表１　複数の職種あるいは市民との間で比較可能な項目の一覧（１）

	医師			薬剤師			一般市民		
現状に関する質問									
	よくある	まれにある	ない	よくある	まれにある	ない	よくある	まれにある	ない
業務目的で参照することがあるか？	72	22	5	67	26	6	—	—	—
自身かスタッフが診療情報を手書きで手帳に記載することはあるか？	37	33	28	14	46	40	—	—	—
自身かスタッフが診療情報を医療機関のシステムの電子データから紙やシールへ印刷して提供するなど、患者が紙で活用するために提供することはあるか？	41	29	29	82	12	7	—	—	—
電子データで患者へ提供することはあるか？（画像情報を除く）	14	10	75	26	14	59	—	—	—
一般論としての質問									
医療機関（薬局含む）のシステムから患者へ（紙、電子データに関わらず）医療情報を提供することについて、どう思うか？	大変良い	良いが問題もある	問題が多くやるべきでない	大変良い	良いが問題もある	問題が多くやるべきでない	大変良い	良いが問題もある	問題が多くやるべきでない
	66	14	1	64	19	1	77	7	1
医療機関のシステムから患者へ紙印刷あるいは電子データで提供する場合に、どのような手段が最も望ましいか？	紙	電子媒体	紙と電子媒体両方	紙	電子媒体	紙と電子媒体両方	—	—	—
	63	8	28	57	5	37	—	—	—
患者が自宅や職場で自己測定したなんらかの記録を記載あるいは入力した健康記録・医療記録（体重記録、血圧手帳、血糖手帳や万歩計の記録など）を医療機関へ見せて診療に使うことに対してどう思うか？	良い	良いが問題もある	問題が多くやるべきでない	—	—	—	良い	良いが問題もある	問題が多くやるべきでない
	86	8	0	—	—	—	77	4	1

表２　複数の職種あるいは市民との間で比較可能な項目の一覧（２）

（数字は%）	医療機関（薬局含む）から患者へ渡す情報の電子化が進むと仮定した場合、渡す方法はどれが望ましいか？						医療機関から患者へ渡す情報の電子化が進むと仮定した場合、そのコストは誰が支払うべきだと思うか？					
	CD、USBメモリーなどの一時的な電子媒体	情報提供目的に特化されたICカードなどの電子媒体	スマートホンなどへ電子的に渡す（2次元バーコード等）	オンラインで提供することによりインターネットで閲覧する	電子的には渡すべきではない	それ以外	患者	医療機関	保険者	行政	それ以外	わからない
医師	24	35	10	15	32	2	75	10	16	20	0	6
薬剤師	10	32	33	27	29	2	40	29	23	38	1	14
一般市民	9	24	12	33	—（※）	7	23	46	32	33	2	11

※　一般市民の選択肢には、「電子的には渡すべきではない」はなく、「紙媒体」があり、52%であった

厚生労働科学研究補助金（地域医療基盤開発推進研究事業）
分担研究報告書

患者に受容可能な技術調査

研究分担者　田中　勝弥（東京大学医学部附属病院）

研究要旨
前年度調査結果により、一定のITリテラシーを持つ国民の多くは自らの医療・健康情報を電子的に提供公的基盤として整備されることを望んでいることが明らかとなった。また、電子化情報のインターフェイスとしてはPCより、スマートホンやタブレットなど、より使いやすいデバイスが求められているが、セキュリティへの不安はあり、制度的、技術的対策を急ぐ必要があると考えられる。現在、患者自身による健康管理を目的とした各種スマートホン上でのアプリケーションの普及や、「電子お薬手帳」にみられるように医療機関から提供された情報をスマートホンで読み取り、患者のデバイス内に情報を蓄積し閲覧する、といったアプリケーション開発・実証が行われている。安全に安心して自身の健康情報・診療情報を蓄積、継続使用できることが求められる状況下で、本研究では、タブレット、スマートホンといった患者が所有する携帯端末を使用する際の技術的対策について文献調査より検討を実施するとともに、Bluetoothキーデバイスを使用した新たな内在情報保護のための手法を提案し、試作により評価を行った。

A. 研究目的

個人が情報を取り扱う場合、現在では様々な手段があるが、最も利活用性の高い手段として携帯電話やスマートホンの利用が考えられる。しかしながら、これらの携帯端末に健康情報を内在させる場合には紛失・盗難などの事故発生リスクが少なからず存在し、また、端末に保存されている情報が容易に閲覧できる場合も多く、内在された情報が漏洩する危険が大きい。

本研究では、携帯端末に格納された情報の安全性を保つ技術について、現在利用可能な既存の認証・暗号化技術を中心に文献調査により調査、整理し、それぞれの手法のリスクについて検討すること、また、調査結果をもとに、利便性を損なわない新たな内在情報保護のための手法の提案を試みることを目的とする。

B. 研究方法

現在、PCおよび一部スマートホン、タブレットなどの携帯デバイスで利用可能な内在情報保護のための認証技術を文献調査し、個々の技術について残存リスクの有無を検討する。また、既存技術を参考に、安全性および利便性を損なわないことを主眼とした新たな技術手法の提案と試作による評価、検討を行う。

C. 研究結果

C.1. 調査結果

現在利用可能な既存の認証・暗号化対策としては、以下のものがある。

1） ID・パスワード方式

最も一般的に利用されている端末へのアクセス権の検証手段が、端末に設定したID/パスワードによる認証方式である。スマートホンの場合、画面ロックを目的としてパスワードとして通常4ケタの数字が用いられる。遠隔で画面ロックを制御可能なサービスも利用可能である。

