いる仕組みが適切である。また、この仕組みは、厚生労働省が導入を推進する電子処方箋の運用において、例えば、保護者が子供の個人番号カードを用いて薬を受け取るなどの際にも利用できると考えられる。

D．考察

昨年度の本研究において、JPKI の電子利用者証明機能を利用して、健康保険等の資格確認を行う手法を提案したが、その仕組みは、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報告書 10 ページの【個人番号カードの 公的認証を活用したオンライン資格確仕組み】[2]に反映されており、本年度提案した仕組みについても今後その必要性を含め検討が進められると想定される。また、医療等ＩＤの検討結果についても、我々が提案した考え方を基にした JPKI の利用方法が、第 9 回医療等分野における番号制度の活用等に関する研究会において日本医師会より示されており[3]、今後本研究で提案した手法をベースとした検討が進められると想定される。

しかしながら、今後多くの医療機関、薬局や介護機関などで利用されるようになった場合、患者のプライバシーを侵害するような誤った利用がされる可能性もあるため、機関認証 JPKI の利用認定機関の認定基準、機能の利用手順などの策定を今後行っていく必要がある。

E．結論

本研究では、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医療分野での利用について検討を行った。本年度は、前年度検討したオンライン保険資格確認応用や医療等IDの運用等について特に検討を行ったが、新たな公的個人認証サービスは、今後、医療での利用にとどまらず、金融分野など他の民間分野での利用も想定されており、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ることが必要である。

F．健康危険情報

特になし

G. 研究発表

[1] Takashi Obi, "New Japan e-ID Card toward Infrastructure of e-Health and e-Business, " World e-ID and Cybersecurity 2015, Sep. 2015

参考文献

[1] 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

[2] 医療等分野における番号制度の活用等に関する研究会報告書, http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000106609.pdf, 2015年12月

[3] 日本医師会 医療等 ID の発番・運用について, 第 9 回 医療等分野における番号制度の活用等に関する研究会資料, http://www.mhlw.go.jp/stf/shingi2/0000102013.html

研究成果の刊行に関する一覧表

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
Mukai Masami, Yutaka Ando, Yuki Yokooka, Yasuo Okuda, Masayoshi Seki, Masahiro Kimura, Hiroshi Tsuji, Tadashi Kamada	Development of clinical database system specialized for heavy particle therapy	MEDINFO 2015: eHealth-enabled health		933	2015
大山永昭	マイナンバー制度と医療保険の資格確認	神奈川のこくほ・かいご/潮流	Vol.378	3 - 6	2015
大山永昭	ハード・ソフト・データの市場性こそ大事	日経グローカル	No. 267	19	2015
Takashi Obi	New Japan e-ID Card toward Infrastructure of e-Health and e-Business	World e-ID and Cybersecurity 2015			2015
D. A. Dzissah, H. Suzuki, Lee Joong-Sun, T. Obi, N. Ohyama	An Access Control System for Home Based Healthcare Information Sharing using Smart Gateway	The 2016 IEICE General Conference	A-15-10	220	2016

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

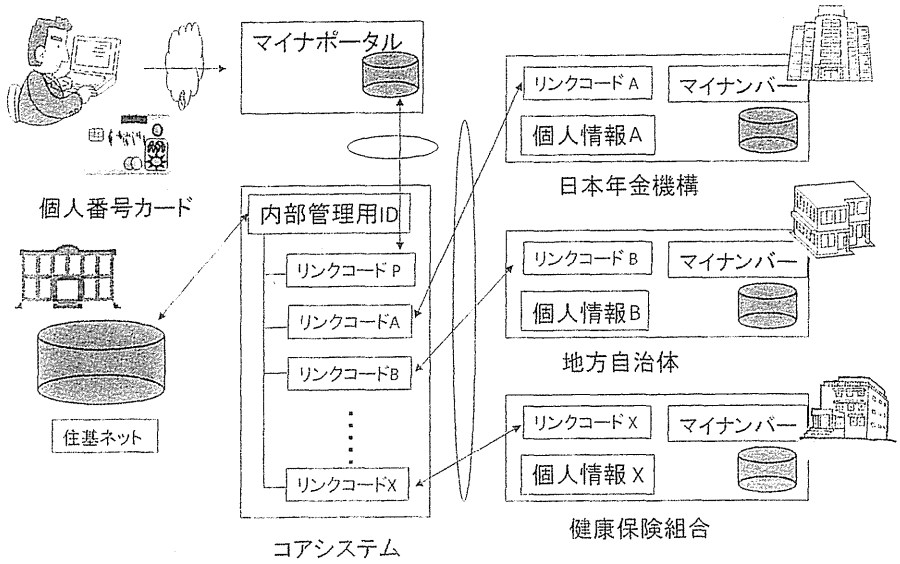
平成28年1月、いよいよマイナンバー制度が実施される。よく知られているように、本法の施行目的は、社会保障制度のきめ細やかかつ的確な実施、行政業務の正確性および効率の向上、国民の利便性向上等とされている。本制度については、すでに多数の解説記事等があることから、ここではマイナンバーの利用範囲と個人情報保護について述べ、次に制度実施に伴う変化について解説する。そして、医療保険業務への影響に触れ、最後に医療保険の資格確認と更なる展開について紹介する。

