「これまでの議論の整理」においては、カードのＩＣチップに収録する本人を特定する鍵となる情報（本人識別情報）について、①制度共通の統一的な番号[2]又は②カードの識別子を基本として更に検討を進めると述べたところである。

ところで、本人識別情報は、制度内・制度間で利用者の識別を行うための情報であり、電子的に利用者の情報にアクセスするためには、別途オンライン上で認証を行うこととなるが、この際、①制度共通の統一的な番号又は②カードの識別子をそのままＩＣチップに収録して、個人の識別に用いる場合には、暗号化等の措置をとったとしても、住民基本台帳カードのように専用端末を用いるなどの適切な保護を講じなければ、ＩＣチップから送り出される情報を不正に読み出されるおそれを完全に否定できない。

一方で、社会保障カード（仮称）は、健康保険証として医療機関等で利用されることが想定されているが、すべての医療機関等において専用端末を用いて資格確認等を行うことは考えにくい。

そのため、情報を読み出す端末を無条件に信頼することができないことを考えれば、①制度共通の統一的な番号又は②カードの識別子を情報の送り手と受け手で持ち合うことで本人を認証する方法より、情報の送り手と受け手とで異なる情報を持ち、ＩＣチップの演算機能を活用する公開鍵暗号の技術[3]を活用する方法の方が安全性においては優位である。

また、この公開鍵暗号技術を用いた認証の方法については、認証しうることをもって識別に代えることも可能であることから、利用者の識別・認証のための方法としては、当該方法を用いることを仮定し、今後更に検討を進めることとする。

---

[2] 制度共通の統一的な番号の例については、『「社会保障番号」に関する実務的な議論の整理』（平成 18 年９月 22 日・社会保障番号に関する関係省庁連絡会議）では、「住民票コード」、「基礎年金番号」、「新規番号の付番」が挙げられている。

[3] ＩＣチップから送り出される情報が膨大な桁数の乱数とＩＣチップ内で生成される関数であり、ＩＣチップの内部にのみ格納される別の乱数との演算の結果が合致することにより、本人を認証する方法。なお、公開鍵の電子証明書には重複を避けるための整理番号が付けられることになるが、これは本人の識別に用いられるものではない。

（２）中継データベース（中継ＤＢ）について

①　中継ＤＢの必要性

先に述べたとおり、社会保障カード（仮称）の仕組みについては、プライバシー侵害・情報の一元的管理に対する不安を極力解消しつつ、将来の用途拡大に対応できるものとする必要がある。

この観点から、「これまでの議論の整理」においては、社会保障カード（仮称）の仕組みのイメージについて、以下のように述べたところである。

・　カードのＩＣチップには保険資格情報や情報閲覧の対象となる年金記録等の情報は収録せず、ＩＣチップ内情報の書き換えの機会を極力減らしＩＣカードのセキュリティを確保する。必要な情報の取得にはＩＣチップ内の本人識別情報を用いて外部のデータベースにアクセスする

・　保険資格情報や閲覧情報は、現在と同様に各保険者が保有する（一方で、各保険者は、本人識別情報や他の保険者が管理する被保険者記号番号等を保有しない）。また、保険者のデータベースを集約・集積して情報を一元管理することは、

－プライバシーが侵害されるのではないかという不安を惹起する

－サイバー攻撃等の標的にされるおそれがある

ことから、年金・医療・介護に関する様々な情報を一括して保有する大規模なデータベースは設けない

・　これらを前提とすると、ＩＣチップ内に収録された本人識別情報をキーにして、各保険者に分散して保存されている情報に確実にアクセスする仕組みとして、アクセスを中継するためのリンクのみを保持する機能を持つ中継ＤＢが必要となる。中継ＤＢに様々な情報を持たせることは情報の一元的管理が行われるとの懸念が生じることから、中継ＤＢが持つ情報は本人識別情報、各制度の被保険者記号番号等（各種の公費負担医療も対象とする場合については、それぞれの公費負担者番号、公費負担医療受給者番号）といった必要最小限の情報とする

以上のように、中継ＤＢは、本人識別情報、各制度の被保険者記号番号等といった必要最小限の情報を保有し、それらをもとに利用者の情報へのアクセス要求を各保険者に振り分ける機能を持つ。この場合、各保険者が持つ被保険者記号番号等を各制度共通の統一的な番号で置き換えることも考えられるが、これについては、

・　情報漏洩の際に、各保険者が保有する情報がマッチングされ、利用者のプライバシーが侵害されるリスクが高まること。また、医療等の現場で活用する番号は可視的であることが求められること