2） 生体認証方式

パスワードの代わりに、指紋や声、顔画像、手書き文字などによる認証が現在利用可能である。スマートホンの場合、端末ロックの解除が主眼であり、内在データまでは対象としていない。

3） キーデバイス装着方式

キーデバイスとしてUSBを使用するものが主流であり、専用のUSBキーを装着することにより、端末へのログオン、画面ロック、ファイル・フォルダの暗号化、電子証明書によるシングルサインオンなどの機能が利用可能である。主にPC向けの技術手法であり、複数製品化されている。キーデバイスの紛失時対応のために、その再設定のための機構が別途必要とされる。

4） キーデバイス通信方式

本体に直接装着するのではなく無線を介してキー情報を取得、利用する方式で、NFC（Near Field Communication）が使用される。携帯電話・スマートホンでは、お財布携帯などに利用されているRFID（Radio Frequency Identification）を利用して近距離の機器間通信に適用される6)。

5）暗号化方式

ハードディスクやフォルダ/ファイルへの暗号化を行い、第三者による不正閲覧やウィルス対策などの主にソフトウェア的な漏えい防止対策として使用される。ただし、端末本体の盗難時は内在するデータへのアクセス制限は期待できない。

C.2 患者に受容可能な手法の検討

上記の調査結果を踏まえ、患者デバイスに蓄積される診療情報の利活用場面で内在データの保護に対して重要と考えられる要素を以下に示す。

1）操作容易性

画面ロックに対する4ケタパスワードに示唆されるように情報参照のたびに多文字にあたるID・パスワード入力を求められる運用は利便性に欠ける。逆に、キーデバイス方式では利便性の低下は小さい。

2）認証継続性

キーデバイス装着方式以外は、利用場面のある一時点での認証を求めており、継続的な認証は行なわないケースが多い。逆にキーデバイス装着方式はキーデバイスの存否に基づく継続的認証であるが、本体と一体化されるため、紛失・盗難を考慮すれば、可搬端末には適用しにくい。また、NFC方式では、本体とキーデバイスを分離でき

るものの、通信距離が短いため位置的分離性に欠ける。

3）キー情報の分離性
キーデバイスを使用しない場合は、認証情報そのものが端末に内在されている。このため、盗難・紛失に際しては、アプリケーション・患者データ・キー情報が分離されることなく遺失する。

これら3つの観点から、キーデバイスとして無線方式を採用し、また認証継続性を確保するためのロジックが必要であると考え、これを策定した。本研究で提案する方式は、アプリケーション利用のキーデバイスとして、Bluetooth 搭載機器を採用する。概要は以下のとおりである。

a) キーデバイスの存否をチェックする
b) キーデバイスの存在が確認できるまで待機する
c) アプリケーションの使用を可能とする
d) 一定時間ごとにキーデバイスの存否確認を行い、アプリケーション利用の継続可否を判定する
e) さらに、対応する Bluetooth 搭載機器の存在が確認出来ない状態でアプリケーションが起動されたときは、アプリケーションを強制終了し、データ領域の対象情報を凍結または消去する。

C.3. 提案する手法の実装
現在、スマートホン OS として主要な Android および iOS の2つの OS において実装利用可能な Bluetooth 用のライブラリを調査した。図1に結果を示す。

Bluetooth 用ライブラリは Android OS は標準的な API（Application Programmable Interface）で利用可能である。一方、iOS はバージョンおよび Bluetooth タイプにより利用可能な API が異なるが、いずれの場合にも、最新の API では、デバイスの電波強度を取得し、電波の強弱による近接状況を評価することが可能である。

また、携帯端末内へデータを蓄積する手段としては、単純なテキストファイルによる保持のほか、SQLite や FileMaker といったファイルベースのデータベースが標準的に利用できる。多くの場合、こうしたファイルベースのデータベースへ情報を格納し、アプリケーションで利用する形態が一般的であると考えられる。この場合、内在するデータベースファイルをファイルとしていかに安全に退避するか、ということが情報を保護する上での課題となる。
手法としては、単純なファイルの暗号化でもよいし、盗難や紛失時のデータ救済を考慮すれば、暗号化した上でクラウドサービス上に退避するのがより最善と考える。現在、Android 端末では「Google ドライブ」、iOS 端末では、「iCloud」といったクラウド型のストレージサービスが端末に標準でインストールされており、無償利用が可能である。また、これらのサービスを利用するための API も公開されており、一般的に利用できるため、こうしたクラウド型ストレージへデータを退避しておくのがよい。

本研究では、Android OS 4.3 を用いて、

図2のように試作を行い、動作および評価試験を行った。ここでは、Bluetooth キーデバイスの存否確認を行うタスクをタイマー処理により作成し、電波強度による存否判定を行っている。とくに、端末とキーデバイスにおける Bluetooth のペアリングは必要としないこととした。これは、ペアリングを行うと、ペアリングしたデバイス情報が端末側に記憶されてしまうためである。

また、キーデバイスの選択や保持のためには、何らかのキーデバイスの登録操作が必要となるが、盗難を考慮すると、この操作には何らかの認証機構が必要である。

D. 考察

本稿で記載した技術対策は単独ですべての情報保護を担保できるものではなく、必要な場面に応じて複数を組み合わせて利用されるべきと考える。

本研究では、患者が使用する際の利便性を重要視しており、キーボード入力を省力すること、紛失・盗難時を考慮して認証を継続的に行うキーデバイス方式であることに焦点を置いている。ただし、キーデバイス方式は、USB キーのように正常利用時でも紛失等により利用継続ができなくなる可能性が少なからず予想され、キーデバイスの再設定については考慮しておかねばならい。たとえば、別のマスターデバイスをあらかじめ用意しておく、非常時の多文字パスコードを設定しておく、などの対応が考えられる。

