名を確認することで、記された時刻にそのデータが存在していたことと、それ以後データが改ざんされていないことを確認することができる。

3.3 HPKI

ISO TS17090 に規定された医師等の資格を記述することができる保健医療福祉分野の X509 電子証明書の規格。日本では、厚生労働省が「保健医療福祉分野 PKI 認証局 証明書ポリシ」として署名用 HPKI 電子証明書のポリシを定めている。

4. 電子署名・タイムスタンプ

電子署名・タイムスタンプの対象にては、CDA 文書の本文ファイルについてのみとする。CDA 文書から参照される外部参照ファイルに関しては直接の署名対象とはしない。これらの外部参照ファイルに改竄のないことを証明し、参照したことに関する責任の所在を明らかにするために、CDA 文書の本文ファイルへの署名の効果を及ぼしたい場合は、本文ファイルの参照ポイントを記載する部分に参照ポイントを示す URI のほかに、対象外部参照ファイルのハッシュ値およびそのハッシュを計算したハッシュ関数の識別子を記載する。ハッシュ値およびハッシュ関数の識別子は HL7 ver.3 のデータタイプ ED を用いて記載する。したがってとりうるハッシュ関数は SHA-1 および SHA-256 に限定される。実際の記法は CDA Release 1 に準拠した CDA 文書の場合は本規格の付属書 A を参照すること。CDA Release 2 に準拠した文書の場合は referrence によって示し、ExternalAct、 ExternalDocument、ExternalObservation、および External Procedure においては text: ED を必須とする。

4.1 電子署名タイムスタンプの形式

電子署名タイムスタンプの形式については、RFC3275 に規定される形式の中で、Enveloping signature を使用する。多重署名を許容可能とする。またタイムスタンプが要求される場合は W3C の XAdES-T 形式で記述される。長期署名を行う場合は XAdES の関連規格に基づいて記述される。

4.2 電子署名

法律・規則で定められた署名または記名・押印に代えて電子署名を行い場合は電子署名法および関連規則に準拠した電子署名を行う。認定特定認定事業者の発行する署名用公開鍵証明書、公的個人認証サービスの公開鍵証明書および厚生労働省 HPKI 認証局専門家会議の認める HPKI 認証局の発行する署名用公開鍵証明書を用いる。署名の付与および検証は RFC3275 従う。ただし Enveloping Signature を用いるものとする。

HPKI 認証局の発行する署名用公開鍵証明書を用いる場合は Subject Directory Attributes の HcRole Attribute を検証時に確認する必要がある。

公的個人認証サービスを用いる場合は現状では特定の法人、団体、行政機関等しか検証できないことに留意しなければならない。

4.2.1 署名アルゴリズムについて

電子署名を行う際に使用する暗号化アルゴリズム及びハッシュアルゴリズムの組み合わせは以下のもののいずれかを使用し、検証アプリケーションは対象となる署名に用いられている証明書を発行したＣＡのＣＰまたはＣＰＳに検証に関する事項が規定されている場合は、それにしたがって検証できなければならない。特に規定がない場合は証明書プロファイルの仕様にしたがって検証できなければならない。

- sha1WithRSA Encryption（1.2.840.113549.1.1.5）
- sha256WithRSA Encryption（1.2.840.113549.1.1.11）
- sha384WithRSAEncryption (1.2.840.113549.1.1.12)
- sha512WithRSAEncryption (1.2.840.113549.1.1.13)

4.3 タイムスタンプ

RFC3161 に定義されるタイムスタンププロトコルを用い、TSA（Time Stamp Authority）からタイムスタンプトークンを取得する。取得したタイムスタンプトークンは署名付与時に生成される W3C の XAdES-T 形式で記述される。

タイムスタンプは、「タイムスタンプビジネスに係る指針―ネットワークの安心な利用と電子データの安全な長期保存のために―」（総務省、編成 16 年 11 月）等で示されている時刻認証業務の基準に準拠し、財団法人日本データ通信協会が認証した時刻認証業者のものを用いるものとし、第 3 者がタイムスタンプを検証できるものとする。

- 署名文書にはタイムスタンプを付与し、安全な電子保存を可能とする。
- TSA とのインターフェイスは RFC3161 で定義されるプロトコルに従って実装される。

付属書 A　CDA Release1 準拠文書における外部文書の参照　（Informative）

CDA Release1 準拠の CDA 文書において外部参照ファイルを用い、電子署名の影響を外部ファイルに及ぼす手段の例を記載する。

外部参照リンクは CDA 文書の本文の levelone – body – section – paragraph – content – local_markup に記載する。

local_markup タグの下に mref タグ、digest_method タグ、digest_value タグを持ち、mref タグで参照先ファイルの URI を指定する。digest_method タグで参照先ファイルのダイジェストを作成するハッシュ関数を OID で指定する。ハッシュ関数は SHA-1 および SHA-256 が使用可能であるが SHA-256 を推奨する。digest_vaue タグでは参照先ファイルのダイジェスト値を格納する。ダイジェスト値の表示は、もとのハッシュ値（バイナリ）を BASE64 でエンコードした文字列とする。

