

200501296A

厚生労働科学研究費補助金

医療技術評価総合研究事業

医療の質の向上、効率化の為の先進的 I T 技術に関する研究

平成 17 年度 総括研究報告書

主任研究者 田中 博

平成 18 年 4 月

目 次

I. 総括研究報告書	
医療の質向上、効率化の為の先進的 IT 技術に関する研究	3
田中 博	
II. 分担報告書	
1. インターネットを活用した健康情報共有システムに関する研究	11
村井 純	
2. 医療の質の向上、効率化の為の先進的 I T 技術に関する研究	14
辰巳 治之	
3. 電子カルテ交換及び A-net での検証	19
秋山 昌範	
4. インターネット技術の医療応用に向けた、DNS サーバの安定運用のための調査研究	23
野川 裕記	
5. インターネットを活用した栄養計算システムの研究開発に関する研究	25
永田 宏	
6. 電子カルテシステムにおける看護支援機能の検証と改善に関する研究	27
楠岡 英雄	
7. インターネット技術の医療応用に向けた、医療機関のネットワーク接続性に関する研究	30
大江 洋介	
III. 研究成果の刊行に関する一覧	32

平成 17 年度厚生科学研究費補助金（医療技術評価総合研究事業）
分担研究報告書

医療の質向上、効率化の為に先進的 IT 技術に関する研究

分担研究者： 田中 博 東京医科歯科大学情報医科学センター 教授

研究要旨： 本分担研究においては、以下の 2 項目について調査研究を行った。

1) セキュアな電子メールシステムに対する定量評価

我々は、セキュアな電子メールシステムとして Identity-Based Encryption (IBE) の利用を提案した。IBE の有効性を調べるため、我々は医療従事者に PKI と IBE を体験してもらい、analytic hierarchy process (AHP) を用いて評価を行った。その結果、医療従事者は利便性が悪いために PKI の利用は避けたいが、IBE ならば利用する可能性があることが判明した。

2) 医療用リアルタイム動画伝送システムにおける、暗号化による画像品質劣化に対する客観的評価

我々は、暗号通信路を用いた場合の DVTS の画像劣化品質を定量的に評価し、複数の医療関係者から得た主観評価と比較検討することで、セキュリティ対策の違いによる DVTS の再現性の違いについても定量的に評価した。さらに、暗号通信路を用いた DVTS の再現性の違いを定量的に評価した。実験の結果、以下のことが判明した： a) DVTS のデータ処理の乱れが画像の定量的指標に大きく影響を与えた、b) 暗号通信路を用いた画像品質の劣化については有意差をもって示すことはできなかった、c) 主観的評価においては、暗号通信路を用いても診断に十分耐えるとの結果を得た。

○ 研究協力者

東京医科歯科大学
情報医科学センター
野川 裕記
穴水 弘光
五味 悠一郎
大橋 久美子
中川 草
長谷川 直紀

A: 研究の目的

1) セキュアな電子メールシステムに対する定量評価

厚生労働省のグランドデザインで述べられているように、医療の質の向上と効率化・重点化には透明性が高く客観的な情報が提供されることが必要である。そのためには EHR の整備が必要不可欠であり、多くの医療機関が EHR システムの導入や開発を行っている。しかし、医療連携のための標準化が不十分なために、施設内での利用に限

定されている。医療連携の標準化には、セキュリティも考慮する必要があり、現在は public key infrastructure (PKI) が推奨されている。ところが、実際に利用しているという事例はほとんど無く、評価した研究もない。その理由として、現状の PKI は受取側が PKI サービスに対応している必要があり、利便性が悪いためだと考える。

そこで我々は Identity-Based Encryption (IBE) という技術を提案する。これは、事前に送付先の公開鍵を取得していなくても、暗号化及び電子署名を可能にするというもので、紹介状など、相手先が事前に分からない状況下でのセキュリティが可能になる。この有効性を調べるため、医療従事者に PKI と IBE を体験してもらい、セキュリティの意識調査と利便性の評価を行った。評価には、analytic hierarchy process (AHP) を用いた。AHP は、選択・判断が心理的な要素に依存するために、定量的な判断が難しい場合に有効である。

評価の対象としては医療情報の世界的な標準である Health Level Seven (HL7) を用いるべきだが、現状では HL7 がセキュリティに対応していないため、本研究では電子メールを採用した。電子メールは広範囲で使われているが、標準ではセキュリティに対応しておらず、様々なセキュリティ手法が考案されている。

