我が国におけるEHRに向けた一考察

──社会保障カード構想を通じて──

中安 一幸

■ 要 旨

医療・健康情報を長期に亘り有用に活用したいとの取組はこれまでにも多くみられたが、近年、我が国においてもEHR(Electronic Health Record)にまつわる議論が各方面で進捗中である。社会基盤としてのEHRを論じようとするとき、厳格な本人識別とそれに基づく確かな認証が不可欠となるが、現下、医療分野に有用なID基盤が存在しない。

「年金手帳、健康保険証、介護保険証としての役割を果たし、年金の記録等を自宅においても常時、安全かつ迅速に確認できるものとしつつ、将来的な用途拡大にも対応可能なものとする。」とした社会保障カード構想は、EHRで用いるID基盤に最も近いものであると期待されたところであるが、この構想における検討をモチーフに、ID基盤の在り方と個人のプライバシー権の関係性、またそれらが内含する課題等について考察し、解決に向けた制度的検討、技術的検討の方向性を模索する。

■ キーワード

社会保障カード、EHR(Electronic Health Record)、ID、プライバシー権

社会保障カード(仮称)構想に至るまで

情報技術は日進月歩の進歩を続けており、情報を電磁的記録として保存する方法や媒体は、品質や使い勝手、安全性、低価格化という観点でも格段に向上している。

市場に新しい情報技術が紹介されると、それを医療分野でも活用できないかと考える向きが現れるのは至極当然のことであり、これまでのすべての発想が実現をみたわけではないが、そういった挑戦と失敗、ならびにその失敗の評価・分析なくしては、今日進捗しつつある医療のIT化はなかったであろう。

相当以前から、本人の医療情報を何らかの媒体に格納して持ち帰り、本人が参照したり、ほかの医療機関に提示して医療者の判断の一助としたりするなどのことが構想されてきた。浮かんでは消えていった過去のこのような構想においては、カルテデータを磁気テープに記録して持ち歩き、診療にかかる際にその記録を再生して提示するというようなものに端を発し、格納媒体も時代の変遷に応ずるようにさまざまなものが提案された。この段階までは「紙でもらえる医療情報をフォルダに挟んで持って帰る」ことと比べて、そう大きな違和感を覚えない。

その後、ネットワークと暗号というものが、一般的な用途に使えるまでに普遍化してきた頃から、それ以上の利便を要求することも可能になった。

「一般に情報化とは、情報のネットワーク化が実現されることにより、科学的、客観的データの蓄積が可能となるとともに、大量の最新情報がリアルタイムに伝送、共有されることが可能となることであり、医療分野においては、診療

情報の電子化・高速伝送・同時共有がなされ、最新医療情報の多方向アクセスが可能となることを意味している。これが医療に与える影響は多方面にわたるが、大別すれば、医療の質の向上、医療の効率的提供、という好ましい効果が期待できる。」「保健医療分野における情報化については、『情報の安全性の確保に留意しつつ、サービス利用者の立場から情報処理・通信の技術を活用して情報の高度利用を図ること』を理念とし、『保健医療サービスの質の向上』と『資源の有効活用による合理的・効率的なサービス提供体制の構築』を目的として進めることが適切であり、この理念、目的の意義はますます大きくなっている。」と述べた「保健医療分野の情報化にむけたグランドデザイン[1]」では、医療分野の情報化に向けたロードマップを年次ごとにマイルストーンを置いて示し、それが実現されていくとどうなるかを描いた。これの進捗、達成度を年度ごとに評価し、次のアクションにつなげるPDCAサイクルを確立しようとしたのが「e-Japan戦略」であったが、評価の指標としての「電子カルテの普及率」の数値管理に終始するあまり、この間、機能面の評価や、このキャンペーンが医療分野にもたらした副産物的効果などについてはあまり議論が深められてこなかったことは残念至極である。

これに対し、2006（平成18）年1月に発表された「IT新改革戦略[2]」では、ITを活用して医療をどうしたいのかということに主眼を移している。ITによる社会・経済の構造改革が主要なテーマになり、これに対しては当時、ITは単なる道具の位置づけになったようにみえ、IT産業界が期待するものでなくなったようにみえるとの意見も散見されたものである。しかしこういった意見はIT化される側、つまり医療機関側からみれば、闇雲に、言い換えれば誰も望んでいなくても進めようとする極めて単眼思考的な意見として映りかねない。政策としてのIT化、とりわけ、これまでIT化に積極的でなかった分野におけるそれは、IT産業振興のためだけに推進されるものではない（無論、そのことも目的の一つではあるが）ため、課題解決の道具として役立つからこそ広く活用されるべきとの方針転換を図るべく、ITの利活用に視点を移した「IT新改革戦略」はむしろ評価されてもよく、そのような流れは、これ以降示される戦略に引き継がれていくこととなる。

この頃から、ネットワーク越しの認証により医療保険の資格確認に使えるなどの用途が考えられるようになったことは、レセプト転記ミスによる「資格過誤」での返戻を減少させることを期待させ、このことは医療機関にとってはもちろん、審査機関などでも再審査などの手間や費用が減少するというわかりやすいメリットをもたらすものでもあった。医療機関と保険者をネットワーク化できるということになれば、資格情報の問い合わせにとどまることなく、レセプトそのものを伝送できるのではないかとの発想は、それを蓄積する必然を伴い、そうするとそれを単なる診療報酬の請求明細書として処理するのみでなく、二次的に活用して何かの役に立てようと考えるのはまた、当然の流れであると言える。

一方で健康増進・健康維持のための健診情報の長期的活用が構想された特定健診の制度が検討中でもあったこのとき、保険者や医療機関に散在する本人の医療情報にアクセスするためのキーとして構想されたのが「健康ITカード[3]」というものであった。医療機関における診療情報、保険者におけるレセプト情報および健診情報が電子化して蓄積され、ネットワーク化されて伝送して活用することの可能性が見え始めたこの頃、「保健医療分野の情報化にむけたグランドデザイン」に描かれたような情報化の姿がようやく具現化してきたといえる。