付録２

CDA 文書暗号化規格

ver. 1.00

日本 HL7 協会

目次

まえがき

昨今、患者あるいは家族から診療の把握、あるいはセカンドオピニオンを得たいという要求が高まってきている。また、医療・介護機関の機能分化と施設間連携を通じた医療・介護の効率向上が求められている。これらの要求を満たすために、適切に電子化された診療に関する情報を提供あるいは交換することが求められ、それらの文書の規格として HL7 CDA が存在する。CDA に準拠した文書は紙などの物理媒体と比べて大量の情報を含めることが可能で、一定の程度の安全性確保をすることがのぞましい。本規格は CDA 文書に安全性確保の目的で暗号化する場合の暗号化の手段を記述するものである。なお、この規格は暗号化を強制するものではなく、暗号化を行うかどうかは他の規格やドメインでの規約などで強制されない限り、CDA 文書を作成し、使用する当事者が自由に決めることができる。また暗号化の強度を用いる暗号の最高強度以下の任意のレベルに自由に設定できるように、鍵長を 16 octet より短く設定した場合のパディングルールを含めている。

ただし、鍵長を 16 octet より短く設定した場合はパディングルールを公開しているために、この規格が採用している暗号化方式の本来の強度が期待できないことに十分留意して使用する必要がある。

なお、本規格の目標は、以下のとおりである。

(1) 患者ケア情報の提供に重点をおく
(2) システムを低コストで実現できるようにする
(3) 記述された情報は、再利用の可能性があるものとする
(4) さまざまなドキュメント生成アプリケーションで互換性をもつようにする
(5) その文書の転送方式や格納のメカニズムとは独立である
(6) すみやかに設計書を提供する
(7) オープンな標準を使う

5. 適用

本規格は、特定の目的を持つ CDA 文書を可搬電子媒体に記録し使用する場合にデータを暗号化する際の仕様に適用する。暗号化を行うかどうかは本規格では規定しない。

6. 引用規格

本規格は、以下の規格を引用する。日付の付いた引用規格については、その日付以降に発行された修正票または改訂版は参照しない。しかしながら、本仕様書を使用する場合は、各規格の最新版を調べて適用するよう努めなければならない。

ISO/IEC 18033-3 :2005 Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers

XML Encryption Syntax and Processing (W3C 2002)

患者診療情報提供書規格 V1.00 (日本 HL7 協会 2006)

CDA 文書電子署名規格 V1.00 (日本 HL7 協会 2006)

7. 用語と定義

本規格では、以下の用語と定義が適用される。

3.1 可搬電子媒体

持ち運び可能な記録媒体のこと。CD-R、DVD、MO などを指す

3.2 共通鍵暗号

共通鍵暗号方式(Common key cryptosystem)とは、暗号化と復号に同一の鍵を用いる暗号方式である。秘密鍵暗号方式 (secret key cryptosystem) や対称鍵暗号 (Symmetric key encryption scheme) とも呼ばれる。

3.3 ブロック暗号

ブロック暗号 (Block cipher) とは、共通鍵暗号の一種で、ブロックと呼ばれる固定長のデータを単位として暗号化復号を行う暗号である。これに対して、ビット単位やバイト単位で暗号化を行う暗号はストリーム暗号と呼ばれる。

3.4 AES

AES は、 アメリカの国家新標準暗号規格 (Advanced Encryption Standard) で規格

化された共通鍵暗号方式である。 1977 年に発行された暗号規格 DES が技術進歩により時代遅れとなったため、新たな暗号方式の公募を行い、2001 年 3 月に FIPS PUB 197 として公表された。

3.5 SEED

SEED は 1998 年から韓国情報 Korea Information Security Agency と専門家のグループによって開発された 128 ビットの共通鍵ブロック暗号である。

3.6 Camelia

NTT と三菱電機で開発された共通鍵ブロック暗号である。鍵長は 128 ビット、192 ビット、256 ビットを選択できる。

3.7 ファイル名称

ファイルを可搬電子媒体上で一意に指し示すことができるラベル

3.8 拡張子

ファイルの属性等を示すために使われるファイル名称の部分文字列、JIS X 0606 のファイル拡張名など

8. 暗号化

可搬電子媒体には個人情報、および診療情報が含まれる。媒体は紛失、盗難の恐れがあるため、データの暗号化を行うことが望ましい。可搬電子媒体に含まれる診療情報ファイルを暗号化する場合は個別に暗号化を行う事とする。暗号化する診療情報には CT のシリーズ画像等も含まれる事があり、暗号化する電子ファイルの数が膨大となる可能性があるため IC カードでの暗号化の処理を必須としない。暗号化を行った電子ファイルの情報はデータを暗号化する際にログとして記述し、暗号化したファイルを復号する際に使用する。このファイル名を CRYPTLOG.XML とする。CRYPTLOG.XML は本規格による暗号化を行ってはならない。