さらに、現在利用可能な Bluetooth 搭載機器として、マイクやスピーカなどの音響機器だけでなく、腕時計などの常時身に装着するデバイスが入手可能であり、このような機器を選択することによって、キーデバイス操作に対する煩雑性も解消されることが期待できる。

キーデバイス消失時のアクションについては、データの消去、あるいは暗号化等による利用継続の停止、が考えられるが、これは、対象となる健康データが再生可能であるかどうかに依存する。お薬手帳のように現状では紙媒体情報の読み取りによってインポートされる形式のデータは再生可能であり消去も可能であると考えられるが、患者自らが記録することにより長期にわたり生成・蓄積されたデータは消去すると復元が困難であると予想されるため、クラウドストレージのようなスマートホンからアクセス可能な外部ストレージへ復号可能な状態で退避しておくのが利便性を損なわないと思われる。ただし、端末本体の盗難時にはデータへのアクセスが容易であるため、復元可能な暗号化対策が必須である。

E. 結論

患者がタブレット、スマートホンなどの端末を利用して内在された健康情報を閲覧し、自らデータを入力する場合、機微な健康情報が当該端末の不正利用による閲覧や漏洩したりすることを防ぐ技術について、文献調査を行い各々の特質を整理した。また、広く患者に受容可能であるための観点から Bluetooth デバイスを使用したアクセス認証のための手法を提案し、試作により実装可能性を確認するとともに、残存課題を検討した。

F. 健康危険情報

なし

G. 研究発表

1. 論文発表

なし

2. 学会発表

第 33 回医療情報学連合大会

「モバイル診療情報参照システムにおける個人情報の保護機能に関する検討」

H. 知的財産権の出願・登録状況

1. 特許取得

なし

2. 実用新案登録

なし

3. その他

なし

OS Ver.	Bluetooth API	Bluetooth 対応規格	電波強度	データ ベース
Android	標準API	Bluetooth 2.0 4.0、BLE	数値	SQLite
iOS v7 ～	CoreLocation iBeacon	BLEのみ	3段階 数値	SQLite FileMaker
iOS v5 ～	CoreBluetooth	Bluetooth 4.0 BLE	3段階	
iOS	GameKit	Bluetooth 2.0	取得不可	
iOS	Bluetooth Manager (非公開)	Bluetooth 2.0	取得不可	

図 1 OS および Bluetooth API

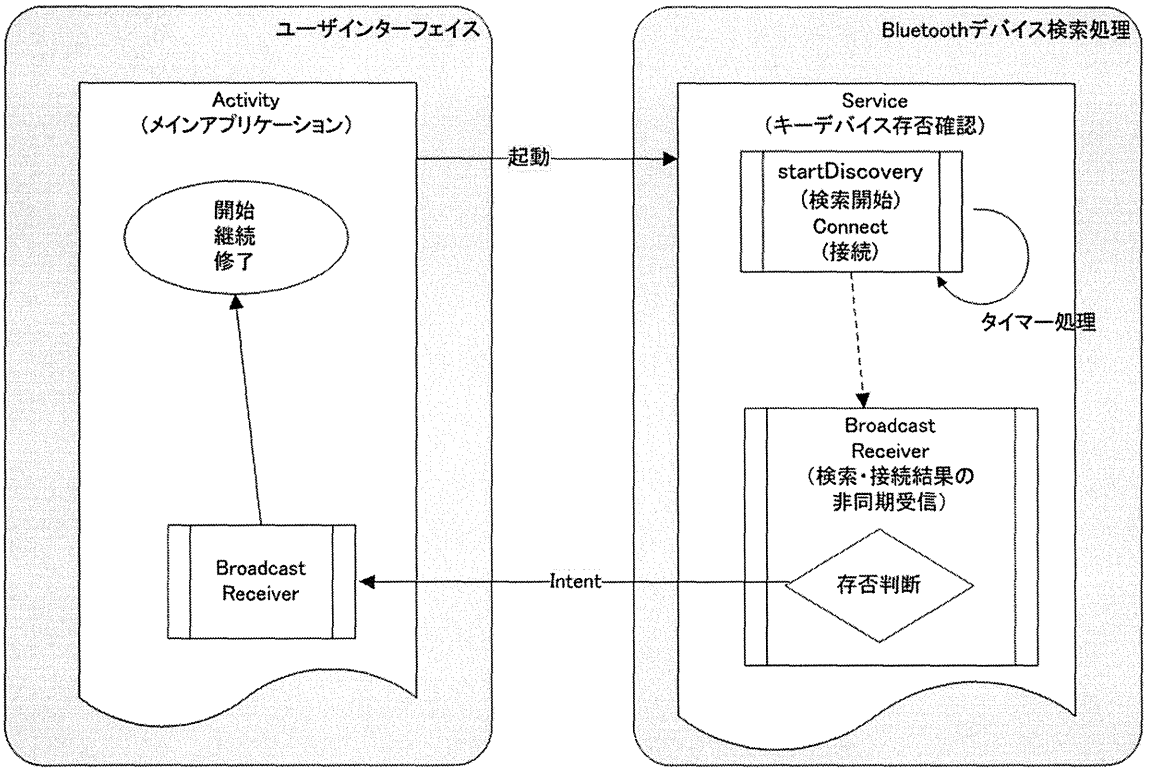

図 2 Android 4.3 での実装例

患者に受容可能な技術調査

刊行物

書籍　なし

著者氏名	論文タイトル名	書籍全体の編集者名	書　籍　名	出版社名	出版地	出版年	ページ

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
吉田真弓、篠田秀範、田中勝弥、山本隆一	電子化診療情報の取り扱いに対する一般市民の意識調査に関する報告	医療情報学連合大会論文集（医療情報学別冊）		318 － 321	2013
田中勝弥、吉田真弓、篠田秀範、山本隆一	モバイル診療情報参照システムにおける個人情報の保護機能に関する検討	医療情報学連合大会論文集（医療情報学別冊）		322 － 325	2013

