Release 2 は External Act として定義されるために独自の拡張は使うべきではない。そこで、HL7 RIM で定義済みで、ハッシュ値およびハッシュ関数種別を格納可能な ED (Encapsulated Data)データタイプの使用を必須とした。本来の CDA Release 2 では External Act では ED データタイプの属性はオプショナルではあるが、必須とすることで実装上の問題は生じない。

また暗号化は暗号強度の最大値を現時点で一般に利用されるブロック暗号の十分なものとし、その上で鍵長を短くして運用する場合のパディングルールを定義した。短い鍵長で運用することは暗号強度を下げることになるが、結果の項で述べたように、診療情報の提供書は常に高度な機密性を必要とするわけではない。ノートＰＣや携帯電話のプライバシーシートのような、他者からは見えにくい程度でよい場合もある。その一方で暗号強度を上げれば鍵の管理等の運用面での対策もそれなりに強化する必要があり、患者にも医療機関にも負担が増加する。例えば社会的差別につながるような疾患に関する情報が含まれるといった場合は運用上の負荷が高くても鍵長を最長で類推困難なものとし暗号強度を上げなければならない場合もあるだろう。逆にほとんど機密性が必要ない場合もあり、このような場合は電車の中で置き忘れた場合でも PC に挿入するだけで、すべての情報がすぐに見えることはない、程度で十分である。例えば誕生日を鍵にした４桁の数字でもことたりる。このような大きな差のある状況でも本研究で提案した規格は容易に対応することができるし実装の一通りでよい。

なお本規格の作成段階で、最終案とほぼ同じ内容で実証実験をおこなった。この実験は本研究費ではなく、経済産業省の補助事業である相互運用性実証事業の一環として医療情報システム開発センターが主体となって、高岡公立病院を中心に複数の医療機関と 10 数名の患者さんの協力でおこなったもので、電子署名、暗号化ともに実装が可能で十分効果があることが確認できた。

E．結論

A-net 上の情報の二次利用を可搬媒体を用いて行う場合の安全管理を研究する手段として医療機関間の診療情報提供書および患者等への情報提供をモデルとして電子署名と暗号化の標準規格を作成し提案した。本研究の成果は日本 HL7 協会の規格として採用され、また HELICS 標準に申請している。

F．健康危険情報

特になし。

G．発表

論文

１．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、日本看護協会出版会、東京、2005

２．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、医歯薬出版株式会社、東京、2005

３．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、メヂカルフレンド社、東京、2005

４．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、(社) 日本病院会、東京、2005

H．知的財産権の登録・出願状況

現在のところなし。

I. 謝辞

本研究の成果は日本HL7協会のCDA作業班ならびに医療情報システム開発センターの多大な貢献による。深謝したい。

付録1

CDA 文書電子署名規格

ver. 1.01

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高度化し、医療・介護の率向上が求められている。このような要求を満たすためには、医療・介護機関間および医療・介護機関と患者・利用者の間で流通する情報を電子化し、情報の密度や可用性を飛躍的に向上させることが有用よ考えられている。そしてこのような電子化文書の規格として HL7 CDA が存在する。

医療・介護は様々な法律規則に則って行われるもので、さまざまな理由で作成される文書には作成者・責任者の署名または記名・押印が求められるものが存在する。電子化文書では電子署名法によって電子署名で署名または記名・押印に代えることができるが、本規格は CDA 文書に電子署名を行い際の規格を記述するものである。また診療文書には添付情報が存在するものが数多くあり、電子署名の対象情報にこれらの添付情報を含めることがもとめられることも多い。そのため、本規格には外部参照情報も電子署名の対象とする場合についても規定する。

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

1. 適用

本規格は、さまざまな目的で作成される CDA 文書に電子署名を付与する際に適用する。電子署名が必要か否かは本規格では規定しない。

2. 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必要に応じて適用するよう努めなければならない。

RFC3275　XML-Signature Syntax and Processing

保健医療福祉分野 PKI 認証局 証明書ポリシ(厚生労働省　平成 17 年)

ISO TS17090-1:2002 Health informatics -- Public key infrastructure -- Part 1: Framework and overview

ISO/TS 17090-2:2002 Health informatics -- Public key infrastructure -- Part 2: Certificate profile

ISO/TS 17090-3:2002 Health informatics -- Public key infrastructure -- Part 3: Policy management of certification authority

「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、平成 16 年)

RFC3161　Internet X.509 Public Key Infrastructure Time-Stamp Protocol

XML Advanced Electronic Signatures (XAdES), (W3C 2003)

