

を活用することが望ましいが、これについても、病院や診療所の開設許可申請・届出との整合性を検証し、増改築や変更などにもなっておこりうるデータベースごとの情報乖離を防止する必要がある。

研究報告書

医療機関の組織認証に関する調査・検討

分担研究者 秋山 昌範 国立国際医療センター情報システム部長

研究要旨 各地域における包括的地域ケアシステムにおける取り組みやその他の地域に計画中の施設認証の仕組みを調査し、地域医療連携における医療機関の組織認証に関する調査・検討を行った。本研究で、医師会情報システムを利用した資格確認や本人認証の方策の構築可能性を検討し、具体的にプロジェクトが進行している新宿区医師会において地域医療システムを調査した。その結果、新宿区では利用者認証を医師会事務局で行うこととしていた。医師会事務局は入会審査時に医師免許番号を本人より調査しており、データベース管理されている。したがって、医師である資格審査をする代行機関として適当であると考えられたからである。1999年度より、包括的地域ケアシステムとして電子認証を使った地域医療システムが開始されたが、実運用において医師会事務局で個人の資格認証を行うことに問題点は見られなかった。

A. 研究目的

インターネットは、医療の世界でも広く使われるようになってきている。日本では、利用者がまだ大学関係者に多く、一般の医療の世界で広く使われるようになったわけではないが、医師会などでもインターネットへの取り組みが始まっている。新宿区における包括的地域ケアシステムにおける取り組みやその他の地域に計画中の施設認証の仕組みを調査し、地域医療連携における医療機関の組織認証に関する調査・検討を行う。

B. 研究方法

新宿区医師会の包括的地域ケアシステムとしての病診連携システムにおける医療機関の組織認証に関して調査する。新宿区医師会関係者や同事務局に対し調査を行い、その結果を分析する。その他、全国に構築中の地域連携システムにおける組織認証方法について調査する。新宿と山形県鶴岡地区間の連携における組織認証についての検討も行う。また、医師会組織が資格認証可能かどうかの調査・検討を行う。

C. 研究結果

1) 包括的地域ケアシステムとしての病診連携の推進

医療・福祉分野において、病院・診療所の連携および、一般病院・長期療養型病院の連携を実現することは重要である。しかし、従来型の対策では、情報伝達の迅速度や共有性に限界があり、必ずしも普及しているとは言えない。そこで、新宿区医師会においてコンピュータネットワークによる情報システムの構築を図り、新宿区地域での、1カルテ/1患者の実現を図る。この1カルテ/1

患者システムの実現により、患者にとっては、任意の医療機関での受診が可能となり、利便性が向上する。医療施行側にとっては、医療の分業化が推進され、かかりつけ医師制度の普及の推進となる。また、同一地域での医療の重複を省くことにより医療費の抑制を図る事も可能になる。

共有カルテの内容には、病名のみならず、血液や画像等の各種検査情報や投薬、アレルギー歴も含まれる。すなわち、外来診療は主に開業医にて行い、一般の診療所では難しい高度な医療や入院が必要な検査・加療等を、中核病院で診療の継続性を確保しながら担当することが可能になる。

2) その他の医療連携：山形県置賜地区医療圏におけるサテライト医療施設方式

山形県置賜地区医療圏における医療連携は独自の形態をとっている。高度医療を提供する拠点病院である基幹病院と住民のより身近な医療施設として、初期医療や慢性期の治療を行うサテライト医療施設に機能分化されているので、その方式を調査した。

置賜地域は山形県内でも最も高齢化の進んだ地域であり、全国的に見ても山形県の三大成人病による死亡率は高く、その中でも置賜地域における心疾患の死亡率は県平均よりも高い割合となっている。今後の高齢者の慢性疾患増加に対処するため公立置賜総合病院を基幹病院として新たに設置した。公立置賜総合病院は、優秀なスタッフと最新鋭の高度医療機器を配備し、21世紀における病院の拠点となる病院と位置づけられており、救命救急センターが併設されている。救命救急センターには、専門の医師や看護婦が常時待機しており、脳卒中、急性心筋梗塞、頭部損傷等の救急患者を24時間体制で対応している。また、

サテライト医療施設と救命救急センターが連携して救命医療を行うことにより、急な病気や不慮の事故の場合でも安心して医療が受けられる仕組みになっている。

すなわち、高度・救命医療は公立置賜総合病院が行い、サテライト医療施設は住民のより身近な医療施設として、初期医療や慢性期の治療を行うように機能分化されている。また、一部の診療科では公立置賜総合病院の医師が、実際にサテライト医療施設に定期的に出張して診察を行うなど、継続した治療を行うことが可能となっている。さらに、共通診察カードの発行、電子カルテを利用した情報ネットワークの構築による患者情報の共有化など、患者さんの利便性に配慮した運営を行っている。

このように、置賜医療圏では、従来合った病院を再編成して、機能分化を図り、その間をネットワークでつないでいる。ここで利用されているシステムは、単一のアプリケーションであり、基幹施設のシステムをサテライト医療施設がリモートで利用する形態をとっているため、資格認証は機関側のシステムで一元化していた。したがって、異なる施設間の資格認証というよりは、すべての従事者を基幹施設側のシステムに登録し、同一施設内の資格認証という形式をとっていた。