電子化診療情報の取り扱いに対する一般市民の意識調査に関する報告

吉田 真弓[*1] 篠田 英範[*2] 田中 勝弥[*3] 山本 隆一[*1]
[*1]東京大学大学院医学系研究科医療経営政策学講座
[*2]一般社団法人保健医療福祉情報システム工業会
[*3]東京大学医学部附属病院企画情報運営部

An Investigation Report of Citizen's attitudes toward the handling of Electronic Medical Information

Mayumi Yoshida[*1] Hidenori Shinoda[*2] Katsuya Tanaka[*3] Ryuichi Yamamoto[*1]
[*1]The University of Tokyo [*2]JAHIS [*3]The University of Tokyo Hospital

A Personal Health Record, or PHR, is a health record where health data and information related to the care of a patient is maintained by the patient. It covers wide range of healthcare information and includes sometimes subtle information of a patient, and it might be hard for a patient to always understand what it means correctly.

Therefore, we tried to investigate how people expect to get and utilize the health data and information.

We conducted a survey in the form of a questionnaire to more than three thousand people over 20 years old on the web. The questionnaire covers about ways of information acquisition, their knowledge on information technology, how and who manages the information, how the information should be utilized, etc.

94% of them answered a PHR should be put into practice, 45% of them hoped it should be developed and managed by public administrations, more than 40% of them accepted the information could be acquired electronically, and so on. We thought Japanese people expect the PHR may be a practical service for healthcare, but it should be managed and utilized on the proper balance between public and private services.

Keywords: Privacy, Electronic Medical Information, Personal Health Record, Questionnaire Survey, Personal Data Protection

1. はじめに

診療情報の電子化は確実に進行している。また、医療機関で診察や各検査などで取得される診療情報は様々であり多量である。プライバシーの原則からは、本来は患者の診療情報は患者本人がコントロール権を持つべきであるが、医療特有の医療従事者と患者の知識格差は当然ながら存在し、診療情報の全てを患者本人がコントロールできるわけではない。ただ、今後、どこでもマイ病院やPHRの整備がすすめば、患者の生涯にわたる健康医療情報の蓄積と健康管理、将来の病気への活用などにも利用できる。ただ、適切な運用のためには患者本人に被害が及ばず、また医療機関なども不必要に責任を負う必要がないためには、将来は患者が自分の診療情報に対して、どの情報をどう利用したいか患者本人が適切に選択する必要があると思われる。[1)]

2. 方法

本研究では、一定のITリテラシーのある一般市民を対象に、自らの健康・医療情報の提供を受けることに対する、ニーズや意識の調査を行った。WEBアンケート方式で、一般人3090名を対象とした。WEBアンケートというITリテラシーに関してはバイアスのある調査法を選択したが、これは、本研究の目的が近い将来における患者への電子化医療・健康情報の提供のあり方であり、適切な調査法であると考えた。

アンケート対象者は、宮城県、東京都、愛知県、和歌山県、福岡県在住の20歳以上の人とし、年齢は20代、30代というように10歳ごとにカテゴリ化し、70歳以上を一つのカテゴリとしたが、大きな偏りはなく、男女比は女性がやや多かった。質問項目は総合病院へのアクセスや駅などへの交通手段などの居住環境や年齢、健康状態や家族構成などのプロファイル情報を尋ねた上で、受診した際の検査結果や調剤薬局での服薬情報の管理方法、紙や携帯端末、PCなど診療情報等の望ましい受取方法、PHR等で蓄積された場合の自分の診療情報や処方情報の利活用の方法、自分以外の人間が利用するにあたっての許可の方法、PHR整備や運用への意見や感想など35問を尋ねた。全体の結果を分析した上で、年齢や自分の健康状態、健康状態に不安のある家族の有無などに分けてクロス集計し、その結果の比較を行った。

3. 結果

3.1 対象者のプロファイル情報

アンケート対象者のプロファイルは、男女比は43:57で女性がやや多く、年齢構成は20代が16%、30代29%、40代30%、50代15%、60代7%、70才以上2%であった。

医療機関へのアクセスに関しては、最寄りの総合病院へのアクセスの容易さを聞いたが、徒歩や自転車で15分以内が44%、公共交通機関を利用して15分以内が7%、自家用車、タクシーで15分以内が25%で、ほぼ8割が15分以内に最寄りの総合病院へのアクセルが可能であった。

また健康に何らかの問題がある人が、37%で、63%は問題を感じていない人であった。年代別の結果では、通院中が70代では6割、20代では2割以下で、年代による健康状態や受診率の変化は顕著であった。

スマートフォンや携帯電話の利用方法については、電話とメール以外では、情報の検索や地図の利用などが多かった。年齢別では、高齢者はメールと電話のみの利用が7割程度であった。ただ、健康管理を目的としたアプリの利用は、どの年代でも15%程度であった。