患者診療情報提供書規格　V1.00　(日本 HL7 協会　2006)

CDA 文書暗号化規格　V1.00　(日本 HL7 協会　2006)

3. 用語と定義

3.1 XML 電子署名

RFC3275 に規定される XML 文書に添付して文書作成者の身元を証明し、またその文書が改竄されていないことを保証するデータ。XML 文書全体ではなくその一部にだけ署名を付けたり、また XML 文書の中に署名を含めたりといったことができる。

3.2 タイムスタンプサービス

データがある時刻に存在していたことを証明するサービス。データの作成者はタイムスタンプサービスを提供している第三者機関に依頼し、データの内容と現在時刻から作られたハッシュ値を用いるなどして電子署名を発行してもらう。データの受信者はその署

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、

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

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。

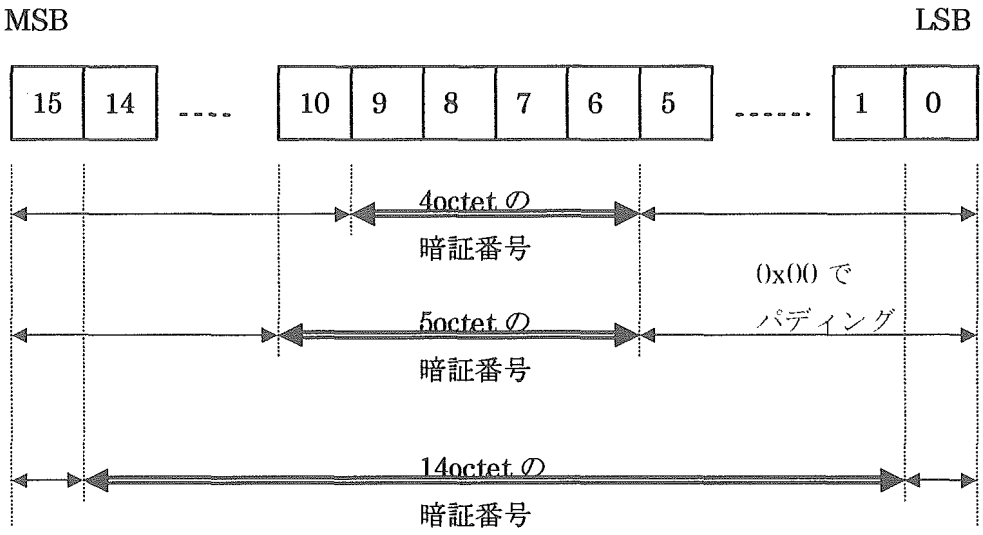


図 4.1 パディングの例

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。

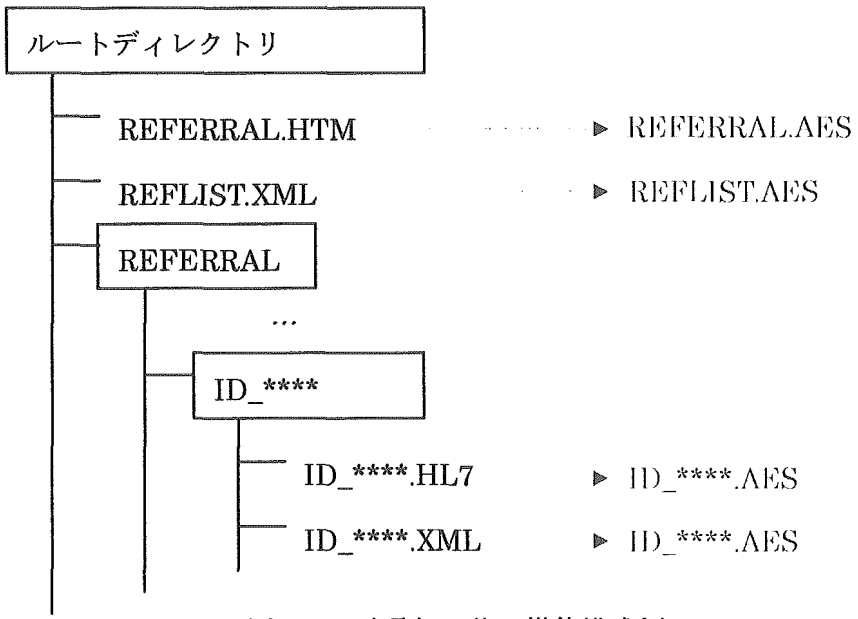


図 4.2 暗号処理後の媒体構成例

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ー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>
```

診療情報の活用におけるプライバシー保護に関する検討

分担研究者　高橋紘士　立教大学 コミュニティ福祉学部 教授
横内清光　文教大学情報学部　教授

研究要旨　エイズ治療において本人の診療情報を研究情報として転用し、エイズ治療技術の向上に資するために必要な条件について患者の視点からみた、プライバシー保護および情報保護と研究情報への活用についての意識を探るための調査をおこなうために最終的な調査項目の確定をおこなった。一方、個人情報保護法施行を踏まえて、その対応を検討する必要が生じた。特に、データの二次利用におけるプライバシー確保のため、国民が求めるセキュリティ要件も明らかにしたが、今後も検討が必要と思われる。プライバシーを保護に関して、患者側の同意という側面では、当初より同意書の中に研究に関する同意事項も盛り込まれているために、研究利用も問題ないと考えられていたが、研究目的が必ずしも明確でない場合もあり、研究目的の明確化、具体化が必要と考えられる。一方、同意書が利用拡大の最大の阻害要因になっていることも調査研究で明らかになっており、現在の運用指針ではA-net利用者以外の研究利用を禁止していることから、疫学者や臨床工学者等は研究利用ができない。そこで、研究の利用者拡大を可能にする方法を検討した。具体的には、広報学的アプローチを用いソシュールの記号論を検討し、情報をデノテーション（内包的）、コノテーション（外延的）に分解してアプローチする手法の有効性が示唆された。