平成18年度に、3〜4年後の導入を目途として始まったこの構想は、折しも顕在化した年金記録問題の再発防止方策の一環として、また、当初に構想したサービス範囲と関係の深いほかの制度への適用可否の検討などを踏まえて、平成19年度には「社会保障カード[4]」の構想へと引き継がれる形で終結する。

EHRへのアプローチと社会保障カード

EHR（Electronic Health Record）については必ずしも確立された定義があるとは言えないながら、本特集では、別の項（山本論文）においてこれを試み詳述されているためそちらを参照されたいが、小括すると、おおむねEHRというものは、

① 医療機関などにおいて電磁的記録による医療情報の蓄積や提供が可能な状況にあって、
② それにより蓄積される医療情報を関係者間で適切に共有し、
③ 医療の効率化や質の向上、医学研究や医療政策のevidenceとして活用できるような社会基盤

を指すものであると考えることができよう。またそのような社会基盤が成立した折には、

④ 相当の長期にわたり本人の健康増進などのために電子化された医療情報を活用できるサービスを提供することまたはそのサービス

を指してPHR（Personal Health Record）というものであると思われる。

しかしこのようなことを構想するにあたって、長期にわたりかつ散在する情報を、間違いなく本人のものであると同定し続けることの困難さは、いわゆる年金記録問題を想起する限りにおいて想像に難くない。一方で、情報の提供者となる医療従事者や保険者に要求されている個人情報の取扱責任の重さに鑑みれば、適切な本人認証を経ずして機微な医療情報を安易に提供できようはずもない。また医療情報の公益に資する活用の場面においても、データの二重取得の防止や、公衆衛生上の観点から厳格な本人同定を必要とする局面も想起されるところである。

そうすると確実な本人認証・本人同定のためには、厳格な本人識別に基づいたクレデンシャルと、それを用いた適切な名寄せの手段が必要となることは論をまたず、そのための医療分野におけるID連携基盤の確立が必要となる。

これまで述べてきたような目的を達しようとする観点からは「医療分野におけるID連携基盤」として、「年金手帳、健康保険証、介護保険証としての役割を果たし、年金の記録等を自宅においても常時、安全かつ迅速に確認できるものとしつつ、将来的な用途拡大にも対応可能なものとする。」とした社会保障カード構想に寄せる期待は決して小さくはないだろう。

ではなぜ、EHRの構築を目指す観点から「社会保障カード構想」に期待が寄せられるのか。それは、必要不可欠ながら運用の仕方によっては重大なプライバシーリスクにも繋がりかねないID連携基盤の構築を委ねることができるからであり、EHR-IDとでもいうべきID基盤を別に作るとなるとそれだけで相当な労力を要し、社会コストを引き上げてしまうからである。そこに手間取って、例えば十年実現が遠のけば、十年間の貴重な情報が失われると言ってもよい。社会保障カード側からすれば、EHRの基盤として活用され、社会的価値が高まることはもちろん大歓迎であろう。

もとより筆者ごときが職責上、制度・政策を云々できる立場にないので、これより先の多くは私見となってしまうが、このような制度を設計するに当たって、十分に留意しておかねばないと考える点につき述べておくこととする。

EHR-IDとプライバシー権

我が国の医療制度は、フリーアクセスの確保を旨としてきた。医療自体は医師または医療機関という民間事業者によるサービスであっても、制度としては国民が医療を受ける機会を「いつでもどこでも誰でも」保障[5]しようというものである。したがって、国民皆保険体制にある上では、社会保障カードで医療保険資格を確認できるということは、「確認してよい権限を付されている限りにおいては」医療分野で患者を一意に識別でき得るIDであるということと意味的に大差ない。

そうすると、そのIDが盗み取られて制度や本人すら予期しない名寄せに用いられるようなことがあってはならない。また一方で、情報取扱者が相互に個人の情報を共有して事務を執るからこそ効率化が進むということや、患者の追跡性が向上することにより、治療成績の向上や医学研究の効率化が期待されるが故にEHRというものの構築を目指すということもまた事実であろうことから、万が一にも情報取扱者の恣意によりIDが運用されるようなことがあれば、それはある方面で「国民総背番号」などと言われるプライバシー上の脅威に繋がるおそれがある。

EHRにおけるIDが、専ら自らの情報へのアクセスキーとしての設計を念頭に置くはずのものであり、いわゆる国民総背番号制というものが、知らず知らずのうちに国家から一方的に管理されるという脅威を指すものであれば、決してそのようなことを目指すものでないことは明らかであり、そのことは社会保障カード構想においても同様である[6]。

それでもなお社会保障カードには反対であるとする意見もある。

その一つを挙げてみると、

「このような社会保障カードの『番号』が導入された場合、この番号は、

① すべての国民と在留外国人に付された、
② 原則不変の、
③ 重複しない識別番号となり、しかも、
④ 民間利用が前提となる

ものであるから、市民生活のあらゆる場面の個人情報とともに、この『番号』が記録されることになる可能性が高い。すると、この『番号』をマスターキーとすることにより、官民の保有する数多くの個人情報を検索・名寄せし、データマッチングすることが可能となる。しかも、データマッチングが行われうる情報には、病名、投薬名、受診医療機関名などのレセプト情報、特定健診情報、そして、勤務先などの年金情報という極めて要保護性の高い情報が含まれるのである。その上、「費用対効果」を考えれば、今後、社会保障カードの用途拡大が必須となってくる[7]。」というものである。

もともと、プライバシーの侵害には4つの類型があるといわれ、それはすなわち、

① 私生活に侵入されること
② 他人に知られたくないような私事を公開されること
③ 事実の公開により、真実でない誤った印象を与えること
④ 氏名や肖像を他人の利得のために流用されること

