るなど、グローバルなインターネット社会の発展にこれまで以上に大きく貢献するようになる。

少々話が広がりすぎてしまった感があるが、つまりは全国民がその恩恵を受けられる情報ネットワーク社会が着実に整備されつつあるということである。次で述べるが、その整いつつある情報社会の一部に医療も含まれてくる。

5つの重点政策分野

e-Japan重点計画では、高度情報通信ネットワーク社会の実現のために特に重点的に施策を講ずべき5分野、即ち

1. 世界最高水準の高度情報通信ネットワークの形成
2. 教育及び学習の振興並びに人材の育成
3. 電子商取引等の促進
4. 行政の情報化及び公共分野における情報通信技術の活用の推進
5. 高度情報通信ネットワークの安全性及び信頼性の確保

に集中的に取り組むこととしている。

特に4.の中で、「ITの活用による公共分野におけるサービスの多様化及び質の向上を図ること等により、広く国民がITの恩恵を享受できる社会を実現する」という目標が掲げられている。

その中でも、保健、医療、福祉分野では、情報化を進め、サービスの質の向上、効率化を進めるとともに、ITを活用し、遠隔医療等新たなサービスニーズへの対応を進める、また、高齢者・障害者が使いやすい情報通信機器・システムの開発・普及を通じ、全ての人にやさしいバリアフリー環境の整備を行なうとしている。

電子カルテについては、データ交換の際のフォーマット、電子的情報交換手段、情報セキュリティ技術等を開発し、2003年度までにその標準化を行なう。電子カルテのベースとなるオーダリングシステム(薬剤、検査、医療事務等の間での医療情報の電子化)については、2005年度までに病院での導入率を2割程度まで引き上げることを目指すとしている。

電子カルテシステム

現在、その発展が著しい病院情報システムにおいて核をなしているのが、医師が診察状況を読みながら他の部門へ注文を送る「オーダリングシステム」である。薬剤オーダや検査オーダ、会計オーダなど機能は様々に及ぶが、そのオーダリングシステムも結局は電子カルテを介するため、電子カルテはすでに病院

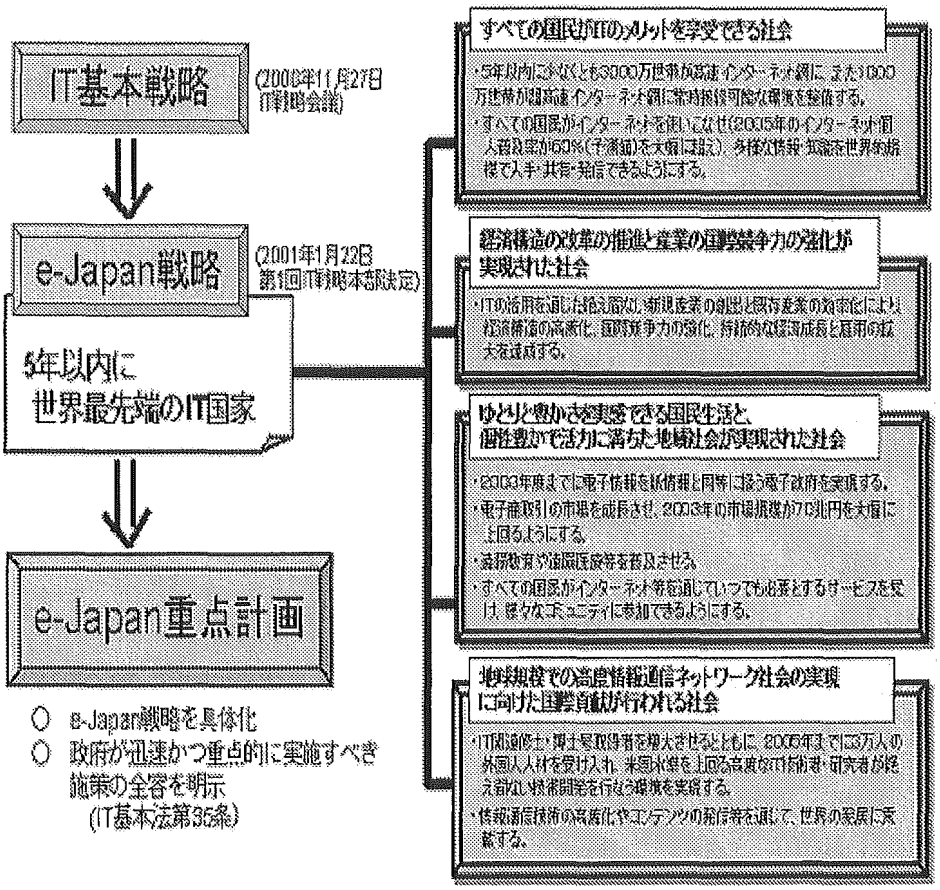


図 B.6: e-Japan 重点計画 (案) 基本的方針

情報システムの一部に組み込まれていると言える。

電子カルテの意義は、診療を電子的に支援することにあって、単に患者情報を貼り付けるだけでは十分価値を発揮したとはいえない。様々な付加機能を有機的に備え、病状記録といったカルテの枠を越えた域まで昇華させてこそ、電子カルテシステムとしてその価値が存分に発揮されるであろう。

その付加機能の中でも、ネットワークを介して情報の流動性を高めるという機能に注目して、この電子カルテシステムをインターネットに接続することで地域医療ネットワークを構築し、連携を達成するために患者情報を相互参照、共有しようとする動きが盛んである。

IC カード

クレジットカードに似たプラスチック製のカードにICチップを埋め込んだカードをICカード(欧米ではスマートカード)と呼ぶ。

ICカードは、現在広く利用されている磁気カードに比べより大量のデータを扱うことができること、セキュリティ(安全性)にすぐれることから次世代のカードとして広く注目を集めている。特に、エレクトリック・パース(電子貨幣、電子マネー)や電子商取引(エレクトリック・コマース)などでは、セキュリティが極めて重要であるため、ICカードの利用が不可欠でさえある。