3) 医師会の組織率

異なる施設の情報を一元的に持っている団体として医師会がある。そこで、医師会組織による資格認証の可能性について、最新のデータなどを調査した。平成13年8月1日現在、日本医師会員数は、155,662人であり、平成10年末の我が国の医師数が248,611人であることから、日本医師会における組織率（医師が医師会に入会している割合）は、62.6%になる（別添資料）。医師会には、入会時に医籍番号を登録しているため、医師会員であればある程度の認証は可能と考える。医師会以外に、認証をする機関としては保健所や保健センターが考えられるが、IT化に関しては、医師会の方が進んでいる。

今年度の経済産業省の補助事業である「先進的IT活用による医療を中心としたネットワーク化推進事業」においても、大学や中核医療機関よりは、地域医師会が中心的な役割を果たしていた。

D. 考察

情報ネットワークによる患者紹介・逆紹介等医療機関の緊密な連携を行うことにより、患者の症状等に応じた適切な治療をおこない、診療所におけるかかりつけ医機能、中核病院における高次医療機能の実現を図るためには、情報技術の利用時

の施設認証や資格認証が必要になる。

新宿区医師会におけるコンピュータネットワークを利用した包括的地域ケアシステムを十分に生かすためには電子カルテも整備されていた方が望ましい。その電子カルテは医療情報データベースであるが、医療情報はそれに関係する全ての人々が共有すべきものであり、決して医師だけのものではない。すなわち、患者、医師、看護婦、臨床検査技師、薬剤師、診療放射線技師、事務職員など、様々な人々が参照できる必要がある。このような電子カルテができてはじめて、医師同士や、スタッフとの意見のやりとり、施設を越えたコンサルテーションなどが有効に利用できるようになる。ただし、実用化に当たっては、データの安全性が非常に重要であり、患者のデータが無関係な人に勝手に扱ってはならない。

そのためには、医療従事者として資格確認や本人認証を行う必要がある。この認証ができると、患者紹介時などにデータを電子的に紹介先へ送ることができる。また、様々な医療上の照会・調査も診療所の情報システムに蓄積されているものを編集して利用できる。新宿区のシステムでは、ネットワークセキュリティの対策としてクローズドなネットワークとしており、インターネットとは接続していなかった。すなわち、医師会事務局と各地域医療中核病院、訪問看護ステーションは専用線接続されていた。また、診療所や学校、在宅患者宅はデジタル公衆回線を利用していたが、そこでは統合化セキュリティ (ISCL: Integrated Secure Communication Layer Protocols) 技術を利用して、電子認証や暗号化によりセキュリティを確保している。認証にあたっては、医師会事務局で資格認証を行うこととしていた。医師会事務局が行う理由は、医師会の入会審査時に医師免許証番号を照会しているからであり、医師である資格審査をする代行機関として適当であると考えられた。しかし、前述したように、医療機関には、医師以外にも看護婦、検査技師、薬剤師、レントゲン技師、事務職員など、様々な人々が関与する。それらコメディカルスタッフの認証にあたって、雇用者である診療所側の情報システム化が図られつつあるので、今後構築される医師会の情報システムによる認証の可能性についての検討が必要であると考えられた。しかし、介護保険等の導入により、医師以外の職種で、医療機関に属さない場合も出てくる可能性があり、将来的には保健所等の公的組織で認証する必要が出てくる可能性もあると考えられる。

E. 結論

情報の共有化を図る前提として、ファイアーウォールなどで安全なネットワークを構築すると共に、医療従事者として資格確認や本人認証を行う必要がある。実際に医師会により資格認証している例として、新宿区地域において医師会情報システムにおける資格確認や本人認証は、医師会事務局で資格認証を行うこととしていた。その理由は、医師か医院の入会審査時に医師免許証番号を照会しているからである。したがって、医師である資格審査をする代行機関として、医師会事務局は適当であると考えられた。

F. 健康危険情報

なし。

G. 研究発表

1. 論文発表

秋山昌範、地域医療連携システム～1地域・1患者・1カルテの実現～、医療マネジメント学会監修、新たな医療連携の実践～その現状と方策、pp147-153、じほう、東京、2001.

H. 知的財産権の出願・登録状況

なし。

日本医師会及び都道府県医師会会員数・勤務医会員数

(平成13年8月1日現在)

