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，

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~~以下~~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）~~ため~~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．

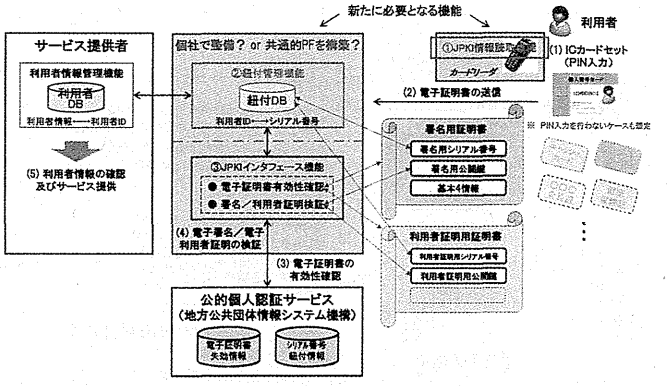

図 1　JPKI の活用における基本システム構成

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」~~について，~~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 ~~プラットフォーム~~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~~ため~~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．

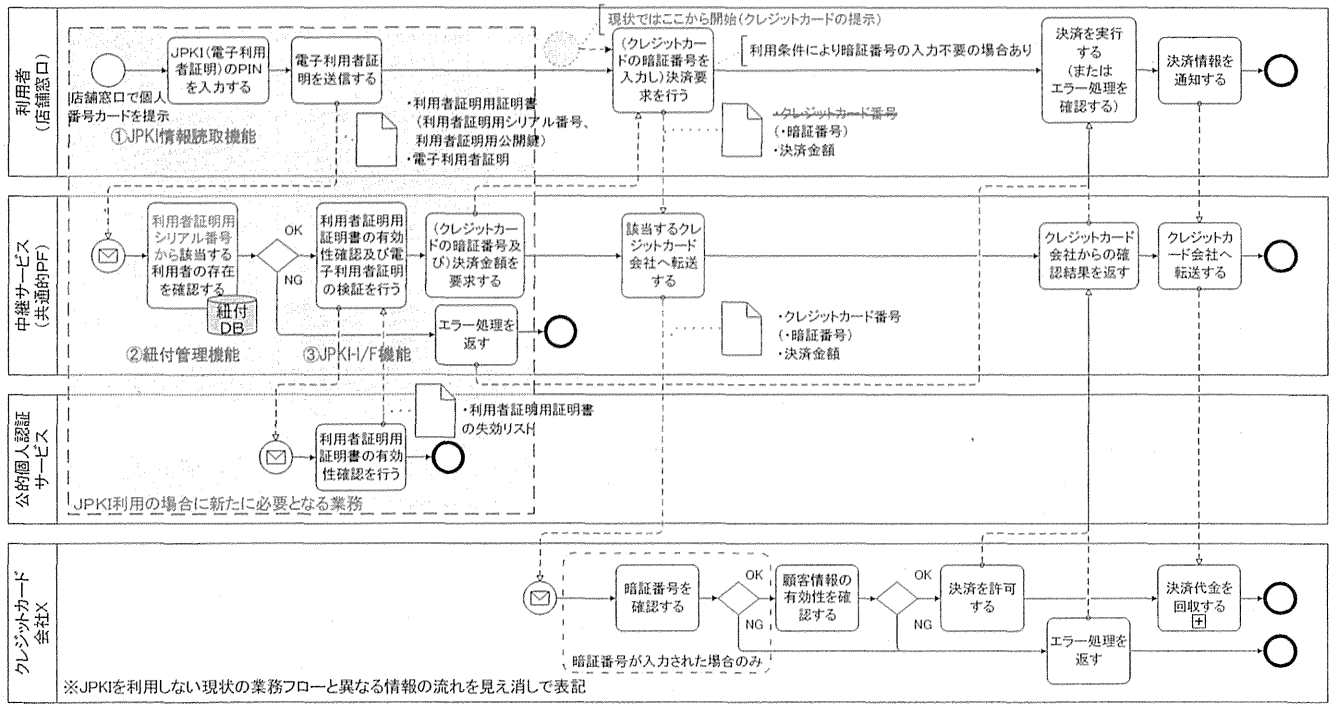

図 2　クレジットカード機能の実現の一例

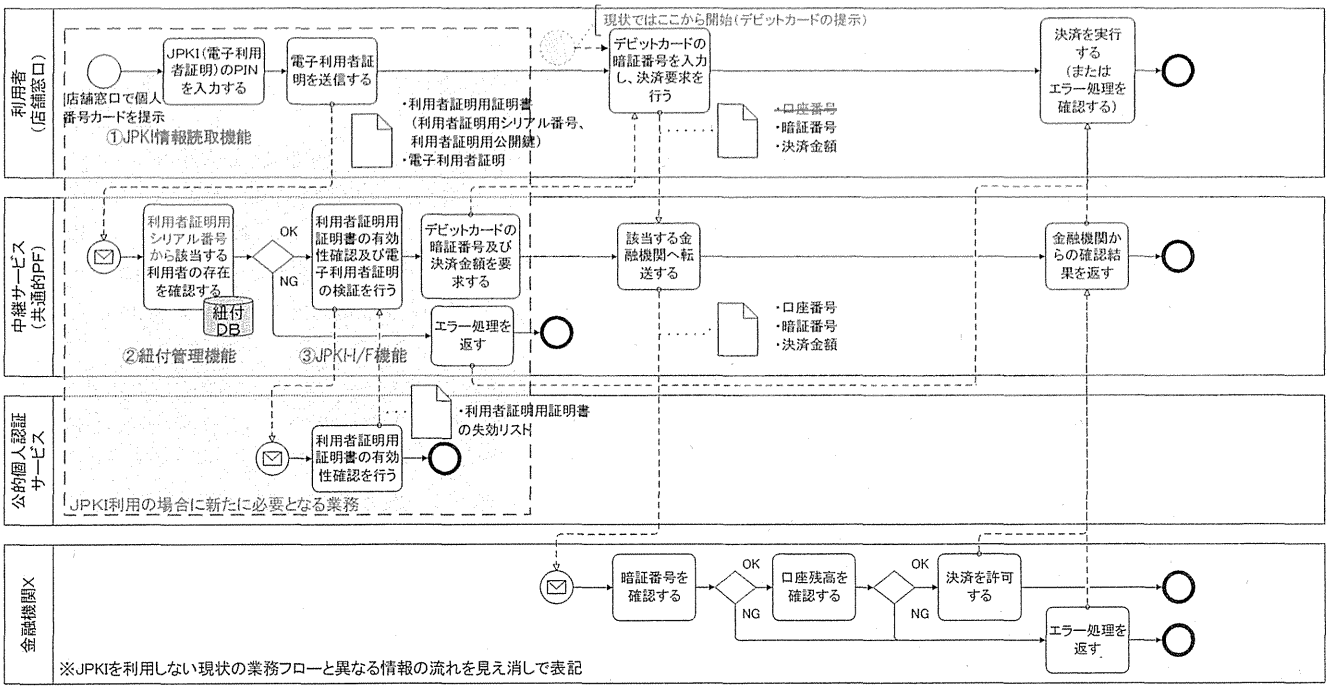

図 3　デビットカード機能の実現の一例

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」~~について，~~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~~ため~~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 ~~より~~から送信されてきた利用者証明用シリアル番号~~から~~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~~から~~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．

