

Tachibana , Masahiro Omatsu	Technique	cal Society of North America2007			
三輪健太, 梅田徳男, 阿見年典, 福地奈緒, 山本修司, 大川明子, 橘英伸, 大松将彦	電子透かし技術を用いた医用画像の秘匿性確保・著作権保護システムの構築	医療情報学会秋季大会予稿集		1-3	2007
Okawa A., Umeda T., Fukuchi M., Miwa K., Hashiguchi N.	Development of a tele-support system for cancer outpatients	The Kitasato Medical Journal	Vol.38 No.1	1-8	2008

# 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  
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
- ②2004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
- ⑤EBM(Evidence Based Medicine)

およびEBH(Evidence Based Healthcare)の推進

- ⑥ITを活用した山間僻地・離島への遠隔医療の実現

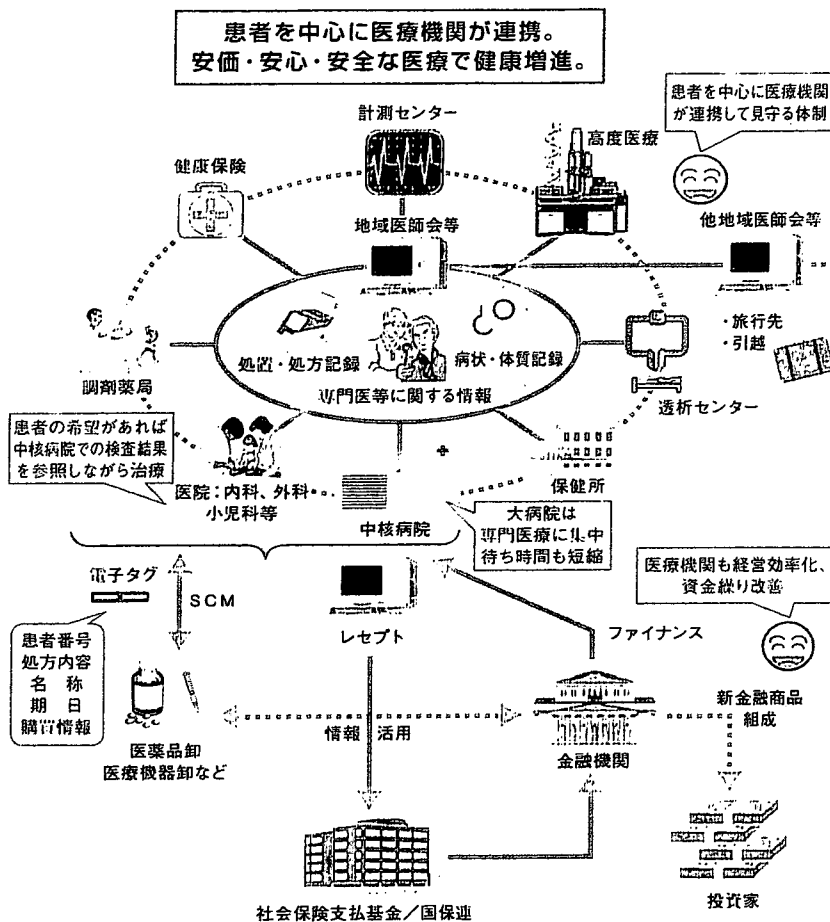
これらの課題は、その後の施策に反映され、その目標を徐々に達成しつつあるが、②およびグランドデザインに記された電子カルテシステムを2006年度までに60%普及させるという目標の達成は、残念ながら大幅に遅れている。

## 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稼働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。

### 3 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と、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ため、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て上で、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」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家会議の設置

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(オーダーリングシステム、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。

#### 特別にあたって

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。

## 2階層PKIを用いたオンデマンドVPNシステム

高橋 成文<sup>†1</sup> 東川 淳紀<sup>†1</sup> 山本 修一郎<sup>†1</sup>  
小尾 高史<sup>†2</sup> 谷内田 益善<sup>†3</sup> 大山 永昭<sup>†4</sup>

VPNの普及によりインターネットを利用したセキュアな情報通信が実現可能な環境となった。しかし、VPNの設定やメンテナンスには専門的なスキルが必要であり利用までに時間やコストがかかる問題がある。また、設定後は暗号鍵漏洩や設定情報の複製によるなりすましなどにより機密性が損なわれる問題があり企業や家庭で広く利用されるまでに至っていないのが現状である。筆者らは、H14年度に総務省よりインターネット等において各種通信サービスを安全に行うためのネットワーク基盤技術の調査研究を受託し、鍵を安全に配送するネットワーク基盤技術として Secure e-key Networkの調査研究を実施している。本稿は Secure e-key Networkの基本構想に基づき、VPN利用者の要求に対しネットワークを利用して即座にVPNをセキュアに開通するオンデマンドVPNシステムを提案する。オンデマンドVPNシステムは、機器認証やサービス認証を行うことでリモート環境からVPN機器にセキュアに設定情報を配信・保存できる。本提案の実用性評価として、ICカードを用いたVPNルータにより検証環境を構成し、任意の拠点をオンデマンドにVPN構築可能であることを検証した。また、そのターンアラウンド時間の測定結果を報告する。

### On-demand VPN System Using Two Layer PKI

SHIGEFUMI TAKAHASHI,<sup>†1</sup> ATSUNORI HIGASHIKAWA,<sup>†1</sup>  
SHUICHIRO YAMAMOTO,<sup>†1</sup> TAKASHI OBI,<sup>†2</sup> MASUYOSHI YACHIDA<sup>†3</sup>  
and NAGAACKI OHYAMA<sup>†4</sup>

Due to recent progress of VPN technology, secure environment for internet communications becomes available for end users. However the secure communications with VPN is not widely deployed for business or home use at the moment. Because professional skills are expected for configuring and maintaining, extra time and cost are required to employ it to existing networks. Moreover, the users have risks such as spoofing caused by leakage of encryption keys or illegal reproduction of setting information. We have been developing the secure key distribution infrastructure over the Internet, which we call Secure e-Key Network, in a research project supervised by Ministry of Public Management, Home Affairs, Posts and Telecommunications. This paper presents the On-demand VPN system which enables immediate establishment of VPN connections whenever users request. It provides a way of secure distribution of configuration parameters to relevant devices for establishing VPN connections from remote site by authenticating both devices and services. For evaluating its feasibility, we developed a prototype system consists of VPN routers with smart cards and verified if VPN connections could be established on demand between any given sites. Finally we report the evaluation result through the analysis of turnaround time measured during the experiment.

#### 1. はじめに

今日、インターネットを利用したVPNサービスの利用が進んでいる。VPNサービスにはインターネットサービスプロバイダ (ISP) が独自回線を利用する方式と利用者がインターネットを利用して構築する方式がある。ISPが提供するVPNを利用する場合、設置や設置情報の変更に対する日程をISPの都合と合わせる必要があり、コストや時間がかかる問題があるが、利用者は設置作業や開設確認をする必要がないことや、回線がISPの独自網なのでセキュリティ上の

†1 株式会社 NTT データ技術開発本部  
Reserch and Development Headquarters, NTT DATA CORPORATION

†2 東京工業大学大学院総合理工学研究科  
Interdisciplinary Graduate School of Science and Engineering, Tokyo Institute of Technology

†3 東京工業大学像情報工学研究施設  
Imaging Science and Engineering Laboratory, Tokyo Institute of Technology

†4 東京工業大学フロンティア創造共同研究センター  
Frontier Collaborative Research Center, Tokyo Institute of Technology

安心感があるなどのメリットを持つ。一方、利用者がインターネットを利用してVPNを構築する場合は、ルータの設置や情報の変更に対する自由度はあるものの、利用者自身にネットワークの専門知識が必要となえ、設定などを間違えると情報セキュリティ上多大な影響が発生する恐れがあるなど、だれもが容易に設置できる状況に至っていない。企業連携やSOHO連携、個人間の連携などでは、インターネット環境の構築後ただちにVPNを利用した機密情報の授受を必要とする場合があるが、先の問題から利用者がVPNを利用したいときに環境をただちに構築できる状況にないのが現状である。