であるとされる[8]。

我が国ではこのプライバシーを侵害されない権利は、憲法13条により保障されているとされる。この権利とIDとの関係性については、平成20年の住基ネットにかかる最高裁判決[9]を巡り、種々の議論がなされているところである。

概説するとこの事案は、行政機関が住民基本台帳ネットワークシステムにより被上告人らの個人情報を収集、管理または利用することは、憲法13条の保障するプライバシー権そのほかの人格権を違法に侵害するものであるなどと主張

して、上記の人格権に基づく妨害排除請求として、住民基本台帳からの被上告人らの住民票コードの削除を求めたものである。この原告の主張を高裁が支持する判決を下した。しかし上告を受けた最高裁では一転、原判決を破棄、住民基本台帳ネットワークシステムにより行政機関が住民の本人確認情報を収集、管理または利用する行為は、当該住民がこれに同意していないとしても、憲法13条の保障する個人に関する情報をみだりに第三者に開示または公表されない自由を侵害するものではないとしたものである。

最高裁判決はこう述べた上で、住基ネットからの離脱を認めないとした主張を違憲でないとしたものの、この判決にはいくつかの問題があると多方面から指摘されている[10]とおり、IDそのものの問題がないと判示するものではない。EHRを構想するに必要であろうID基盤の構築が、最高裁判決を先例として、憲法13条との関係において、何らの問題がなくなったと考えることは、必ずしも妥当しないと考えるべきであると思慮する。

判例研究そのものが本稿の主たる目的でないため、あまりに深く立ち入ることは別の機会に譲ることとするが、最高裁が、原審の言うような「具体的な危険」があるとまでは言えない、とした要件は、制度として検討していく上での重要な留意点を示唆してくれる。

大きく言えば、それらは以下のように整理することができる。

① 4情報（氏名、性別、生年月日、住所）に住民票コードとその変更情報を加えたもの。これらはいずれも個人の内面にかかわるような秘匿性の高い情報とは言えない

② 個人情報を一元的に管理することができる機関または主体は存在しない

③ システム技術上または法制度上の不備があり、そのために（中略）具体的な危険が生じているということはできない

（a）本人確認情報の管理、利用等は、法令等の根拠に基づき、正当な行政目的の範囲内で行われている

（b）本人の予期しないときに予期しない範囲で行政機関に保有され、利用される具体的危険については、刑罰をもって禁止されている

（c）同じ領域に適用される一般法（個人情報保護法）と特別法（住民基本台帳法）がある場合は特別法が優先して適用される

住基コード（と4情報、住基コードの変更情報を加えたもの）の秘匿性はそう高くないと判示するが、それはあくまで、住民票コードとして住基ネット上で取り扱われるからであるということに留意が必要である。もともと、紙の台帳に記録されても序列がつくものであるし、何らかのデータベース上に記録しようとすれば、何某かのIDは付されているものである。問題となっているのは、住基ネットというネットワーク上で一意に識別されるという広範さである。EHRについて考えてみると、そのキーをもってさまざまな情報へのアクセスを可能にし、連携して個人情報を活用することを主旨とした情報基盤を構築しようとするものであるから、IDにより連携して活用される情報の範囲が、住基コードによって連携される行政情報よりもさらに広範になる点や、IDを利用する関係者も多岐に渡ることとなるため、キーとなるID自体の秘匿性が高くないと評価することは必ずしも妥当しないのではないか。なかんずく、多分野にわたる統一IDを多くの関係者で共有して用いるなどを想起する場合、IDの秘匿性を高く評価して対策を講じなければ、制度や本人が予期しない名寄せリスクの可能性は、飛躍的に高まるのではないだろうか。

そうすると、最高裁判決が示す当該要件の一

でも欠くこととなると、「具体的な危険がない」とは言えなくなることはもとより、住基ネットと同等の措置を講じていたとしても、その利用目的や利用範囲に照らして、具体的な危険がないとまでは言い切れない局面も起こり得るのではないかと考えるべきである。

しかも本人確認情報の管理、利用等は、法令等の根拠に基づき、正当な行政目的の範囲内で行われていなければならないのであるから、そろそろEHRというものの在り方について、法制上、どうとらえるのかということを考えるべき時期にきているのではないだろうか。

もう一つのプライバシー権

この最高裁判決を巡ってはもう一点、重要な議論がなされている。諸説あって必ずしも結論めいたものが得られているわけではないが、原審は憲法13条により保障される権利を「プライバシーを侵害されない権利」と「本人の情報をコントロールする権利[11]」の2つであると主張し、その保護を求めたものであるが、最高裁判決では「本人の情報をコントロールする権利(いわゆる『自己情報コントロール権』)」について、必ずしも精緻に論じられたわけでない[12]というものである。

もとより本件が、行政機関が住民基本台帳ネットワークシステムにより個人情報を収集、管理または利用することに対する人格権に基づく妨害排除請求として、住民基本台帳からの住民票コードの削除を求めた裁判であり、結局のところこれがプライバシーに関する権利のうち、「放っておいてもらう権利」と「自らの情報の消除(や開示、訂正等)を請求する権利」、すなわち自由権か請求権かのいずれを巡って争ったものかといったことについて、筆者のような専門外の人間にはこれ以上考察を深める手立てもないが、通常の使用場面において住基コードが主として行政機関内部における通牒として用いられることが多いのに対して、EHRで用いられるIDについては、正に「自己情報をコントロール」するためにこそ用いられることが多いと考えられる。住基ネットのケースはどうあれ、EHR/PHRに関して言えば、これを正しくとらえておかなければ、IDを設け運用することとそれに伴うリスクとの比較衡量が難しいのではないだろうか。

のみならず、収集、蓄積、伝達、開示等のそれぞれのプロセスにおいて、自己情報をコントロールしようとするならば、それが憲法に保障された権利であるからというばかりでなく、具体的な請求手続きなどについて別に法に定めるなどの措置が必要となろう。ここでもEHRが法制上どう位置づけられるか、公共の利益のために構築を目指す情報基盤の在り方と、個人のプライバシーに関する権利の保障と行使の方法をどのように整理するかという問題に行き当たる。