本研究の結果、既存のセキュリティ手法が浸透しない理由が示唆され、医療情報セキュリティに対する IBE の有効性を検討した。

2) 医療用リアルタイム動画伝送システムにおける、暗号化による画像品質劣化に対する客観的評価

我々は、広帯域インターネットを遠隔医療へ応用するべく、DV over IP 方式の動画伝送システムを用いたりリアルタイム動画伝送システムの研究に取り組んできた。我々の以前の実験で、動画像のリアルタイム伝送が実用的な遅延時間内に可能で、かつ診断に耐えうるものであることを示した。

DV over IP 方式の動画伝送システムは数種類あるが、今回の実験では DVTS を用いた。DVTS は DV 動画配信システムのソフトウェアの1つで、日本のインターネット研究プロジェクトの WIDE プロジェクトが開発したものである。DVTS は UDP を用いており、UDP の性質として転送速度は高いが信頼性は低いため、暗号処理による遅延が画像の乱れ、あるいはブロックノイズを生じる可能性を含んでいた。我々の以前の実験では、専門医師が伝送画像から評価をおこなったが、デジタル動画像の評価方法には国際基準が設けられており (ITU-R Rec.500-7 など)、この点において、従来の実験における画像評価には問題があった。国際基準に基づいた画像評価手法は、人間の目による主観評価実験のみであり、この手法は多大な労力とコストを要するにもかかわらず、再現性やリアルタイム性がない。特に、労力とコストの面で、国際基準に基づいた画像評価を測定するのは1研究室が行えるものではなかった。

ところが、最近になって、国際基準で規定される画像の品質を高い精度で自動測定する技術が開発された。この技術は、入力画像信号と出力画像信号の同期合わせを正確におこなうことができ、両画像を比較し、その差分信号に視覚特性を考慮して、画像品質を測定するものである。

一方で、実際の医療現場で動画伝送システムを使用するには、情報の漏えいを防ぐためセキュリティを確保する必要がある。そのため、暗号化による画質品質の劣化を客観的に評価し、画像品質劣化の診断に対する影響を検討する必要がある。

そこで、今回は暗号通信路を用いたリアルタイム動画伝送システムの画像品質劣化を、先ほどの画像品質を自動的に測定する技術を用いて評価し、a) 内視鏡動画を、暗号アルゴリズムを利用する暗号通信路上で伝送し、そのときの画像品質劣化を、国際基準に基づいた客観的指標を用いて評価する。b) 同様の動画を医療従事者に評価してもらい、a) の結果と比較する、この2点の実験を行った。

B：研究方法

1) セキュアな電子メールシステムに対する定量評価

12名の医療関係者が体験及び評価を行った。メールを暗号化及び署名して送信する場合、PKIは事前に受信者が鍵管理サーバで公開鍵の発行手続きを行う必要があるが、IBEはその必要は無く、受信者がIBEに対応していなくても問題はない。IBEでは、鍵管理サーバが各IBEユーザの公開パラメータを全IBEユーザに配布し、各IBEユーザの秘密パラメータは本人に配布する。メールを暗号化する場合には受信者の公開パラメータとメールアドレスを元に暗号化し、復号化する場合には自分の秘密パラメータとメールアドレスを用いる。なお、PKIとIBEは公開鍵の交換方法が違っただけで、セキュリティ強度は同一である。実験に利用するメールソフトは、IBEとPKIの双方

に対応しているMicrosoft Outlook Express(OE)を採用した。また、比較対象を公開鍵の交換方法に限定するため、セキュリティを施していない非セキュアOEも比較対象とし、ユーザインターフェースの影響を抑えた。

被験者には、三種類のOE(非セキュア、PKI、IBE)を設定から実際の送受信まで実際に体験し、Web上からアンケートに回答してもらった。送受信には紹介状のサンプルを用い、定量的な判断指標がない場合に有効なAHPを用いて評価した。この手法は、評価要素を心理構造に基づいて構造化し、それぞれの評価要素の一对比較により他の要素との重要度の違いを測定し、代替案との重要度の違いを評価する。

分析手法としてAHPを利用するため、紹介状を医療機関内で電子メールを利用する際の心理構造モデルを構築した。このモデルは、最終目標、評価基準、代替案の三種類の要素で構成され、それぞれ複数の因子を有している。このモデルに基づき、一对比較による評価尺度を用いたアンケート調査票を作成し、体験後に被験者に回答してもらった。