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、

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

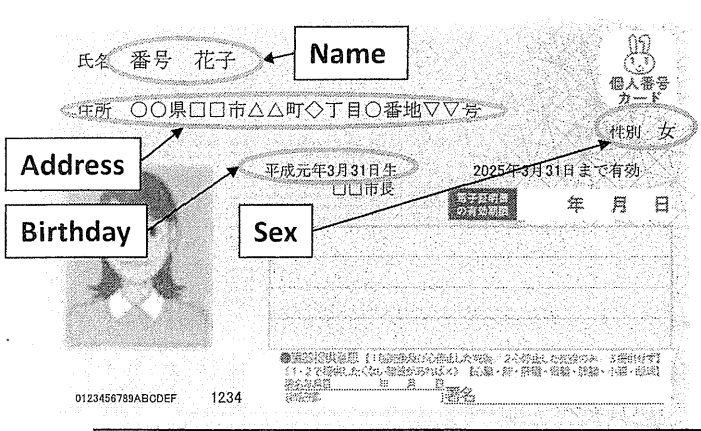
- The Number Use act (Act on the User of Number to Identify a Specific Individual in the Administrative Procedure) promulgated on May 31th 2013.
- Based on this act, every resident, Japanese or foreign, will receive his/her 12 digits ID number on Oct 1st 2015 and a Individual Number (called "My Number") 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.

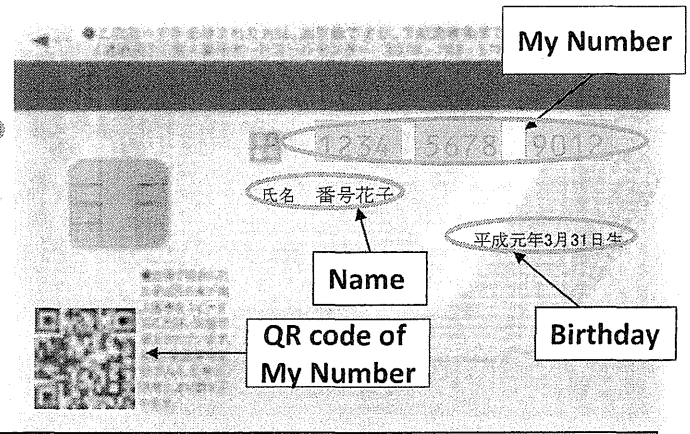
New e-ID card -My number card-

- 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.