ICカードの応用分野はこれだけに留まらず、本研究対象である医療分野でもその情報積載量、セキュリティに注目して、診察券や住民カードに病歴、治療記録、保健情報などを記録することによりサービスの向上と事務の合理化をはかるためにICカードの利用が検討されている。保険証の機能をICカードに組み込むとすると、カードサイズなので保険証より持ち運びが楽、家族単位でなく個人で保険証が持てるといった利便性が挙げられる。

このように、ICカードの応用範囲は非常に多岐にわたり、その他のカードを必要とするアプリケーションやシステムでも広く利用が検討されている。

しかし当然ではあるが、ICカードは良くも悪くも個人で管理するものなので、リスクとして紛失した際の責任などは全て自己のものとなる。

地域医療ネットワーク事例

2001年1月5日に経済産業省および医療情報システム開発センター(MEDIS)が公募したプロジェクト「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ー電子カルテを中心とし

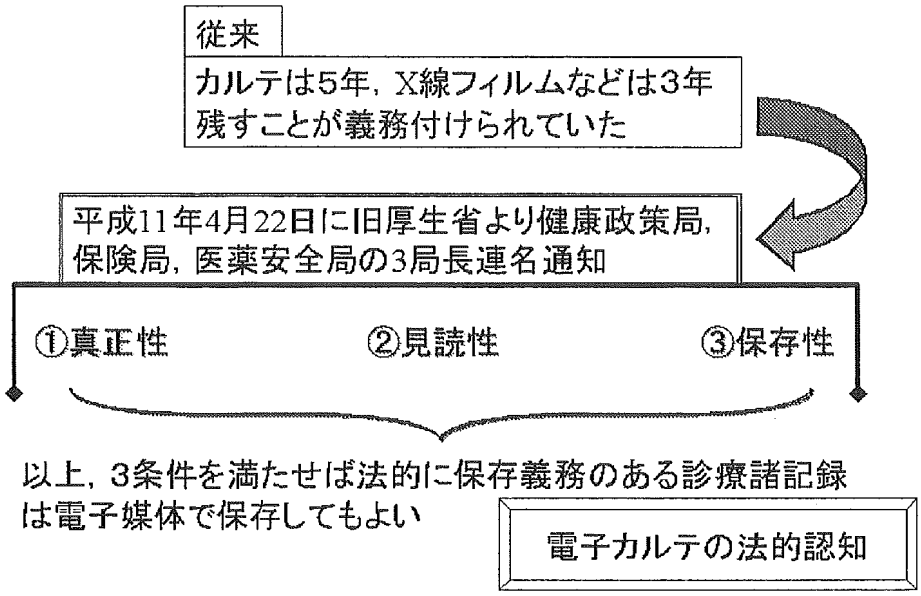


図 B.7: 紙媒体から電子カルテへ

表 B.1: 主な IC カードと新サービスの内容

企業名	特徴
JCB	鉄道やバスなどの運賃を後払い決済
UC カード	学校向けの入退出管理・出欠確認。学食での代金決済等
三井住友カード	中小商店向けの買い物ポイント管理
ソニーファイナンスインターナショナル	コンサートなどのチケットとしての入場料を決済
トヨタファイナンス	携帯電話に組み込んで決済に利用
DC カード	伊勢丹や東急百貨店などと専用共通ポイント導入
ポケットカード	視力データを入力し、眼科診察券も兼用
OMC カード	山梨交通と組み、バス定期・クレジットを一体化

た地域医療情報化ー」がある。

この事業は、26地域において地域内の医療機関が保有している診療録等を共通利用するネットワークシステムの開発・実験であり、事業の重点は、患者の個人情報保護や医療従事者の守秘義務などに配慮したセキュリティを確保できるシステムの構築である。通常の情報システムはデータとシステムの保護が第一の目的であるが、医療情報システムは、患者のプライバシーを保護し、守秘を徹底することが第一の目的である。守秘とは、信頼関係が成立しており、その信頼関係に基づいてプライベートな情報が他者と共有されている状態のことを指し、患者個人情報を共有する医療従事者の倫理観が問われるところである。

この採択候補に選ばれた26件は、全てネットワークに繋がれているデータベースに患者の情報を載せることを前提としている。

医療機関の連携による患者へのメリットはあるが、データベースに情報を載せること自体のデメリット(プライバシーの問題)は考慮されていない。確かに情報を共有することによる則したメリットは非常に優れているかもしれないが、まずは患者ありきで地域医療ネットワークを構築して行くべきだと考える。

癌研究会付属病院などの事例

癌研究会付属病院（東京・豊島）など都内の有力3病院と大学、医師会が連携し、患者情報の共有や先端医療機器の共同利用に乗り出す。2005年をめどにカルテを電子化してデータベースを作り、参加医療機関が共通のカルテに基づいて診療できるようにする。医療の情報技術（IT）化で病院は専門性を高め、患者は病状に応じた最適な診療を受けられるようになる。

各病院と医師会はまずカルテを電子化し、共同でデータベースを構築する。医師が患者の病歴や治療歴を容易に参照できるようにして治療効果を高める。緊急時に専門医が不在の際、別の病院から遠隔診療などを受けられるようにするほか、集めたデータを分析して治療効果の検証も進める。微小ながんも見つけられるポジトロン断層撮影装置など高額な先端医療機器を備えた共同の検査・診療センターの設立も計画している。高額化する先端医療機器の設備投資を抑えるのが狙いである。