コード	都道府県	日本医師会							都道府県医師会			参考 平成10年 末医師数
		会員数					勤務医 会員数	構成割合 (%)	会員数	勤務医 会員数	構成割合 (%)	
		総数	A①	A②	B	C						
1	北海道	6,175	2,635	1,555	1,797	188	3,540	57.3	7,998	5,313	66.4	10,990
2	青森	1,260	837	215	208	0	399	31.7	1,448	551	38.1	2,487
3	岩手	1,751	717	141	884	9	990	56.5	2,206	1,432	64.9	2,390
4	宮城	2,832	1,307	737	780	8	1,525	53.8	2,913	1,686	57.9	4,350
5	秋田	1,488	601	134	734	19	887	59.6	1,488	887	59.6	2,127
6	山形	1,583	697	220	666	0	834	52.7	1,583	834	52.7	2,220
7	福島	2,480	1,103	500	877	0	1,274	51.4	2,480	1,274	51.4	3,534
8	茨城	2,227	1,332	437	458	0	785	35.2	2,554	1,092	42.8	4,087
9	栃木	1,791	1,131	300	360	0	665	37.1	1,837	700	38.1	3,681
10	群馬	1,945	1,295	369	279	2	648	33.3	2,238	913	40.8	3,805
11	埼玉	5,109	3,091	689	1,329	0	2,018	39.5	5,109	2,018	39.5	8,004
12	千葉	3,627	2,762	348	517	0	870	24.0	4,580	1,599	34.9	8,140
13	東京	18,383	9,391	2,062	6,525	405	8,992	48.9	19,230	9,633	50.1	31,295
14	神奈川	7,389	4,707	912	1,769	1	2,682	36.3	7,398	2,684	36.3	13,766
15	新潟	3,167	1,330	398	1,438	1	1,837	58.0	3,171	1,839	58.0	4,209
16	富山	1,273	716	87	468	2	510	40.1	1,553	759	48.9	2,338
17	石川	1,128	756	188	184	0	372	33.0	1,576	752	47.7	3,004
18	福井	913	487	172	251	3	414	45.3	925	425	46.0	1,636
19	山梨	954	505	113	336	0	443	46.4	1,031	520	50.4	1,613
20	長野	2,052	1,182	411	459	0	837	40.8	2,607	1,348	51.7	4,003
21	岐阜	2,379	1,276	171	931	1	1,082	45.5	2,416	1,119	46.3	3,405
22	静岡	3,720	2,047	520	1,153	0	1,673	45.0	3,736	1,687	45.2	5,735
23	愛知	7,638	4,053	780	2,502	303	3,282	43.0	7,644	3,287	43.0	12,170
24	三重	2,150	1,154	443	553	0	954	44.4	2,228	1,142	51.3	3,268
25	滋賀	1,415	699	174	542	0	698	49.3	1,772	999	56.4	2,333
26	京都	2,940	2,125	406	408	1	813	27.7	4,139	1,688	40.8	6,925
27	大阪	15,439	7,515	5,514	2,249	161	8,608	55.8	16,826	9,867	58.6	20,154
28	兵庫	8,483	4,392	2,382	1,638	71	4,091	48.2	8,686	4,269	49.2	10,576
29	奈良	1,804	922	308	463	111	868	48.1	1,946	971	49.9	2,607
30	和歌山	1,476	996	244	236	0	542	36.7	1,494	559	37.4	2,382
31	鳥取	702	427	115	160	0	275	39.2	1,188	749	63.1	1,573
32	島根	917	534	145	238	0	366	39.9	1,156	600	51.9	1,747
33	岡山	2,533	1,409	376	748	0	981	38.7	2,983	1,378	46.2	4,640
34	広島	4,708	2,351	1,744	556	57	2,357	50.1	6,190	3,809	61.5	6,427
35	山口	2,106	1,197	557	352	0	862	40.9	2,544	1,046	41.1	3,342
36	徳島	1,364	726	296	342	0	638	46.8	1,364	638	46.8	2,188
37	香川	1,814	724	417	673	0	1,034	57.0	1,814	1,034	57.0	2,405
38	愛媛	2,613	1,106	1,041	466	0	1,466	56.1	2,885	1,731	60.0	3,294
39	高知	1,412	557	482	373	0	806	57.1	1,441	835	58.0	2,097
40	福岡	6,900	3,801	1,301	1,798	0	3,099	44.9	7,078	3,276	46.3	12,575
41	佐賀	1,333	661	372	298	2	664	49.8	1,333	664	49.8	1,854
42	長崎	3,015	1,280	1,113	622	0	1,691	56.1	3,015	1,691	56.1	3,638
43	熊本	2,764	1,396	557	811	0	1,304	47.2	2,764	1,304	47.2	4,471
44	大分	1,889	883	541	453	12	1,006	53.3	1,889	1,006	53.3	2,694
45	宮崎	1,575	797	320	458	0	757	48.1	1,575	757	48.1	2,343
46	鹿児島	3,562	1,210	1,912	440	0	2,232	62.7	3,562	2,232	62.7	3,791
47	沖縄	1,484	616	449	419	0	853	57.5	1,834	1,198	65.3	2,298
	計	155,662	81,436	32,668	40,201	1,357	73,624	47.2	169,427	85,795	50.6	248,611

(「勤務医会員数・勤務医部会設立状況等調査」より)

研究要旨 資格認証の実証システム構築のために、資格認証に付随する処理形態の検討を電子資格証明書の発行と利用フェーズに分け、また電子資格証明書の形式を鍵付と鍵無し証明書に分けて考察した。セキュリティを含めて鍵生成コストが安い場合は鍵付の電子資格証明書が使いやすい。また、既取得の個人認証電子証明書が流用でき、一人が各種の資格を取得する場合は鍵無し証明書が有効で、今後の電子政府や電子自治体の個人認証基盤の整備動向あるいは特定認証業務の普及と協調して進めることが重要である。この際、法案が準備されている公的個人認証サービスの利用は有用である。また、医師資格確認として、公的個人認証サービスの情報と医籍簿のみの照合では資格保有者をユニークに同定できない場合があり、証明書を国家試験合格時に発行しない場合は何らかの補助的手段が必要である。また、医師の電子資格証明書の発行機関は電子医師免許証として位置づけるのであれば厚生省かその委託機関となる。また電子資格証明書を取り扱うためのソフトウェアは未成熟なので、標準ソフトウェア開発の推進も重要である。

