日本型セルフケアへのあゆみ

児玉龍彦
東京大学先端科学技術研究センターがん・代謝プロジェクトリーダー
日本セルフケア推進協議会業務執行理事

人生において，元気でいることは誰にとっても大事なことである．自分の健康と病気に関わることは正確に知りたい．さまざまな薬や治療法があるなら，自分の希望で決めたい．そうした願いをもとに，大きな転換がはじまろうとしている．インターネットの普及により，医薬品・健康食品・病院に関する情報に誰でも容易にアクセスできるようになったが，正確性に欠けた情報も溢れかえっている．本シリーズでは，地に足をつけた“日本型セルフケア”へのあゆみを提唱していく．

第2回 電子カルテをスマホでみる
――確実な個人認証には何が必要か？

POINT

- **飯田市を中心とする南信州広域連合などで，各医療機関を結ぶ電子カルテのクラウド化が進んでいる．その利便性を最大限にいかすと，患者の許可のもと，カルテや処方箋をさまざまな医療機関で利用できるようになる．**
- **患者の許可を得るにあたり，個人認証をどう行うかが課題となる．政府はマイナンバーを用いた認証を進めようとしているが，アメリカで全国民の約半数，1億4千万人分の社会保障番号が漏出した事例を踏まえ，生体認証の重要性が注目されている．**
- **確実な個人認証には，「知識」「所有物」「身体的特徴」の3つの組み合わせが望ましいとされる．保険証（またはマイナンバー）と生体認証付きのスマホの組み合わせが最も現実的だが，スマホを持っていない場合は固定式のFAXとの組み合わせなどが代案となる．**

地域で進む電子カルテ共有：南信州の例

長野県南部にある飯田市は現在，東京-名古屋間のリニア新幹線の新駅ができることで脚光を浴びている．飯田市を中心とした市町村で構成される南信州広域連合（**図1-A**）は，実は電子カルテ化の先進地域としても注目されている．

南信州広域連合は1,929 km^{2}と香川県よりも大きな地域をカバーするが，信州大学附属病院（松本）や愛知県がんセンター（名古屋）などの高度専門医療を担う医療機関との距離が遠く離れるという問題がある．そうした背景から，産科や救急において，病院間および病院-開業医間の連携がいち早く進んできた歴史がある．たとえば産科では，妊娠8カ月ごろまでの健診などを各地域の診療所が担い，以降分娩までを飯田市立病院が担うという連携が行われている．さらに最近では，介護施設やケアマネジャー，また調剤薬局も巻き込んだ連携が進もうとしている．

2009年，地域での電子カルテ共有の先がけとして，飯田市民病院を中心に［ism-Link］（イズムリンク）という診療情報の連携システムの検討がなされ，2011年には情報開示6病院を中心に本格的な運用がはじまった[1]．2016年4月に南信州広域連合に事務局が設置され，在宅医療と介護の推進協議会の小委員会で，システムの改善が進められている．2021年の次期システム更新へ向けて，残る2つの基幹病院も参加して「地域の医療，介護情報インフラ」として適切なシステムを作ることが検討されている．

図1-B，表1に示すように，地域の病院は100%，診療所の65%，調剤薬局の93%，訪問看護ステーションの100%，そして患者だけでなく

[1]：南信州在宅医療・介護連携推進協議会，飯田下伊那診療情報連携システム運営小員会．〈2018年度〉ism-Linkの検証．（http://ism-link.minami.nagano.jp/wp-content/uploads/2019/06/2018_ism-link_usage-verification.pdf）