また、可搬電子媒体に CDA 文書およびそこから参照されている情報以外のデータファイルやビュアソフトなどのプログラムファイルが含まれる場合には本規格による暗号化を行ってはならない。

4.1 要求事項

- 電子診療情報提供書には個人情報および診療情報が含まれるため、電子診療情報提供書に対するセキュリティを確保する必要がある。必要なセキュリティとして個人情報保護に関する法律や関連するガイドラインに適合する必要がある。

・ 紹介元と紹介先の機器のＯＳが異なっていてもデータが性格に伝達されなければならない。そのため、暗号化についてはファイルシステムに依存しない方法をとる。

4.2 データの暗号化

4.2.1 暗号アルゴリズム

暗号化に使用するアルゴリズムは 128 ビット共通鍵ブロック暗号方式とする。、利用できる暗号方式としては、ISO/IEC18933Part-2:2005 で規定されている以下の 3 方式とする。なお、鍵長・ブロック長は 128bit 固定とする。また、ユーザのセキュリティポリシにあわせて、最小4octet(32bit)から最大16octet(128bit)まで1octet 単位で任意の長さの鍵長の「暗証番号」を使用することができるものとする。暗証番号の長さが 16 octet より短い場合は、7.4.2 に述べる方法でパディングし鍵長を 16octet に拡張する。暗証番号はユーザが生成しシステムに入力する場合と、システムがランダムに生成する場合を選択できるように構成することが望まれる。システムによっては、入力または生成する暗証番号を数字のみや英数字と特殊文字などのように限定してもよい。

表4. 1 利用可能な暗号

項	暗 号	拡張子(利用可能な場合)
1	AES	AES
2	SEED	SED
3	Camelia	CAM

- 鍵長: 128bit
- ブロック長: 128bit

4.2.2 暗証番号のパディング・アルゴリズム

128bit の秘密鍵の LSB から順に 0octet,1octet,.....15octet と各オクテットを命名する。ユーザ又はシステムが生成した暗証番号の長さを n octet(4≦n≦16)とする。暗証番号は、

$$8 - [n / 2] \ \text{(octet)から} \quad 7 + [(n + 1) / 2] \ \text{(octet)}$$

に配置する。

ただし [] オペーレータは、小数点以下を切り捨て整数化するオペレーションを意味するものとする。

暗証番号の上位 octet を 0xff でパディングする。また、暗証番号の下位 octet を 0x00 でパディングする。

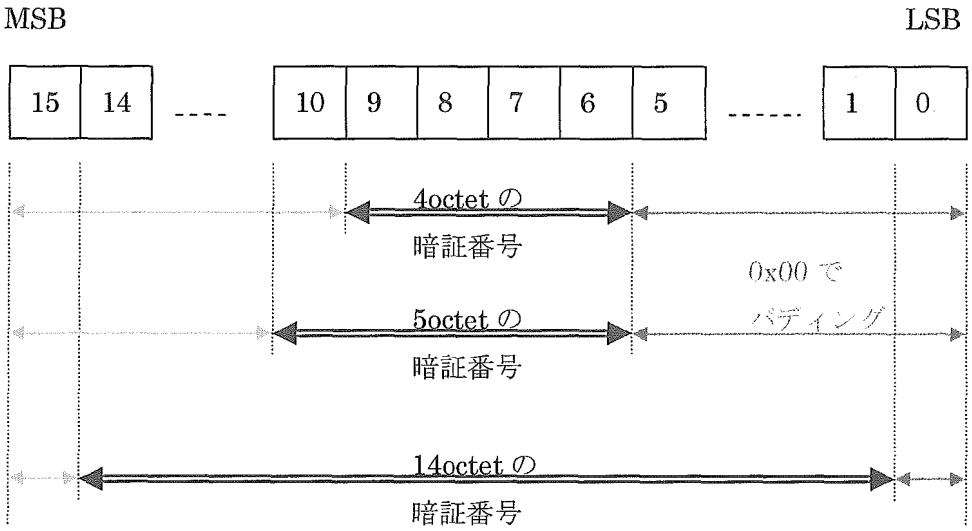


図 4.1 パディングの例

4.2.3 暗号処理後の媒体構成

暗号化処理は CDA 文書およびそれから参照されるファイルを対象とする。暗号化処理を行った後のファイル名称は暗号化処理前のファイル名称と区別できるもとし、CRYPTLOG.XML にファイル名称を記載する。可搬電子媒体に含まれるファイルのディレクトリ構成は暗号処理を施す前のものと同様とする。図４．２に例を示す。