東京工業大学大山研究室では、これまで高度なセキュリティ機能を持つICカードの新たな利用として、機器にICチップを搭載することでセキュアチップとして機器のセキュリティを確保する仕組みの提案や技術実験を行っている<sup>1)~5)</sup>。これらの研究成果や経験から培ったアイデアをもとに、産学が連携してH14年度に総務省よりインターネットなどにおいて各種通信サービスを安全に行うためのネットワーク基盤技術の調査研究を受託し、鍵を安全に配送するネットワーク基盤技術としてSecure e-key Networkの調査研究を実施している<sup>6)</sup>。本調査研究において東京工業大学はNTTデータより受託研究契約に基づき共同で調査研究を実施している。

筆者らは、Secure e-key Networkのフレームワークを応用し、利用者の要求に応じてネットワークを利用した鍵配送としてVPN鍵を配送し、ただちにVPNを構築可能な環境を構築したので報告する。大学においてVPNサービスを具体的に実現するうえでの要件整理やICチップを利用する鍵管理方式について検討を主導し、企業においてシステム構成検討や実装を分担することで、新たな認証技術を実サービスに近い環境で構成することができた。

2章でSecure e-key Networkのフレームワークを説明し、それをVPNルータに適用しVPN鍵を配信するための構成を示す。3章では、VPN鍵の配送問題を明らかにし、本方式がセキュアにVPN鍵を配送する仕組みを示す。4章は、ネットワークを利用してVPNルータに鍵を配送するシステムの実装方法について説明し、5章で利用者のVPNの設定依頼からVPN構築までの動作手順とターンアラウンド時間を紹介する。6章、7章は考察とまとめである。

## 2. VPNの情報設定

### 2.1 情報設定の課題

ルータ間でVPNを構築するための設定情報には、機器相互のIPアドレスや鍵情報がある。たとえば、拠点間VPNに利用されるIPsec-VPNでは、VPNの鍵交換にIKE (Internet Key Exchange) が一般に用いられている<sup>7)</sup>。IKEは、相手認証やSA (Security Association) の折衝と管理、共有秘密鍵管理などを行いIPsecによるVPNの鍵交換機能を受け持つ。このとき、IKEで利用する情報を事前にVPNルータに設定する必要があるが、これらの情報が漏洩すると機器のなりすましも可能となり、機密情報の漏洩にもつながる。また、VPNルータの設定にはネットワークの専門知識も必要となり、だれもが簡単・安全に情報設定や設定変更できる状況でない。

そこで、これらの課題を解決する手段として、Secure e-Key Networkのフレームワークを応用し、利用者の要求に応じてネットワークを利用して設定情報を安全に配送する仕組みが構築できるのではないかと考え本研究を推進している。

### 2.2 Secure e-Key Network

オンデマンドVPNシステムの構築にあたり、Secure e-key Networkのフレームワークを参照している。Secure e-Key NetworkはICカードで実現されている基本モデルをネットワークに適用し、ネットワーク機能としてセキュアにサービスの利用権(サービスの鍵)の配送を実現、提供する基盤技術である(図1)。e-Keyチップは耐タンパ性を有し2階層PKI技術を実装しているICチップであり、情報流通機器に組み込むことを想定している。機器管理者はe-Keyチップの登録、状態の管理を行い、利用権管理者はチップアプリケーションの設定と利用権の配送を管理する。サービス提供者は、利用権を用いた各種サービスを提

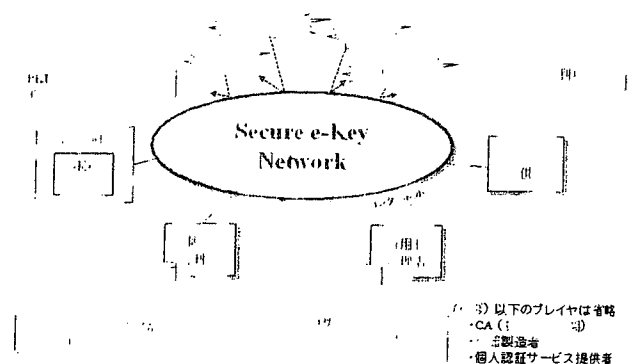


図1 Secure e-key Networkの概念  
Fig. 1 Concept of Secure e-key Network.



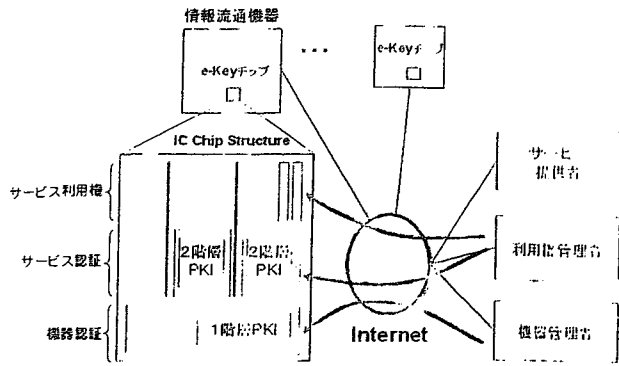


図 2 2 階層 PKI の概念  
Fig. 2 Concept of Two Layer PKI.

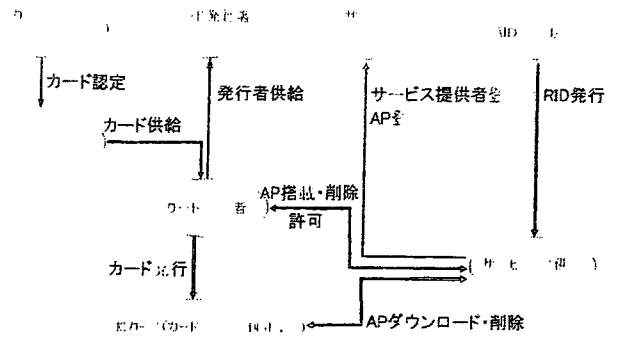


図 3 NICSS フレームワーク (プレイヤーモデル)  
Fig. 3 NICSS framework (player model).

供する。

2 階層 PKI 技術は、1 階層目の PKI を利用して e-Key チップ発行後でも自由にチップアプリケーションを発行設定し、各チップアプリケーションが独自に 2 階層目の PKI を利用してサービスを提供できるなど、サービス間のセキュリティを保ちながら幅広いサービスが提供可能な技術である。図 2 は 2 階層 PKI 情報と利用権の設定概要を示している。まず、e-Key チップを搭載した情報流通機器が機器管理者に認証されると 1 階層目の PKI 情報が設定される。次に、機器管理者より e-Key チップ利用の承諾を得た利用権管理者によって、チップアプリケーションと 2 階層目の PKI 情報が設定される。このとき、1 階層目の PKI 情報を利用したセキュアチャネルにより情報が設定される。なお、各層の PKI 情報はチップ内で生成してもよい。さらに異なる利用権管理者が、機器管理者の承諾を得て新たなチップアプリケーションと 2 階層目の PKI 情報を設定する場合も先と同様な手順で実施される。これにより、e-Key チップ発行後も複数のサービスが登録可能となり、各サービスの登録情報は当該利用権管理者のみ扱うことが可能となる。サービス提供時は、チップアプリケーションと利用権管理者が 2 階層目の PKI 情報を利用したセキュアチャネルにより利用権が設定される。

2 階層 PKI 技術をベースとした IC カードの管理運用モデルとして NICSS フレームワーク<sup>8)</sup>が提案されており、Secure e-Key Network フレームワークを構築する際に参考としている。NICSS フレームワークとは、次世代 IC カードシステムの基本仕様を作成するためのモデルとして、システムコンセプト、業務モデル、基本要件、仕様規定範囲を規定している。図 3 に NICSS フレームワークを示す。

一方、Secure e-Key Network のフレームワークでは、e-Key チップが情報流通機器に内蔵され販売され

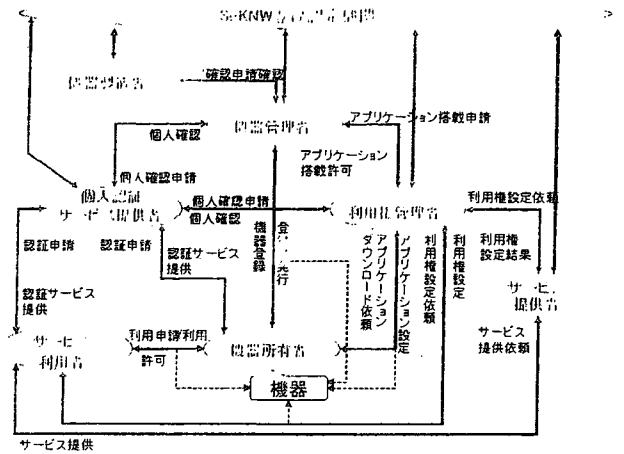


図 4 Secure e-Key Network のフレームワーク (プレイヤーモデル)  
Fig. 4 Secure e-Key Network framework (player model).