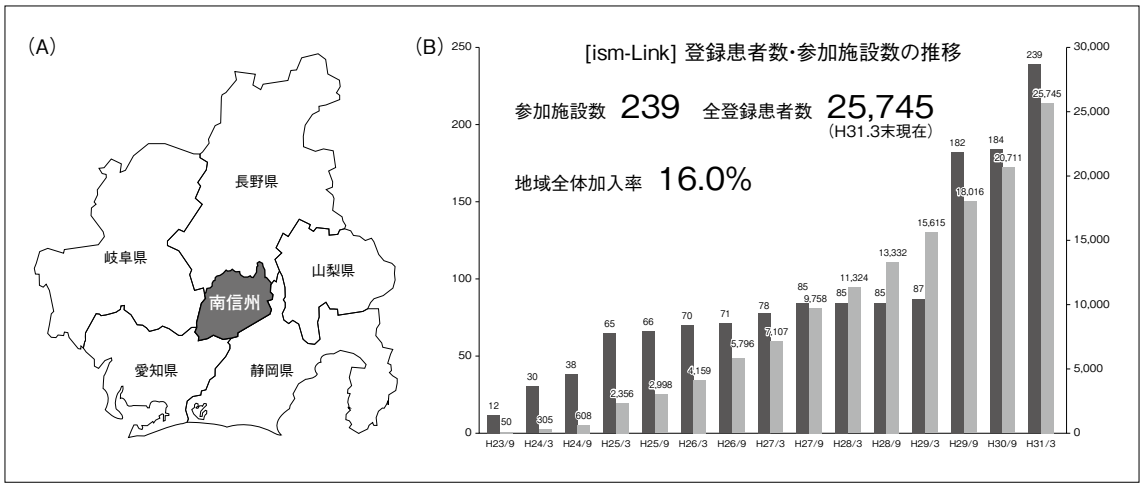

図 1　南信州広域連合と医療情報ism-Link
A：カバーする地域．B：登録患者数と参加施設数の推移．

表 1　ism-Linkの参加施設

施設	参加施設数	参加率
病院	10	100
診療所	68	65
歯科診療所	24	29
調剤薬局	59	93
訪問看護ステーション	7	100
介護関係事業所	66	54
その他(圏域外の施設)	2	
合計	239	

数値は出典[1]の原文ママ．

全住民の16%が情報の利用に参加しているという先進地域となっている．また医師や看護師だけでなく，調剤薬局の薬剤師，介護関係者の参加も増えている．いわば，地域の健康，医療のインフラとして欠かせないものになっている．

安全に診療データを送るには

こうした取り組みの次の段階は，診療や処方箋のデータを地域住民が自ら利用できるようにして，さらなる利便性をはかることである．しかし，たとえば病院から薬局へ処方箋を送ってもらうにあたり，目の前の患者が本人かどうかの認証が必要になる．検査結果や処方箋は究極の個人情報でもある．制がん剤を投与していることがわかれば，その患者がどんながんに罹患しているのかも推測できてしまう．電子カルテのクラウド化と多施設での共有が進むほど，安全性の高い認証システムが必須となる．

電子カルテのネットワークに病院，医院，歯科医院，介護施設，訪問介護ステーション，調剤薬局が加わることは，セルフケアを大きく変革するであろう．たとえば，病院-調剤薬局で情報をシェアすることで，一包化などの希望があった場合に逐一医師に書き換えてもらう必要がなくなるなど，患者の細やかなニーズに迅速に対応できる可能性がある．すでに薬局チェーンでは処方履歴をスマホの電子お薬手帳でみれるサービスを展開しているが，各チェーンで仕様が異なるため一元化して管理できないなどの課題が指摘されている．南信州広域連合では，地域内のどの病院の院内処方でも，どの薬局での調剤でも，まとめて参照できることをめざしている．

南信州だけではない．すでに，全国の多くの病院で，電子カルテをスマホでみられるようにする取り組みが進みつつある．愛知県一宮市の社会医療法人・大雄会は，2019年4月に，検査画像や診察履歴をいつでもスマホでみられるサービスをはじめた[2]．3月下旬から登録を受け付け，5月時点ですでに520人が利用している．大雄会とサービ