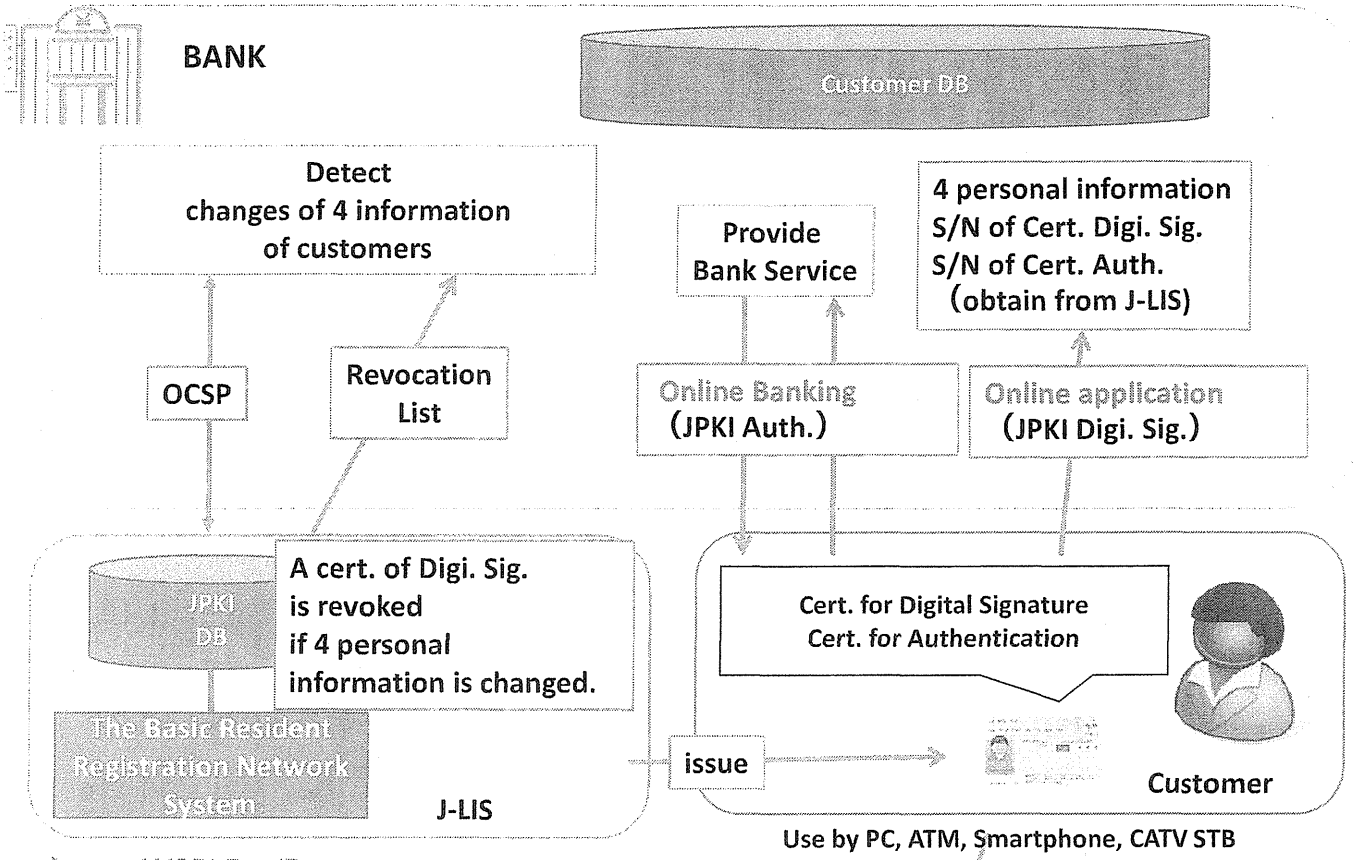
New JAPAN e-ID card toward infrastructure of e-Gov, e-Health, e-Business

- 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.