評価に使う重要度重み付け係数(ウェイト)は、アンケート項目ごとに因子の重要度を比の値として数量化し、因子ごとに比の値を幾何平均して、全因子の総和が1.0となるように標準化したものである。なお、複数人による評価を行うため、一对比較行列に入力するスコアとして、複数の被験者のスコアを幾何平均したものをを用いた。ただし、測定結果に大きな矛盾が生じているデータを除外するため、被験者ごとに各回答の整合度を算出し、その値が基準値以内である回答を採用した。最終的に算出され

たウェイトから総合評価値を算出し、その値を元に有効性を検討した。

最後に、各メールソフトの総合評価値が統計的に意味のある物なのかを調べるため、被験者ごとに総合評価値を算出し、フリードマンの検定を行った。

2) 医療用リアルタイム動画伝送システムにおける、暗号化による画像品質劣化に対する客観的評価

今回はローカルネットワークで伝送実験を行った。具体的な実験方法は以下の通りである。

- a) 送信元と送信先に DVTS をインストールした PC と DV デッキをそれぞれ設置した。
- b) 送信元の DV デッキで内視鏡動画(DVテープ)を再生し、ルータを経由して相手先の PC に送信した。
- c) DV デッキで送信元の動画信号と受信した動画信号を DV から NTSC 変換した。その信号について画像評価装置を使用して評価した。
- d) a) ~c) を、以下の 4 つの方法で行い、結果を比較した。d-1)暗号化(DES4) なし、d-2)暗号化 (DES) あり、かつ ESP over UDP (UDP トンネル) あり、d-3)暗号化 (DES) あり、かつ ESP over UDP なし d-4)ルータなし
- e) 同様に、医師免許を持つ 5 名により送信元の動画と送信先の動画を、ITU (国際電気通信連合) が勧告する 2 重刺激連続品質尺度評価法 (DSCQS: The double stimulus continuous quality-scale method) に準じた評価を行った。

(倫理面への配慮)

1) 「セキュアな電子メールシステムに対する定量評価」、においては実データを用いておらず、倫理的な問題は発生しない。

2) 「医療用リアルタイム動画伝送システムにおける、暗号化による画像品質劣化に対する客観的評価」においては、実際の内視鏡画像データを用いたが患者データは一切付属しておらず、倫理的問題はないと判断している。

C: 研究結果

1) セキュアな電子メールシステムに対する定量評価

被験者全員のスコアの整合度が基準値以内だったので、全てのスコアを採用した。AHP による総合評価は、IBE メールソフトが最も評価が高く($r=0.369$)、次いで非セキュアメールソフト($r=0.328$)、PKI メールソフト($r=0.304$)となった。選択要因の中で最も重要視されたのが「送信先公開鍵を事前に取得不要」という因子($r=0.172$)で、あまり重要視されていないのが「否認」($r=0.085$)であった。非セキュアメールソフトは利便性の良さの重要度が高い傾向があり、PKI メールソフトと IBE メールソフトはセキュリティの高さの重要度が高い傾向がみられた。

フリードマンの検定を行うために各被験者のウェイトを算出した。全被験者の総合評価値を算術平均した結果、メールソフトの順位に変動は無く、各因子のウェイトは全被験者の標準偏差の範囲内であった。標準偏差が高い因子として「初期導入が容易」($S.D. = 0.145$)と「送付先公開鍵の事前取得不要」($S.D. = 0.109$)があり、低い因子として「メール送信作業が容易」($S.D. = 0.036$)

と「メール受信作業が容易」(S.D. = 0.029)が挙げられる。

フリードマンの検定は、メールソフト、全ての選択要因、利便性に関する選択要因、セキュリティに関する選択要因の4つのグループに対して行った。その結果、メールソフト($p=0.013$)とセキュリティ($p=0.031$)に関する選択要因には有意差が見られたが、全ての選択要因($p=0.358$)と利便性に関する選択要因($p=0.537$)には有意差が見いだせなかった。