3.2 オンラインショッピングの経験と安全面での不安

オンラインショッピングは図1のように75%の人が利用したことがあり、その内、44%の人がしばしば利用している。年代別での差は見られなかった。

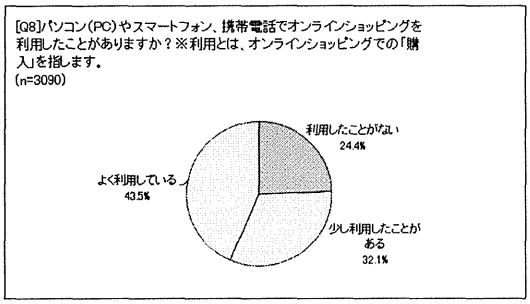

図1 オンラインショッピングの経験

その一方でオンラインショッピングの安全面に関する不安の有無を聞いたところ、図2に示すように「不安はない」という人が28%で多くの人が不安を感じながら使用しているという状態だった。年齢や健康状態での比較も、差は見られず、ほぼ同じ割合であった。また、クレジットカード決済についての問いは、支払いをしてもいいと思うのでカード決済したが7割、支払いをしても良いと思わないのでカード決済しないが1割程度で、中でも年齢別では20代が2割と最も多かった。

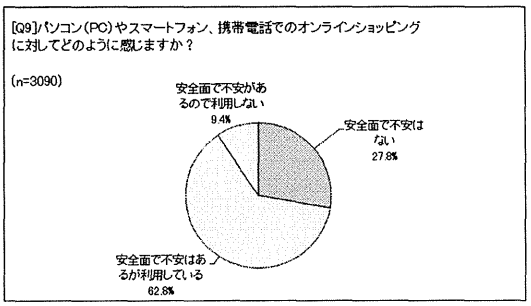

図2 オンラインショッピングの安全面での不安

セキュリティ知識に関する質問では、SSLやTSLを聞いた事があるが7割で、具体的な内容については「安全な情報の通信方式」が7割で最も多かったが、他の選択肢は3割以下であった。

3.3 お薬手帳について

次にお薬手帳について質問をした。結果は図3に示す通りで、貰ったことがない人を除くと、少なくとも医療機関や薬局には持って行く人が40%で、保管はしているが16%、44%の人がお薬手帳を使っていないという回答だった。年齢別では、高齢者の内60代では4割、70才以上は3割が使っていないという結果であった。

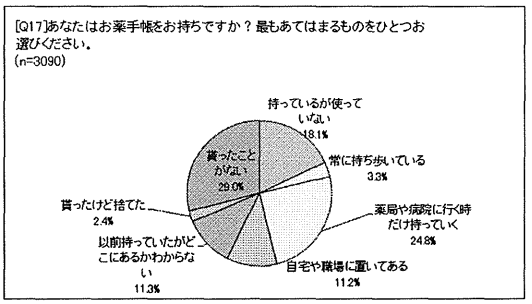

図3 お薬手帳について

3.4 診療情報の受取方法について

診療情報を医療機関等から受け取る場合のメディアについて聞いた。図4に示すように紙で受け取りたいという人が57%、39%の人が電子媒体で受け取りたいという意向を示しており、紙や電子媒体の如何にかかわらず情報を受け取りたくないという人は、4%であった。これらの結果は年齢別のデータでもほぼ同じ傾向であった。

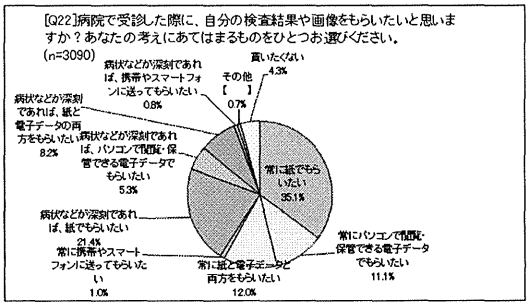

図4 診療情報の受取方法

3.5 PHRの整備と要件について

次にPHRについて質問を行った。図5に示すようにPHRの整備は94%の人が望んでいるが、単純に民間事業者で良いと考えている人は13%に過ぎず、一定の規制の下に民間事業者が行うが35%で、付加的サービスなどを除いて、基本的には国や自治体が整備運営するべきと考える人は45%であった。まだ、民間事業者に完全にPHR事業を任せるのは不安があり、費用負担の面でも、税金などでまかなうべきという意見が多く、公的基盤としてのPHRの整備が望まれている。

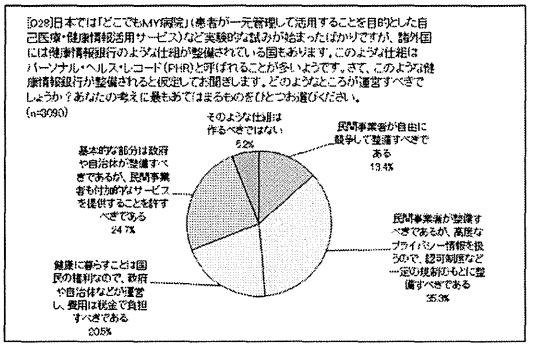

図5 PHRの整備について

PHRに保存される自分の情報については、保存の都度許可を得て欲しいは37%、PHRの利用は自分で選び利用すると決めたら医療機関や薬局が必要とする情報は保存してもらって良いが44%、健康な時には健康情報に無関心なため本人の意思に関わらず医学的な情報は保存されるべきは19%であった。年齢別のデータでも同じような割合だったが、70才以上の高齢者は保存の都度許可が必要は18%で、Pre-PopulationやAuto-Populationを希望する意見が8割以上だった。また、PHRに蓄えられた情報を匿名化した場合の利用については、匿名化情報でも利用には必ず自分の許可が必要は30%、インフルエンザなど感染症の広がりの把握など公衆衛生に利用なら利用を許可するが59%、製薬会社などに匿名化情報を有料で提供することでPHRの運用コストを下げられるならば利用してよいが11%であった。