A. 研究目的

個人情報保護に配慮しつつ医療情報をサイバースペースで活用するためには、医師または薬剤師等の公的資格に関する署名の確認やアクセス権限制御等での認証機能が必要である。住基カードを用いて医師等の国家資格医療従事者の認証をネットワーク上で行うことを目指した実証システム構築のために資格認証に付随する処理ステップの検討と各ステップでの処理形態の列挙を行い、システムとしてあるべき処理形態を考察する。

B. 研究方法

資格認証システムの構築のために電子的な証明書すなわち電子資格証明書（電子免許証）を住基カードのようなマルチアプリケーションを考慮したICカード内に格納して使用することを検討する。その為に処理の異なる「電子資格証明書発行フェーズ」と「電子資格証明書利用フェーズ」に分けて検討を行う。また、電子資格証明書に対応する秘密鍵は資格保有者の所有するICカードに格納するものとした。電子資格証明書はICカードの容量やシステム設計上の都合で必ずしもICカードの中に無くてもよく、LDAPのようなサーバにあってても良いが、基本的パターンとしてICカードに格納されている場合を検討する。ここでは医療従事者用の専門カー

ドの代表として、医師の専門家カードを検討し、それを対象とした各ステップでの処理方法、形態および必要項目を列挙し、考察を行う。

C. 研究結果

1. 資格証明書の形式と処理フェーズ

電子資格証明書の形式としては以下の2通りの形式がある。

- a) 鍵付電子資格証明書形式（公開鍵証明書単独方式）
- b) 鍵無し電子資格証明書形式（公開鍵証明書分離方式）
 - a) の場合は公開鍵証明書の拡張領域に資格を記述する形式で、証明書発行申請の際、資格を証明するものと電子資格証明書に添付する公開鍵を提出する必要がある。
 - b) の場合は本人を認証する公開鍵証明書と資格を示す属性証明書を分離する形式で、申請の際は資格を証明するものと既に取得した公開鍵証明書を提出し、これにリンクした形で属性証明書を発行してもらう。既得の適当な公開鍵証明書の無い場合は新たに入手の必要がある。

資格認証システムとして検討する場合、以下の2つのフェーズに分けられ、それぞれ処理が異なり、独立して検討することができる。

a) 電子資格証明書発行フェーズ

b) 電子資格証明書利用フェーズ

以下、この2フェーズと前期2形式を勘案し、各フェーズのステップとその時必要な処理方法および形態を列挙する。

2. 電子資格証明書発行処理フェーズ

2. 1 発行の処理ステップ

発行処理ステップとしては以下が代表的手順である。

- a) 専門家がRA (Registration Authority : 登録局) に電子資格証明書発行を申請
- b) RAは申請者が本人であることおよび資格保有を確認
- c) RAはIA (Issuing Authority : 発行局) へ公開鍵を送り証明書の発行を依頼
- d) IAよりRAへ公開鍵証明書を受領
- e) RAより申請者へ証明書を交付

2. 2 各ステップの主要処理

以下各ステップに必要な主な処理について検討する。

2. 2. 1 鍵ペアの発生処理方法

秘密鍵と公開鍵の生成方法は以下の方法が考えられる。

- a) 秘密鍵を申請者の管理するシステムで発生し、ICカードにIMPORTし、公開鍵を申請時提出。
- b) ICカード内で発生させ公開鍵を外部にEXPORTして申請時提出。
- c) RAで発生させ秘密鍵をICカードにIMPORTし、公開鍵をRAで受取、IAへ伝送 (IAで発生させる場合も含む)

2. 2. 2 本人確認

以下にそれぞれの項目で考えられる方式を列挙する。

1) 実在性の確認

下記方式により本人が実在していることが確認できる。

- a) 公的個人認証サービスの電子証明書の利用
公的個人認証サービスにより市町村は住所、氏名、生年月日、性別および公開鍵を含んだ電子証明書の発行を行う。本公的個人認証サービスに関する法案は本年度国会提出予定で、個人の印鑑登録の電子的なものにあたる。CRL (Certificate Revocation List) で失効していないかの確認が必要である。
- b) 特定認証業務の発行した公開鍵証明書の利用

特定認証業務として本人の実在性の確認として電子証明書が発行される。CRLでの失効確認が必要である。

c) 住民基本台帳の利用

申請書に記載された申請者の基本4情報と当該市町村が備える住民基本台帳に記録されている情報を照合することにより、申請者が実在することを確認。例として住民票の提出がある。

2) 申請者本人性の確認

次の方法のいずれかのもにより、申請者と称する者が実在性の確認された申請者本人であることを確認する。

a) 公的個人認証サービスの秘密鍵の利用

公的個人認証サービスで証明された秘密鍵により電子資格証明書申請書に電子署名を行ったものを提出させる。

b) 写真添付の公的証明書の利用

官公署の発行した電子資格証明書、運転免許証、旅券その他本人であることを証明できる書面であって、本人の写真を貼付してあるものの提示を求める方法

c) 写真無し他公的証明書と知識の利用

本人であることを証明できる上記以外の書面 (各種健康保険の被保険者証、各種年金の年金手帳等 (申請の受付窓口において、当該書面に係る原簿データを閲覧できるもの)) の提示を求めるとともに、当該書面に係る原簿データに記録されている本人に関する事項について適宜質問し、当該データと照合して確認する方法