・　仕組みの早期実現のためには、保険者のデータベースの改修を可能な限り小規模なものにすべきところ、より大規模な改修が必要となると考えられること

などの課題がある。

なお、~~保険者のデータベースについては、現在、複数の保険者が共同で運用を行っている例などが見られるところであるが、新たにこれを行うに当たっては、~~各保険者におけるデータベースの整備状況やセキュリティ対策の状況を踏まえ、複数の保険者が共同してデータベースを運用すること等の措置について~~る必要があることから、適切な共同運用の在り方等については~~、今後引き続き検討を行うこととする。

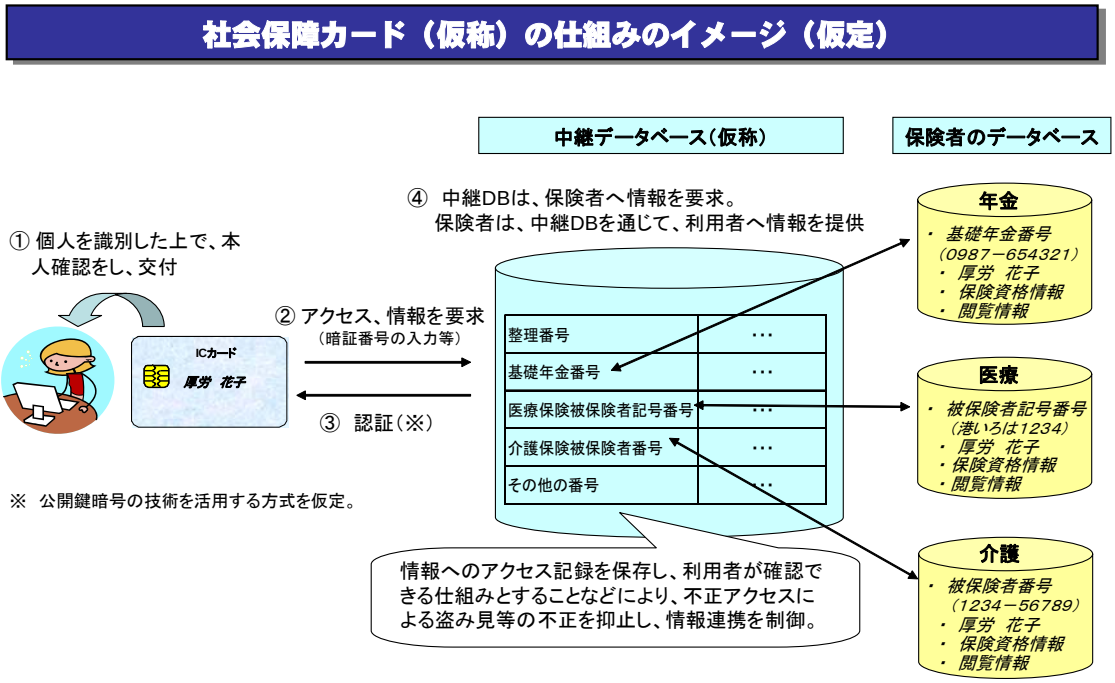

図２：社会保障カード（仮称）の仕組みのイメージ（仮定）

② 中継ＤＢの具体的な機能について

オンラインによる保険資格の確認については、医療機関等からの資格確認の要求を、中継ＤＢを経由して各保険者のデータベースにアクセスさせることで行う。

年金記録やレセプト等の情報を閲覧する際にも、各保険者が有する情報にアクセスすることになるが、各保険者のデータベースに個人が直接アクセスすることは利用者にとって不便であり、また、セキュリティ上も脅威が高まることから、中継ＤＢの仕組みを利用することにより、利用者の閲覧要求を中継する機能を持たせることが可能と考えられる。

上記に加え、中継ＤＢにおける自分のデータへのアクセス記録を保存することとし、その記録を自分自身で中継ＤＢのリンク機能を活用してポータルを通じて確認できる仕組みとすることで、不正アクセスによる盗み見等の不安を払拭するとともに不正を抑止する仕組みとすることが可能となる。

また、中継ＤＢを利用することで、各制度における保険者間や制度をまたがる保険者間の情報連携を円滑かつ安全に行うことができ、事務の効率化が可能となる。

中継ＤＢはこれらの機能を有するが、次世代電子行政サービス構想における「行政情報の共同利用支援センター（仮称）」や電子私書箱（仮称）構想における「電子私書箱（仮称）プラットフォーム」は、中継ＤＢと類似の機能を持つものと考えられることから、これらについては、重複した投資を避け、共通の基盤として構築することを目指すべきである。