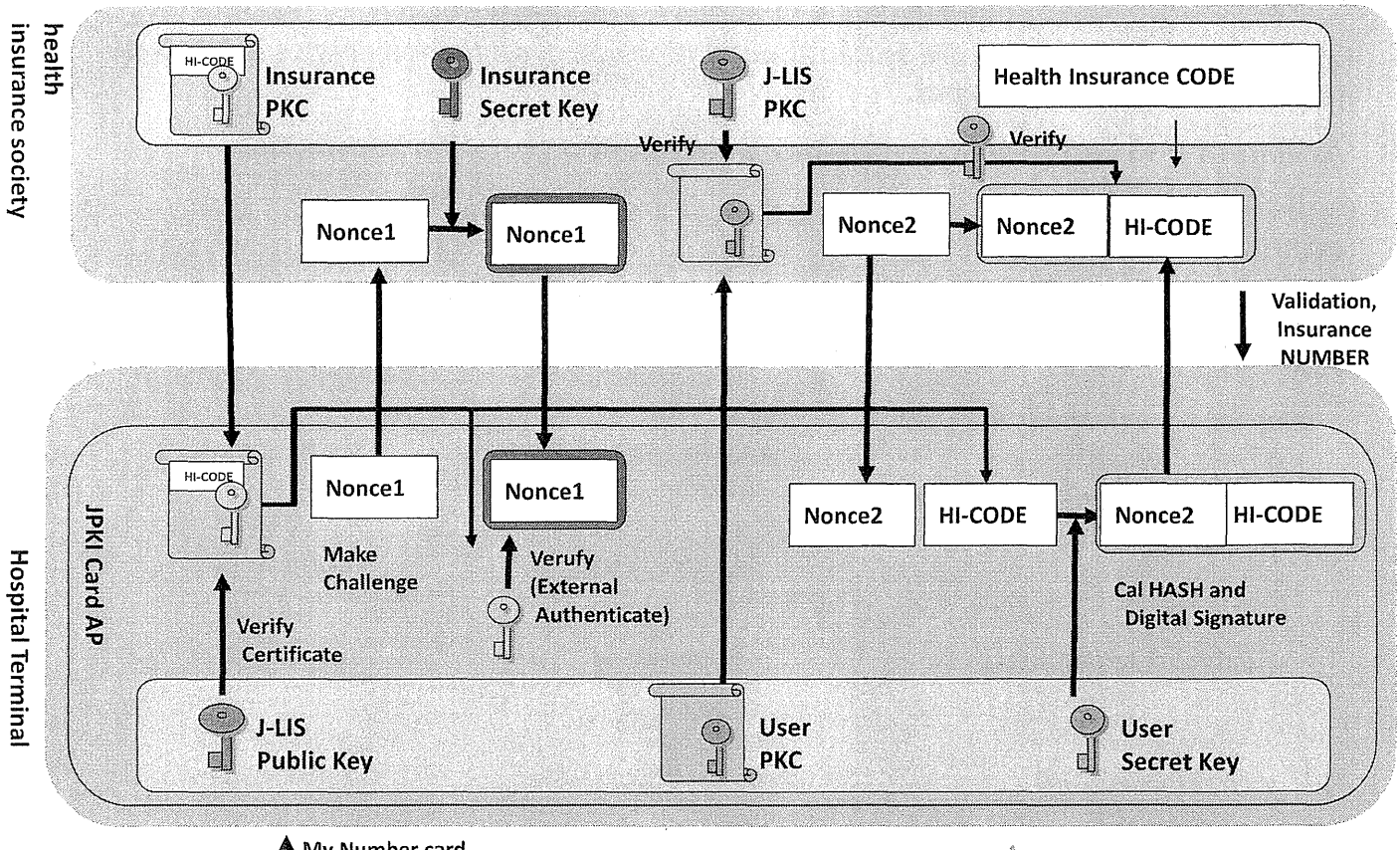
Verifiers of JPKI Certificate can recognize a change of registration information.