d) 特定認証業務により発行された証明書に対応する秘密鍵で申請書に電子署名を行った者を提出させる。

3) 受取者本人性の確認

電子資格証明書を正当な申請者に受け取らせる必要がある。

a) 対面での受取

証明書の申請や受け取りを対面で行う場合は2) の本人性確認と同様におこなえる。

b) ネットワーク経由の受取

ネットワーク上で証明書を伝送する場合は相手が申請した受取相手が確認の必要がある。この場合は相互の秘密鍵でそれぞれ、その時にユニークな乱数を暗号化する等の方法で相互認証を行い相手の本人性の確認を行う。

c) 郵便による送付

転送禁止便にて本人の住所へ証明書を送付する。

2. 2. 3 資格確認

電子資格証明書を発行する際に申請者が資格を保有しているか確認する方法として考えられる方法を以下に列挙する。ここでは列挙にとどめ評価は考察で行う。

- a) 医師免許のコピーを提出させる
- b) RAが4基本情報をもとに医籍簿をチェックする
- c) RAが厚生統計情報部の2年に1回行う医師調査のデータベースをチェックする。
- d) 施設責任者等グループの責任者で公的電子資格証明書の既取得者に申請者が医師であることを署名させる。

3. 電子資格証明書の利用フェーズ

3. 1 電子署名への適用

3. 1. 1 電子署名の実施

紹介状、処方箋等医師が内容に責任を持つ意味で電子署名を行う場合を想定する。処理の代表的例を以下に示す。

- a) 文書のハッシュ値をとり対応する秘密鍵で暗号化を行いMAC (Message Authentication Code) を作成する。
- b) 文書、MAC、証明書類を伝送するためにファイルをパッケージ化する。
- c) 送り先へ送信する。

3. 1. 2 電子署名の検証

受取側の処理ステップを説明する。

- a) 公開鍵証明書が正当か検証する。(証明書の有効期限、CRL等による有効性、認証局の正当性の検証)
- b) 鍵無し電子資格証明書形式の場合は電子資格証明書の正当性を検証する。
- c) 資格を証明書から抽出する。
- d) 文章のハッシュをとりMACを公開鍵で復号したものと同一値になれば公開鍵に対応する本人が正当に署名したものとし署名者および資格を表示する。

2. 1 アクセス権限制御への適用

クライアント側からアクセスしたサーバが医師にしか見せないデータへのアクセスを許可する場合を想定して処理ステップを記述する。

- a) クライアントがサーバを選択し、必要データを選択する。
- b) そのデータが医師にしか許可されていない場合は医師であることの認証を要求する。
- c) クライアントは電子資格証明書に関連した個人認証の秘密鍵を使ってサーバ主導で作成された乱数を暗号化した値をサーバに送り返す。この時、電子資格証明書、分離方式の場合は個人認証用公開鍵証明書も付属させて送り返す。
- d) サーバ側は電子証明書の正当性を確認する。
- e) サーバ側は暗号を電子証明書の公開鍵で復号し、元の乱数と同じになれば、アクセス者が正当な医師と確認する。
- f) サーバはクライアントに要求のデータを伝送する。

3. ハードウェア

秘密鍵および電子資格証明書はICカードに格納するものとする。秘密鍵と公開鍵の発生はICカード内で発生させる必要はなく、外部で発生させ、秘密鍵のIMPORTも可能とする。

4. ソフトウェア

電子資格証明書が公開鍵付場合はISO/TS17090-2(参考文献1)に従ってその中の”HcRole”の項目に”Medical Doctor”(医師)を記録する。分離する場合はX509の属性証明書の形式で電子資格証明書を発行する。ISO/TS17090に属性証明書も記述されているが流動的である。この原典はIETFより発行されたdraftであるので、参考文献2)に示すIETFサイトをフォローする必要がある。

こうした電子資格証明書を扱えるフリーウェアは現在無く、CA用のOpen SSL等を改造して使用する必要がある。名古屋工業大学の岩田研究室で開発した、AICAは比較的改造しやすく、電子資格証明書発行プロトタイプとして使用するには便利である。今回、実際に改造できることを確認し、その結果は参考文献3)に示されている。

5. 認証局の証明書ポリシー

電子資格証明書を発行する認証局はCP (Certificate Policy: 証明書ポリシー) を公開しなくてはならない。これに関しIETF RFC 2527 “Internet X.509 Public Key

Infrastructure Certificate Policy and Certification Practices

Framework”に認証局が運用し定めなければならない項目が定められている。医療情報の場合は参考文献1)でTS化されている。この項目および運用が電子証明書の信頼性や互換性を定めるので重要である。主な要求項目は以下である。

- 1) はじめに
- 2) 一般条項
- 3) 利用者の識別方法と本人確認方法
- 4) 業務手続き
- 5) 建物・関連設備、運用、要員のセキュリティ管理
- 6) 技術的なセキュリティ管理
- 7) 証明書と失効管理のプロファイル
- 8) 本ポリシーの管理

D. 考察

1. 公的個人認証サービスの活用

平成14年2月28日に総務庁より報道された「地方公共団体による公的個人認証サービス」によって検討をおこなった。国会審議をへて法制化されるので今後変更されることがありうる。現在は以下のような運用になっている。