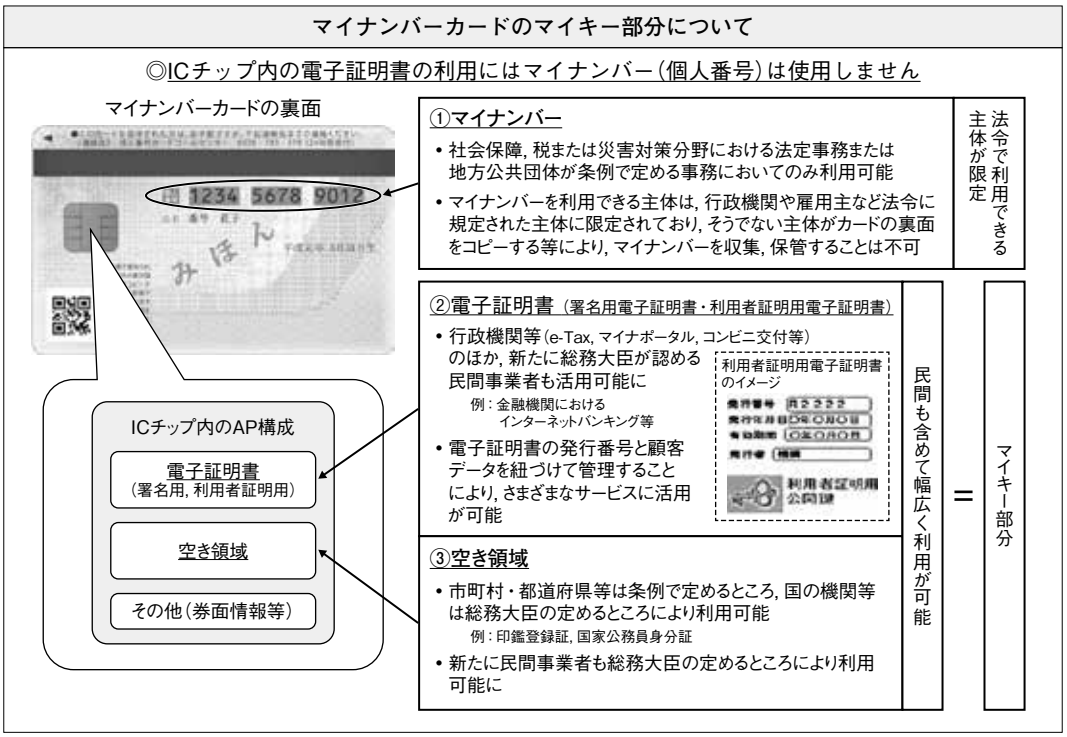

図 2　マイナンバーカード
総務省ウェブサイトより引用（http://www.soumu.go.jp/kojinbango_card/03.html）.

スの開発会社メディカルデータビジョンは登録者を 1 年間で 5,000 人に増やすとの意気込みを示した.

診療データを簡単に参照できるようにしようという同様の動きは，政府でも検討されている．マイナンバーを用いて，ネット上で過去の投薬履歴や特定健診のデータをすべて閲覧できるようにする取り組みである．2021 年 3 月からマイナンバーカードを健康保険証として使用可能にし，そして領収書や面倒な計算の手間をなくして，医療費を自動的に計算してくれるという展望である[3].

電子カルテの情報の重みは千差万別

利便性を追求するあまり，もしマイナンバーが漏れたらあらゆる情報がみられてしまうのではないか，という心配もでてくる．検査データや，処方箋，電子カルテの中身というのは，人それぞれ重みが異なる．たとえば，通常は検診結果というと「コレステロールが少し高め」くらいの結果で終わるので，他人に覗き見されても大したことはないだろう．だがそれが，「内視鏡検査の結果，胃がんが見つかりました」などの結果になると，当然だが重みがまったく違う.

処方箋の内容も，専門家がみれば病名まで類推できる，いわば究極の個人情報である．たとえば第三者が患者本人になりすまして処方箋を閲覧し，制がん剤を増量しているという情報を得たら，がんが悪化していることが周囲に漏れてしまうかもしれない．ずさんな認証システムにより個人情報が流出すると，重大な不利益を及ぼしかねないのである.

[2]：中日新聞．検査画像や診察履歴をいつでもスマホで　一宮市の「大雄会」．2019 年 5 月 9 日朝刊.
[3]：日本経済新聞．投薬履歴 マイナンバーで確認　政府，カード普及促す．2019 年 6 月 3 日電子版．（https://www.nikkei.com/article/DGXMZO45590670S9A600C1PE8000/）

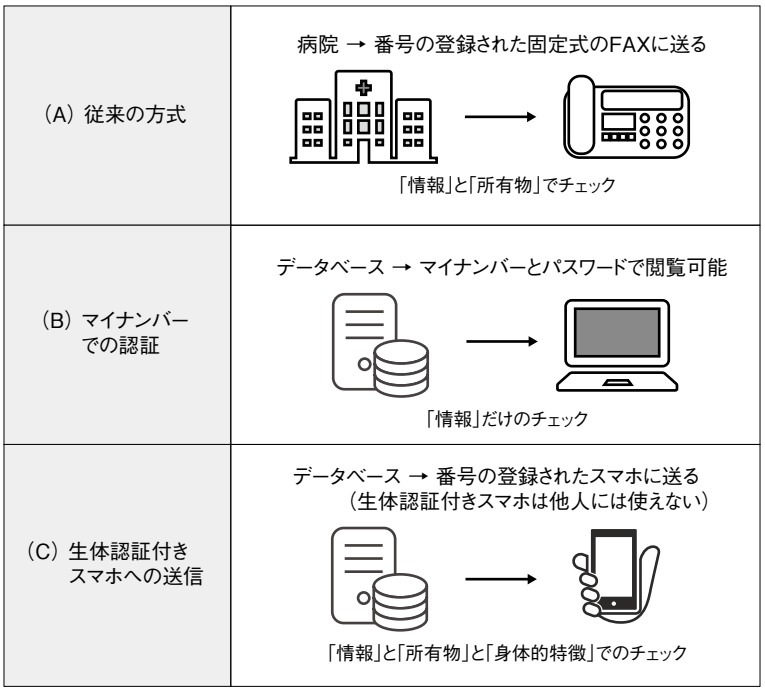

図 3　個人認証の3要素：「情報」「所有物」「生体認証」

他にも，ウイルスなどの保因者，たとえばHIVウイルスの保因者などという情報は非常にデリケートである．病名や薬剤名が知られたことが原因で，コミュニティ内での隔離・迫害の対象となった事例は枚挙に暇がない．近年だと小学校の寄生虫検査のデータが手荒く扱われ，いじめにつながった深刻な例などが挙げられる．