表 1 Secure e-Key Network プレイヤの説明  
Table 1 Explanation of Secure e-Key Network Player.

プレイヤー	説明
SeKNW	Secure e-Key Network 環境を提供するために必要な認証情報を管理する役割
登録認定機関	e-Key チップを搭載する機器を製造する役割
機器製造者	e-Key チップを搭載した機器を登録し、e-Key チップ上の資源を管理する役割
機器管理者	機器所有者、サービス利用者が本人であることを証明する役割
個人認証サービス提供者	利用権管理アプリケーションの発行を行う役割。利用権の発行・管理を行う役割
利用権管理者	サービス利用者にサービスを提供する役割
サービス提供者	e-Key チップを搭載した機器を所有する主体
機器所有者	サービスを利用する主体

ることや、機器の所有者と機器の利用者が必ずしも一致しない点、それらにともない機器認証が必要となる点などに注意し、プレイヤーモデルの確立を行っている。図 4 に Secure e-key Network のフレームワークを示す。また、プレイヤーの役割を表 1 に示す。

NICSS フレームワークが IC カードの貸与を前提

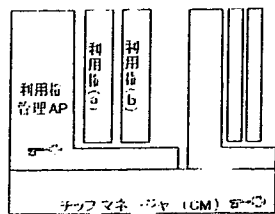


図 5 e-Key チップによる利用権管理イメージ

Fig. 5 Image of right to use management of e-key chip.

とする管理運用モデルであるのに対し、Secure e-Key Network フレームワークでは、機器の販売を前提とする管理運用モデルを確立している。具体的には、以下の点で NICSS フレームワークと異なる。

- 機器の所有権は機器管理者ではなく、機器所有者にある。NICSS フレームワークでは、カードの所有権は発行者にある。
- 利用権管理サービスを提供する利用権管理者とサービス提供者が分離している。NICSS フレームワークでは、サービス提供者が利用権管理サービス相当も提供している。
- 個人認証サービス提供者が分離している。NICSS フレームワークでは個人認証サービスを定義していない。

また、利用におけるフェーズとして、ネットワーク基盤フェーズと利用権管理・配送フェーズに分けることができる。ネットワーク基盤フェーズでは、各プレイヤーの登録認定や認証サービス登録、機器登録 (1 階層目の PKI 登録)、利用権管理 AP 登録 (2 階層目の PKI 登録)、利用者登録を行う。そして、利用権管理・配送フェーズでは利用権取得のためのサービス利用者のサーバ登録や利用権取得、サービス利用、利用権譲渡が行われる。

利用権の配送により e-Key チップに保存される利用権のイメージを図 5 に示す。1 階層 PKI の上に利用権管理 AP が独立して 2 階層 PKI として搭載され、その中に利用権が保存される構成となる。

### 3. オンデマンド VPN システム

#### 3.1 インターネット VPN の現状

インターネット VPN では、VPN の各種設定を利用者自ら行う必要があり、特にネットワーク技術者を持たない企業や家庭では VPN 装置の購入と同時に設置作業も業者に依頼することになり、オンデマンドな VPN 開通が難しい状況にある。さらに、VPN の接続構成を頻繁に変更する場合など、利用者の設定の負担が大きく、VPN の利用促進を阻害しているのが現状である。この状況に対し VPN 設定の利用者の負担を

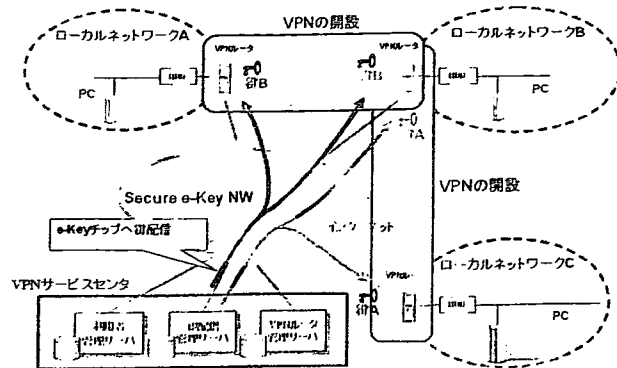


図 6 オンデマンド VPN のサービス例

Fig. 6 Service example of on-demand VPN.

低減する試みとして、辻本ら<sup>9)</sup>は、VPN の接続ポリシーをセンタで管理し動的に接続可能な構成を提案しているが、利用者があらかじめ VPN ルータに構成情報をセキュアに設定するための仕組みについて提案をしていない。また、アジアビジョン・ジャパン (株)<sup>10)</sup>では、IC カードをルータに差し込むことで設定情報を自動でルータに設定する仕組みを実用化しているが、情報の変更が生じた場合には IC カードの配送に時間がかかることからオンデマンドに設定が完了する方式は提供していない。Niwano らは<sup>11)</sup>、遠隔環境から IC カードへの書き込み方式として、マルチアプリケーション型 IC カードを扱うプラットフォームを提案しているが、VPN を扱うためのフレームワークの提案や処理方式についての検討は行っていない。

そこで筆者らは、インターネットを利用して VPN を構成する各種情報を利用者の要求に応じてセキュアかつオンデマンドに配信するオンデマンド VPN システムを検討した。遠隔から安全に VPN 機器を制御する仕組みとして、先に紹介した Secure e-key Network を適用した。図 6 はオンデマンド VPN のサービス例を示している。利用者の VPN 開設要求に対し、鍵配送センタがインターネットを利用して VPN 鍵を VPN ルータに配信している。センタとチップ間で相互認証されセキュア通信路が構築されるため、高いセキュリティを確保して情報の設定が可能となる。配信後、VPN ルータ間で VPN が開設される。

#### 3.2 オンデマンド VPN システムによる情報設定

オンデマンド VPN システムでは、2 章で示した Secure e-Key Network のフレームワークに VPN サービスを適用している。オンデマンド VPN のプレイヤー説明を表 2 に示す。オンデマンド VPN システムでは、利用権管理者より利用権として VPN 鍵が e-Key チップに設定される。

本フレームワークにおいて、VPN が構築されるま

表 2 オンデマンド VPN のプレイヤ説明  
Table 2 Explanation of on-demand VPN Player.

