第３章　具体化の手法の骨格

基本構想に関する報告書に基づき、具体的な仕組みについての検討を行ってきたところであるが、その中でも特に中心となる部分につき、第３章で述べる。

（１）本人を特定する鍵となる情報（本人識別情報）について

第２章で述べたような社会保障に関する情報の可視化を進め、効率的にきめ細かなサービスを提供すること等を実現するためには、制度内・制度間での加入者特定が必要となる。

そのため、基本構想に関する報告書では、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）として、以下の５案を提示した。

> **案１　各制度共通の統一的な番号を利用**
> **案２　カードの識別子を利用**
> **案３　各制度の現在の被保険者番号を利用**
> **　案３―２　各制度内で不変的な番号を創設し、利用**
> **案４　基本４情報（氏名、生年月日、性別、住所）を利用**

この５案の比較検討を更に行ったところ、

・「案３：各制度の現在の被保険者番号」については、保険者が変わる都度、カードの書き換えの必要が生じること、
・「案３―２：各制度内で不変的な番号を創設」については、全ての医療保険者や介護保険者のシステム改修が必要となること、
・「案４：基本４情報（氏名、生年月日、性別、住所）」については、同姓同名同住所の例、外字の用い方による不突合等が起こる可能性があること

等を踏まえ、差し当たり、「案１　制度共通の統一的な番号[1]」又は「案２　カードの識別子」を基本として更に検討を進めることとした。

また、上記２案に加え「公開鍵暗号の仕組み[2]」を用いる方法についても、国際標準技術が確立しておりセキュリティを確保しやすいことから、併せて検討することとした。

---

1 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。

2 公開鍵暗号の仕組みを使って電子的に認証する仕組みをいう。本来、識別と認証は異なるものであるが、上述の統一的な番号や識別子と同様、識別のためにも用いることから、ここでは、識別する行為を含むものとして用いている。以下同じ。

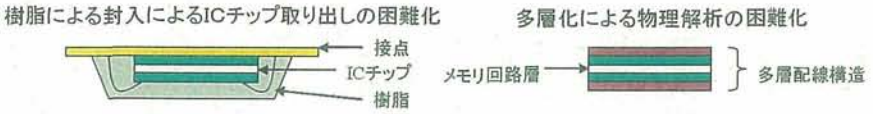
（２）ＩＣカードの活用について

ＩＣカードは、ＩＣチップ内に情報を収録することで視覚的に情報を隠すことができることに加え、不正な解析等に対する防御対策がなされた「耐タンパ性」を有するといったＩＣチップの性質上、偽造や不正使用が難しく、安全性が高いことから、一般的に利用されている。

ICカードの安全性

○耐タンパ性（ICカードを不正に解析する脅威等からの防御対策）

－チップを取り出した信号解析や顕微鏡解析による不正情報取得、消費電力や電圧および処理時間の変化からの情報や鍵の推定などの脅威等に対応した対策をしている。



○鍵（暗号鍵あるいはパスワード）の設定による利用条件制限

－情報が記録されるメモリ上のデータファイルは、ファイルごとに鍵を設定して保護される

－正しい鍵が確認された時に、鍵に応じた読み書きの利用権が与えられる

－あらかじめ設定された回数の照合や認証に失敗すると、鍵の利用を自動的に停止することが可能

※磁気カードやICタグは、読取装置があれば、データが読める
磁気カードライターは比較的簡単に入手可能で、偽造も可能
※メモリカードは、自由に読書き可能

その一方で、例えば統一的な番号やカードの識別子といった情報をそのまま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、住基カードのように専用端末を用いるなど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が、社会保障カード（仮称）については医療機関等で利用されることが想定されており、すべての医療機関で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ると、統一的な番号等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仕組み[3]を活用する方が、安全性においては優位であると考えられる。

---

[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。

ただし、将来を見据えた社会保障制度の有用な基盤として検討を進めつつ、当分の間は、情報化が進んでいない手続等と併存する期間が一定程度存在すること、様々な理由でＩＣカードの機能を利用できない事由も考えられることから、ＩＣカードの機能に依存しない方法も併せて検討を行う必要がある（ＩＣカードの機能を利用できない事由は第６章で詳述。）。

ＩＣカードの機能に依存しない場合における手続等の利便性や正確性の確保については、例えば本人識別情報をカードの券面等に記載して可視化した場合には、制度・本人の意図しないところで名寄せに使われるなどのリスクが高まる可能性が考えられる一方、何らかの可視的な番号等を情報連携のキーに利用することにより簡便な仕組みにすることができるとの期待もあることに留意する必要がある。

そのため、本人識別の方法としては、安全性に優れた公開鍵暗号の仕組みの利用を基本としつつ、必要に応じて可視的な番号等を用いることも検討の範囲からは除かないこととし、その適切な在り方についても併せて検討していくこととする。