医療機関は患者のデータを共有することで、得意分野ごとに役割を分担できるようになる。患者は病状に応じた治療を受けやすくなるほか、専門の病院で手術した後、地域のかかりつけ医でも同じデータに基づいて治療を受け

られる。研究会は事業を進めるため各病院などによる共同出資会社か非営利組織（NPO）の設立を検討している。新しく作る事業体は医薬品や医療機器の共同購入のほか医療事務などの受託も視野に入れ、病院改善につなげる。

B.2　医療情報に対する患者の意識調査

B.2.1　アンケート調査

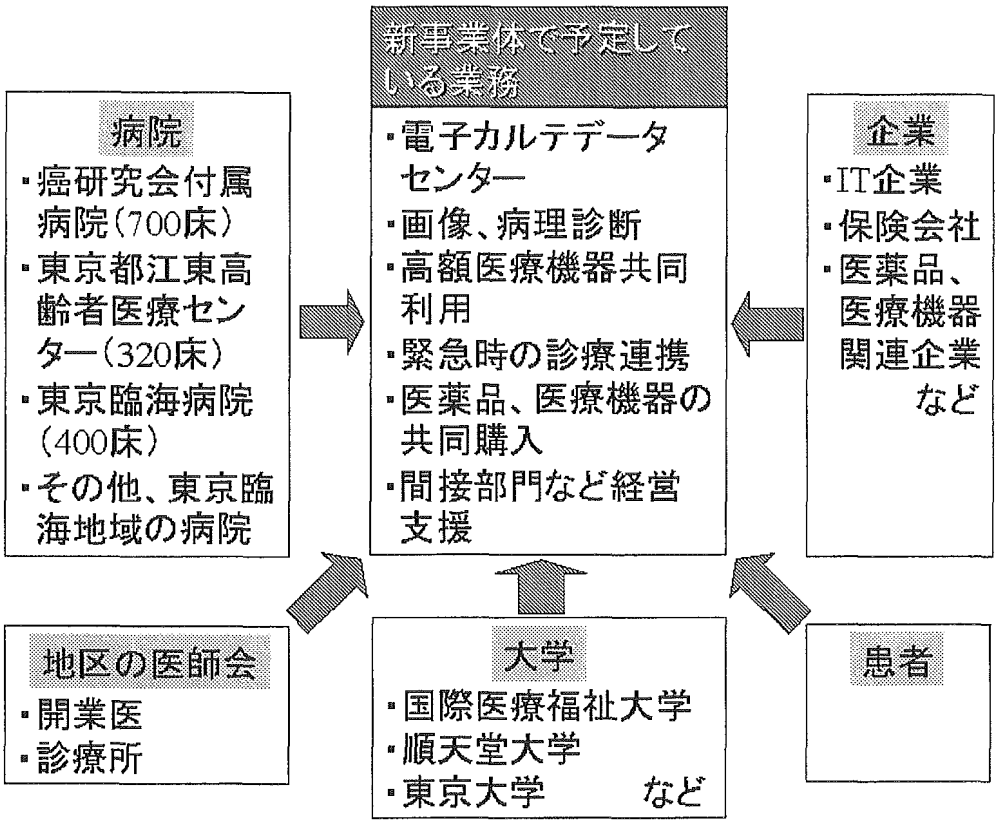
現状の医療情報システムでは、患者が利用することを考慮していないため、本研究では患者視点に立った医療情報システムを構築していく。医療情報システムには医療従事者が患者の情報を共有するという一面と、患者が医療機関側の情報を閲覧するという一面がある。ここで、患者はどのような情報を知りたがっているのか、ということが重要となってくる。患者にとって知りたくない情報を準備しておくことは効率的ではないし、情報を閲覧する際にも情報が多すぎて煩雑になるという問題点がある。そこで、患者が知りたいと思う情報を効率的に選択できるように、以下のようなアンケート調査を行なった。

問8 あなたは初めての病院にかかる時に、事前にどのような情報を知りたいと思いますか。下記の項目から優先順位として　上位の１位から５位　まで選び、その順位の番号を記入してください。

- 住所／交通の便
- 予約の方法
- 診療曜日・時間
- 駐車場の有無
- 診療科目
- 専門領域・治療方法
- 実績
- 混雑程度
- 設備
- その他

問10 では、その病院の医師については、どのような情報を知りたいと思いますか。下記の項目から優先順位として　上位の１位から５位　まで選び、その順位の番号を記入してください。