公共の利益と個人の権利

こういった公共の利益とプライバシーを論ずる上で、代表的なものをもう一つ挙げておくと、繁華街などの街中に設置された防犯カメラ[13]というものがある。

犯罪の抑止・防止は社会全体の願いであり、公共の利益であるし、住民一人一人からすればそれでも起きる犯罪に巻き込まれないか、巻き込まれても被害が大きくならないうちに素早く救出されるなどのことを願えば「防犯カメラ」がそこにあることは、個人にとっても「安心な社会」であるということになり、これは個々人の利益であるということになる。

しかし一方で、そこにいるだけで勝手に撮影されるということになる個人のプライバシーとの関係性を鑑みれば、運用に厳格な配慮が求め

られるところである。

これについては種々の問題を指摘する意見もありながら、紙幅の関係もあってここではその一々を取り上げて詳細に立ち入ることはしないが、その中にはただ反対だと主張するだけでなく、重要な論点を述べたものがある。引用すると、

「監視カメラがあっても、常に人がその映像をリアルタイムで見ていて、犯罪が起こったと言われたらすぐ助けに行けなければ『防犯』にならない。ロンドンでは監視カメラが本当に多いが、イギリスはそういう方向に向かおうとしている。日本はカメラだけ付けておしまいになっているケースも多いのではないか。

そのようなものは『防犯』になっていないので、実態に合わせて『監視』カメラと呼ぶべき。犯罪を起こす人は起こす必要があって起こしているのであって、監視カメラがあれば犯罪を起こさないわけではない[14]。」

というものであり、さらには

「イギリスでは撮られた人はだれでも申請すれば自分の映像をもらえるという仕組みがあり、一般人による1つの監視チェックである。」

と述べられている。

それを監視と呼ぼうが防犯と呼ぼうが、カメラが設置されていることで一定の犯罪抑止に繋がっている（当然にそれ以外にも考慮すべき要素はあるとしても）こと自体は否定されてはおらず、プライバシー上の問題があるからといってそれを除去せよというものではない。設置の本来の目的を達するために必要と考えられるはずの措置の不十分さを指摘し、運用に関する不安を払拭する具体的措置を講じる必要性を示唆するものである。

設置の目的といえば筆者も含めた「ただの一般人」を監視しようというものでないことはおそらくあるまい。

また運用に当たっては、一般的には記録された映像の取扱について明文化された規程があり、大抵はそれに反した扱いがなされれば罰則が適用される仕組みになっていることなどの措置が講じられており、その中では第三者機関による運用の監視について定められていることが多い。それでもなお本人による「監視の状況の監視」の方策を講じる必要があるとする意見は、絶対的な信頼を寄せられるべき職に就く者が不祥事を起こすこともあることに鑑みれば、（それが行政であるとしても）情報取扱者の悪意により不都合な事態（例えば個人情報の漏示や売買）が起きる可能性がないではなく、規程や罰則に一定の抑止効果が期待されるとはいえ、罰を受けることも覚悟で働かれる悪事はどうしようもない。さらには、情報取扱者の個人的な悪事ばかりでなく、独占的に情報を保持する組織・機関が暴走して、独善的にその情報を使う（例えば政府機関による国民監視）という脅威もあり得る。そういったときに、その機関の意を汲んで設置された第三者機関など、それを抑止できるのか甚だ疑問がある、との対立的構造から導き出されるものであるかもしれない。

EHRなどという制度の基盤構築にあたっては、情報取扱者による不用意なミスや悪意によって起こり得るすべてのリスクを想定し、取り得る限りの予防策を取っておくことは当然の配慮といえ、プライバシー情報というものは、万が一不都合な事態が起こった際には、本人にとっては深刻な被害をもたらしかねないものであり、医療・健康にかかわる情報はそのセンシティヴ性ゆえに要保護性の最も高いものである。社会保障カードの議論においてもそのことは重要視され、本人の情報（属性情報そのものを取り扱うわけではないが、本人識別情報によって、本人

の属性情報のコントロールを可能にするという意味において同義である)がどのように取り扱われているかを本人が確認できる仕組みを講じておく必要があることは、報告書[15]にも述べられているところである。

そのような監査や証跡管理という技術は「やったこと」の証明をするものであり、その精度というか確からしさを向上させることや、説明責任の一端として、理解しやすさを向上させることは可能でもあり、情報取扱者(この場合は政府機関等)に措置を義務付けることも出来ると考えられる。しかしどのようにその技術が向上しようとも、それが「全数であること」の保障などできようはずがない。「最近はやりのITでなら、なんとかなるだろう」ぐらいに考える人たちが多いかもしれないが、突き詰めれば「やっていないこと」の証明などできないという限界も存在するのが事実である。

そうすると、

① 「確認できる権利」が、対立的構造を示した上での権利であると、万一の不都合が起こったときにも「確認したのだからそれ以降の不都合はすべて患者の責任である」などと極端な解釈をするものとなってしまうこと

② 「取れていないログ」は当然に見せることもできないため「まだ隠しているだろう」と疑い続けられれば、情報取扱者としては隠していないことの証明ができず、途方に暮れることになること

などが懸念されるところである。

社会保障カードの報告書にある「本人の情報がどのように取り扱われているかを本人が確認できる仕組みを講じておく必要」というのは、制度の透明性を高め、制度への信頼性を向上させることを願って書かれたものである。

EHRのような制度は、「プライバシー上の不安」という不愉快さとトレードオフに、個々人の健康の増進という個の益、医学研究や医療政策、医療経済などがよくなるという公の益をもたらすことを目論むものである。それならば、自己情報コントロール権を確保する責任も個と公の対立的構造から導くものではなく、受益者を本人と政府とした信託における受託者の忠実義務の一つであるというように考えるわけにはいかないものだろうか。