2) 医療用リアルタイム動画伝送システムにおける、暗号化による画像品質劣化に対する客観的評価

a) 受信した動画像をモニターで確認しながら DSCQS 値の推移をみると、ブロックノイズが発生した箇所は、DSCQS 値が非常に高い値になった。そのため、DSCQS 値が比較的安定しているところから 1200frame の範囲を抜き出して比較することにした。各群に対して t 検定を行い平均の差を検定したところ、各群に対して有意差は示せなかった。

b) 医師による動画像評価

医師による評価結果については、人の目で見れば劣化(細かいノイズ、輪郭がややぼやける、パケット落ちによるブロックノイズなど)はあるものの、5名の方からいずれも診断には十分耐えうる画像であると評価された。

D: 考察

1) セキュアな電子メールシステムに対する定量評価

AHPの結果から、PKIメールソフトとIBE

メールソフトを比較すると、セキュリティ関連因子に差が殆ど現れなかった。これは、セキュリティ強度は同一だと判断されたためだと考える。また、「初期導入が容易」及び「メール送信作業が容易」に差異がある。これは、利用の際に若干分りにくい箇所があったため、GUI実装の改善により対応できると考えている。代替案の総合評価がこの様な順番になった理由として、IBEとPKIは非セキュアメールソフトと比べてセキュリティは評価されているが、PKIがIBEや非セキュアメールソフトと比べて著しく利便性が悪いと評価されたためと考える。

選択要因の中で「送信先公開鍵を事前取得不要」因子が最も大きなウェイトを占めている。これは被験者がセキュリティよりも利便性の方を重要視しているためだと考える。また、セキュリティ関連因子の中では「改竄対策」を最も重要視していることがわかる。これは、紹介状を電子化する場合、改竄されることを一番恐れているためだと推測する。逆に「否認対策」が最もウェイトが低くなっているが、これは医療現場では現実には発生しにくい状況のためだと考える。

基本統計量からウェイトが統計的に妥当であることが分かる。標準偏差が因子によって違いが見られる理由としては、セキュリティに関する知識が被験者ごとに違うために「初期導入が容易」と「送信先公開鍵の事前取得不要」の標準偏差は高くなり、普段からメールソフトを利用しているため判断のし易い「メール送信作業が容易」と「メール受信作業が容易」の標準偏差は低くなったと考える。また、フリードマンの検定結果から、今回の手法によって算出さ

れるメールソフトの評価順位と、セキュリティに関する因子の評価順位が妥当であることが分かる。これらのことから、医療情報システムの評価手法として、被験者のスコアを幾何平均した値を用いた AHP が有効であると考えられる。

今回実施したセキュリティの実態調査により、医療関係者は「改竄」を一番危険視していることが判明した。この対策には電子署名と暗号化が有効であるが、本研究により PKI は利便性が悪いため現場での利用は難しいことが示唆された。我々はこのことが医療現場で PKI サービスが浸透しない理由と考える。しかし、利便性が良くなれば、多少手間が掛かったとしても、医療従事者はセキュリティ技術を利用する可能性も示唆された。本研究は試行研究であるために被験者数が少なく、まだ結論づけることは出来ないが、IBE という技術は医療情報の標準化に大いに貢献すると考えている。

IBE は電子メールに限らず、DVD や USB 等の電子情報記録デバイスを用いて運搬する際にも適用が可能であり、医療情報を取り扱う広範囲な分野に応用が可能である。

2) 医療用リアルタイム動画伝送システムにおける、暗号化による画像品質劣化に対する客観的評価

4 分の間 DSCQS 値が終始安定しなかったのは、ソフトウェアの DVTS のデータ処理の遅れの集積が大きな要因であったと推測する。つまり、同期の遅れを修正処理するたびに画像がスキップしてしまい、それによる同期の修正までの時間がかかるために安定したデータをとれなかったと推測する。さらに、元の DV テープの画像の品質も要

因として考えている。

DSCQS 値の暗号化の違いによる有意差は示せず医師による評価でも大きな差異は認められなかったことから、暗号化は DVTS の画像品質劣化には影響をあたえないと考える。

今回の実験ではルータがボトルネックになる証拠は見つからず、今回使用したルータの DES 使用時でのスループットは 73.6Mbps と記載されていることから、ルータでは DVTS の帯域 30Mbps は十分保証されていると考えている。このことは画像評価装置を用いることにより、ルータの性能を調査することが可能であることを示唆している。

画像評価装置の測定結果と医師の評価を比較すると、人間の目には認識できない遅延時間のゆらぎが画像評価装置に影響を与えたと推測する。この遅延時間のゆらぎを制御することが測定結果の精度の向上につながると思われる。