- 出身大学
- 医師としての経歴
- 得意な領域
- 診察のモットー
- 顔写真
- 診療担当日時
- その他



出典：日経新聞 2002 年 12 月 30 日 1 面

図 B.8: 癌研究会付属病院などによる共同事業にイメージ

表 B.2: 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採択案一覧

地域事業名	事業主体
1 生涯/1 患者/1 カルテ機能を持つ地域電子カルテ構築事業	社団法人 鶴岡地区医師会
宮城県における医療 ASP 網 (みやぎメディカルモール) の構築	株式会社 仙台ソフトウェアセンター
わかしお医療ネットワーク 先進的医療連携・遺伝子診療モデル事業	千葉県立東金病院
在宅医療・慢性疾患のための地域共有電子カルテシステム	社団法人 松戸市医師会
亀田病院を中心とした南房総地域の医療情報ネットワーク推進事業	医療法人鉄蕉会 亀田総合病院
診療情報の電子化による診療の質と安全の向上を踏まえた医療連携	医療法人財団 河北総合病院
EO 電子カルテ中心の高度セキュリティ地域医療情報ネットワーク	社団法人 東京都港区医師会
玉川地域における「家庭医」発信型の医療ネットワークの構築	株式会社 メディヴァ
診療情報と施設情報を統合した患者指向型地域医療連携システム	社団法人 横浜市青葉区メディカルセンター
地域医療向上に資する横須賀市医療情報ネットワークの開発、検証	社団法人 横須賀市医師会
10 年間の共有・蓄積データを活用した電子カルテと EBM の実証	社団法人 富士吉田医師会
静清合併と東海地震を踏まえた県中部医療ネットワーク推進事業	株式会社 エスビーエス情報システム
地域医療の機能分化と連携を促進する IT ネットワーク構築事業	トヨタ自動車株式会社 トヨタ記念病院
岐阜市における電子カルテを中心とした診療ネットワークの構築	社団法人 岐阜市医師会
地域保健医療福祉情報ネットワーク推進事業	社団法人 久居一志地区医師会
大阪府における産婦人科救急医療情報ネットワーク構築事業	株式会社 アイ・ビー・ティ
ネットワーク型電子カルテによる病院・診療所連携情報システム	財団法人 千里国際情報事業財団
医師会による診療情報共有のための医療機関連携ネットワーク	社団法人 神戸市医師会
岡山市立市民病院を中心とした地域医療情報化の推進	総合病院 岡山市立市民病院
地域チーム医療と遠隔医療のための電子カルテ統合ネットの構築	島根県立中央病院
四国 4 県電子カルテネットワーク連携プロジェクト	財団法人 四国産業・技術振興センター
IT 技術活用による包括的地域医療ネットワーク構築事業	社団法人 宗像医師会病院
公開鍵基盤を利用した広域分散型糖尿病電子カルテ開発事業	社団法人 福岡市医師会成人病センター
情報共有型電子カルテによる熊本地域健康福祉ネットワーク	財団法人 肥後医育振興会
地域医療情報の共有・活用を目的とした宮崎健康福祉ネットワーク	社団法人 宮崎県医師会
EBM 評価機能による病診連携支援型広域電子カルテ事業	沖縄県中部病院

B.3 医療情報のセキュリティ問題

B.3.1 情報セキュリティとは

情報セキュリティとは、正当な権利を持つ個人や組織が、情報やシステムを意図通りに制御できる性質である。その目的は、情報システムや情報自体を、さまざまな危険や脅威から保護し、正常な機能・状態を保持することによって、情報システムや情報の信頼性を高めたり、情報システムの利用者が安心して情報システムを利用できるようにすることである。そのための情報システムは下に示す情報セキュリティ上の要件がある。

- 機密性：情報を権限のない第三者に秘匿できること
- 完全性：情報を改ざん・破壊されないこと
- 可用性：除法を必要なときに利用できること
- 真正性：利用者やシステムの身元が確認できること
- 責任追跡性：操作の形跡をたどれること
- 信頼性：意図した動作と結果に整合性があること

現在、情報システムを安全に構築・運用するために国際的な枠組みが整備されつつある。セキュリティ機能面は情報セキュリティの評価基準であるISO15408で、管理と運用は情報セキュリティマネージメントの規格であるISO17799でカバーされている。

ISO15408に準拠した開発では、プロテクションファイル（PP）やセキュリティターゲット（ST）と呼ばれるセキュリティ仕様書の作成が必要である。セキュリティ仕様書では情報セキュリティ上の要件を損なう脅威とその対策を明確にしなければならない。ISO15408はPart1からPart3までの3部構成になっている。Part1「概説と一般モデル」は、セキュリティと評価の考え方やセキュリティ仕様書の記述方法を説明している。Part2「セキュリティ機能要件」は、一般的な情報システムで必要とされる対策を、具体的なセキュリティ機能要件として網羅したセキュリティ機能の要件朱である。また、セキュリティ機能を確実に実装するための保証要件は、Part3「セキュリティ保証要件」にまとめられている。

一方、セキュリティ仕様書ではまず評価対象の範囲やセキュリティ上の前提条件などを定義し、評価の対象となる情報システムを明確化する。次に評価対象がさらされる脅威を明確にし、これらの脅威に対して情報システムが備えるべき対策として、セキュリティ機能要件を記述する。この機能要件は、ISO15408 Part2「セキュリティ機能要件」から参照する。このように、ISO15408に準拠した開発では、情報システムがさらされる全ての脅威を洗い出し、漏れのないように対策をとらなければならない。

B.3.2　患者プライバシー

個人情報の保護に関して

医療において、患者のカルテの保存義務は医療機関にあるが、カルテの内容は患者のプライバシーそのものであるから、患者の同意なしに他の医療機関に開示はできない。逆に、患者自身がカルテの内容を自己責任において他の医療機関に見せるのは自由である。医療機関側が圧倒的に不利な印象であるが、「供給側は徹底的な情報開示、消費側のプライバシーの保護」が高度情報化社会の掟である。

近年、民間企業や行政機関全般にわたり、コンピュータやネットワークを利用して大量の個人情報を処理している。こうした個人情報の取り扱いは今後益々拡大していくものと考えられており、国でも対策に乗り出している。いったん誤った取り扱いをされると、個人に取り返しのつかない被害を及ぼす恐れ

がある個人情報の性格を危惧し、国民が安心してIT社会の便益が受けられるよう、権利利益に侵害を未然に防止しようとすべく、個人情報の適正な取り扱いのルールとして「個人情報の保護に関する法律案」が2001年3月に国会へ提出された。この中では、本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止できる状態で、「1：第三者への提供を利用目的とすること、2：第三者に提供される個人情報の項目、3：第三者への提供の手段又は方法、4：本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止すること」の4つの事項をあらかじめ本人に通知しておくか、本人が情報提供を容易に知りえる場合においては、個人情報を第三者に提供することができるとしている。

この法律の対象となる個人情報は、現に生存している個人に関する情報であって、特定の個人を識別することができるものである。氏名、住所、生年月日等が典型だが、これに限らず、特定の個人を識別することができる限り、個人の身体、財産、社会的地位等に関する事実、評価を表す情報等もこの法律の対象となる。つまり、医療に関する個人情報もこの法律の対象に含まれる。