A．研究目的

エイズ治療において、プライバシー保護は重層的な構造である。患者のプライバシーが保護されているという感情を前提として、臨床データを活用できる環境はどのような条件が必要かを検討するための調査デザインをおこない実査をおこなうことが本研究の目的である。

B．方法

1）アンケート方法の検討

調査を実施するための検討を踏まえて、調査票の確定をおこなった。なお、その際、調査実施予定先の国立国際医療センターにおける倫理委員会の検討がなされこれらの調査項目について精査がおこなわれ、その指摘にしたがい，調査票の改善ををおこなった。

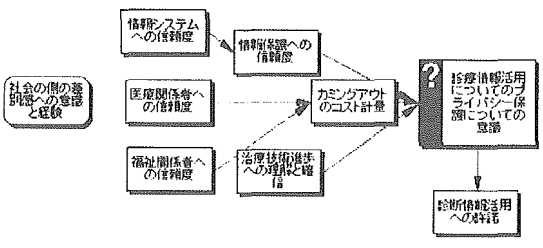
2）プライバシー保護に関する社会学的、心理学的要因の検討

A-net は、実働しているネットワーク型電子カルテとして希有な存在である。しかしながら一方で、IT というなじみのない技術を使うことによる躊躇も見られる。本研究ではマーケッティングの専門家に加わっていただき、新技術への適応に関し、集団心理面からの検討を行う。

C．結果

1）アンケート方法の検討

調査のフレームは以下の通りである。



調査対象

国立国際医療センターのエイズ外来への来院者約３００名を調査対象者として調査を実施する。（倫理委員会の調査実施についての審議を受け、委員会での実施の許可がえられた。）

さらに、この調査を終了後、調査対象を拡げる予定である。

解析の方針

基礎属性別の集計

性年齢別、受療機関別集計等

質問間別クロス集計

A- net利用への認識別集計
登録データの許容度別集計
専門職の情報守秘状況への意識別集計
HIV感染者の社会意識別集計

回答者のパターン分析

回答者の回答パターンに着目して、回答者をいくつかのグループにわけ、その要因を分析する。

情報保護に関する意識が厳格のグループとそうでないグループ、専門職への情報守秘意識について厳しいグループとそうでないグループ

保健医療従事者と福祉サービス従事者への回答パターン

2）プライバシー保護に関する社会学的、心理学的要因の検討

A-net の受容には何が必要か、また A-net の受容を阻害する要因がどこにあるか、マーケッティング理論を用いて検討を進めた。具体的には、スイスのソシュールが唱えた記号論を検討し、情報を本質機能であるデノテーション（内包的機能）とその付加価値であるコノテーション（外延的機能）に分解してアプローチする手法が有効性であると判明した。そこで、目標を「A-net の周知」から、「A-net『技術情報』の周知」と限定させ、その上で各ステークホルダー（利害関係者）の認知度や好感度等を調査する必要があると考えている。また記号論によると、