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

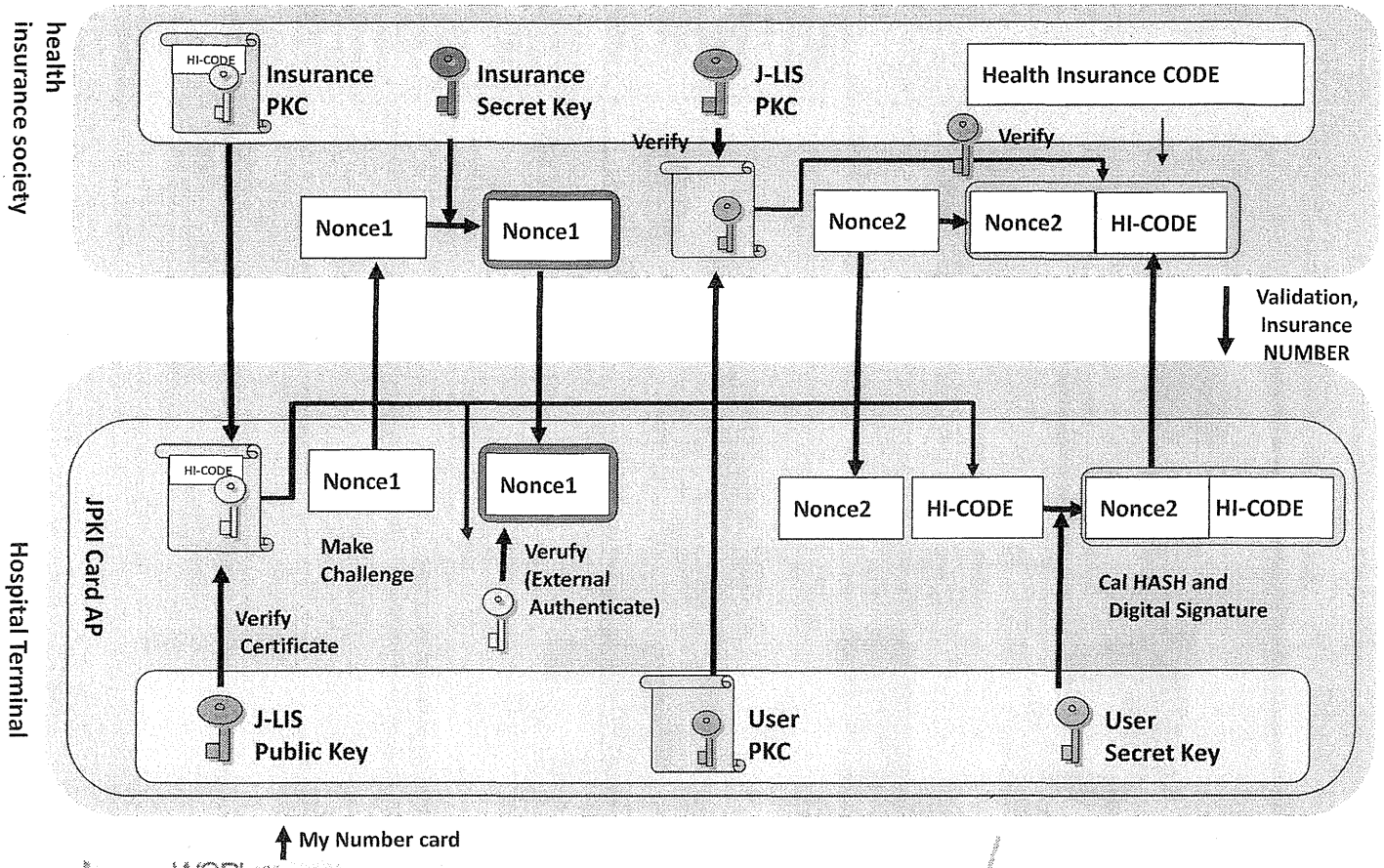
Enrichment of JPKI services

- 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