社会保障カード構想のすがた

ところで「社会保障カード」という語感からは、「ICカード」であるという即物的な議論ととらえられがちであるが、当然ながらこの構想の主役はICカードそのものではない。

医療機関、各種保険者、行政機関その他の関係者の情報化が完成し、ネットワーク化されており、それらのデータベースにアクセスするための認証手段や、情報伝達のために必要な用語、コード、データ項目、それらが伝達された際に人手を介さずとも機械可読な形式のメッセージ構造、などの種々の取り決め、すなわちさまざまな標準化がなされた上で情報の相互運用性が確保されており、セキュリティポリシ、プライバシーポリシ、SLA[16](Service Level Agreement)等の整備がなされることをもって情報化の基盤整備が整った上で「本人が保険資格を有することを主張できるようになっている仕組み」や「本人が散在する本人情報を手許に引き寄せて活用できる仕組み」の基盤整備こそがその本質である。

しかしセンシティヴ情報を巨大な「個人情報一元化データベース」にしてはならないことは、先の最高裁判決にも述べられているとおりであり、情報セキュリティ上も好ましいことでもない。そうすると、各情報保持者が自らの責任で情報を保持したまま、適切な認証を経て、情報の開示や共有をするための仕組みが必要である。

そのような仕組みは、国民の誰でもが利用できるユニバーサルサービスであらねばならないため、利用の不便は極力排さなければならないが、反面、これまで述べてきたような制度上の課題を多く抱える高度なセンシティヴ性を有する情報を扱うシステムである。加えて、第三者機関を設置するとか罰則を付した法制上の措置などを十分に講ずるとしても、医療情報は暴露による被害の救済が困難なケースがあり得る。

事後規制で十分な保護が働かないケースがあり得るのであれば、不都合な事態を招きそうな不注意や悪意による取扱を可能な限り排除するシステムを構築するほかない。このような場合、技術面の検討の重要性は、制度的検討に勝るとも劣らない。

何であれ、情報システムを通じてサービスを受けようとすると、アクセスの制御というプロセスが必要である。大きく言えばこれは「識別（identification）」と「認証（authentication）」と「認可（authorization）」、それを「監査（audit）」する仕組みからなる。ここでは差し当たり簡単に、識別とは本人を間違いなく実存する本人であると同定すること、認証とはアクセスしてきたのがその本人であることを認識すること、認可とは本人確認ができたのでサービスの提供（データを読んだり、プログラムを実行したりすること）を許可すること、監査とはそれらのプロセスとどのようなサービスを利用したかを記録しておくこととしておく。

そもそも、社会保障カード構想のような社会システムを設計するとき、使用場面ごとにどのような手続きとなっていて、どの程度の信頼確認を要しているかを見極めなければならない。社会保障カードの活用事例の中でも代表的な「医療機関における医療保険資格の資格確認」を例にとってみれば、保険資格情報を医療機関端末に返さねばならない保険者が、資格確認要求をどう信用して情報を開示するかということになる。

(a) カードの正当性と所持者との結びつき
(b) カードとカードリーダ、医療機関のワークステーション端末の結びつき
(c) 医療機関内のネットワークと職員のログイン等認証、情報取扱の権限管理
(d) 医療機関と中継データベース（仮称）と保険者の間のネットワーク
(e) 中継データベースによるID連携の確からしさ

これらの一つでも信頼に足る状況になければ、IDを「認証」して情報の開示を「認可」することができない。これに加えてIDそのものが厳格な本人識別に基づいているものかどうか、そのIDの格納・送出が適切でなりすましなどの脅威が排されているかどうかが信頼の根拠となる。

「ICカード」はそのような情報基盤において、所持者（申請者）が確実に本人であることの証明書であるID、すなわち「アクセスキー」を格納しておく媒体に過ぎない。

とはいえ、プライバシー情報のうちでも、最も機微なものであるとされる医療情報へのアクセスをなさしめるものであるから、相当に厳格な本人確認を経て発行され、間違いなく正当な所持者に交付されており、その正当な所持者がカードを行使していることが担保されていなければ、サービス提供者はこれを信頼して認証することができない。ICカード自体の発行・交付プロセスの信頼性と媒体そのものの耐タンパ性（内部の情報を読み取ろうとする行為に対する耐性）が高次に要求されるのは当然のことである。

言わずもがなこういった検討の過程においては、種々の媒体について比較検討を加えている。券面への番号記載と目視または口頭告知による運用等は本来の目的外の利用を抑制し難いこと、情報取扱に関係する人間を増やすこととなることがかえってセキュリティホールとなりかねな

いことなど、また磁気カードについてはスキミングのおそれがあるため、金融系のカードがICカードに移行し、もはや一般的となった経緯を踏まえると、選択肢からは除外してもよいのではないかと思慮されるところである。USBトークンといったものも考えられるが、関係機関(端末)が相当の多数になることを考えると、インストールを必要とするような運用は現実的でないと考えられる。

ICカードについては、昨今、媒体そのものについても動作を定義するアプリケーションなどについても各方面で規格化されており、それらを適切に引用することにより、安全性についての説明責任を果たすことが容易となるというメリットもある。

そうしたことから、現在はこれが適していると考えられたものであるが、こういった構想が具現化する際に、さらに優れた媒体があったとしたら、それを採択することに何らの躊躇がないであろう。

医療情報の取扱にまつわるルールやそれを扱うに適したネットワークなどについては、関係各省からガイドラインなど[17]が公表されているため当然にそれに従うものとして、ここでは詳細に立ち入ることは控えるが、その余の重要な技術的論点としてはID連携とSSO(Single Sign-On)の仕組みに関することがある。SSOとはいくつかのサービスに認証、認可を要求する手続き(サイン‐オン)を、利便に鑑みて1回で済ませようというものであり、このことも社会保障カード構想の要求事項である。