プレイヤー	説明
SeKNW 登録認定機関	Secure e-Key Network 環境を提供するために必要な認証情報を管理する役割
VPN 機器製造者	e-Key チップを搭載する VPN ルータを製造する役割
VPN 機器管理者	e-Key チップを搭載した VPN 機器を登録し、e-Key チップ上の資源を管理する役割
個人認証 サービス提供者	VPN 機器所有者、VPN サービス利用者が本人であることを証明する役割
利用権管理者	利用権管理アプリケーション (VPN サービス) の発行を行う役割. 利用権 (VPN 鍵) の発行・管理を行う役割
VPN サービス提供者	VPN サービス利用者に VPN サービスを提供する役割
VPN 機器所有者	e-Key チップを搭載した VPN 機器を所有する主体
VPN サービス利用者	VPN サービスを利用する主体

での流れを示す。VPN 機器製造者は、SeKNW 登録認定機関より認定を受け、VPN 機器製造時に e-Key チップ内に 1 階層目の PKI 情報を仮鍵として設定し、VPN 機器を販売する。次に、VPN 機器を購入した VPN 機器所有者は、インターネットを利用して、VPN 機器管理者に対して VPN 機器の登録を行う。このとき、SeKNW 登録認定機関より認定された VPN 機器管理者は、e-Key チップに設定された仮鍵で機器認証を行い、認証に成功すれば e-Key チップ内の 1 階層目の PKI 情報を仮鍵から本鍵に再登録する。さらに、VPN 機器所有者が VPN サービス提供者にサービス要求すると、利用権管理者は VPN 機器管理者にチップアプリケーションの搭載許可を得る。そして、VPN 機器管理者によって構築されるセキュアチャネルを用いて、VPN サービスのためのチップアプリケーションを e-key チップにダウンロードし、2 階層目の PKI 情報を設定する。また、VPN サービス提供者に対し、VPN 機器所有者より VPN の接続ポリシーや VPN 機器を利用可能な利用者の登録が行われる。これで、VPN 機器登録にともなう初期設定が完了する。

VPN サービスを利用する場合は、まず利用者が VPN サービス提供者に対して VPN サービスの依頼を行う。VPN サービス提供者は、VPN 機器所有者が設定したポリシーを確認し、接続可能な場合は利用権管理者に VPN 鍵の配送を依頼する。利用権管理者は、VPN 接続する 2 点間の VPN 機器の e-Key チップに設定された VPN サービスアプリケーションと通信し、2 階層目の PKI を利用して相互認証 (機器認証) を行い正当な機器であれば VPN 鍵を e-Key チップに配信する。2 点間の VPN 機器に VPN 鍵が配信される

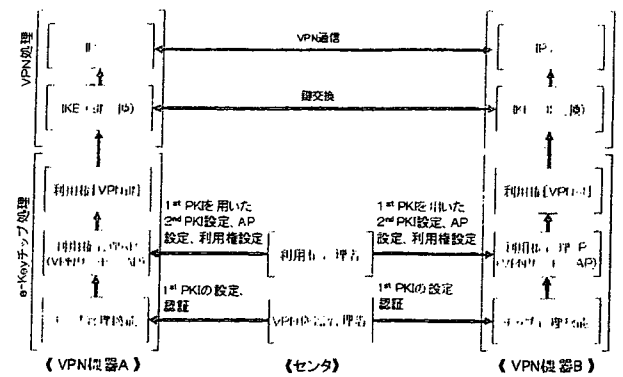


図 7 オンデマンド VPN 構成例  
Fig. 7 Configuration example of on-demand VPN.

と VPN 機器は設定された情報を用いて VPN の構築を行う。

図 7 は VPN の構成として鍵交換に IKE (Internet Key Exchange), 暗号通信に IPsec を用いた場合の 2 階層 PKI と VPN 構築の関係を示している。まず VPN 機器管理者が、1 階層目の PKI により e-key チップと認証する。次に利用権管理者は、利用権管理 AP のダウンロードおよび 2 階層目の PKI 情報の設定を行う。以後、利用者の VPN 接続要求に基づき利用権管理者は、利用権管理 AP と 2 階層目の PKI を用いて認証を行い利用権をダウンロードする。そして VPN 機器間で IKE, IPsec が利用され VPN が構成される。

#### 4. オンデマンド VPN システムの実装

ADSL ルータを用いてオンデマンド VPN システムのプロトタイプを開発した。開発システムでは、ルータが持つ PCMCIA インタフェースに IC カード R/W を設置し、e-key チップの利用環境を構成した。e-Key チップには、2 階層 PKI 構造を持つ IC カードを用いた。セクタ機能として、VPN サービス提供者機能と VPN の利用権管理者機能を 1 台の PC に構成した。利用者からの接続要求を受け付けると、接続ポリシーを確認し、VPN 鍵の配信を実行する。また、VPN サービス提供者機能として、ルータの別名と IP アドレスのマッピング情報を提供する VPN ディレクトリセンタを構築した。なお、ルータの登録を行う VPN 機器管理者機能と、利用権管理者機能の一部 (利用権管理 AP や 2 階層目の PKI 情報を設定) は、IC カード管理システムで実現検証済みであったため割愛した。ソフトウェア構成を図 8 に示す。ルータ-セクタ間の VPN 鍵にかかわるデータ授受は WWW サーバを介して実装した。

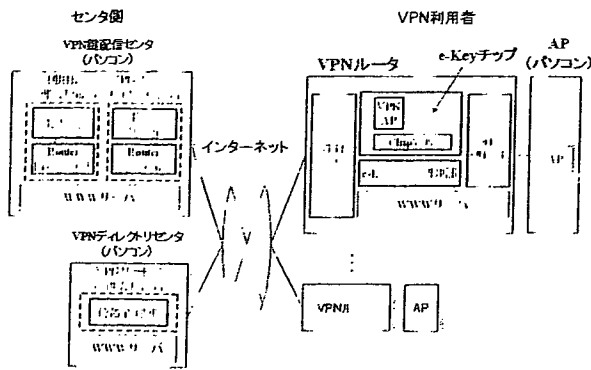


図 8 ソフトウェア構成

Fig. 8 Software configuration.

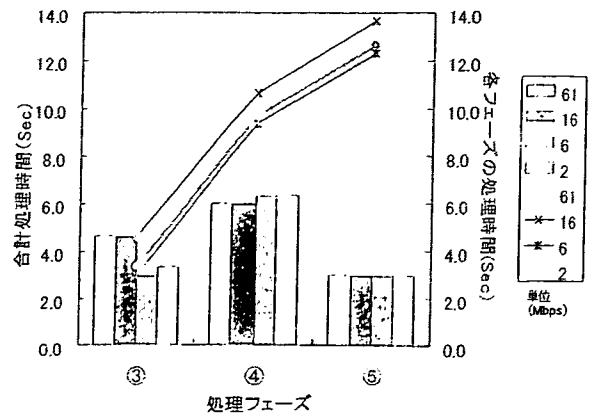


図 9 ターンアラウンド時間

Fig. 9 Turnaround time.

## 5. プロトタイプシステムの動作手順と動作時間

プロトタイプシステムは、利用者の要求から VPN が開設されるまで以下の手順をとる。

- (1) 利用者の PC よりルータにアクセスし、ルータにログインする。ここで、ログイン処理は、VPN 機器登録時に事前に e-Key チップに設定される利用者情報の一致確認によって行われる。
- (2) ログインに成功すると、ルータを通して登録された VPN ディレクタセンタにアクセス可能となり、センタの接続先リストから VPN の接続先を選択する。
- (3) 選択した VPN 接続先と自ルータの接続情報をリストにして、自ルータを経由して登録された VPN 鍵配信センタに接続依頼を行う。このとき、e-Key チップでデジタル署名を生成しリストに添付することで依頼元ルータの依頼情報の正当性をセンタ側で検証する。また、VPN 間で VPN 構成ポリシーに問題がないか相互確認を行い、相手先ルータが接続に合意していなければ、受付を拒否する。
- (4) 署名検証とポリシーチェックに成功しいったん VPN 鍵の配信依頼を受け付けると、VPN 鍵配信センタより各リストのルータに鍵の配信が行われる。センタとチップは相互認証とセキュアチャネルにより VPN 鍵をセキュアに e-Key チップに格納する。
- (5) VPN 鍵の格納が完了すると、ルータは格納した VPN 鍵をもとに IKE によるセッション鍵交換を行い IPsec による VPN 通信を構築する。

いったん VPN が構築された 2 点間では、利用者の要求により VPN 削除処理が VPN 鍵配信と同様な手順で行うことができる。また、一時的に VPN 鍵を無効化することも可能となっている。