なお、このように、中継ＤＢを置く仕組みとすることは、カードを使って新たなサービスを利用できるようにする際に、中継ＤＢに新たなサービスに関するデータベースへのリンクを持たせることでその機能を拡張することが可能であり、ＩＣチップ内に新たなアプリケーションを書き込む必要はないことから、将来的なカードの用途拡大に対応しやすい仕組みと言うことができる。

２．２　仮定の検証

２．１では、仮置きではあるが、社会保障カード（仮称）の仕組みのイメージを示した。今後は、平成 23 年度中を目途とした社会保障カード（仮称）の実現に向け、この「仮置き」の仕組みについて、課題を洗い出すとともに、対応策を検討する必要がある。

厚生労働省は、平成 21 年度に、社会保障カード（仮称）に関する実証実験を行う予定であるが、その実施に当たっては電子政府等の関連する取組との連携を図るとともに、実証実験の実施~~その~~状況や結果、サービスの体験者等の声を踏まえ、ＩＴの利用に不慣れな方等、様々な利用者への配慮が必要であることについても留意しながら、社会保障カード（仮称）の仕組みがより良いものとなるよう検討を進めていくことが必要である。

３．　年金記録等の閲覧について

現在、利用者が、各保険者の保有する自らの情報を取得する場合は、年金・医療・介護等取得を希望する情報の種類によって、それぞれ当該情報を保有する保険者に対して請求を行う必要がある。

オンラインによる年金記録等の情報閲覧[4]機能は、社会保障カード（仮称）の主要な機能の一つであるが、２．で述べた仕組みを活用すれば、利用者は、閲覧する情報によってそれを提供する保険者が様々であることを意識することなく、ワンストップで必要な情報にオンラインでアクセスすることができる。

ここでは、２．で述べた仮置きの仕組みに基づき、社会保障カード（仮称）を用いたオンラインによる年金記録等の情報閲覧の具体的な仕組みについて、セキュリティの確保や利用者の利便性を考慮しながら述べる。

なお、１．３で述べたように、社会保障カード（仮称）の仕組みに基づく情報閲覧を可能とするためには、その前提として、情報を提供する各保険者の環境整備（閲覧用データベースの整備、情報の標準化・可視化等）が必要となることに留意が必要である。

（１）情報閲覧に関するセキュリティ上の要件と対策

社会保障に関する情報はプライバシー性の高いものが多く、特に、年金記録や特定健診情報等は、健康保険証等に記載されている保険資格情報と比べ

[4] パソコン等の端末と社会保障カード（仮称）を使って、自宅などで、オンラインで保険者のデータベースにアクセスし、自分の情報を端末の画面上に表示して確認すること及び当該情報を取得することをいう。

て特に機微な情報であることから、自宅などからオンラインでこれらの情報を閲覧することができるようにするためには、セキュリティ確保のための措置を講じるとともに、オンライン上で厳格な本人確認を行うことが必要不可欠である。

オンライン上での厳格な本人確認については、既存の仕組みを最大限に活用し、費用対効果に優れた仕組みとする観点から、現在、電子申請において安全性と信頼性が確保された電子署名を行うための手段を提供している公的個人認証サービスを利用する方法等を検討する必要がある。

なお、公的個人認証サービスについては、利用サービスの拡大に向けた取組のひとつとして、オンライン認証の実現に関する検討が行われる予定であり、検討を進めるに当たっては、その動向にも留意する必要がある。

また、その他セキュリティ確保のための要件と対策としては、以下のものが考えられる。

【セキュリティ上の要件と対策】

① 正しいカードが、正しい所有者によって利用されていることの確認
端末や中継ＤＢ等のシステムが、カードの正当性の確認を行う等の措置をとるとともに、本人確認の観点からは、カードの所有者に、暗証番号（PIN）の入力等を求めることが望ましい

② 改ざんなどがない状態で正しい情報が確認できること
閲覧情報へのアクセス履歴を保存・確認することや、情報の登録・更新を行う者の正当性を確認する等の措置をとる

③ 悪意のある者や不正な機器からの攻撃に耐えられること
カードが、端末や中継ＤＢ等のシステムの正当性を確認するとともに、情報の暗号化やウイルス対策等を行うことが必要である

なお、これらの対策を講じた上で残るリスクや課題について、誰がどのように対処するかということに関しては、費用対効果の観点も含め、引き続き、総合的に検討を行う。