住民基本台帳ネットワークを例に

住民基本台帳ネットワークとは、全国民に11ケタの住民票コードを付け、氏名などの個人情報をネットワークで一元管理するシステムで、2002年8月5日より運用開始された。国民の利便性向上などの利点が訴えられていたものの、「郵送された住民票コードが封筒から透けて見える」といった問題や、各市町村が利用するコンピュータのウイルス対策ソフトが2カ月以上も更新されていないなどの実態が明らかになった。

福島県岩代町町民の個人情報を収めた住民基本台帳ネットワークシステム(住基ネット)のバックアップデータが盗難に遭った。同町がデータ管理を委託していたコンピューターシステム会社、エフコム(本社郡山市)の車が荒らされ、データを保存していたマイクロテープが盗まれた。盗まれたマイクロテープは計3本で、全町民約9,600人分のデータが入っていた。岩代町は災害などに備えバックアップデータを作製し、全面的に同社に管理を委託していた。

福島県岩代町の住民基本台帳の個人データが入ったデジタル・テープが盗まれた問題で、岩代町は31日、町民約9,600人の住民票コードの変更作業で、12世帯の31人が「個人情報保護に不安を感じた」などとして、住民基本台帳

ネットワーク (住基ネット) からの離脱を希望したと明らかにした。

どのような手段であれ、個人情報が漏れる可能性がゼロではないということを再認識させられる事件であり、患者＝国民と考えれば、まさに地域医療ネットワークにも同じような問題が指摘でき、患者のプライバシーを最優先させなければならないことが伺える。

B.3.3 バイオメトリクス認証技術

バイオメトリクス認証技術とは

バイオメトリクスの語源は、biology（生物学）と metrics（測定）の合成語 Biometrics であり、生物測定学などと訳されていて、ミシガン州立大学の Anil Jain らは「Biometrics deals with identification of individuals based on their biological or behavioral characteristics」と定義している。したがって、Biometrics とは「行動的あるいは身体的な特徴を用い個人を自動的に同定する技術」と定義できる。

バイオメトリクス認証技術は、従来、アクセス制御におけるパスワード代替利用の形態が主であったが、現在は、多くの情報がネットワークを介して共有化され、また、サービスが提供されている。このため、アクセス制御における許認可を確認するための手段から、非対面での状況でサービスに対する利用者課金などを行う際の本人を同定するための本人認証手段の位置付けとなっている。

バイオメトリクス認証モデルにおける認証は、センサからのデータ入力、特徴抽出などの前処理の後、事前に登録しておいた生体情報（テンプレートデータ）との照合処理により類似度を算出する。

バイオメトリクス認証処理のフローは以下のようになる。

1. データ入力機能：ユーザーが提示した生体データをシステムに取り込む入力センサ機能。

2. 特徴抽出機能：特徴抽出機能は前処理機能と特徴抽出機能を分ける場合もある。

   (a) 前処理：システムに取り込んだ生体データから、判定処理に不要な環境要因の除去処理や保管したテンプレートとの比較判定を効率よく行うために、空間的位置や大きさ、時間的な変化などを正規化する処理。

   (b) 特徴抽出:前処理により、環境要因の除去、正規化を行った

データより、判定処理に必要な個人の特徴を抽出する処理。

3. 判定機能：登録テンプレートデータと入力データの特徴量の類似性を照合比較し、所定の判定水準を越えたか否かで本人であるか他人とみなすか同定を行う。

4. 登録データ保管機能：本人認証を行う者の生体データを特徴量の形で事前に特徴抽出処理し、システムに保管しておく。

バイオメトリクス応用事例

指紋

指紋は現在もっとも普及しているバイオメトリクス技術である。古くは犯罪捜査に使われた指紋であるが、1970年頃からコンピューターを使った指紋解析作業が一般化されるようになり、ここ数年で、一気にパーソナルユース、ビジネスコンシューマレベルで認証を行うための製品が登場するようになった。

認証時に、指の一部しか使わないので装置を小型化できるというものも大きなメリットである。また、バイオメトリクス認証の中で一番多くのメーカーが参入している分野なので、競争が激しくコストとダウンの効果も見込める。

製品としての熟成度も高く、本人拒否率、他人許容率なども良い結果を残しているが、もともと犯罪捜査に使われてきたという経緯から、指紋の登録を不快に感じる人も少なくない。また、数百人に一人の割合で識別できる指紋がとれない、または、取りにくいという人もいる。利用する部位が指のため、外的な要因によってすり減ったり、傷がつくことで認識率が下がるという面もある。

また、最近は米国でシリコンラバーを使って偽造し、犯罪に悪用するケースなども出てきている。一部の指紋認証装置メーカーは、指の温度なども確認して正確に認証できる高機能製品も出しているが、全ての装置にそのような機能が組み込まれているわけではない。特に、安価な製品を使う場合、そうした機能はないので、偽造の可能性にも注意を払うべきである。

虹彩（アイリス）

虹彩とは、黒目の内側で瞳孔を取り巻くドーナツ上の部分のことをいう。人間の虹彩は極めて複雑なパターンで形成されており、妊娠7、8ヶ月頃までに形作られ、生後2～3歳でその成長が止まる。以後は一切形が変わることがないという。場所が目の内部になるので傷もつきにくく、生体としては最高レベルの「同一性」を保っているといえる。