2 点間の VPN 構築時間として、(3)~(5) で示し

た動作時間を測定した (図 9)。利用するネットワークの通信速度による VPN 構築時間の影響を確認するため、実効通信速度を 4 段階 (約 61 Mbps, 16 Mbps, 6 Mbps, 2 Mbps) に設定したときの構築時間を測定した。図 9 より、2 点間の VPN 構築として、(3) における VPN 接続依頼から接続受付完了まで約 4 秒、(4) に約 6 秒 (2 点間のルータへの配信)、(5) に約 3 秒を要し、全体として 13 秒程度で VPN 構築が可能であることを確認した。通信速度の違いによる VPN 構築時間の影響は、本測定範囲では軽微であった。

## 6. 考 察

2 階層 PKI を用いたオンデマンド VPN の効果を 5 章の結果を用いて議論する。一般に VPN 構築では、VPN 機器をインターネットに設置する前に接続する相互の VPN 機器に設定情報を保存する必要があり、VPN 技術者が設置拠点に出張して設置する場合や VPN 機器を技術者に送付して設定してもらう必要があった。これらの手間は数時間から数日かかることが予想され、本システムによればそれらの手間の相当量を削減できる可能性があることが分かった。

VPN 情報の配送・保存において、センタと耐タンパチップが直接暗号通信により設定することで、設定情報の漏洩問題も改善することが確認できた。また、VPN 構築時間のおよそ半分が配送処理にかかわる時間であり、ネットワーク通信速度にそれほど依存しないことから、センタや端末内の配信処理時間の向上が VPN 構築時間の改善に有効なことが分かった。特に、耐タンパチップはメモリ容量や処理速度に制限があることから、VPN 接続拠点数が増加した状況では、チップ側の VPN 情報の受信処理の効率化が課題になると想定される。

実装システムでは既存の ADSL ルータに IC カード

を組み合わせる擬似的に構築しているため、IC カードの脱落、抜き取りによる紛失・盗難の問題が残ること、今後実用に向けて克服すべき課題である。

## 7. ま と め

Secure e-Key Network を参照フレームワークとし、2 階層 PKI を利用したオンデマンド VPN システムを開発した。オンデマンド VPN システムは、インターネットで利用が進展している VPN において、設定や設定変更の煩わしさ、セキュリティの課題を解決し、利用者の要求に応じて即時 VPN を開設可能とした。開発システムは、大学において VPN サービスを具体的に実現するうえでのフレームワークや 2 階層 PKI 技術を利用する鍵管理方式について検討を主導し、企業にてシステム構成検討や ADSL ルータを利用した実装を分担することで、新たな認証技術を実サービスに近い環境で構成することができた。

現在、本研究は総務省が実施する平成 16 年度情報通信技術の研究開発である高度ネットワーク認証基盤技術の研究開発を受託し、オンデマンド VPN 技術の研究開発として引き続き産学連携で推進しており、今後は 1 階層目の PKI を利用する機器登録機能の実装や複数拠点での VPN 構築における効率的な VPN 鍵配信技術、配信済み VPN 鍵管理のセキュリティ向上技術などについて検討を進め、インターネットを利用して安全簡単に VPN を取扱い、だれもが安心して情報流通可能な技術の完成に向けて技術開発を進める予定である。

謝辞 本研究は、総務省が実施した H14 年度「インターネット等において各種通信サービスを安全に行うためのネットワーク基盤技術の調査研究」として、「鍵を安全に配送するネットワーク基盤技術」についての調査研究成果を活用したものである。ご協力いただいた関係者各位に感謝する。また、オンデマンド VPN システム開発において、VPN ルータの改造を受け持っていたいただいた沖電気工業 (株)、NTT コムウェア (株) に感謝する。

## 参 考 文 献

- 1) 大山永昭：ユビキタスネットワークを支える技術 (第 3 回) —IC カードと IC タグ, 蔵前ジャーナル, 8, 973 (2003).
- 2) 大山永昭ほか：セキュアチップを用いた機器・コンテンツ利用権管理による高度情報サービス基盤の研究開発, 通信・放送機構平成 14 年度研究開発成果報告書 (2003).
- 3) 大山永昭ほか：多機能 IC チップに関するシステ

ム試作報告書, ニューメディア開発協会平成 14 年度報告書 (2003).

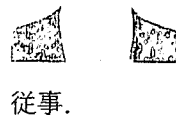
- 4) 小尾高史, 山谷泰賀, 谷内田益義, 山口雅浩, 大山永昭：多機能 IC チップを利用した映像メディア配信システムの検討, 2003 年情報科学技術フォーラム講演論文集, M-121 (2003).
- 5) 小尾高史, 山谷泰賀, 谷内田益義, 山口雅浩, 大山永昭：セキュアチップを利用したコンテンツ配信システムの開発, 第 5 回 YRP 移動体通信産官学シンポジウム講演論文集, pp.96-97 (2003).
- 6) 小尾高史ほか：オープンネットワーク環境で安全な鍵配送を実現するネットワーク基盤, 電子情報通信学会 2004 年総合大会予稿集 (2004).
- 7) 馬場達也：マスタリング IPsec, pp.178-193, オライリー・ジャパン (2001).
- 8) NICSS (次世代 IC カードシステム研究会). <http://www.nicss.or.jp/>
- 9) 辻元孝博ほか：IPv6 IPsec による End-to-End VPN 構築方式に関する考察, 情報処理学会, コンピュータセキュリティ14-28 (2001 年 7 月 25 日).
- 10) アジアビジョン・ジャパン (株). <http://www.avj.co.jp/>
- 11) Niwano, E., Hashimoto, J., Senda, S., Yamamoto, S. and Hatanaka, M.: Smart Card Information Sharing Platform towards Global Nomadic World, *IEICE*, Vol.E87-D No.4 (2004).

(平成 16 年 9 月 2 日受付)

(平成 17 年 2 月 1 日採録)

高橋 成文

(株) NTT データ技術開発本部勤務。平成元年東京農工大学大学院工学研究科修士課程修了。同年 (株) NTT データ開発本部入社。ユビキタスネットワーク技術の研究開発に従事。



東川 淳紀



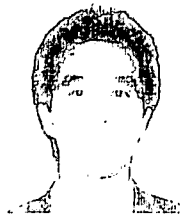
(株) NTT データ技術開発本部勤務。平成 11 年京都大学大学院工学研究科情報通信工学専攻修士課程修了。同年 (株) NTT データ技術開発本部入社。IC カードシステムおよびモバイルセキュリティ等の研究開発に従事。電子情報通信学会会員。

## 山本修一郎 (正会員)



(株) NTT データ技術開発本部副本部長。昭和 54 年名古屋大学大学院工学研究科情報工学専攻修了。同年日本電信電話公社入社。平成 2 年日本電信電話株式会社ソフトウェア研究所主幹研究員を経て、平成 11 年同社情報流通プラットフォーム研究所主幹研究員となり、平成 14 年より現職。ソフトウェア工学、ユビキタスコンピューティングの研究に従事。電子情報通信学会、日本ソフトウェア科学会、人工知能学会、日本データベース学会各会員。平成 13 年度情報処理学会業績賞。平成 14 年度電子情報通信学会業績賞。平成 15 年度通信協会前島賞。

## 小尾 高史



東京工業大学大学院総合理工学研究科助教授。平成 7 年同大学大学院物理情報工学専攻博士課程修了。同大学教務職員、助手を経て平成 15 年より現職。医用画像処理、医療情報処理、ネットワークセキュリティの研究に従事。電子情報通信学会、応用物理学会、日本医用画像工学会各会員。

## 谷内田益善



東京工業大学像情報工学研究施設特任助教授。平成元年同大学大学院物理情報工学専攻博士課程修了。高知医科大学助手、平成 3 年(株)リコー入社、平成 13 年より現職。情報セキュリティ、オフィスシステムの研究等に従事。応用物理学会、日本医学放射線学会、日本放射線技術学会各会員。