1. 1 署名検証者

署名検証者は次の者のうち、あらかじめ都道府県知事に届け出た者とする。

- a) 行政機関等（国の機関・地方公共団体の機関等）
- b) 特定認証業務を行う民間認証事業者で一定の信頼性を有するもの

1. 2 使用制限

利用者から受け取った電子証明書をオンライン申請等の電子署名の検証以外の目的で利用することを禁止する。

1. 3 サービスの活用

- a) 行政手続のオンライン申請等の手続保障
- b) 民間認証事業者が行う特定認証業務の本人確認
- c) 特定認証業務のみを行う場合のほか、特定認証業務とあわせて本人の資格等の属性を証明する業務を行う場合も想定

電子公的資格証明書の発行は、行政手続と考えられ

るので行政機関が電子資格証明書を発行するのであれば本人確認に使用することができる。また、特定認証業務のオンライン申請時の確認として既述の申請書本人性の確認として2. 2. 2 2) a)の採用が有効となる。

2. 資格確認での成りすまし防止

医師免許および医籍簿は「免許番号、氏名、生年月日、本籍、発行年月日」で管理されている。一方、公的個人認証サービスは「氏名、生年月日、住所、性別」で管理されている。

両者をつなぐキーは「氏名、生年月日」である。これが一致している対象者が複数存在する場合、医籍簿の確認のみでは証明を誤る可能性があり何らかの補助的確認手段が必要である。

また、医籍簿は変更が届け出制のため改姓等の変更にもこまめに対応しているとは言いがたく、申請者への変更確認が必要である。

これは国家試験合格後医師免許証としてまたは免許証と平行してICカードを発行する場合は合格証等での確認ができるので、これの更新を継続していくことにより成りすましを防ぐことができる。しかし、既に医籍簿に登録された医師の資格証明カードを発行する場合はその申請時、補助的確認手段の配慮が必要である。

3. 電子資格証明書の形態

研究結果の章で記述したように電子資格証明書の形式として鍵付形式と鍵無し形式がある。署名や認証の際は認証のための鍵が必要になるのどちらも鍵を意識する必要がある。

3. 1 電子資格証明書発行フェーズ

申請者側の違いは電子資格証明書申請時、公開鍵の提出か、別途事前に保有している公開鍵証明書の提出かになる。

発行者側の違いは公開鍵証明書を作成するのか、属性証明書を作成するのかの違いになる。前者の場合は申請者が公開鍵に対応する秘密鍵を保有しているかの確認が必要になる。あるいは発行者側で鍵を生成する場合はその分の取扱が必要になる。後者は提出された公開鍵証明書の有効性確認が必要である。

従って鍵を安全に生成できるコストと失効確認のコス

トの比較になる。

3. 2 電子資格証明書利用フェーズ

利用での両者の違いは鍵付の場合は証明書が1枚であるが、鍵無しの場合は2枚必要になり、その2枚間の対応性の確認が必要となる。処理ソフトウェアとしては公開鍵のエリアからの抽出ソフトか2枚の証明書処理ソフトの違いになり、一般的に後者の方が開発工数がかかるが、一度開発すれば、その後の評価はメンテナンスコストとメモリー容量や処理速度の評価になる。

4. 電子資格証明書発行機関

電子資格証明書を医師免許と同等な位置付けで与えるのであれば、厚生省かその委託先になる。その場合RAとIAの分離は可能である。

この場合、電子政府で実施される大臣印等の職印で発行されると思われる証明書との違いを明確にすべきであるが、この場合は公開鍵との結合は考えにくい資格認証カード発行としては別のシステムとした方が業務の単純化につながると考えられる。

E. 結論

電子資格証明書の形式としては、鍵生成コストの安い場合は鍵付資格証明書が良い。この場合は秘密鍵の管理の信頼性がポイントになる。また、個人で資格証明書をいくつも取る場合で公的に信頼できる鍵生成のコストが高い場合は信頼できる個人認証用の公開鍵証明書と分離した鍵無しの資格証明書が良い。この場合、公的個人認証サービスの電子証明書が使用できることが望ましいが、現在の法案では行政への電子申請か、特定認証業務の本人確認に限られているため、別手段が必要である。この問題は医療情報システムだけの課題ではなく、電子政府や電子自治体の基盤整備の動向とあわせて検討していくべきである。

本人認証を確実にオンライン等、デジタル的に行うには公的レベルで本人確認が保障される公的個人認証サービスを利用することが推奨される。

資格確認は現在の医籍簿のみに対して検索をする方式のみでは不十分で、医籍簿の情報を増やし、メンテナンスをよくするか、別途確認のための補助的手段の併用が

望ましい。

電子資格証明書の発行機関は医師免許と同等に電子免許証として与えるのであれば厚生省かその委託を受けた団体とすべきである。また、運用上で医師資格認証用の証明書の発行であれば国民に信頼される機関であれば発行可能である。その場合も本人確認に公的個人認証サービスを利用することが望ましく、その場合少なくとも特定認証業務の認定をうけた者が行う必要がある。また、証明書発行ポリシーを公開し国民や運用関係者の信頼を得る必要がある。

資格証明書発行用ソフトウェア、資格証明書利用ソフトウェア、資格証明書検証ソフトウェアは標準的なものが開発されていないので証明自体の記述の標準化とあわせて開発体制を考慮すべきである。