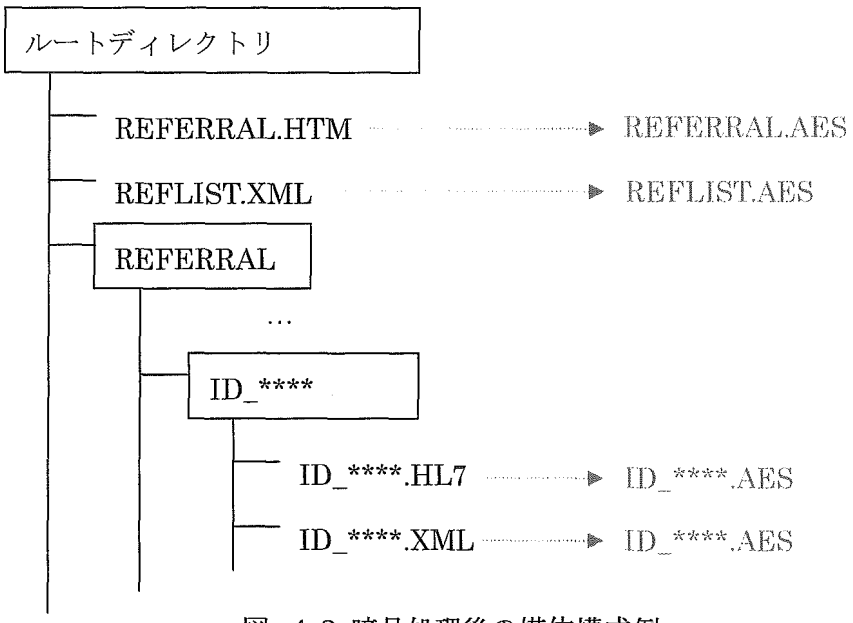


図 4.2 暗号処理後の媒体構成例

4.2.4 暗号化ログファイル

暗号化を行ったファイルの情報はデータを暗号化する際にログとして、ファイル名とその属性(ファイルサイズ、タイムスタンプ、暗号アルゴリズム等)を CRYPTLOG.XML ファイルに記述する。このファイルは全ての暗号処理が終了した時点で書き込み、復号化の際に使用する。ファイルに記述する項目については表 4.2 を参照のこと。

なお、CRYPTLOG.XML はできる限りトップディレクトリに置くことが望ましいが、媒体ファイル仕様により最上位ディレクトリに置かない場合は、別途各媒体ファイル構造規格で規定されたい。(CRYPTLOG.XML の XML スキーマについては表4．3を参照)

表 4.2　CRYPTLOG. XML の内容

項目	内容
データ暗号日時	暗号処理を開始した日時 (yyyy/mm/dd:HH:MM:SS)
暗号化ファイル数	媒体に含まれる暗号化処理を行ったファイルの数
暗号アルゴリズム	暗号処理に使用したアルゴリズム名称
オリジナルファイル名称	暗号処理前のファイル名称 (媒体のルートフォルダからのパス情報も含む)
暗号後のファイル名称	暗号処理後のファイル名称 (媒体のルートフォルダからのパス情報も含む)
暗号処理のステータス	暗号処理の成否

4.2.5 暗号化の解除方法について

暗号化された媒体はどのような環境でも暗号化解除できることが望まれる。そのため、復号化の処理に使用する暗証番号は容易に取得でき、かつ安全に保管されなければならない。暗証番号は診療情報を保存する媒体とは別の媒体－紙媒体等のに暗号化の際に記録する。暗証番号を記録する媒体は診療情報媒体とは別の場所に保管され、復号処理の際にのみ使用される事が望まれる。暗証番号を記録する媒体は紛失・破壊の恐れがあるため、媒体に記録すると同時に必ずバックアップを保存しておくこと。

暗号化解除を行った後にデータを書き込む媒体は、暗号化された媒体とは別の CD-R(DVD-R)、FD 等の媒体、又は復号処理を行う PC のローカルハードディスクで提供される。復号化の際に媒体を別途用意する場合は媒体に、別媒体で用意する場合は別媒体に、暗号化に関する情報、および暗号化を解除するための手順書を格納あるいは記載されることが望まれる。また、暗号化に関する免責を記載することが望まれる。

※媒体を上書きするためには、ライティングソフト等が必要になることが想定され

る。PC によってはライティングソフトが利用できないことも考えられるため、暗号化した情報をローカルハードディスクに展開して参照するといった運用も可能とする。

表 4.3 CRYPTOLOG.XML ファイルーXML スキーマ

```
<<?xml version="1.0"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <xsd:element name="EncryptInfo" type="EncryptInfo_type"/>
        <xsd:element name="FileInfo" type="FileInfo_type"/>
        <xsd:element name="File" type="File_type"/>
        <xsd:complexType name="EncryptInfo_type">
                <xsd:sequence>
                        <xsd:element name="Date" type="xsd:dateTime"/>
                        <xsd:element name="FileCount" type="xsd:integer"/>
                        <xsd:element name="Algorithm" type="xsd:string"/>
                </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name="FileInfo_type">
                <xsd:sequence>
                        <xsd:element ref="File" minOccurs="0" maxOccurs="unbounded"/>
                </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name="File_type">
                <xsd:sequence>
                        <xsd:element name="OriginalFileName" type="xsd:string"/>
                        <xsd:element name="EncryptFileName" type="xsd:string"/>
                        <xsd:element name="EncryptStatus" type="xsd:string"/>
                </xsd:sequence>
        </xsd:complexType>
</xsd:schema>
```