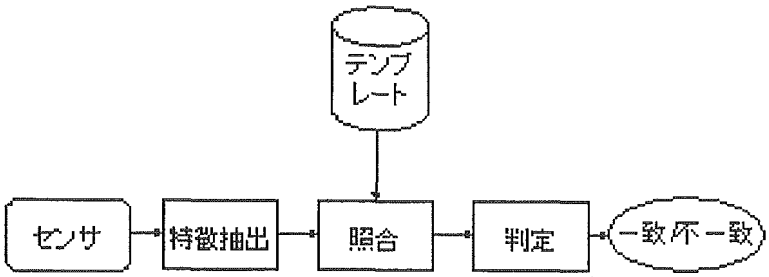


図 B.9: バイオメトリクス認証モデル

虹彩を使って認証を行う場合、利用者はカメラの前に立ち、内部を覗くだけでよい。虹彩認証用のカメラは非接触型なので、指紋のように多くの利用者が代わる代わる触るといったことがなく、衛生面でもメリットが大きい。

また、本人拒否率や他人許容率なども、数あるバイオメトリスクの中で最高レベルという特徴をもつ。事実上、バイオメトリクスの決定版と見られている。それにもかかわらず、あまり普及していないのは、装置のコストが非常に高価だからである。指紋認証装置と比べると、約1.5倍〜2倍の価格差があり、これが導入をためらう原因になっている。

また、最近の研究では虹彩でその人の病歴がわかるという学説も出てきた。それが事実だとすると、必要な認証情報以外の個人情報が登録されることに対して、不快感を感じる人が出てくる可能性もある。

署名

純粋な意味での生体情報ではないが、本人の動き、行動をパターン化するという意味ではバイオメトリクスのカテゴリーに入る。具体的には、署名を行なう梳きの筆跡、筆圧、筆順、書くのにかかった時間などを登録しておき、それをデータとして保持することで同一人物が書いたものかどうかを判断する。

ペンさえあれば、どこでも利用できる手軽さがある半面、手を怪我して書けない場合は利用できないことがあったり、登録時に変な書き方をすると認識率が下がるというデメリットもある。管理するソフトウエアのアルゴリズムや設定などによって、認識率を上げたり、認識までの時間を短くすることができる。

ただし、認識率を上げ厳密なチェックを行い始めると、その分、本人拒否率も上がるので、バランスが難しい。また、日本のようにサイン慣れていないという、文化的な拒否反応もある。一部の

PDA（携帯情報端末）のOSには署名を認識する機能が組み込まれているが、本格的な普及はまだこれからの段階である。

顔

我々が誰かと出会ったとき、視覚を使って相手の顔を見てその人を判断する。こうした当り前の作業を機会で行うのがバイオメトリクスの顔認証である。

仕組みとしては、人間の顔をカメラを使って撮影し、あらかじめ登録された顔の画面の特徴点（鼻、眉、目、口、頬など）と比較対照することで認証を行う。

顔認証の最大のメリットは、普段から人との付き合いで自然と行っている認証方法を機会が肩代わりするだけなので、指紋などと比べて心理的な抵抗が少ないことにある。また、認証時は、特別な操作を意識せず、カメラの前に立つだけでいいので、利便性も高い。

ただし、顔認証はその特性上、双子の厳密な識別が困難であったり、暗い場所で利用できないといったデメリットがある。また、サングラスや髪を短くした場合、認証されにくくなることもあり、この場合は再登録の作業が必要になる。他のバイオメトリクス認証技術と比べると、本人拒否率、他人許容率の値が悪いので、その部分をどうやって解消するかが今後の課題になる。

声紋

普段、電話などで話している感覚で利用できるので、指紋や顔のデータを取られるのに抵抗がある人でも心理的な抵抗感が少ない。また、登録してある音声の処理は一般的なパソコン、音声認識用のソフト、それにマイクがあればできるので汎用性が高く、ほかのバイオメトリクス認証と比べてコストをかけずに実現することができる。

ただし、その性質上、本人拒否率、他人許容率は高めに出る。また、音声を録音するにはある程度、静かな場所が必要なので、使う場所が限られてくるという問題もある。そのため、声紋による認証は単体で使われるよりも、他の認証技術（バイオメトリクスやICカードなど）と組み合わせて使われることが多い。

掌形

人間の手のひらを見たときに、指の長さや太さがわずかづつ違うということをバイオメトリクス認証に応用したもの。ほかのバイオメトリクス技術と比べ、認証時間が早いというメリットがあり1秒前後で認証を行えるのが魅

力である。出入りの激しいオフィスの入退室などに使うのが効果的である。

ただし、手のひらを装置にかざして認証を行うため、装置の設置場所面積は大きくなる。認証作業が高速というメリットがあるが、小さなオフィスなどで使うには向いていない。また、製造している企業が少なく、価格が高いのも難点である。

掌形の場合、照合時に点灯したガイドLEDを、ガイドピンを指で挟む行為で消す必要があり、このときに生体反応もチェックしている。そのため、たとえ手首ごと切り落とされたとしても、「成りすまし」を行うことが不可能である。

静脈パターン

1995年、発見された、新しいバイオメトリクス認証技術である。手の甲に現れる静脈が、個人によってパターン差があることに着眼したもの。静脈パターン認証は、虹彩を同じ高レベルのセキュリティを誇っている（本人拒否率、他人許容率の値は、最高レベル）。デバイスの価格が下がれば虹彩によるバイオメトリクス認証を脅かす可能性もある。

新しい技術だけあって、製品の絶対数は少ないが、マウスに静脈パターンの認証装置を組み込んだ製品の開発を発表された。価格はまだ明らかにされていないが、コンシューマレベルで購入できる安価なものであれば、一気に広まる可能性も考えられる。

網膜

虹彩とは異なり、目の網膜内の血管パターンを健康に害を及ぼさない赤外線で測定するバイオメトリクス技術である。1985年に米国で開発され、米国を中心に普及している。

本人拒否率、他人許容率が極めて低くセキュリティレベルは最高クラスを誇る。銀行や軍などのハイセキュリティ施設へ設置される例が多い。米国では既に一部の銀行で網膜認証を使ったATMが稼動し始めている。