E : 結論

本分担研究における結論は以下の 2 項目である。

1) セキュアな電子メールシステムに対する定量評価

我々は Identity-Based Encryption (IBE) という技術を提案し、この技術の有効性を調べるため、医療従事者に PKI と IBE を体験してもらい、セキュリティの意識調査と利便性の評価を行った。評価には、analytic hierarchy process (AHP) を用いた。

評価の対象としては医療情報の世界的な標準である Health Level Seven (HL7) を用いるべきだが、現状では HL7 がセキュリテ

ィに対応していないため、本研究では電子メールを採用した。

AHPによる総合評価は、IBEメールソフトが最も評価が高く、次いで非セキュアメールソフト、PKIメールソフトとなった。選択要因の中で最も重要視されたのが「送信先公開鍵を事前に取得不要」という因子で、あまり重要視されていないのが「否認」であった。非セキュアメールソフトは利便性の良さの重要度が高い傾向があり、PKIメールソフトとIBEメールソフトはセキュリティの高さの重要度が高い傾向がみられた。

選択要因の中で「送信先公開鍵を事前に取得不要」因子が最も大きなウェイトを占めている。これは被験者がセキュリティよりも利便性の方を重要視しているためだと考える。また、セキュリティ関連因子の中では「改竄対策」を最も重要視していることがわかる。これは、紹介状を電子化する場合、改竄されることを一番恐れているためだと推測する。逆に「否認対策」が最もウェイトが低くなっているが、これは医療現場では現実には発生しにくい状況のためだと考える。

2) 医療用リアルタイム動画伝送システムにおける、暗号化による画像品質劣化に対する客観的評価

本研究により、DVTSを用いた医療動画像の評価測定が自動評価装置を用いて行えることが示せた。しかし、DVTSそのものの遅延時間のゆらぎのために、測定結果が不安定であった。測定精度の向上のためにはDVTSの遅延時間のゆらぎを制御することが必須である。

現在わが国のインターネット接続サービス

の契約数は2005年末で3千万にのぼり、広帯域ネットワークも普及しつつある。本研究の動画伝送システムが遠隔医療や地域医療ネットワークに貢献することを期待している。

F: 研究発表

1. 論文発表

1) Akina Suwa, Yuichiro Gomi, Hiroki Nogawa, Hiroshi Tanaka. Objective Motion Picture Quality Assessment in Secured Realtime Transmission System for Medical Application. CJKMI'2005 Proceedings of the Seventh China-Japan-Korea Joint Symposium on Medical Informatics, Vol. 2005, pp. 69-72, Nov 2005

2) Yuichiro Gomi, Hiroki Nogawa, Michihiko Koeda, Hiroshi Tanaka. Analysis of Secured E-mail Systems for Electronic Health Record. CJKMI'2005 Proceedings of the Seventh China-Japan-Korea Joint Symposium on Medical Informatics, Vol. 2005, pp. 19-23, Nov 2005

3) Kumiko Ohashi, Yuichiro Gomi, Hiroki Nogawa, Hiroshi Mizushima, Hiroshi Tanaka. Development of Secured Medical Network with TCP2 for Telemedicine. Connecting Medical Informatics and Bio-Informatics: Proceedings of MIE2005 - The XIXth International Congress of the European Federation for Medical Informatics, Vol. 116/2005, pp. 397-402, Aug 2005

2. 学会発表

1) 諏訪 秋奈, 五味 悠一郎, 野川

裕記, 田中 博. 医療用リアルタイム動画伝送システムにおける、暗号化による画像品質劣化に対する客観的評価. 医療情報学, Vol. 25(Suppl.), pp. 635-638 Nov 2005

2) 五味 悠一郎, 野川 裕記, 田中 博. 医療機関における安全な通信：受信者が特定できない場合の暗号化について. 医療情報学, Vol. 25(Suppl.), pp. 902-905 Nov 2005

G：知的所有権の取得状況

1. 特許取得： なし
2. 実用新案登録： なし
3. その他： なし

インターネットを活用した健康情報共有システムに関する研究

分担研究者： 村井 純 慶應義塾大学環境情報学部 教授

研究要旨： 予防医学的な観点から、昨年度の「運動指導」を支援するインターネットを利用した情報コミュニケーションシステムをより広く展開するために、より汎用的な健康に関する情報を効率的かつセキュアに共有するシステムの研究を推進した。本研究は、昨年度までの成果に基づいて「通信の安全性確保」「個人の識別と認証」「長期間の保存」を技術的に解決すると共に、専門家とのコミュニケーションを効率的に行うことを目指している。