II. 研究成果の刊行に関する一覧表

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	次期「e-Japan戦略」における医療分野関連の重要課題（案）について	行政&ADP	41	4-8	2005
高橋成文, 東川淳紀, 山本修一郎, 小尾高史, 谷内田益義, 大山永昭	2階層PKIを用いたオンデマンドVPNシステム	情報処理学会論文誌	46 (5)	1129-1136	2005
秋山昌範	不正行為を調査するデジタル・フォレンジック医療分野における重要性	COMPUTER & NETWORK LAN	23 (3)	27-32	2005
山本隆一	海外の医療現場での個人情報保護の動き	INR インターナショナルナーシングレビュー	28 (5)	42-45	2005
山本隆一	診療情報システムと個人情報保護	医学のあゆみ	215 (4)	231-234	2005
山本隆一	プライバシーの考え方と個人情報保護	看護展望	30 (5)	17-20	2005
山本隆一	医療における個人情報保護とセキュリティ	日本病院会雑誌	52 (1)	106-124	2005

次期「e-Japan戦略」における医療分野関連の重要課題(案)について

東京工業大学
像情報工学研究施設
大山　永昭

1 医療分野の情報化に関する従来の取り組み

医療分野の情報化は1980年頃に始まり、①医療サービスの公正性・公平性の確保、②医療サービスの質の向上、③医療サービスの地域格差の是正、④新たなニーズへの対応などを目的としてきた。その後1995年頃からは、法令等で保存が義務付けられているX線写真やカルテなどの電子保存の容認や電子カルテの開発・導入などにより情報化が本格化し、2001年には保健医療分野のグランドデザインが策定され現在に至っている。このグランドデザインの考え方と方向性を勘案し、さらに情報化の進展を促進するために、2003年に公表された「e-Japan戦略Ⅱ」には、以下にある具体的なテーマが記されている(**図参照**)。

① 健康増進に役立てるための総合的な保健・医療サービスが提供される体制の整備
② 2004年からレセプトのオンライン化を開始し、2010年までに希望するところは100%実現
③ 電子カルテ情報のネットワーク伝送と外部保存の容認
④ 資格認証(医療従事者の免許等を認証するもので、具体的にはHPKI：Healthcare Public Key Infrastructureを意味している)システムの構築
⑤ EBM(Evidence Based Medicine)およびEBH(Evidence Based Healthcare)の推進
⑥ ITを活用した山間僻地・離島への遠隔医療の実現

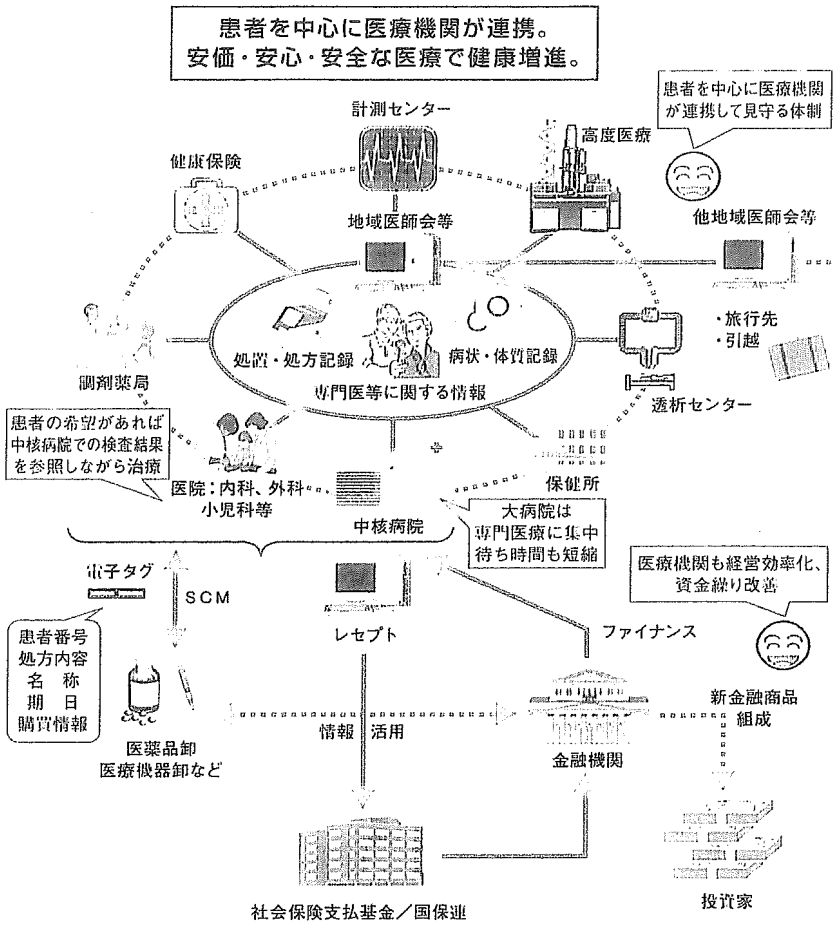
これらの課題は、その後の施策に反映され、その目標を徐々に達成しつつあるが、②およびグランドデザインに記された電子カルテシステムを2006年度までに60%普及させるという目標の達成は、残念ながら大幅に遅れている。