## 大山 永昭



東京工業大学フロンティア創造共同研究センター教授。昭和 57 年同大学大学院物理情報工学専攻博士課程修了。同大学助手、助教授を経て平成 5 年より工学部教授となり、平成 12 年より現職。情報処理、医用画像工学の研究に従事。電子情報通信学会、日本放射線技術学会、応用物理学会各会員。

特集 不正行為を調査する デジタル・フォレンジック

- 10 デジタル・フォレンジックとは  
辻井 聡男 清成セキュリティ大学院大学
- 12 個人情報保護と企業がなすべき対応  
安藤 業 皇経防衛大学
- 20 米国での問題解決例  
Eric Thompson アクセスデータ社
- 23 デジタル・フォレンジックはどこまで有用なのか  
高橋 郁夫 宇都宮大学
- 27 医療分野における重要性  
秋山 昌範 国立保健医療センター  
デジタル・フォレンジックと犯罪防止
- 33 法律面から見たデジタル証拠の扱われ方  
石井 徹哉 千葉大学
- 37 デジタル証拠の法的活用  
舟橋 啓 NPOデジタル・フォレンジック研究会  
技術解説
- 40 クライアントPCに対するフォレンジック技術  
守本 正宏 網UBIC
- 45 初歩的な適用例と対応策  
萩原 崇幸 (社)コンピュータソフトウェア著作権協会  
構築事例
- 50 個人情報流出事故・再発防止対策に向けた基盤構築  
足立 正浩 シーア・インサイト セキュリティ㈱  
デジタル・フォレンジック・コミュニティ2004 in TOKYOレポート
- 54 パネルディスカッション/アメリカの状況  
編集部  
フォレンジック・ソリューション紹介
- 60 米国製各社フォレンジック製品  
守本 正宏 NPOデジタル・フォレンジック研究会
- 64 ネットワーク・フォレンジック・ツール  
向井 徹 シーア・インサイト・セキュリティ㈱

広告目次

- あ アンペール  
[www.amper.co.jp](http://www.amper.co.jp) No.003
- か 株式会社タイプセンター  
[www.type.co.jp](http://www.type.co.jp) No.004
- き 摂津金属工業㈱  
[www.setsu.co.jp](http://www.setsu.co.jp) No.007
- た 中央電子㈱  
[www.ccc.co.jp](http://www.ccc.co.jp) No.002

- 東芝三菱電機産業システム㈱  
[www.tmelc.co.jp](http://www.tmelc.co.jp) No.008
- 全 ノーテルネットワークス㈱  
[www.nortelnetworks.co.jp](http://www.nortelnetworks.co.jp)
- 世 双葉電子工業㈱  
[www.futaba.co.jp](http://www.futaba.co.jp) No.006
- プロネットシステム㈱  
[www.pronetsystem.co.jp](http://www.pronetsystem.co.jp) No.005
- 網UBIC  
[www.ubic.co.jp](http://www.ubic.co.jp) No.001

資料請求サービス

下記アドレスから掲載商品資料請求をクリックしてください。ご希望の広告主への資料請求が簡単にできます。  
<http://www.ohmsha.co.jp/cnlan/>

## 医療分野における 重要性



秋山 昌範 (あきやま まさのり)

国立国際医療センター 医療情報システム開発研究部長

医療分野でもプライバシー保護は重要な課題であるが、人の命を預かる現場であるため、通常の職場とは異なったポリシーが必要になる。そのために重要な技術要素がデジタル・フォレンジックである。

### 医療の進歩とIT化

今日の社会では工業化、情報化が進み、遺伝子工学や医療技術の高度化によって社会も変化した。特に、環境権、知る権利、プライバシーの権利などの「新しい人権」が登場した。また、個人の生き方や生活の仕方について、自由で自律的な決定を尊重すべきであるという、自己決定権も提唱されている。

そこで、医療の高度化、専門分化が進む中で、質の高い医療従事者の養成や、質の高い医療提供の環境整備を図っていくとともに、患者・国民の適切な選択によって良質な医療が提供されるよう、情報の積極的な提供を図る必要がある。同時に、医療の質の確保ということでは、近年続発している医療事故について、患者の安全を守るという観点から、行政や医療機関がともに総合的に取り組むことが求められる。患者に信頼されるためには、危険性も含めた十分なインフォームド・コンセントや診療情報提供が大切であることは当然であるが、病院情報システムの導入・更新時に、情報システムによる医療過誤対策を考慮することも重要と考えられる。

その際、診療情報の共有化を図るには、それを遂行するインフラや運用指針が必要である。また、患者データを共有するためには、高度のセキュリティ・レベルが要求される。そして、今後の有効活用を図るためには、インターネットなどを介して、各施設内の診療システム間の有機的な連携を図る必要があるが、その際にセキュリティを維持する方法は確立

していない。一方、IT化によって、従来想定していなかった形でプライバシーが損なわれそうになったり損なわれる事例が出てきた。

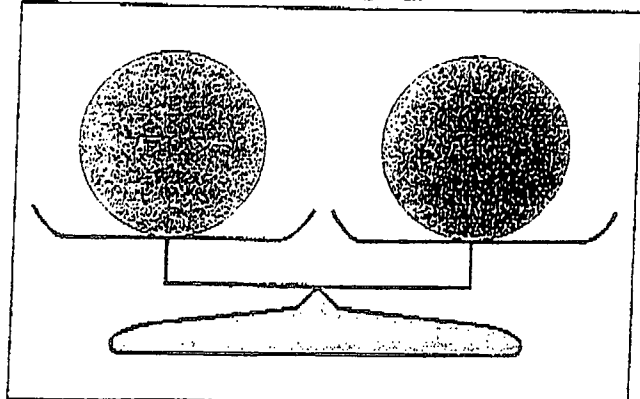
そこで、個人情報保護法が必要となり、その実施を踏まえて国民のプライバシーを守るため情報技術を踏まえた対策が必要となってきたのである。

### 医療分野とデジタル・フォレンジック

#### 【1】プライバシーと公共性

プライバシーとは「個人が自己に属する情報」で、個人情報保護とは「他人には知られたいくないもの」で「目的以外では使われたいくないもの」を意味する。医療分野における取り扱いとしては、診療目的にはよいが、研究目的には本人の承

図1 医療分野における個人情報保護の扱い





消なしに利用することは否とされる。しかし、個人情報を守りすぎることによって、公共の利益が損なわれる場合も生ずる(図1)。

たとえば、感染症情報などでは疫学上、SARS、エボラなどの新興感染症の発生情報を周知させることで予防が可能であることがわかっているが、患者のプライバシーを考慮すると、発生数の少ないときには個人が特定される恐れがある。とはいえ、感染症予防や拡散防止には迅速かつ広範な情報提供が必須であり、プライバシー保護との両立が難しい。また、医療の進歩は診療情報の解析によってなされる。たとえば、新薬の臨床試験(治験)や移植のドナー情報、レシピエントの治療状況が挙げられる。これらも、個人情報保護と公共の利益の両立が困難である。

## 【2】目的外利用での安心の担保

このように、公共性と個人の尊厳のトレードオフの問題に関しては、公共性を重視すれば、個人情報はある程度(本来の)目的外利用せざるを得ない。その場合に患者、国民の安心を担保するために、万一漏えいした場合の責任が明確になることが必要である。つまり、訴訟などで証拠として用いられるだけの担保が重要であり、その根拠としてデジタル・フォレンジックが必要になるのである。

デジタル・フォレンジックといえば、一般的には「コンピュータやネットワークを利用したなんらかの犯罪や事件が起きた場合に、その原因究明や捜査などのために必要な証拠を収集・保存する技術」を指し、証拠情報学と訳される。これによって、外部のみでなく内部から悪意ある情報漏えいが起きた場合や、不可抗力として内部のミスによって情報漏えいが起きた場合でも、漏えいを立証できることで遵守させることが可能と考えられ、国民の安心を得られるであろう。