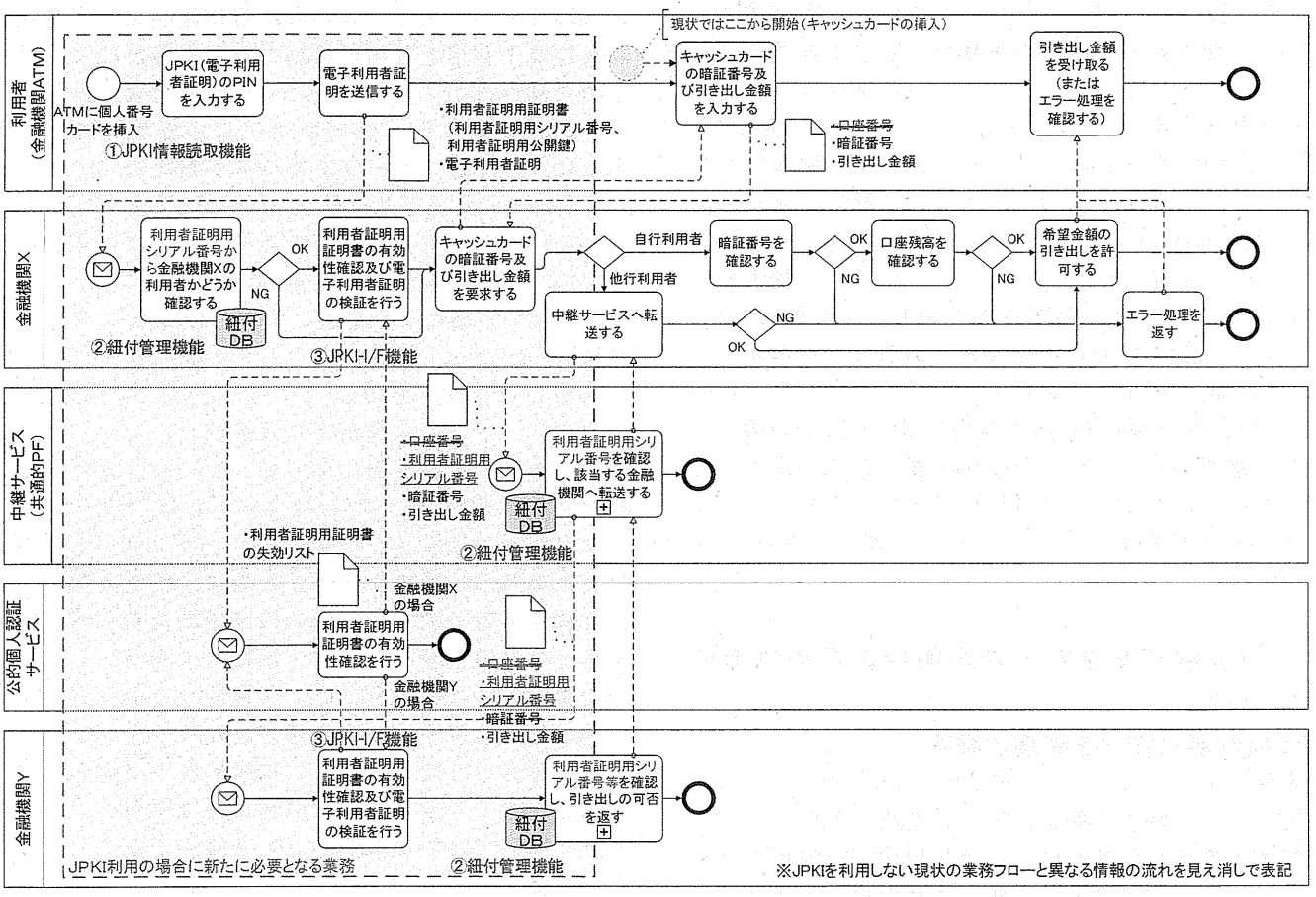

図 4　キャッシュカード機能の実現の一例

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~~以下次~~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 プラットフォーム）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 プラットフォームに置かれ，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 プラットフォーム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 プラットフォームに「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 プラットフォーム（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 プラットフォーム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 プラットフォームが「代行」する，すなわち，共通的 PF プラットフォーム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 プラットフォーム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 プラットフォーム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，検証者ではないためので，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 プラットフォームに渡し，共通的 PF プラットフォーム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