2 医療分野の情報化の課題 ―電子政府の構築との比較を通じて

医療分野の情報化の実現と電子政府の構築が持つ課題には、多くの共通点があるように思われる。例えば、標準的なパッケージソフトではなくカスタマイズされたソフトが多く使われていること、その結果、システムの導入費用が低廉にならないこと、用語やコードなどの統一化が実現していないこと、さらにはIT自体が医療機関等の経営の武器になっていないことなどがあげられる。

このような課題を解決するのは、もちろん容易なことではないが、これまで中央政府や先進的な自治体が行ってきた各種の取り組みは大いに参考になると思われる。細かな説明は他の文献に譲るが、功を奏しつつある事例を見ると、知事や首長のリーダーシップが発揮されていること、発注者側がITに関する十分な知識

図



出典）IT戦略本部「e-Japan戦略Ⅱ」

を会得していること、競争入札を実施していることなどが主な要因であると考えられる。そしてこれらの事例では、レガシーシステムをオープンシステムに入れ替え、業務プロセスを簡素化するなどの業務・システムの最適化を実施しており、これによりシステムの運用経費の削減が実現されている。さらに、削減された費用を用いて行政サービスの質の向上に振り向けているところもある。

電子政府の構築は、我が国の情報化を推進するために設立された高度情報通信社会推進本部の基本方針に明記された1995年から開始され、すでにKWAN（霞が関WANの略で全府省を結ぶネットワーク）やLGWAN（Local Government WANの略で地方自治体間を結ぶネットワーク）、さらにはGPKI（Government PKIの略で、大臣等の役職印の電子署名版）やLGPKI（Local GPKI）の整備による第2ステップを終了し、インターネットを介した各種の申請・申告のオンライン化などを可能とする第3ステップに入っている。そして現在は、世界最先端の電子政府を構築するための努力が行われており、2005年度末までに96%以上の行政手続きはオンライン化の準備が完了する予定である。このことから電子政府は、2006年度には従来の構築のフェーズから安定実稼動のフェーズに移行するといえる。もちろん良く知られているように、現状では利用率が低迷しており、その改善が喫緊の課題であることは言うまでもないことである。

上記の電子政府を構築する3つのステップを医療分野に当てはめると、①医療機関内の情報化、②医療機関間のネットワーク化、③インターネット等を介した医療機関と国民との情報交換になることが分かる。一方、現実には電子カルテや事務・会計システムなどの導入の促進と、HPKIの実施準備を進めていることから、医療分野の情報化は未だ第1フェーズであり、ようやく第2フェーズの一部に進展し始めたところであるといえる。言うまでもなく、第2フェーズのアプリケーションを実施するには、電子政府の構築におけるKWANやLGWANと同じように、病院、検診センター、薬局、保険組合、介護施設など約20万の組織を結ぶ安全なネットワークが必要にな

る。さらに第3フェーズに進むには、インターネット等を介して機微な医療情報のやり取りを行うことから、本人確認と秘匿通信を実現することが不可欠である。

次期「e-Japan戦略」における医療分野の情報化に関する重点課題(案)

2001年に策定された「e-Japan戦略」が2005年度で終了するに当たり、次の5ヵ年すなわち2010年度末を目標とする新たな戦略の起草が2005年7月に開始された。そして2005年9月末までに、新戦略の基本理念として、①改革から飛躍への視点、②利用者視点・生活者視点、③国際競争力・国際貢献の視点の3つを定め、10月末に、IT戦略本部の民間有識者から①世界一の電子行政の実現、②医療の構造改革としてのIT利用の促進、③IT人材の育成と教育のIT化、④世界一安全な防犯・防災社会の実現などの9つの重点課題が例示された。その後は、12月初めにパブリックコメントにかけるための新戦略の素案を作成し、2006年1月に正式決定を行う予定である。

ここでは、2005年10月25日に開催された第33回のIT戦略本部に提案された医療分野のIT化に関する重点課題の案について解説する。

3-1. 留意点

既に多くの方から指摘されているように、ITは単なる道具の一つであるが、その力がきわめて強力であるため、今やITをうまく使いこなすことが民間分野にとって不可欠になっている。このようなITが持つ能力は、少子高齢化や環境問題など21世紀の社会が持つ各種のジレンマを解決する可能性を有していることから、医療分野の情報化の目標についても、前述したように「医療の構造改革を目指したITの利用促進」とされている。