## 医療分野特有の問題

個人情報保護のもっとも重要な要素として、使用目的の明示と目的外利用の原則禁止がある。しかし、医療の場合にはかなり微妙な問題が数多く存在し、医療従事者と一般の人の間で、診療情報の目的に対しての考え方が一致していない。特に、前述した臨床研究の公益性に関する差異が大きい。個人情報保護法では、法律で許された範囲以外の利用に関しては通知することが原則であるが、診療情報の取得目的を整理して考える必要があり、通知の方法も検討の必要がある。

また、プライバシー保護に役立つセキュリティ技術と臨床現場で利用可能な利便性が、いかなるレベルで運用・維持で

きるかを検証する必要もある。検証方法としては、情報技術を中心に検討するのみならず、データの二次利用におけるセキュリティでは、無名性確保のための方法や運用ガイドラインの検討も必要である。さらに、前述したプライバシー保護に関する社会的、心理学的要因を排除するためには、データを臨床研究に応用する際、患者のプライバシーを損なわないための指針作成が必要である。

このような対策によって、臨床研究の促進を図り、患者の診療レベルを向上させることが可能になる。

## データの二次利用におけるセキュリティ要件

### 【1】二次利用におけるプライバシー保護は無名性の確保

診療情報を診療以外で使用する場合を二次利用と呼ぶ。二次利用における患者のプライバシー保護とは、利用する際に個人が特定できないことを意味する。したがって、研究する際のデータの中に個人を特定する情報が含まれていないと、本人のプライバシーは保護される。

しかし、現実には診療情報の中には、個人を特定するデータと考えられる、氏名、住所、電話番号、生年月日などが登録されている。その個人を特定するデータと、解析に用いる診療データが連結可能な状態であると個人が特定されるので、プライバシーは保護されていない状態になる。また、両者が連結できないと保護できていないことになる。

そこで、どのようにすれば、連結できない状態である無名性を確保できるかの検討を行った。具体的には、病院の電子カルテに蓄えられている診療情報項目を用い、無名性の定量化を試みた。

無名性確保のための方法と、運用ガイドラインの検討、患者情報の収集や参照を行うためには、ネットワークのセキュリティが重要になる。ネットワークや情報技術の問題点として、データセンターから各病院までの回線の安全性について確保(専用線またはVPNなどの仮想専用線網を利用)が必要であり、さらに各医療機関内における病院情報システムとの接続が課題となる。

また、各病院内における管理形態やセキュリティ・ポリシーの統一化が必要であるのみならず、セキュリティのある情報基盤を整備する必要もある。これらは、病院ごとにレベルがちまちちであり、各病院内における電子カルテ端末と診療・研究支援システムの相互利用をめざすためには、まだ課題が多く見られた。

表1 患者情報32万件に対する絞り込み結果

絞り込み条件	人数
生年月日 (年、月、日)	30.6人
生年月日 (年、月、日) + 性別 (女性)	15.3人
生年月日 (年、月)	368人
生年月日 (年、月) + 性別 (女性)	152人

## 【2】診療情報システムにおけるセキュリティ要件の検討

一方、集積されたデータを臨床研究などに活用する際に重要になる、診療情報システムにおける患者のプライバシー保護を行うためのセキュリティ要件を検討した。

まず、各種個人データの行政などにおける海外を含む事例やその利用形態について、調査研究を行った。具体的に第一点は、無名性の定義を定め、大規模病院情報システムに蓄えられている患者情報32万件の診療情報項目を用い、無名性の定量化を試みた。以下に、生年月日の粒度別や特定の年齢、および特定の住所の最小特定人数、他の情報項目との組み合わせの最小特定人数を示す。

その結果、患者の「生年月日 (年、月、日)」のみで30.6人に絞り込まれた。さらに、「生年月日 (年、月、日) + 性別 (女性)」で15.3人、「生年月日 (年、月)」で368人、「生年月日 (年、月) + 性別 (女性)」では152人であった (表1)。そして、患者年齢が60歳の場合、2万5千人であるが、「患者年齢が60歳かつ性別が女性」では1万1千人になり、さらに保険適用傷病名称 (胃がん) まで絞り込むと89人になった。

医学研究においては、病名や年齢、性別は必須要件になるが、氏名、住所を秘匿してもかなり絞り込めることが判明した。

したがって、個人情報保護法案に基づいた、医療分野での個人情報保護ガイドラインが重要である。このような診療データの研究への二次利用に関する検討として、今後は遺伝子情報データベースの研究応用などへの応用も期待される。

## プライバシー保護に関する社会的、心理的要因の検討

### 【1】意識調査の実施

このような情報システムを用いた場合のプライバシー保護に関する社会的、心理的要因の検討として、HIV診療支援ネットワーク・システム (A-net) における利用者や患者、国民の意識調査のため、各施設利用者への意識調査のためのアンケート表作成を行っている。

この研究においては、患者側に電子化することによる情報漏えい不安が存在し、利活用を阻害していた。そのため、登録されることを拒否する患者が多く見られた。さらに、情報工学的な問題以外に、社会的要因が存在することが判明した。

そこで、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の解析が不十分であり、それを克服するための同意書が利用拡大の最大の阻害要因となっていた。すなわち、同意書をとる必要があるということは、プライバシーが漏れやすいことを意味すると勘ちがいされるのである。

しかし、現在の運用指針では診療目的以外の利用 (研究など) を禁止しており、疫学者や臨床工学者などは研究利用ができないし、研究の利用者拡大を図らないと医学の進歩が停滞する恐れがあり、行き過ぎたプライバシー保護によって医学の進歩を阻害し、公共の利益を損なう可能性さえあると危惧された。一方で、アンケートは意識データの収集のみならず、啓発活動としても有用であることがわかり、同時にビデオ上映や配布による啓発が有効であることも示唆された。

これらの手法は、国民にデータ二次利用の安全性の理解を深める効果も期待でき、デジタル・フォレンジックの啓発にも有効と思われる。

### 【2】診療情報提供に関する解析

また、HIV患者の身体障害者手帳利用の際の調査研究より、直接診療目的以外の利用におけるカミングアウトと、そのコスト計量を社会的・心理学的に行う必要があると考えられたが、研究利用ではさらに不安が強くなることが予想される。

そこで、診療情報提供による結果としての「自分の病名を他者に知られるなどのデメリットや不安感」と「治療の向上といった利益が受けられる」というバランス意識を、社会制度やITに対する理解などと関連づけて解析する研究を行っている。

具体的には、研究利用などにおいても治療技術の向上についての意識のありかたや、自らの情報を提供することが仲間の治療に貢献できるのだという意識のありかた、自分の情報を提供しても医学の進歩に貢献したという実感があるかないかなどの調査研究のデザインを検討し、研究利用における社会的問題点の検討を行うことが有用である。

このように、患者の個人情報を診療に使う場合と研究に使う場合では、差があることが類推される。また、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。この躊躇を克服するために、デジタル・フォレンジックの応用が必要に