耳介

生涯にわたってほとんど成長がなく、固体ごとの特徴点を多く持つバイオメトリクス認証技術である。ただし、現在は実験段階で、今のところの技術を活かした製品は登場していない。

DNA

近年は犯罪捜査にも使われる人間のDNA（遺伝子情報）をバイオメトリクス認証に応用したものである。具体的には、DNAの情報を基に、鍵となる

「DNA-ID」を作成し、ICカードなどに2次元バーコードなどで埋め込む。DNA-IDを基に公開鍵と秘密鍵を作成し、公開鍵を「実印」のように利用すれば、生体情報を組み込んだ法的効力のある署名が行える。

ただし、現在はDNA-IDを作成するためには多くの時間やコストがかかるので、今後数年は具体的な製品が出てくることはない。認証方法が他のバイオメトリクスと違うため、ICカードと併用される可能性も高い。

バイオメトリクス認証技術の危険性

バイオメトリクス認証の脆弱性

バイオメトリクス認証の脆弱性とは、脅威につながるバイオメトリクス認証自身の性質やバイオメトリクス認証システムの設計・実装・運用のミスなどである。ここでいうバイオメトリクス認証とは、バイオメトリクス認証システムのハードウェアやソフトウェアだけでなく、個人を認証するための情報（個人認証情報）として生体情報を用いる個人識別のスキーム全体を言う。

バイオメトリクス認証の脆弱性には、バイオメトリクス認証特有の性質に起因する脆弱性と、パスワードやIDカードなどのほかの個人認証方法にも共通する脆弱性の二つがあると考えられる。例えば、入力装置をタッピングして生体情報を入手するバイオメトリクス認証装置と、キーボードをタッピングしてパスワードを入手できる個人認証装置は、どちらも「タッピングにより個人認証情報を入手できる」といった脆弱性をもつ。また、パスワードやIDカードは、失念や紛失により個人認証を利用できなくなるが、バイオメトリクス認証にはこうした問題が無い。逆にバイオメトリクス認証絵は本人拒否が発生するが、IDカードにはこのような問題は無い。

一般的な情報システムに共通する対策は、ISO150408のセキュリティ機能要件として網羅されている。従って、バイオメトリクス認証の脆弱性を検討する場合には、バイオメトリクス認証特有の性質に起因する脆弱性がより重要と考えられる。

個人認証は、あらかじめ登録した個人認証情報と、認証時に提示した個人認証情報が一致、または正しく対応していることを確認することで行われる。これは、IDカード、バイオメトリクス認証に共通したフレームワークである。従って、バイオメトリクス認証特有の性質は、個人認証情報として用いられている生体情報に起因すると考えられる。言い換えれば、生体情報がパスワードやIDカードなどの個人認証情報とは異

なる性質をもつため、バイオメトリクス認証特有の性質や脆弱性をもつといえる。

既存のバイオメトリクス認証技術の危険性について

国連機関ITU（国際電気通信連合）のために指紋照合装置の安全性について研究している横浜国立大学大学院の松本勉教授（環境情報研究院・学府）とそのチームは、柔らかいプラスティック素材に指紋を押し付けるだけで、グミに似たゼラチン質の人工指を簡単に作れることを実証している。

また、あるドイツの研究チームは、容量性リアクタンス技術を使用している指紋照合装置など、各種の照合装置を騙した方法を報告している。指紋照合装置は、誰かが使用した後の指紋読みとり部に水を入れたビニール袋を押し当てることで騙された。表面に残された指紋の油分から、直前に使用した人物の指紋パターンが読みとられたという。この研究チームはさらに、カメラに短いビデオ録画を見せることで顔認識装置が騙されたことや、高解像度のカラー・レーザー・プリンタで印刷した虹彩の写真を使うことで虹彩照合装置が騙されたことも報告している。

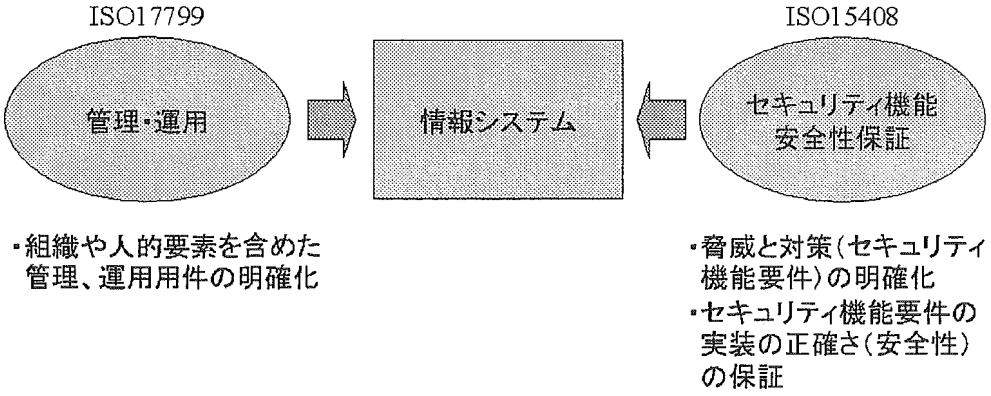
アメリカのセキュリティ専門家は、声の録音によって音声認識システムが騙される危険性があり、また、本人の正当なアクセスが拒否されるケースもあると述べている。また、バイオメトリクス・データは秘密情報ではなく、さまざまなことを行なうのに一日中利用しているこの体の特徴のため、その生体情報（指紋など）の痕跡を行く先々に残しており、その情報を盗むための好機が多く存在すると発言している。

バイオメトリクス認証の運用方法による危険性について

バイオメトリクス認証技術は運用次第で、単なるパスワード認証よりも低いセキュリティ・レベルになる恐れがある。

具体的な例として、バイオメトリクス認証のバックアップとして、パスワード認証を使用している場合があげられる。この場合、バックアップ用のパスワードが低いセキュリティ・レベルの原因となると考えられる。