IDというのは情報システム上で本人を一意に特定する情報、と解してよい。社会保障カード構想のような情報基盤においては、それによりアクセスされる情報の機微性に鑑みれば、そのIDは厳格な「識別」を経ていなければならないと言える。その主な用途は、

(a) サービスを利用するための認証や認可
(b) 制度間や制度内の組織間での給付に関する情報連携

の2つである。

これらの用途からすると、(a)に用いるときには他人に知覚され、本人も制度も予期していないような名寄せに使われるなどのリスクがあることから、秘匿性こそが重要であり、(b)に用いるときには情報を保持する関係者(この場合は保険者等)には通知されないと情報連携に必要な情報共有や開示のための認証も認可もできないということになる。この場合、システムやネットワークの障害や異常に対する対応も考慮しておくと、人が確認できることが必要な局面も想定される。

このように秘匿と公開という二律相反する性格をもつIDが必要であるが、一つの番号や識別情報をもってそれとすることは実はかなり困難を伴う。

このようなIDを用いることによって発生する、名寄せやなりすましといった脅威を防ぐためには、

① 認証や認可(用途a)と情報連携(用途b)のための情報を分離すること、
② 認証や認可にかかわる情報を秘匿すること、
③ 認証や認可にかかわる設定権限を脅威となりえる者に与えないこと、

の三つのことが必須である。

社会保障カードにおいては、IDを可視化しないで用いる(IDを用いたと同様の効果を得る)ため、PKI[18](Public Key Infrastructure;公開鍵基盤)という暗号技術を使うことが検討された。ICカードが「電子証明書の堅牢な格納媒体」だとして、一応、本人が送出するIDは秘匿できたとしよう。それのみをもってして安全で利便性の高いID連携が完成するというわけではない。そこで構想したのが「中継データベース(仮称)」という仕組

みである。中継データベースは文字通り、本人と保険者等のサービス提供者の中間に位置するものと考えていただきたい。紙幅の都合から簡単に概説しておくと、

(a) 本人からPKIによる認証を要求された中継データベースは、認証できた上でポータル画面からサービス(医療保険か年金保険か、など)をメニューとして提示する

(b) 中継データベースは認証できた本人が選択したサービスへの接続を認可するため、当該保険者が従前から使用している被保険者番号で、保険者のデータベースにアクセスの許可を求める

(c) 本人からの情報開示の要求ならば、保険者データベースは認証でき次第、開示を認可することになる(サービス認証、認可にかかわる情報は秘匿されたままである)

(d) 保険者A‐保険者B間で情報の連携が必要な場合、本人のIDは秘匿されたままであるから使えないこととなる。そこで保険者Aは中継データベースにアクセスし、中継データベースが提供する「仮名」を用いて保険者Bに認証を要求し、保険者Bは中継データベースが提供する「仮名」と被保険者番号の結びつきをもって認証し、情報の送出を認可することになる

一見、複雑な仕組みであるが、例えばSAML[19]という技術と、それを活用したID-FF[20]というシングルサインオンのフレームワークにより実装が可能である。

このようなことを思慮に含めると、その構想の外観は、おおむね「社会保障カード(仮称)の基本的な計画に関する報告書」にあるような姿となる。ただし、この報告書については、未確定の種々の要素につき、さまざまな仮定を置きながらの検討の途上にとりまとめて公表したものである。

この報告書において仮定としたさまざまな構成要素を検証すべく、2009年度から実証事業を開始したところであり、本年はその2年目に当たる。

実証事業の実施にあたっては、事業のねらいとして以下の4点を掲げて公募した。

① 社会保障カード(仮称)の在り方に関する検討会において仮定した中継データベースなどのシングルサインオン・関係機関の情報連携の仕組みが実際に機能することを検証すること。

公開された標準による連携方式であるSAML2.0/ID-WSF[21]2.0方式を標準仕様とし、また、シングルサインオンの実現方式は、SAML2.0方式を標準仕様として「中継データベース」を構築することを実証事業受託者の公募における要件としたところである。

これについては、既存の規格、特定の技術の採択を強制するものでないため、これによらないほかの方式で中継データベースを設計することは、提案の評価には一切影響しないこととしたが、これによらないこととした理由と併せて、実装を予定する方式を前述との対比において説明することを必須とした。つまりこれは、「社会保障カード(仮称)の基本的な計画に関する報告書」で仮定した仕組みの有効性の検証と、ほかの方策による利便性、安全性の比較検証を実施するための配慮である。

② 社会保障カード(仮称)が便利で安心安全なものと利用者に実感してもらうこと。

これは、実証事業において、最も重要な検証項目である。通信や認証、セキュリティ等に関する技術的検証を行うのは、この項の検証のためであると言っても差し支えない。アプリケーションの開発実証でも単なるシステム検証でもなく(もちろん必要なセ

キュリティにおける論点等の課題は検証するが)「社会保障カード」という基盤があったとしたら、基礎自治体の業務が、医療機関における医療サービスが、住民の受療行動や健康増進への取組や意識が、どう変容するかをうらなう社会実験である。

③ 社会保障カード(仮称)を導入するにあたっての制度運用面等での課題を抽出すること。現下は存在しない「社会保障カード」というものがあったとしたら、という将来構想に向けた実証であるため、現下の規制の過不足がこういう情報化基盤の構築において不都合があるとすれば、それを抽出しようというものである。

④ 実証事業終了後も、当該地域における公共サービスとして継続し、社会保障カード(仮称)の発展的活用のモデルとして機能すること。

7つの地域で実証事業を展開したが、サービスやシステムの構成に、統一的・画一的なモデルの実施を強制しなかった。複数箇所に同じようなものを作ろうとしても、それぞれの地域において医療・健康・行政等の抱える課題等はさまざまであろうし、課題なきところに解決方策は必要ない。何らかの課題解決のために情報化基盤を望むならば、地域に特性が見られて然るべしである。ユニバーサルサービスである「社会保障カード構想」の基盤の上で、それぞれの地域に独自の医療・健康・行政等アプリケーションを配置すれば、地域の社会保障情報基盤として定着するかの創意工夫を各コンソーシアムの特色として評価するものとした。加えて、実証事業が終期を迎えても現地で自活し、公共サービスとして拡張でき得るビジネスモデルの提案力も必要とされるところである。