PHRの要件としては図6に示すようにセキュリティを重視する人が81%、自分の治療に役立てることが53%で公益利用はあまり重視されていない傾向があった。

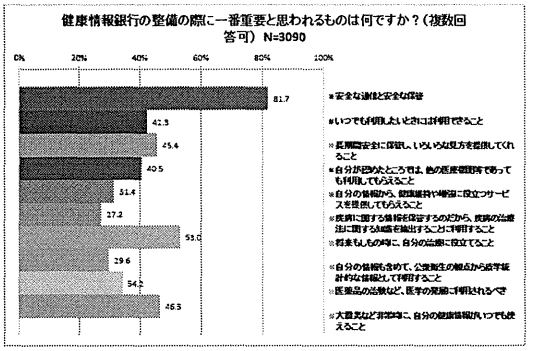

図6 PHRに求められる要件

4. 考察

診療情報を患者等に電子的に提供する際に、いくつかの解決すべき課題があることは容易に想像される。一つは、受け取り側の安全性への懸念であり、本研究の調査でも、オンラインショッピングなどの電子的な個人情報のやりとりに不安を持つ人が大部分であることからも裏付けられる。そのためもあるが、医療情報を医療機関等から受け取る場合、紙媒体を希望する人が57%で半数を超えている。その一方で、オンラインショッピングでも不安はあっても75%の人が利用しているように、約4割の人が自分の診療情報を電子的に受け取ることを希望していることは注目に値する。つまりニーズは確実に存在するものの、電子的に診療情報を授受するには安全面でやや不安をかかえているという実態が明確に表されていると考えられる。

また、現在のお薬手帳の利用率はどの年代においても高いとは言えず、70才以上は受診中や2年以内に入院など、健康に何らかの不安を抱えた人が8割だったにも関わらず、お薬手帳を使っていないが3割、2割以上は貰ったことがないという結果であった。医療機関を受診した際に受け取った検査結果や画像などは、保管し健康日記のような使い方をする、もしくは家族への相談や他の医師へのセカンドオピニオンに利用するが高齢者では7割以上だったが、若年層になるに従い、特に考えていないが半数以上を占めている。診療情報や処方情報が消えていくことを問題と考えてはいても、紙媒体のお薬手帳や検査結果では管理や将来にわたっての利用には適しておらず、電子的な診療情報や処方情報の電子的提供および管理する制度の整備は一般市民の側からも求められていると考えられる。

PHRに保存される自分の情報については、保存の都度許可を得て欲しいが4割近くあり、PHRに蓄えられた情報は例え匿名化情報でも必ず自分の許可が必要は3割程度であり、今後はPre-populationやAuto-populationにあたっては同意の方法についても検討が重要と考えられる。[2)]

PHRの整備は94%の人が望んでいるが、単純に民間事業者で良いと考えている人は13%に過ぎず、一定の規制を下に民間事業者が行うが35%で、付加的サービスなどを除いて基本的には国や自治体が整備運営するべきが45%であった。まだ、民間事業者に完全にPHR事業を任せるのは不安があったり、費用負担の面でも、特に70代以上の高齢者は税金などでまかなうべきという意見も多く、現段階では国民に対して費用負担を任せるのは難しいと思われる。

受診した際に検査結果や画像など、どのような状態で情報を貰いたいかは、深刻な病状の場合も含めると紙で貰いたいは、20代と70代以上で他より高く6割以上だった。これは家族等への相談やセカンドオピニオンなど、紙での情報が他の目的に利用しやすいではないかと考えられる。このように項目によっては年代での差違は多少みられたが、自分や家族の健康状態の状況での違いはそう見られなかった。

また、オンラインショッピングの感想が、何れの状況の場合も7割程度が安全面で何らかの不安があると回答しているが、実際にオンラインショッピングを75%の人が利用しており、4割程度が電子データでの受取を希望しているのは興味深い結果である。電子的な情報の取得に関しては、安全性への不安はあるものの電子化情報の取得には前向きと思われる。自分の診療情報や処方情報の蓄積や管理など、将来や自分の家

族などへの活用を望む意見も多く、PHRの整備は、経済的な運用面も含め、対策は急ぐべきと考えられる。
今後は医療従事者が考える患者への情報提供のあり方も踏まえた上で、患者の求める診療情報の取得や管理方法と、患者本人が安心と考えられる電子化情報の取得などを考察する予定である。

5. 結論

医療・健康情報を医療機関等から本人へ電子的に安全に提供することのニーズは明確になったが、一方でセキュリティの面で、漠然とした不安が存在することも明らかになった。不安はありながらも電子的に受け取ることを希望する人が4割程度存在することは、更に今後は詳細に調査をした上で、安心感を醸成する提供方法の確立が必要である。

参考文献

[1] 山本隆一. 平成24年度厚生労働科学研究補助金総括研究報告書. 2013年5月.
[2] 山本隆一. EHRが変える保健医療－諸外国の取り組みと我が国への示唆－.「海外社会保障研究」172号, P.31-41, 国立社会保障・人口問題研究所, 2010年9月.