F. 参考文献

- 1) Health Informatics – Public Key Infrastructure (ISO/TS17090)
- 2) An Internet Attribute Certificate Profile for Authorization :internet-Draft (Draft-ierf-pkix-ac509prof-09.txt)
- 3) 高橋裕樹・鈴木裕之・小尾高史・山口雅浩・大山水昭・角田 貢・喜多統一, 属性証明書を利用した保健医療分野における資格認証システム, 2002年電子情報通信学会大会予稿集, 2002

G. 研究発表

学会発表

- 1) 高橋裕樹・鈴木裕之・小尾高史・山口雅浩・大山水昭・角田 貢・喜多統一, 属性証明書を利用した保健医療分野における資格認証システム, 2002年電子情報通信学会大会予稿集, 2002

雑誌発表

- 1) 喜多統一, これからのセキュリティのあり方, 新医療, 第28巻第8号, p87~90, 2001
- 2) 喜多統一, 電子カルテとセキュリティ, INNERVISION, 第16巻第7号, p66~69, 2001
- 3) 喜多統一, カードシステム, IT医療白書, p33~39, 2001

厚生科学研究報告書

薬務関連における資格認証の実施方策の調査・検討

分担研究 土屋 文人（東京医科歯科大学歯学部附属病院薬剤部）

（要旨） 処方せんが電子化された場合を想定し、個人認証との関係について研究を行った。処方せんの電子化際としては、単に処方内容等、処方せん記載事項の電子化を考慮すればよいのではなく、現行の紙媒体としての処方せんが有する機能をみることが必要である。具体的には、患者の薬局選択権および患者に対する処方情報の一元管理を強制しないことがある。また現行でも実行されていないが、潜在する問題点として、処方せんのアライバイ情報の確保ができていないという問題がある。電子処方せんについては、疑義照会時の医師・薬剤師の認証をどのように行うかが問題となる。また、病院勤務の薬剤師については、保険薬剤師の登録が義務化されていないため、公的機関による認証ではなく、施設認証とせざるを得ないと思われる。処方せんの電子化については克服すべき問題が多いことから、認証問題の克服までの当面の間、処方箋情報の電子化を促進することで電子処方せんにおける問題点を解決すべきと考える。

1 はじめに

薬剤関連分野において最も認証が求められる場面は、処方せんに関係する場面であると推定される。処方せん発行には医師、歯科医師等が、調剤には薬剤師が関与するが、両者の間には、処方せん疑義照会が行われることから、単に処方せん記載時あるいは調剤時における個人認証にとどまらず、疑義照会においては、処方内容の変更を伴うことが多いことから、診療録との兼ね合いもあり、疑義照会が処方医と薬剤師間で確かに行われたことを担保するための個人認証が必要になってくる。そこで本研究においては処方せんの電子化を行う場合の課題について検討を行う。

2 方法

処方せんを電子化する場合に考慮すべき点を検討するとともに、院外処方せんの発行から調剤終了にいたる過程における個人

認証の必要性およびその問題点について検討を行う。

3 結果および考察

3. 1 処方せんの電子化と資格認証

処方せんの機能としては、患者に対する情報開示の面と、薬剤師に対する調剤に関する指示の面とがある。また調剤を受ける薬局の選択権は一方向的に患者にあるのであって、医療機関が薬局を指定することは療養担当規則により禁止されている。処方せんを電子化することは、患者への情報開示機能が失われ、かつ患者の有する薬局選択権を制限する可能性があることから、この面での調和をどのように図るのが問題となる。

現行において、医療機関にファクスが設置され、患者が調剤を受ける保険薬局にファックス送信を行うことがあるが、その場

合ファックスされ、薬局に出力されたものは、「処方せん情報」であり、「処方せん」ではないという考えである。すなわちファックス送信を受けた薬局では、ファックス送信された「情報紙」を参考に調剤の予備行為を行うが、患者が持参する処方せんを得て、最終的に調剤行為を行うというのが、現行のファックス送信における「処方せん」と「調剤」との関係についての解釈である。従って、電子処方せんを考える場合には、まず、処方せん発行時に患者に対して処方内容を開示することが求められることになる。これについては、お薬手帳等に情報を記載（ラベル発行）する等の方策が現実的と思われる。次に患者の薬局選択権を考慮することなく、電子処方せんを薬局に医師が送信することは、現行において法的に禁止されていると解すべきであろう。医師自身の意志ではなく、患者の強い希望による送信代行を医師が行うとの解釈は可能と思われるが、診察の都度医師が患者に薬局をどこにするのかを尋ねて送信を行うということは、現実には発生しにくいと思われる。

そこで患者の薬局選択権を保持しつつ電子的な媒体で医師が処方せんを発行するためには、データストアを行う施設を設置し、医師はそこに処方せんを送付し、患者に対しては発行した電子処方せん内容を開示した文書を手渡すとともに、患者が所持するICカードに処方せんが発行されたことを示す情報を入れる。患者は調剤を受ける薬局でICカードを定時し、薬局側はそのカードを鍵として、処方せんデータストア施設から取り出す（その際調剤を行う保険薬局の名称等の情報を処方せん発行医療機関にフィードバックし、処方データは消去す

る）という形式が一番可能性が高くなると思われる。患者が持参したIDカードを鍵として利用し、情報が出されたことで内容を消去すれば、処方せんのコピーを利用した詐欺事件等の発生防止にもなるし、現行においては全く知る由もない処方せんの所在情報も医療機関が知ることとなる。