○ 研究協力者
慶應義塾大学 環境情報学部
南 政樹

A：研究の背景と目的

健康増進や生活習慣病予防のために様々な施策が試みられている。その一方で、人々の健康に関する興味は、健康食品やマスコミを通じた健康法の多様化を見ても明らかに高まっている。しかし、これらの情報が必ずしも多くの人に当てはまるわけではない。さらに、様々な施策に対して興味はあるが時間が取れずに途中で諦めてしまう、など主観的な理由によって習慣化しない例が非常に多く見られる。

健康行動を習慣化するための方法論として、健康行動理論が挙げられる。この理論では、当事者の行動変容を促すため、継続的な外部からの介入を一つの方法として挙げている。しかし、そのためには適切なタイミングでコミュニケーションすることが必要とされ、時間と場所に依存してしまうのが現状である。

そこで本研究では、インターネットを介して、個々人の健康状態、健康情報、習慣などを共有する仕組みを提案すると共に、それを普遍的かつ永続的に利用できるような技術的課題について取り組んだ。

ここで技術的課題とは次の3点である。

- 安全な通信と情報管理
- 利用者の簡便な識別と認証
- 一生涯を対象とする長期間保存

B：方法

本研究を進める前提として、インターネットを利用した健康情報の収集と再利用についてのシナリオを作成した。そのシナリオは、いわゆる医療サービス提供者、医療サービス消費者の関係だけではなく、医療サービス提供者間の関係、医療サービス消費者間の関係、消費者の家族やサポートを行う者などの役割を想定することで、より現実に即した内容を目指した。

次に、シナリオをベースとして想定されるコミュニケーションとその中に含まれる内容（コンテンツ）について、プライバシーレベル（どのくらい秘密にしなければならないか）についての検討を行った。

そしてシナリオとそこで行われるコミュニケーションのプライバシーレベルの検討を経て、技術的な検討を行った。ここでは、より簡便な導入を意識することで、費用対効果の高いシステムデザインを念頭に置いた。

C：研究結果

まずシナリオについての検討を行った。先行研究として、愛知県で行われている在宅医療に関する取り組みや我々が神奈川県藤沢市で行った高齢者介護に関する情報共有について、その分析を行った。その結果、現状と目指すべきシナリオについて、図1・図2で示す構図を描くことができた。

図1は、医療サービス提供者（専門家）による情報が医療サービス消費者本人を介して他のロール（役割）に伝わる様子を示している。この関係に言えることは、情報の鮮度と正確さがコミュニケーションの間に人間が挟まることで変化する点である。たとえば、介護事業者から派遣される

ホームヘルパーは、医師などの医療サービス提供者が患者に「生活上注意すべき」と伝えたことを注意事項として知ることが、実際には非常に少ないことがヒアリングの結果明らかになった。また、逆にホームヘルパーが医師などに対して生活の