モバイル診療情報参照システムにおける個人情報の保護機能に関する検討

田中 勝弥[*1] 吉田 真弓[*2] 篠田 英範[*3] 山本 隆一[*2]
[*1]東京大学医学部附属病院 [*2]東京大学大学院医学系研究科
[*3]保健医療福祉情報システム工業会

A study on the functions of personal information protection in mobile clinical information reference systems

Tanaka Katsuya[*1] Yoshida Mayumi[*2] Shinoda Hidenori[*3] Yamamoto Ryuichi[*2]
[*1]The University of Tokyo Hospital
[*2]Graduate School of Medicine, The University of Tokyo
[*3]Japanese Association of Healthcare Information Systems Industry

In the use of a PHR service, the health information management by the patient is necessary. The use of mobile devices such as smart phones and tablets will be accelerated for these purposes, and it is necessary to protect information inherent and to work on the technical measures for using safely. In this research, the technical measures which can be available are investigated in the viewpoint of data protection, and the problems are discussed. Moreover, a new measure for protecting the information which is mainly inherent for data built-in application is proposed so that a patient can use comparatively easily.

Keywords: Personal Information Protection, Information Security, Smart Phone

1. はじめに

一定のITリテラシーを持つ国民の多くは自らの医療・健康情報を電子的に提供公的基盤として整備されることを望んでいることが明らかになった[1]。また、電子化情報のインターフェイスとしてはPCより、スマートフォンやタブレットなど、より使いやすいデバイスが求められているが、セキュリティへの不安はあり、制度的、技術的対策を急ぐ必要があると考えられる[2]。

現在、患者自身による健康管理を目的とした各種スマートフォン上でのアプリケーションの普及や[3]、「電子お薬手帳」にみられるように医療機関から提供された情報をスマートフォンで読み取り、患者のデバイス内に情報を蓄積し閲覧する、といったアプリケーション開発・実証が行われている[4,5]。

安全に安心して自身の健康情報・診療情報を蓄積、継続使用できることが求められる状況下で、タブレット、スマートフォンといった患者が所有する携帯端末を使用する際の技術的対策についても検討を進める必要がある。また、自身の健康情報の管理を安全に行う際には、情報を利用する端末の利便性を損なうことが少なく、利活用の促進を妨げない配慮も必要であると考える。

2. 目的

個人が情報を取り扱う場合、現在では様々な手段があるが、最も利活用性の高い手段として携帯電話やスマートフォンの利用が考えられる。しかしながら、これらの携帯端末に健康情報を内在させる場合には紛失・盗難などの事故発生リスクが少なからず存在し、また、端末に保存されている情報が容易に閲覧できる場合も多く、内在された情報が漏洩する危険が大きい。

本研究では、携帯端末に格納された情報の安全性を保つ技術について、現在利用可能な既存の認証・暗号化技術を中心に文献調査により調査、整理し、それぞれの手法のリスクについて検討すること、また、調査結果をもとに、利便性を損なわない新たな内在情報保護のための手法の提案を試みること、を目的とする。

3. 方法

現在、PCおよび一部スマートフォン、タブレットなどの携帯デバイスで利用可能な内在情報保護のための認証技術を文献調査し、個々の技術について残存課題の有無を検討する。また、既存技術を参考に、安全性および利便性を損なわないことを主眼とした新たな技術手法の提案を行う。

4. 結果

4.1 調査結果

現在利用可能な既存の認証・暗号化対策としては、以下のものがある。

1) ID/パスワード方式

最も一般的に利用されている端末へのアクセス権の検証手段が、端末に設定したID/パスワードによる認証方式である。スマートフォンの場合、画面ロックを目的としてパスワードとして通常4ケタの数字が用いられる。遠隔で画面ロックを制御可能なサービスも利用可能である。

2) 生体認証方式

パスワードの代わりに、指紋や声、顔画像、手書き文字などによる認証が現在利用可能である。スマートフォンの場合、端末ロックの解除が主眼であり、内在データまでは対象としていない。

3) キーデバイス装着方式

キーデバイスとしてUSBを使用するものが主流であり、専用のUSBキーを装着することにより、端末へのログオン、画面ロック、ファイル・フォルダの暗号化、電子

証明書によるシングルサインオンなどの機能が利用可能である。主にPC向けの技術手法であり、複数製品化されている。キーデバイスの紛失時対応のために、その再設定のための機構が別途必要とされる。

4) キーデバイス通信方式
本体に直接装着するのではなく無線を介してキー情報を取得、利用する方式で、NFC(Near Field Communication)が使用される。携帯電話・スマートフォンでは、お財布携帯などに利用されているRFID(Radio Frequency Identification)を利用して近距離の機器間通信に適用される[6]。

5)暗号化方式
ハードディスクやフォルダ/ファイルへの暗号化を行い、第三者による不正閲覧やウィルス対策などの主にソフトウェア的な漏えい防止対策として使用される。ただし、端末本体の盗難時は内在するデータへのアクセス制限は期待できない。

4.2 患者に受容可能な手法の検討

上記の調査結果を踏まえ、患者デバイスに蓄積される診療情報の利活用場面で内在データの保護に対して重要と考えられる要素を以下に示す。

1)操作容易性
画面ロックに対する4ケタパスワードに示唆されるように情報参照のたびに多文字にあたるID・パスワード入力を求められる運用は利便性に欠ける。逆に、キーデバイス方式では利便性の低下は小さい。