これまでの社会保障カードに関する検討の方向性を確かめるべく、報告書[22]をライン・バイ・ラインに分割し、検証項目として各コンソーシアムに割り振って実証せしめる方法を採り、報告書にある方法によらない構築をするコンソーシアムは対案の比較検証となるよう調整を図り、このような制度に対する社会的受容性等の懸念や円滑な導入に向けての課題について明らかにし、社会保障分野の情報化基盤の制度設計において大いに参考にしようというのが、本事業の目的である。

各コンソーシアムは、社会保障カード構想を基盤に、地域ごとの住民ニーズを踏まえ創意工夫を凝らした、いわば「社会保障カード＋α構想」を事業展開した。単なるシステム検証や、医療連携のモデル事業でなく、地域の保険者、行政、何より住民も加わっての、この「＋α」の社会実験こそ、EHRへのトライアルではなかろうか。

社会保障カードについては2009年11月12日の行政刷新会議による「事業仕分け」において次年度の予算計上を見送ることとされた。とりまとめコメントは「来年度の予算計上は見送る。新政権のもとでの方針をしっかり守って、また、省内及び省庁間ですりあわせて、予算要求をしていただきたい。」というものであった。構想自体を廃止せよということでなく、現政権下の他の政策との整合を図り、あらためて検討せよとの指示が含まれる。

制度が複雑化し、さまざまな課題を抱える社会保障分野において、社会保障カードのような基盤は作ることのメリット云々以前の問題として、現下、ないことのデメリットが大きすぎるため、いずれ必要であると考えるが、そうすると今後の議論の方向性が、果たしてEHRに適したものとなるかどうか、ID基盤の設計上、EHRをその射程に含めた制度設計になるかどうかが肝要である。

そう考えれば、現下の社会保障カードとEHRは必ずしも一体不可分のものではなく、その性格の違いから一定の距離を置いていることが必要ではないだろうか。

一定の距離、とするのは、社会保障カード構想が潰えたとしても、EHRは我が国の医療政策上、必要なものであろうし、EHRを意識しなくとも社会保障カードのような情報連携の基盤は必要であろうと思慮されるからである。

要すればこの2つは、道路と旅客・運輸等のサービスのような関係にあると考えればよい。道路自体は何も稼ぎださないし、建設予定地やその周辺の住民には迷惑ですらあるかもしれない。完成した折にはその上を自動車が走り、旅客や運送の利便、効率が向上し、道路の接続先には観光産業の確立や工業の誘致などの経済的効果をもたらす可能性がある。

道路の費用対効果を論ずる際に、活用の度合いとそれがもたらす経済効果の見込みを示さねばならないが、サービスからすればその道路を通らねばならない理屈はどこにもない。仮に道路の建設計画が遅れようともサービスに適さない道路になったとしても、コストの二重化を恐れないなら別の道を作って通ればよく、その先にニーズがあるならばサービスが道路と共倒れになる必要などないのである。

しかしそうなると、利用の見込みの立たない道路の費用対効果は格段に落ち、あまりに費用対効果に乏しい道路は建設の計画自体も批判を受けることとなろう。

先の最高裁判決を見ても、ID基盤を構築してから後に、広範にIDを利用するような用途を追加することには、それなりの困難を伴いそうである。最初から適さない基盤を構築してしまわないためにも、そろそろEHRが何のために作られるのか、誰を関係者として、どう作るのかといった議論が成熟し、要件が示されることが必要な時期に来ているのではないかと考える。

注

1）厚生労働省「保健医療分野の情報化にむけてのグランドデザイン（第一次提言）について」, http://www.mhlw.go.jp/houdou/0108/h0808-4.html

2）首相官邸高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）「IT新改革戦略」, http://www.kantei.go.jp/jp/singi/it2/kettei/060119honbun.pdf

3）当時の検討概要については，例えば「平成19年度第1回医療評価委員会（平成19年7月2日開催）資料4」など.
http://www.kantei.go.jp/jp/singi/it2/iryou/kaisai_h19/dai1/siryou4.pdf

4）「社会保障カード（仮称）」そのものについては，紙幅の関係からここでは深く立ち入ることはしない. 概要については以下を参照されたい.
「社会保障カード（仮称）の基本的な構想に関する報告書について（平成20年1月25日 厚生労働省）」, http://www.mhlw.go.jp/shingi/2008/01/s0125-5.html
『「社会保障カード（仮称）の基本的な計画に関する報告書」の取りまとめについて（平成21年4月30日 厚生労働省）』, http://www.mhlw.go.jp/shingi/2009/04/s0430-4.html

5）国民皆保険体制のほか，医療者の応召義務等（医師法19条，薬剤師法21条，等）による受療の機会の確保，特定の医療機関等への恣意的な誘導を禁ずる等（保険医療機関及び保険医療養担当規則2条の5，保険薬局及び保険薬剤師療養担当規則2条の3第2号）による選択の確保，高額療養費制度等による.

6）前掲注4）.

7）水永誠二＝吉澤宏治「なぜ，今，社会保障カードなのか？」（自由と正義60（5）（通号724）　日本弁護士連合会2009年）21頁.
このほか，日本弁護士連合会「『社会保障カード（仮称）』に関する意見書」（平成19年12月13日）, http://www.nichibenren.or.jp/ja/opinion/report/data/071213.pdf
同「『社会保障カード（仮称）の基本的な構想に関する報告書』に関する意見書」（平成20年8月27日）, http://www.nichibenren.or.jp/ja/opinion/report/data/20080827.pdf
などが同様の指摘をする.

8）William L.Prosser, Privacy, California Law Review, Vol.48, No.3, 1960.