様子や食事の内容などを伝えることはほぼ皆無であった。

専門家の目による貴重な情報や客観的なデータが共有できないモデル

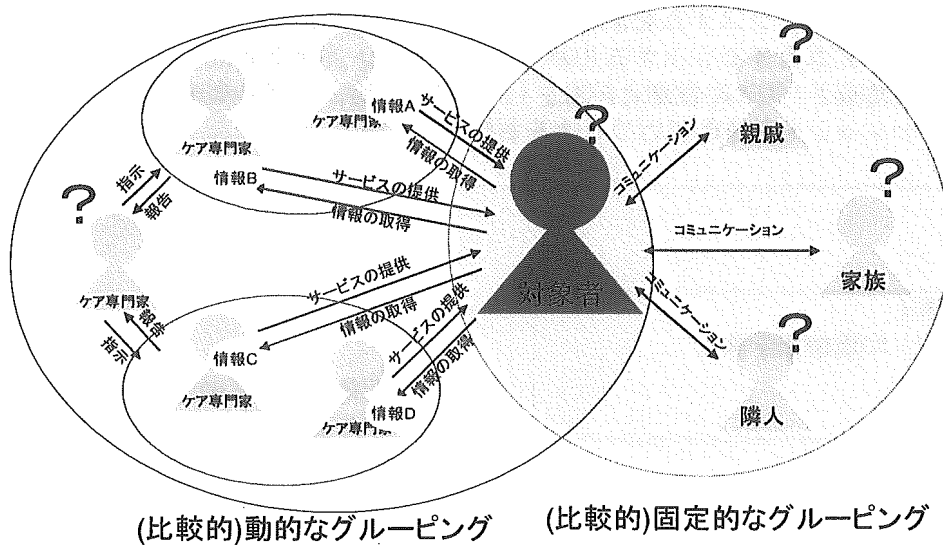


図 1 考えられる情報伝播のあるべき姿

情報の共有とその再利用、外部からの介入が可能な環境の構築

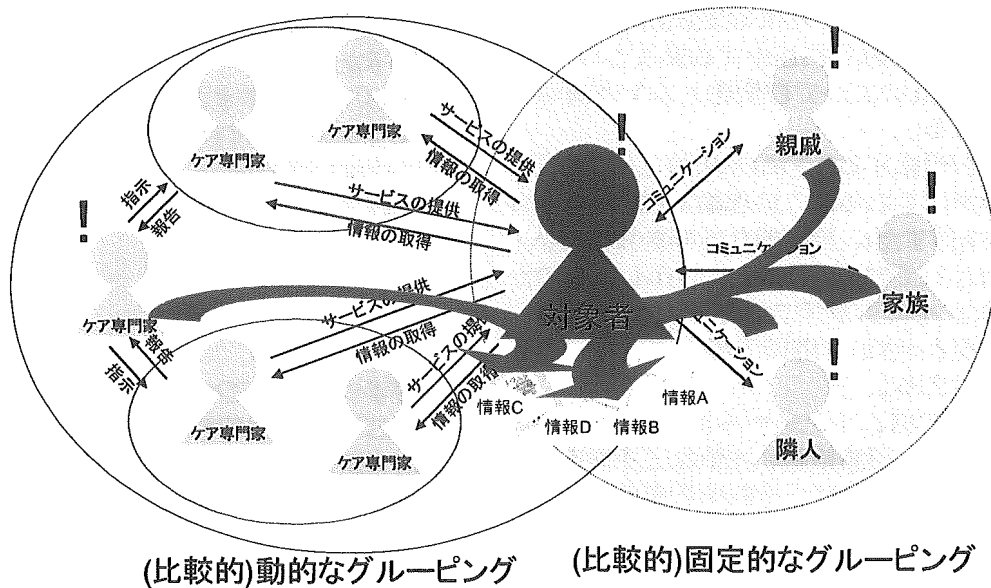


図 2 現状の情報伝播モデル

これらのことから、コミュニケーションパスが設定されていないため、様々なロールが発する情報と、取得した情報が有効に活用されない状態にあることが分かった。

たとえば、図2にあるように、様々な情報が医療サービス消費者を一つのレポジトリ(情報保管のための仮想的なアクセス先)として集約されるようなシナリオでは、医師などの医療サービス提供者が患者(=医療サービス消費者)に提供する情報は、一部のケア専門家(ホームヘルパーなど)には開示した方がよい場合がある。しかし、全てのロールに開示するのは患者のプライバシーなどの問題から避けなければならないケースが多い。

そこで、プライバシーレベルをキーとなる医療サービス消費者である患者と情報の発信者が設定できる情報システムモデルが必要となると考えた。

このことを受け、1) 秘密分散技術による、複数の鍵を利用した情報共有システム 2) Tor を応用した匿名性通信技術 3) P2P アプリケーションで用いられる分散ハッシュテーブルを利用した情報保持者の検索機能を組み合わせた統合的な情報共有システムを構築した。

D: 考察

本研究の成果から、インターネット経由の健康指導には、情報の共有が大切であり、それを安全かつプライバシーを考慮した形で実現することができたと考えることができる。また、医療サービス消費者と提供者双方の利便性について、今後さらに多くの情報が様々なロールから生まれ、様々な機器から発せられることで、今回プロトタイピングを行ったのと同様の仕組みで大きな成果が期待できる。

さらに、このことがスムーズに行えるようになることで、長期入院ではなく在宅医療でも安心して医療サービスの提供が受けられる可能性が現実的になると考える。

この結果からも分かるよう、物理的な制約を排除することで、効果的かつ現実的な健康指導や健康管理、さらには在宅医療のような病院に近い環境での医療サービスを提供することが可能であると考える。