この背景としては、今後ますます増大する医療費の適正化と、国民の健康維持およびその増進を図ることがあげられる。特に、前者の医療費の適正化は、急速に進む高齢化にともなう医療費の増大を抑制せざるを得ない財政状況にあることから、最重要課題とされている。しかしながら、医療は国民が安心して生活するのに不可欠であることから、医療サービスの質の低下は避けなければならない。国民の一生を考えるならば、保健、医療、福祉分野サービスが国民を中心として切れ目なく提供されることが重要なのであり、これらのことを勘案して、次節で述べる個別課題が提案されている。

3-2. 個別課題

第1章で説明したように、「e-Japan戦略Ⅱ」で記された目標は、未だ十分な進展を見ていないものがあるため、これらについては引き続き実現に向けた努力を継続するとした上で、次のような項目が追加された。

1) レセプトのオンライン化による事務経費の削減と予防医療への活用

○医療機関、薬局、審査支払機関、保険者、被保険者の間においてレセプトを完全オンライン化(2010年度末まで)

○レセプトのEDI処理及びデータ活用を前提として、診療報酬体系を抜本的に見直す(2007年度末まで)

○レセプトデータの疫学的利活用の実現に向けた基盤の整備(2007年度まで)

本課題は、公的資金を投入する公的分野については、すべてのサービスについて事務経費を削減するとの基本原則からきているもので、医療分野については、その代表的なものとしてレセプトのEDI(Electric Data Interchange)化を実現する。現状では、医療費の請求に用いられるレセプトの総数は、年間約16億件、30億枚以上の紙による決済処理が行われている。これらをオンライン処理に代えることは、現在の金融分野の状況を見ても大きな経費の削減効果(試算では年2,000億円以上になる)があるとともに、紙の使用量を減らすことは環境保護にも有効であると考えられる。さらに、健康保険証をICカード等に置き換えリアルタイム処理することで、保険証の有効性確

認やいわゆる渡り診療（複数の医療機関に渡り歩いて受診することで、必要以上に服用薬をもらうなどの無駄が生じることがある）の防止などを実現できると期待される。また3つ目の基盤整備は、完全に匿名化したレセプトデータを活用することで、公益に資する各種の疫学的な分析を可能とし、感染症などに対する迅速な対応や健康指導等に役立てることを目的としている。

2）個人が生涯を通じて健康情報を利活用できる基盤作り

○国民の健康増進に資する、生活習慣病等の対策のため、個人の健康情報を「生涯を通じて」利活用できる基盤作り－EHR（Electronic Health Records）の実現－

⋗カルテ及びレセプトの本人情報の開示原則を徹底

⋗公益に資する健康情報の疫学的利活用の実現に向けた基盤の整備

○EHRの効果をより明確にするため、PDCAサイクルで分析して結果を公表する専門者会議の設置

本課題は、われわれ一人ひとりが自分の健康状態を正確に理解し、自ら健康増進を図る意識を高めることを目的としている。具体的には、健康診断結果や医療機関にかかったときの受診歴等を本人が参照・管理できる基盤を作るものである。このためには、カルテやレセプトの本人開示を徹底するとともに、生活習慣病等に有効となる予防医学を確立するために、健康情報の疫学的利活用を可能とする基盤整備を行うものである。さらにEHRの効果をより明確にするために、専門家による分析と結果の公表を行うことが提案されている。

3）医療におけるより効果的なコミュニケーションの実現

○山間僻地・離島において遠隔医療サービスを実施

○地上デジタルテレビ等の双方向通信を利用した受診前医療提供サービスの効果検証と実現可能性の検討

⋗救急搬送依頼時に応急処置の指導等ができる体制の整備

⋗小児救急における受診相談窓口の開設

本課題は、ITが有する距離と時間の壁を越える能力を用いて、医師と医師、医師と患者に代表される関係者間のコミュニケーションをより良くすることで、医療サービスの地域格差の是正および国民が持つ新たなニーズに対応することを目的としている。医師と医師のコミュニケーションの具体例としては、十分な経験や高度な専門知識を有する医師等が不足している山間僻地や離島にある診療所等に対して、都市部にある中核以上の病院から遠隔で診断や治療等の支援を行うことや、高度専門病院に勤務する専門医が他の医療機関の医師に対して教育・支援するものなどがあげられる。他方、後者は、2011年に地上アナログ放送が終了し、すべての家庭に導入されると予想される地上デジタルテレビ等が持つ双方向通信機能（具体的にはインターネット）を用いて、家庭にいる患者等に対して必要な指示や支援を行うものである。特に、救急搬送依頼時に応急措置の指導ができる体制を整備することは、例えば救急車が来る前に、必要な応急措置をどのようにすればよいかを、映像と音声を用いて指導することで迅速な対応を図るものである。また小児救急については、家庭のテレビ等から受診相談窓口を通して、例えば親御さんに適切なアドバイス等を提供することで、不安感を和らげ適切な処置ができるようにすることを目的としている。