この段階における資格認証は、保険医は施設認証、保険薬剤師は都道府県薬剤師会等が認証を行うことも可能と思われる。保険薬局に勤務する非常勤薬剤師の場合、同一都道府県であれば主たる勤務薬局が届けであるのみで、すべての勤務先が登録されているわけではないことから、認証を都道府県単位の薬剤師会等が行うことが必要と思われる。

3. 2 疑義照会における資格認証

処方せん中に疑わしい点があった場合には、薬剤師法第24条により、薬剤師は疑義照会を行った後でなくては調剤してはならないことが定められている。現状における院外処方せんでの疑義照会のほとんどは電話を利用した疑義照会である。その他のケースとしては、ファックスを利用して当該医療機関の薬剤部に疑義照会を行う（ファックスを受けた薬剤部が保険薬局の薬剤師の代わりに医師に疑義照会を行う）場合が存在する。前者の場合には、電話口には処方医が直接である場合もあれば、代理の医師（医局長等）、看護師等、本人以外が対応をする場合が少なからずある。現実としては看護師等の場合には、処方医に口頭で確認し、返答は当該看護師が行う場合が多い。また処方医が不在のため、代理の医師が対応する場面もあることから、このような場

合の資格認証をどのように行うかが問題となる。これは電子処方せんの問題ではなく、現在でも本来問題となってもよいのであるが、実際には性善説に立って処理が行われていることから、問題が潜在化していたものである。種々の電子化において、厳しく原則通りの運用を求められるため、従来から存在した問題が顕在化してきた例である。これらにどのように対応するのかは極めて重要なことであり、早急に関係法令を含め解決すべき問題と思われる。

4 おわりに

処方せんの電子化問題は医師法、薬剤師法等に関連するのみならず、患者の知る権利をどのように担保するのかが問題となっている。今回検討した方式で電子処方せんを実施した場合に、一番の問題は電子化することの意味があるのかということである。確かに、現状において処方せん記載内容を電子化することはそのみを捉えれば、電子化の利点が見えてこないといえる。処方せんを電子化することの意味は、国民にと

って直接の利益を生み出すことであろう。具体的に言えば、最低限、重複投与や相互作用等のチェックが行われることが求められるであろうし、もう少し進化するれば、医薬品の有害作用防止等のめんでの配慮もなされることが求められることになると思われる。そのためには、現在施設毎で異なる各種チェックシステムの標準化が必要となる。医薬品コードの標準化がやっとなされたばかりという現状を考えるとやむを得ないのかもしれないが、e-JAPAN 構想の下、期限を切って各種の基盤整備を行う必要がある。そのような基盤整備なし処方せんの電子化を行ったとしても、それは多くの国民の支持を得ることはできないであろう。薬剤師の資格認証という面からすれば、法的地位を持たない病院薬剤師に対してどのような解決を図るのかも大きな課題である。前述の基盤整備とともに、法的な面での基盤整備も早急に行う必要がある。これらが相俟って初めて資格認証の意味が理解されるのではないかと思われる。

研究成果の刊行に関する一覧表

書籍

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
秋山 昌範	地域医療連携システム～1地域・1患者・1カルテの実現～	医療マネジメント学会監修	新たな医療連携の実践～その現状と方策	じほう	東京	2001	147-153
大山 永昭	電子政府と行政ICカードの方向性	ICカードシステム利用促進協議会	ICカード総覧2001	(株)シーメディア	東京	2001	16-26

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
大山 永昭	個人認証の考え方と制度的な対応	映像情報メディア学会誌	Vol. 55, No. 2	168-171	2001
大山 永昭	電子政府の構築と個人認証の考え方	ハイパーフラッシュ	2月号	2-7	2001
大山 永昭	電子政府とICカード	月刊 Keidanren	2月号	24-25	2001
大山 永昭	サイバーパスポートの実現	edit21	2月号	12-15	2001
大山 永昭	次世代ICカードが拓くIT社会	蔵前ジャーナル	4月号	13-18	2001
大山 永昭	次世代ICカード元年	雑誌エレクトロニクス	6月号	2-3	2001
大山 永昭	電子政府の展開と電子カルテ	INNERVISION	Vol. 16 No. 7	74-77	2001
大山 永昭	住民基本台帳ネットワークシステムの構築とICカードの利用	フォト	8月号	40-41	2001
大山 永昭	医療情報システムを取り巻く社会情勢の変化	日本放射線技術学会第56回総会学術大会	2000. 4. 6～4. 9開催	77	2001
八幡 勝也	Information Sharing System on Periodic Health Examinations by a Regional Medical Association	MEDINFO 2001	2001. 9. 11. 46	1509	2001
八幡 勝也	北九州マルチメディア職域・地域一体健康管理システムの開発と実証実験	信学技報	2001-03	9-16	2001

八幡 勝也	地域医師会を中心とした健康診断情報共有ネットワークの運用結果の検討	医療情報学	21(1),	31-39	2001
喜多 絃一	これからのセキュリティのあり方	新医療	8月号	87-90	2001
喜多 絃一	カードシステム	I T医療白書		33-36	2001

2001122

以降のページは雑誌/図書等に掲載された論文となりますので
「研究成果の刊行に関する一覧表」をご参照ください。