指紋認証を例にとると、いつもは正常にアクセスできる正規ユーザーであっても、指にけがをした場合などは、認証に失敗する可能性がある。そのとき、ユーザーがアクセスできないだけならば問題はない。つまり、失敗した場合には、管理者に依頼しない限りアクセスできない運用ならば、バイオメトリクス認証によるセキュリティ・レベルを維持できているといえる。



出典：「ユビキタス時代のバイオメトリクスセキュリティ」

図 B.10: 情報システムとセキュリティ基準

しかし、問題は、バックアップにパスワード認証を用意している場合で、認証に失敗しても、ユーザー自身がパスワードを入力すればアクセスできる運用である。この運用では、バイオメトリクス認証とパスワード認証のどちらでもアクセスできることになる。

つまり、セキュリティ・レベルはより低い方、すなわちパスワード認証と同じになる。さらに悪いことに、パスワード認証だけを使用する場合よりもセキュリティ・レベルが低くなる恐れが考えられる。なぜなら、この場合のパスワードは、ユーザーの意識では「バックアップ」となるからである。ただでさえ，ユーザーは覚えるべきパスワードの数が多いため、ユーザーは、めったに使わないバックアップ用ともなれば、安易なパスワード（例えば、自分の生年月日など）を設定しがちになる。そのパスワードが破られてしまえば、強固なバイオメトリクス認証を破られたのと同様にアクセスされてしまう。

バイオメトリクスとパスワードのどちらでもアクセスできるようにしておけば、利便性は向上する。しかし、パスワード認証よりもセキュリティ・レベルが高まることはなく、「認証に失敗したときにどうするか」といった運用が重要になる。そのことを十分認識した上で利用する必要がある。

B.4 新しい医療情報システムの展望

B.4.1 院内情報システム

院内情報システムの果たすべき目的は、受付・診察・検査・会計といった患者が受ける一連の行動に対する情報の流れを一本化することである。その結

果として患者自身の流れもスムーズになり、病院・患者双方にとってメリットのあるシステムとならなければならない。電子カルテを所与のものと考えると、この院内情報システムの構築が目指すべき医療情報システムの出発点となるため、非常に重要な役割を担う。

院内情報システムがその役割を果たすためには、

- 受付・診察・検査・会計のそれぞれのシステムが電子カルテに対応していること
- それぞれのシステムがオーダリングシステムでつながっていること
- 病院内にデータベースを設けること

が必要となる。予約システムの有無、サーバ・クライアントPCの規模などは各病院によって異なるが、基本的には上記すべてを満たしていれば、院内情報システムとしての目的は果たすことができる。

北里研究所病院や十三病院などの事例に見られるように、現在では病院内のあらゆる部門がネットワークで連携し、共有の情報で効率的に運用されるべくシステム構築が進められている。よって、院内情報システムにおいては本研究で挙げた事例で十分な役割を果たしているといえる。

B.4.2 地域医療ネットワーク

地域医療ネットワークの必要性

地域医療ネットワークを構築するにあたっては、莫大な費用と時間、手間がかかることになる。病院側から見た地域医療ネットワークの目的は、各病院が患者の情報を共有し、患者の受け渡しをスムーズにすることである。患者の受け渡しをスムーズにするだけならば、患者の情報を共有する必要はない。ICカードを導入してICカードに患者情報を格納し、患者が診察を受ける際に各病院の医師に提示すれば済むからである。これによって、この目的を果たしながら地域医療ネットワークの構築よりも時間・コストともに低く抑えることが可能となる。

しかし、患者情報の受け渡しはリアルタイムのみではない。特殊な病気、大掛かりな検査など、あらかじめ連絡・準備が必要な機会も存在する。このような場合、地域内の各病院がネットワークによって連携していないと、スムーズな受け渡しができるとはいえない。また、事前に患者情報をやりとりするならば、ICカード→ネットワークによって送受信するよりも、データベースによって共有していた方が、利便性が高い。この意味からも、ICカードでは不十分であり、地域医療ネットワークを構

築する必要性がある。

また、患者の立場から考えるとICカードでは自分はカードに格納されている情報を見ることはできない。また、フリーアクセス・フリーチョイスの観点から、患者が医療情報システムに自由にアクセスでき、そこから自由に病院を選択できることが必要である。このことからも、ICカードでは不十分であるといえる。このフリーアクセス・フリーチョイスこそが現状の地域医療ネットワークに決定的に欠如している部分であり、本研究ではこの概念を最重要視する。

地域医療ネットワークには地域内の各病院が連携して情報を共有することと、患者がそのネットワークに自由にアクセスして病院を自由に選択することが必要であるため、次の2つのシステムについて考えていく。

病院間連携システム

地域内の各病院がネットワーク上で連携するためには、各病院の院内情報システムのフォーマットが統一されていることが必要である。フォーマットが統一されている方が、情報のやり取りがスムーズに行くからである。また、同一のサーバー・データベースを参照することからも、院内情報システムの統一は必要である。

次に患者視点から考えると、データベースで共有すべき情報は多すぎてもかえって煩雑になるだけである。とくにインターフェース上では、患者が知りたいと思う情報だけがあればよい。これは第3章でも分析した通り、

- 病院の情報
    1. 診療科目
    2. 専門領域・治療方法
    3. 診察曜日・時間
    4. 住所・交通の便
    5. 実績
    6. 混雑程度
    7. 設備
    8. 予約の方法
    9. その他
- 医師の情報
    1. 医師としての経歴
    2. 診察のモットー
    3. 診療担当日時
    4. 出身大学
    5. その他
    6. 顔写真

の優先順位で情報を扱うことが望ましい。