4）医療情報化インフラの整備

○社会保障全般のサービスを実現するためのICカード、HPKI、セキュアネット基盤等を整備（2007年度末まで）

○部門系HIS（Hospital Information System）およびそれらを連携させた統合系HIS（オーダリングシステム、統合的電子カルテ等）を200床以上の医療機関のほとんどに導入し、業務の効率化、医療安全および診療情報の提供を実現する（400床以上は2008年度まで、400床未満は2010年度まで）

○統合系HIS導入の費用対効果に

乏しい小規模な医療機関に対しては、費用負担の少ない診療情報連携に適した電子カルテシステム等を用いて、診療情報の提供および面的連携を図る（2010年度まで）

○医療情報システムの相互運用性を確保すること等で、情報システムの導入コストを削減し、その普及を促進する

本課題は、前述した3つの重点課題の実現を図るために不可欠なインフラの整備に関するもので、最初の項目は、国民・患者の本人確認と意思確認を安全かつ確実に行うためのICカードと、医師などの医療従事者の資格確認を行うためのHPKI、さらに医療関連機関間を安全につなぐためのセキュアなネット基盤等を整備するものである。次の第2および第3の項目は、従来目標である電子カルテを普及させる本来の意義、すなわち医療機関の連携に要する患者情報の交換を容易にするための方策である。また第4の項目は、統合系HISなどの費用対効果を高めることを目的として、異なるメーカーの機器を組み合わせたシステムの最適化を可能とすることで、システムの導入コストを下げ、その普及を図る試みである。

4 おわりに

電子政府の構築には、電子自治体を含めると、年間2兆円以上もの費用が投じられている。にもかかわらず、電子政府に関連するITシステム産業、とりわけソフトウェアは輸出産業になっていない。その原因は、買い手である政府側にITに関する知識が不足していること、公平な競争環境ができていないことなどが指摘され、すでにITに関する十分な専門知識を有する民間人の全府省への配置や調達制度の改正などに着手している。そして従来型のレガシーシステムのオープン化を目指して、EA（Enterprise Architectureの略で業務・システム最適化と訳している）の導入を図っている。これらの動きは、まさしく戦略的な政府調達を通して、IT化の本来の目的である国民の生活レベルの向上や国の発展を期すための努力である。

医療においても、IHE-Jの活動に見られるように、その重要な課題の一つはEA手法を医療情報システムへ適応することで、医療の質を確保するとともに医療費の増大を抑制することである。これはまさしく医療分野が持つ社会的なジレンマのひとつであり、その解決にITの力を最大限に使う試みである。さらに、前述したITを使った新たなサービスの提供や国民の健康増進などを図ることで、これまで以上に国民が安心して生活できる状況を作ろうとするものである。これらの目標が達成され、その課題解決で培った各種のノウハウを基とした新しい医療情報システムが実現すれば、先進国が共通して持つ社会的なジレンマの解消策を例示できるとともに、結果として医療分野におけるわが国のIT産業の国際競争力が強化できると期待される。そしてそのためには、まさしく今、国、自治体、産業界、医療界、国民が一丸となって課題解決に協力して注力することが不可欠である。

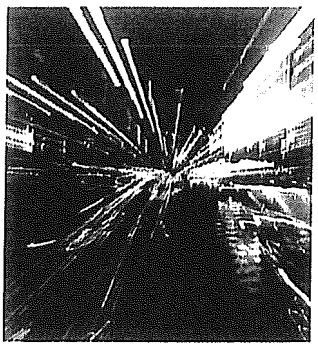
特集にあたって

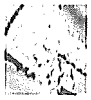
次期「e-Japan戦略」の案で触れたように、2006年までに電子カルテを60%に普及させるとの当初目標は、さまざまな政策的な努力にもかかわらず、達成はほぼ不可能になっている。そこで本特集を組むにあたっては、20年来の懸案事項である医療分野の情報化を振り返り、電子カルテを含むIT化が遅々として進展しない原因を知るために、さまざまな専門性を持つ先生方に現場の状況を踏まえてご執筆いただいた。保健・医療・福祉は、われわれ国民が安心して生活するための基本であり、これらの分野の情報化は、サービスの質の向上と効率化など、わが国が抱える社会的な課題の解決に不可欠なものである。もちろん構造改革的な変化を伴うため、その実現は容易ではないと予想される。聖路加国際病院の斎田先生が書かれているように、今漸く医療分野の近代化が始まることに大いに期待する。

行政&ADP
12 December 2005 Vol.41
行政情報化の総合的推進に向けて

医療分野におけるIT化

次期e-Japan戦略の医療分野関連重要課題
医療過誤を防ぐための病院情報システム
医療サービスの質の向上と電子カルテ　ほか





社団法人行政情報システム研究所
本誌は宝くじの普及宣伝事業として助成を受け刊行しています