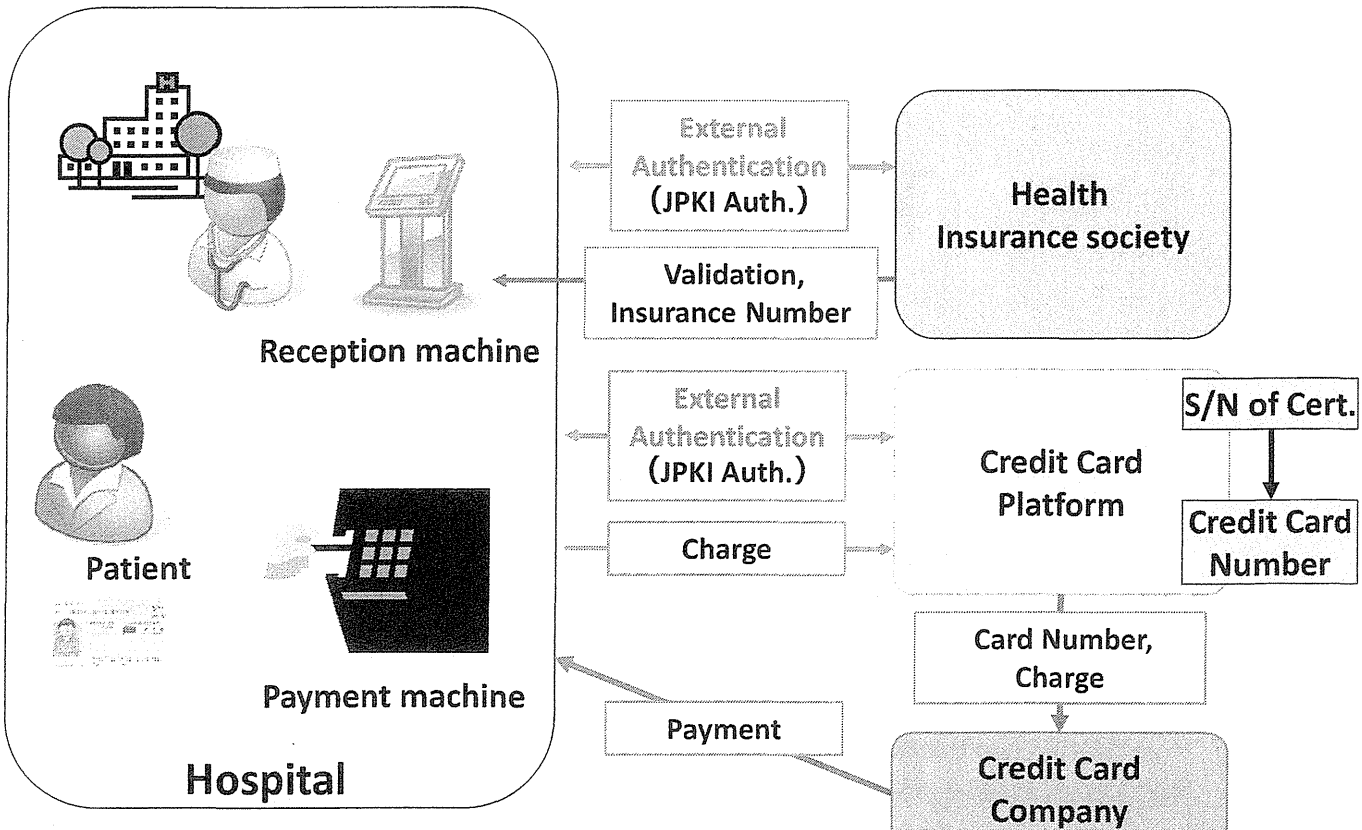
External Auth. Scheme



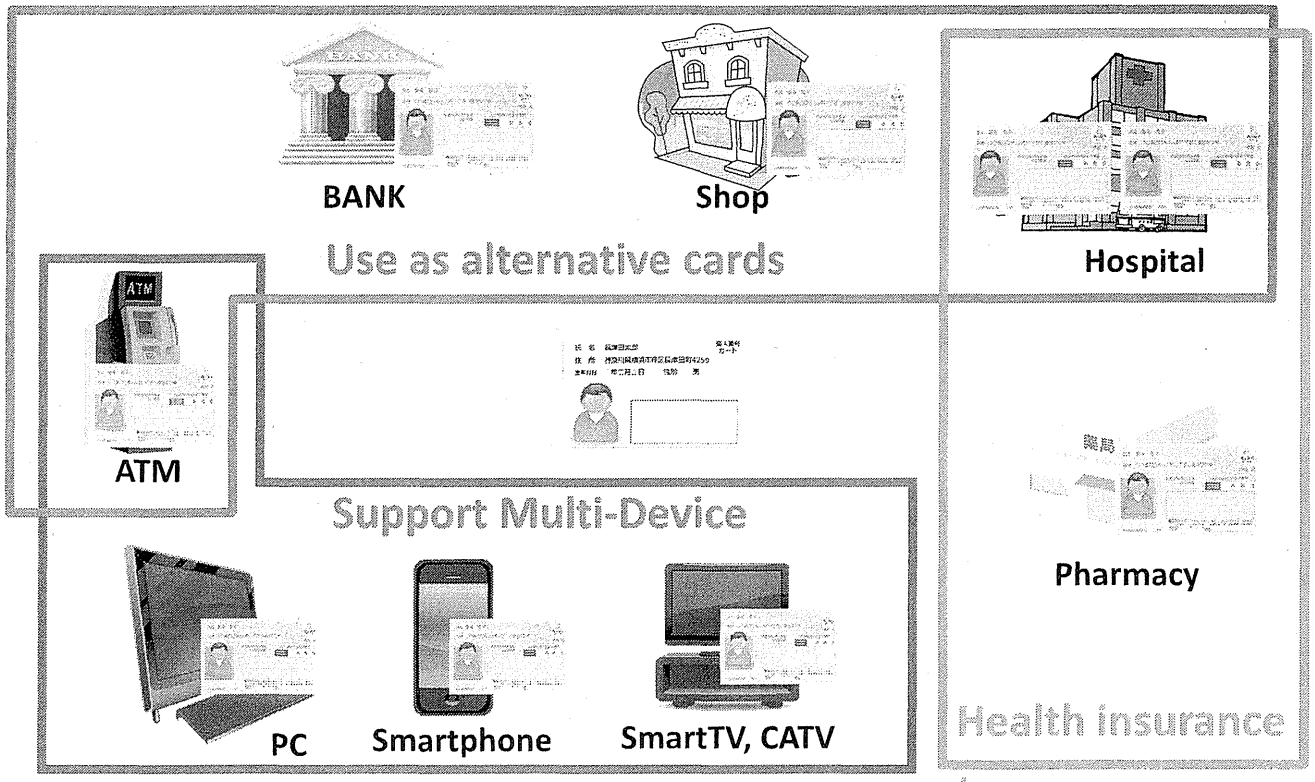
External Auth. Scheme



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.