2)認証継続性
キーデバイス装着方式以外は、利用場面のある一時点での認証を求めており、継続的な認証は行なわないケースが多い。逆にキーデバイス装着方式はキーデバイスの存否に基づく継続的認証であるが、本体と一体化されるため、紛失・盗難を考慮すれば、可搬端末には適用しにくい。また、NFC方式では、本体とキーデバイスを分離できるものの、通信距離が短いため位置的分離性に欠ける。

3)キー情報の分離性
キーデバイスを使用しない場合は、認証情報そのものが端末に内在されている。このため、盗難・紛失に際しては、アプリケーション・患者データ・キー情報が分離されることなく遺失する。

これらの観点から、キーデバイスとして無線方式を採用し、また認証継続性を確保するためのロジックが必要であるとの結論に至り、これを策定した。本研究で提案する方式は、アプリケーション利用のキーデバイスとして、Bluetooth搭載機器を採用する。概要は以下のとおりである(図1)。

a) キーデバイスの存否をチェックする
b) キーデバイスの存在が確認できるまで待機する
c) アプリケーションの使用を可能とする
d) 一定時間ごとにキーデバイスの存否確認を行い、アプリケーション利用の継続可否を判定する
e) さらに、対応するBluetooth搭載機器の存在が確認出来ない状態でアプリケーションが起動されたときは、アプリケーションを強制終了し、データ領域の情報を凍結または消去する。

5. 考察

本稿で記載した技術対策は単独ですべての情報保護を担保できるものではなく、必要な場面に応じて複数を組み合わせて利用されるべきと考える。
本研究では、患者が使用する際の利便性を重要視しており、キーボード入力を省力すること、紛失・盗難時を考慮して認証を継続的に行うキーデバイス方式であることに焦点を置いている。ただし、キーデバイス方式は、USBキーのように正常利用時でも紛失等により利用継続ができなくなる可能性が少なからず予想され、キーデバイスの再設定については考慮しておかねばならい。たとえば、別のマスターデバイスをあらかじめ用意しておく、非常時の多文字パスコードを設定しておく、などの対応が考えられる。
さらに、現在利用可能なBluetooth搭載機器として、マイクやスピーカなどの音響機器だけでなく、腕時計などの常時身に装着するデバイスが入手可能であり、このような機器を選択することによって、キーデバイス操作に対する煩雑性も解消されることが期待できる。
キーデバイス消失時のアクションについては、データの消去、あるいは暗号化等による再利用の凍結、が考えられるが、これは、対象となる健康データが再生可能であるかどうかに依存する。お薬手帳のように現状では紙媒体情報の読み取りによってインポートされる形式のデータは再生可能であり消去も可能であると考えられるが、患者自らが記録することにより生成・蓄積されたデータは消去すると復元が困難であると予想される。

6. おわりに

患者がタブレット、スマートフォンなどの端末を利用して内在された健康情報を閲覧し、自らデータを入力する場合、機微な健康情報が当該端末の不正利用による閲覧や漏洩したりすることを防ぐ技術について、文献調査を行い各々の特質を整理した。また、広く患者に受容可能であるための観点から新たな手法を提案した。現在、提案した手法による試作を進めている。

参考文献

[1] 山本隆一. 医療機関における患者個人への安全な情報提供に関する研究. 平成24年度厚生労働科学研究報告書.
[2] JSSEC | 一般社団法人日本スマートフォンセキュリティ協会. http://www.jssec.org/.
[3] SoftBank HealthCare. http://www.softbank.jp/mobile/service/softbankhealthcare/.
[4] 大阪e-お薬手帳. http://www.e-okusuritecho.jp/.
[5] 内村祐之, 早川雅代, 大前浩司, 脇嘉代, 藤田英雄, 大江和彦. 携帯端末を利用した個人医療健康情報活用基盤の開発. 第32回医療情報学連合大会論文集,2012; 1368-9.
[6] NFC(Near Field Communication)の技術と測定. http://www.rohde-schwarz.co.jp/download/jp/an/1MA182_4J.pdf.

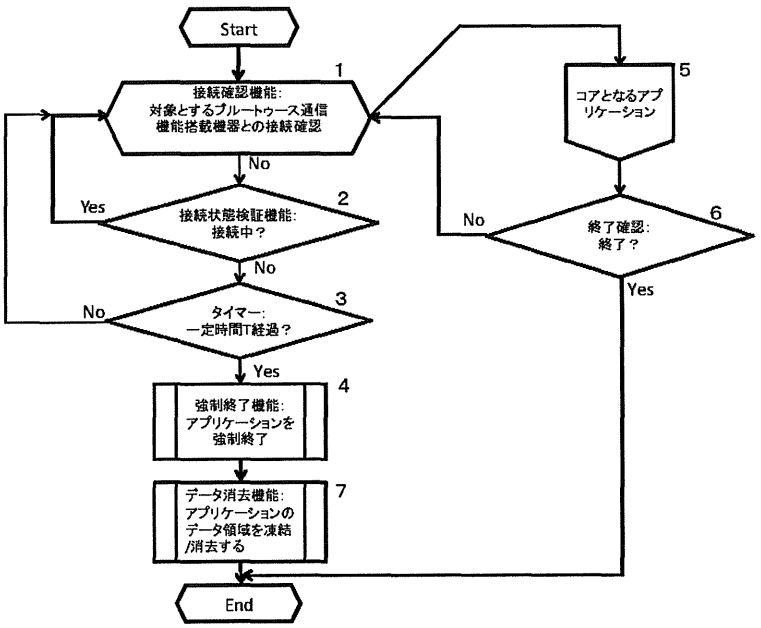

図1 Bluetooth搭載機器を利用したアプリケーションの処理フロー