9）平成19（オ）403　平成20年03月06日　最高裁判所第一小法廷判決　民集　第62巻3号665頁.

10）例えば，田島泰彦「監視社会のなかのプライバシーと住基ネット」(自由と正義60(5)(通号724)　日本弁護士連合会2009年)9-16頁，右崎正博「住基ネットとプライバシー・再論」(獨協ロー・ジャーナル(4)　獨協大学法科大学院2009年)3〜12頁，佐伯彰洋「住基ネット訴訟の論点」(同志社法学60(3)(通号328)　同志社法学会2008年)1175〜1219頁，羽渕雅裕「住基ネットのプライヴァシー性」(帝塚山法学(15)　帝塚山大学法学会2007年)1〜30頁，などを挙げておく．

11）右崎正博「住基ネットとプライバシー・再論」(獨協ロー・ジャーナル(4)　獨協大学法科大学院2009年)5〜6頁，「高度情報通信社会といわれる現代にあって，個人が人格的自律を確保していくためには，プライバシーの権利の保障が不可欠であり，かつてプライバシーの権利は，『一人で放っておいてもらう権利』と観念されたが，高度情報通信社会といわれる現代においては，より積極的に『自己の存在にかかわる情報を開示する範囲を選択できる権利』ないし『自己に関する情報をコントロールする権利』ととらえ直され，個人についての情報の取得・収集，保有，利用・伝播のすべての段階に及ぶと考えられるようになっている．
つまり，プライバシーの権利には，重要な一内容として『自己に関する情報の流れをコントロールする権利』(自己情報コントロール権)が含まれているとするのが，学説のほぼ一致した見方である．」とする．

12）このことを批判する意見も多くみられる一方，「自己情報コントロール権については，法文上の根拠が存在せずその内容，範囲，法的性格に関しては様々な見解があり，権利としての成熟性が認められないから，未だ実体法上の権利とは認められない．そもそも，プライバシーの法的保護の内容は，みだりに私生活(私的生活領域)へ侵入されたり，他人に知られたくない私生活上の事実又は情報を公開されたりしないことを中心的利益とする消極的自由権として把握されてきたものである．自己情報コントロール権を認める見解が主張する個人情報の開示請求権・訂正請求権は，憲法13条の文言解釈を逸脱するものではないかとの疑問があるし，民事法上も極めて困難である．」として最高裁判決はそれらを考慮したのではないかとする意見がある．
工藤敏隆「最近の判例から　住基ネット訴訟最高裁判決」(法律のひろば61(8)　ぎょうせい2008年)62頁．
この意見前段に関して，「自己情報コントロール権」の提唱者である佐藤幸治京都大学名誉教授は以下のように述べている．
「独自の権利であるという以上，できる限り特定性・明確性を備えたものでなければならない．『自己情報コントロール権』説はその結果ですが，その性質上請求権的側面も持ってくることになります．ところが，従来の憲法学では，権利が自由権か請求権かといった厳格な類型論が支配的であり，ここでもすっきりしない主張として受け止められたようです」「自己情報コントロール権につきまず浴びせられた批判は，『情報』の範囲がはっきりしない，『コントロール』といっても何をどのようにコントロールしようというのか明確でない，ということでした．」．
堀部政男＝佐藤幸治「情報ネットワーク法学会特別講演会『個人情報保護，自己情報コントロール権の現状と課題』憲法13条と自己情報コントロール権」(NBL No.912　商事法務2009年)17頁．

13）例えば「街頭防犯カメラシステム」(警視庁ホームページ)，http://www.keishicho.metro.tokyo.jp/seian/gaitoukamera/gaitoukamera.htm

14）田島泰彦＝吉田柳太郎＝高間剛典＝清水勉「ユビキタス社会と法ー座談会」(自由と正義60(5)(通号724)　日本弁護士連合会2009年)21頁．

15）前掲注4)．

16）ここではサービスを提供する者と受けるとの間で，サービスの内容と範囲，品質等に要求される水準を明確にして，あらかじめ合意しておくことを指して用いた．当初に合意しておくだけでなく，継続的に見直しも図られることが望ましい．

17）「医療情報システムの安全管理に関するガイドライン第4.1版(平成22年2月 厚生労働省)」，
http://www.mhlw.go.jp/shingi/2010/02/s0202-4.html
「医療情報を受託管理する情報処理事業者向けガイドライン(平成20年7月 経済産業省)」，
http://www.meti.go.jp/policy/it_policy/privacy/080724iryou-kokuzi.pdf
「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン(平成21年7月 総務省)」，
http://www.soumu.go.jp/main_content/000030806.pdf
など．

18）暗号化(encryption)，デジタル署名(digital signature)，認証(authentication)　といったさまざまなセキュリティ対策を実現するため，公開鍵暗号という暗号技術を用いた通信社会上の基盤．

19）「Security Assertion Markup Language」の略．「OASIS(Organization for the Advancement of Structured Information Standards)」という，webサービスやそれに用いるXMLなどの使用に関する国際標準化団体で策定されたセキュリティ情報(認証，属性，

認可）の交換のXML言語の一つであり，個人情報をきめ細かく管理し，制御することを想定したもの．

20）「Identity Federation Framework」の略．ユーザー認証技術の標準化団体Liberty Alliance Projectが提唱するSSOを実現するための仕様群であり，連携ID，SSO，シングルログアウト等を規定し，IdP間連携，IdP匿名認証を可能にする．

21）「Identity Web service Framework」の略．Liberty Alliance Projectが公表した，認証機能付きWebサービスを展開するためのオープン標準仕様ベースのフレームワーク．パーミッション・ベースの属性共有，認証ディレクトリ・サービス，相互作用サービス，セキュリティ・プロファイル，対応クライアントの拡張といった内容を扱っている．

22）前掲注4）．

（なかやす・かずゆき　厚生労働省
政策統括官付社会保障担当参事官室主査
東北大学大学院客員准教授）