電子カルテのデータを保護するために，利便性とコストを考慮しつつ，対策を考えることが必要になる．

マイキーとマイナンバーの利便性と限界

マイナンバーカードには，マイナンバー情報のほかに，民間も含めて幅広く利用が可能な「ICチップの空き領域」が搭載されている（**図 2**）[4]．

マイナンバーの情報は，税金と社会保障と災害以外には利用できないが，その他の部分はマイナンバー情報とは区別した「マイキー情報」として活用する方法が提案されている．

総務省はマイナンバーカードの取扱いについて以下のように書いている．

「*マイナンバーカードは，金融機関等本人確認の必要な窓口で身分証明書として利用できますが，個人番号をコピー・保管できる事業者は，行政機関や雇用主等，法令に規定された者に限定されているため，規定されていない事業者の窓口において，個人番号が記載されているカードの裏面をコピー・保管することはできません*」[4]．

情報の種類によって，カード表面のマイキーで利用できるもの，裏面のマイナンバーで利用できるものに分かれることになる．表面のマイキー情報を事業者に提供する場合，裏面はコピーされないように注意する必要があるが，カードの使用機会が増えるにつれ，裏面の情報を守るのはかなり難しくなってくるであろう．

[4]：総務省．マイナンバーカード．（http://www.soumu.go.jp/kojinbango_card/03.html）

個人情報の漏洩リスク

わが国のマイナンバーがお手本としたアメリカの社会保障番号では，大量のデータが漏洩し，生体認証を含めてどのように個人認証を強化するかが大きな議論となっている．

アメリカでは，出生と同時に社会保障番号が与えられる．この社会保障番号に，納税から，運転免許，銀行口座まであらゆる情報が紐付いている．

2017年，大手信用情報会社のEquifax社が不正アクセスを受け，顧客の個人情報が流出する事件が起こった．1億4千万人というアメリカ全人口の約半数がこの事件の影響を受け，社会保障番号，生年月日，住所などのほか，20万人分のクレジットカード番号などが漏洩した[5]．

2019年にも，韓国のセキュリティ会社Suprema社のデータベースが流出し，生体認証データを含む2,780万件以上の情報が筒抜けとなる事件が起きた．Suprema社の生体認証技術は世界中の多くの企業に採用されており，クライアントのなかには日本企業も含まれていたという[6]．

「情報」「所有物」「身体的特徴」の組み合わせが大事

電子カルテの病名や，検査結果や，処方履歴といった究極の個人情報が，さまざまな病院，介護施設，薬局，検査機関で活用されるには，本人の同意が必要不可欠となる．

より確実な個人認証を行うにはどうすればよいか？　それには，「情報」「所有物」「身体的特徴」の3つの方法を組み合わせるのが重要と考えられている．

現在とくに期待されているのが，生体認証付きのスマホを利用する仕組みである．スマホの電話番号を登録し，そのスマホが生体認証を行ってくれれば，データの漏洩は非常におこりにくくなる（**図3-C**）．

電子カルテや処方箋のデータが，マイナンバーと1つのパスワードだけで引き出せる場合，確実に保護するのは難しい．所有物や身体的特徴を使わずにマイナンバーとパスワードの「情報」が盗まれただけで，なりすましが非常に容易となる（**図3-B**）．

アップル社のiPhoneなど最近のスマホで生体認証に用いられる指紋や顔のデータは，端末の中に保存されるので，仮にマイナンバーとパスワードのデータが流出しても，個人データは取り出しにくい．

登録されたスマホにデータが送られる仕組みは，「所有物」を持っている人だけみれるので，盗まれる可能性は低くなる．そのうえ，スマホが他人に奪われたりした場合でも，生体認証が有効ならばデータは引き出せない．セキュリティ的には最強といえよう．

この場合，マイナンバーとスマホの電話番号を，あらかじめ病院なり，電子カルテの管理者に登録しておくことになる．少し面倒に感じるが，診断名や，処方箋といった情報の価値は（人によって差があるものの）非常に重要であり，流出のリスクはすこしでも減らしておく必要がある．

一方，スマホを持っていない高齢者などへの対応も必要である．この場合は，保険証（またはマイナンバー）をもとに，自宅か薬局の固定式FAXに，処方箋などのデータを送ってもらうという方法になると思われる（**図3-A**）．

FAXやスマホといった所有物や，生体を用いたチェックを行わず，マイナンバーとパスワードの情報だけで個人認証を行うという，総務省の案では安全性を担保するのは難しい．

---

[5]：アメリカ連邦取引委員会（FTC）．The Equifax Data Breach：What to Do.（https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do）

[6]：vpnMentor. Report：Data Breach in Biometric Security Platform Affecting Millions of Users.（https://www.vpnmentor.com/blog/report-biostar2-leak/）