なる。不注意で漏えいした場合にもその証拠が示されることで、閉止めになると考えられる。

## 患者から見た安心度のレベル

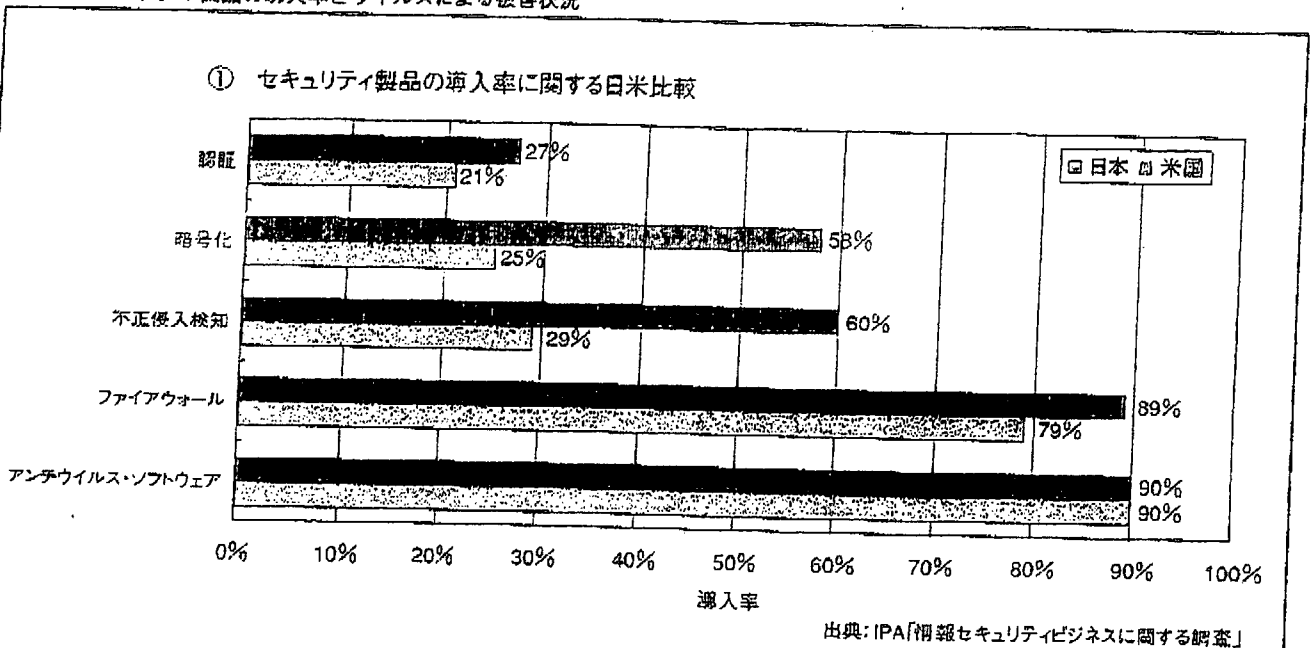
### 【1】高いレベルを要求する患者側

今後はマーケティングで行われているように、新技術への適応に関し、集団心理面からの検討も行う必要がある。さらに、米国における個人情報法の指針であるHIPAAを参考に

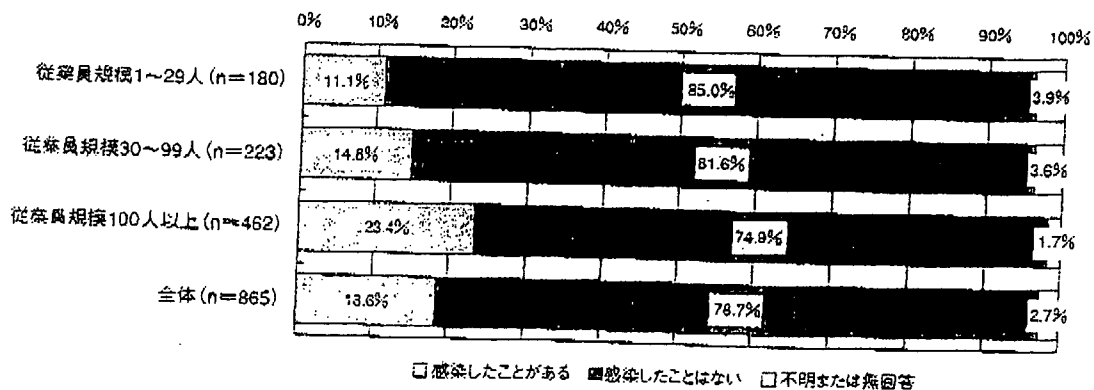
しながら、日本における個人情報保護を踏まえたうえで、情報ネットワーク・システムを利用した臨床研究における情報学的・社会学的指針を制定できると考えられる。

そのなかで、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た、臨床データの活用環境としてはどのような条件が必要なのか、といった観点から、患者の中で「自分はプライバシーが保護されつつ必要な受診を行っている」という意識が成り立つための条件を、あきらかにする必要がある。

図2 セキュリティ製品の導入率とウイルスによる被害状況



### ② MSBlaster、Welchiへの感染の有無



前述した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。その対策には、マーケティング分野における新技術への適応に関し、集団心理面からの対策も有用であろう。

患者から見た安心度のレベルは完全なものではなく、

- 漏れてしまうと、もう漏れる前には戻せない
- 損害を補償できる手段は困難である

など、犯罪（贓）情報と類似点が多い。特に、社会からの信頼、人間関係の回復、係累への影響など、金銭補償（貨幣価値）では解消できないことから、事故対策で要求される管理レベルには高いものが要求される。

## 【2】まだ意識が低い管理側

しかし、システムにおいては、管理側と管理される側で対立する。現に、セキュリティ製品の導入率は100%ではなく、ウイルス（MS Blaster、Welchi）による被害も多く発生している（図2）。

セキュリティ被害の影響度に関する報告では、2003年6月26日のローソン顧客情報56万人分流出被害例のように、6月9日に顧客3名からの通報で発覚（ダイレクトメール）、8月7日には調査報告がWebに掲載され、「氏名、住所、性別、生年月日、自宅・携帯番号」が社外委託先開発コンピュータから故意に流出したが犯人や手法は不明であり、「民間の調査では限度があり情報抜き取り者の特定は困難」とされた。

また、京都の住民情報漏えい事件（2001年12月）被害例では、最高裁において対象被害住民21万件に対し、住民一人あたり1万5千円の賠償責任が判決され、当該自治体では30億円（宇治市2002年度予算案（収入）531億円の6%）の計上を行った。しかし、住所、電話番号から利用される被害を考えると、これでも安すぎると言われている。これが医療機関であった場合の被害は、さらに大きいことが予想され、賠償額も多大なものであるだろう。

## 【3】安全性の指標化

このようにデータの二次利用におけるプライバシーを保護するためには、無名性確保のための方法が重要である。具体的には、「連結不可能な状態」である匿名性の定量化の検討や運用ガイドラインの検討が必要となる。

そこで、個人情報保護のガイドラインを試作するために個人情報保護法案をポイント別に整理し、それに対応するプライバシー保護実施計画および実施要件を定めることで、多施設共同研究を可能とする。研究などの二次利用においては個人情報保護を抜く必要はないが、診療データを研究利用する際に、

表2 医師患者関係を考慮した研究の安全指標（※）

システム の安全性	不安度	小	中	高
高		○	○	△
中		○	△	×
低		△	×	研究不適

- ◎：安全（ゲノムなどでもOK）
- ：通常は安全（通常の臨床研究）
- △：要注意
- ×：改善が望ましい
- ※匿名性の指標として、最少特定人数を用いる。

研究用データと個人情報とを「連結不可能な状態」にする必要がある。ここでいう「連結不可能な状態」の定義と実現方法は、二次利用における無名性を確保することである。

その方法と有効性について検討すると、データを二次利用する際の匿名性の問題は「最少特定人数」を用いることで安全性の半定量化が可能である。さらに、患者が不安材料として抱える因子を抽出し、不安化要素の集計から不安度により研究計画を3段階に分類し、匿名性の確保の程度である「安全性 VS 不安度」のマトリックス構造（表2）で、研究の安全性の指標化を図ることができる。

## 医療情報の研究利用における プライバシー保護

### 【1】運用ガイドラインに従った情報の取り扱い

前述したように、電子化された診療情報の二次利用に関してはプライバシー保護がもっとも重要な課題であり、プライバシーに関する問題を起こさないためには、まず無名性（連結不可能）を確保することが重要である。しかし、どうしても完全な無名化が行えない場合、同意を原則とする運用ガイドラインに従って情報を扱う必要がある。

診療情報の無名化に関して、定量的に無名性を評価する方法を検討すると、無名性の不十分さと危険性は同一ではないことがわかった。たとえば10名に限定できたとしても、そこから個人を特定するためにはかなりの努力が必要である。そして、1名に限定されうるとしても、実際の個人と結びつけるためにはそれなりの調査が必要になる。有名人や社会的地位の高い人など以外にも、遺伝子情報など社会的に影響の強いデータが含まれて、個人特定への関心が強くなる場合などはやはり危険性が高い。

そこで、患者にIC（インフォームド・コンセント）をとる場合、危険性を表す尺度が必要である。匿名化の中にある「連