E: 結論

予防医学を効率よく実践する方法として、情報の適切な共有と外部からの介入が挙げられる。それを容易に導入できるインターネットを利用して実現することができた。プロトタイピングでは、情報開示の制御(アクセス制御)と匿名通信による身元の非開示を確認することができた。このこ

とから、現実社会に普及させるのに十分な資質を備えていることも確信できた。

今後は、インターネットを通じた予防医学の実践指導の方法論を固めなければならないことを課題とし、さらに研究を続けていきたい。

F: 健康危険情報

なし

G: 研究発表

1. 論文発表

なし

2. 学会発表

なし

H: 知的財産権の出願、登録状況

1. 特許取得: なし

2. 実用新案登録: なし

3. その他: なし

医療の質の向上、効率化の為に先進的 IT 技術に関する研究

分担研究者 辰巳 治之 札幌医科大学大学院医学研究科 生体情報形態学 教授

研究要旨: 社会のIT化は加速され、ITの医療応用の可能性には絶大で、そのためには標準化も避けて通れない課題である。インターネットを意識することにより、必然的に医療情報の標準化を考えざるを得なくなる。そこで医療情報のインフラとしてのインターネットのあり方を実証実験しながら検討し、その上に基礎研究から臨床応用までの医学研究を乗せ、徹底した情報化による理想的な電子カルテなどによる情報利用と、経営改善を含む効率化からEBMによる医療の質向上のためのシステムそして、21世紀の新しいライフスタイルのニーズに合わせた新健康サービス産業創造までを視野にいたした研究を目的とする。

次世代医療応用の基礎システムとしてのIPv6ネットワークの構築、そしてその応用のために必要な要素の洗い出し、そしてそれを実現するための技術開発及びその実証実験を行った。さらに種々の健康情報を、どのように収集し、どのように応用できるかの実験を多角的に行いながら、安全で費用対効果のよい健康維持管理システムや臨床応用の可能性を検討した。

○ 研究協力者

札幌医科大学大学院医学研究科生体情報形態学
新見隆彦 助手
札幌医科大学附属情報センター
明石浩史 講師
大西浩文 助手
戸倉 一 訪問研究員
西城一翼 研究生
山口徳蔵 研究生
京都大学学術情報メディアセンター
岡部 寿男 教授
藤川 賢治 助手
東京工業大学
太田 昌孝 講師

A : 研究目的

この研究には大きな柱が3本ある。高度情報化におけるインターネットの役割には絶大なものがあり、この出現により社会のIT化は加速され、標準化も進むようになってきた。医療情報における標準化は避けて通れない課題であり、インターネットを意識することにより、必然的に医療情報の標準化を考えざるを得なくなる。そこで、1) 医療情報のインフラとしてのインターネットのあり方を提案、実証実験しながら、2)その上に基礎研究から臨床応用までの医学研究を乗せ、3) 徹底した情報化による理想的な電子カルテめざし、経営改善を含む効率化からEBMによる医療の質向

上のためのシステムそして、21世紀の新しいライフスタイルのニーズに合わせた新健康サービス産業創造までを視野にいたした研究を目的とする。

B : 研究方法

医療の質向上、効率化の為に先進的ITの利活用にあたっては、抜本的な構造改革が重要で、ITを利活用することにより構造改革すべきところの重み付けができるのではないかと考えている。これらのシステムの次世代ネットワーク(IPv6)化の技術的検討を行い、実証実験をするとともに、その応用範囲を拡大していき、究極の目標である国民一生一カルテをどのようなステップで実現できるかを検討を行う。一方で、IT利用者である未病者参加型の健康維持方法を検討し、理想的な情報ネットワーク上で実現することによる一生一カルテから戦略的防衛医療構想を練る。

C : 研究結果

次世代のインターネットプロトコルであるIPv6の実験環境としては、文科省のSINET及び総務省のJGNや、NTTコミュニケーションズやKDDIにてサービスが提供されているが、すぐには使えない。従ってIPv6 Topological Addressing Policyを実現すべくIPv6ネットワークを構築しようとしたときに大きなボトルネックになる。そこで、まず、我々は何処でもIPv6が使えるような環境をつくるにはどうしたらよいかを検討した。

一方でVPNによる医療専用ネットワーク構築を行う試みも行われているが、Private Networkの管理となると非常に複雑になる。なぜなら、Private Addressなので、その組織の中で勝手にアドレスを割り振ってもよいのだが、組織間で情報交換をするためにVPNを形成しようとする、IPアドレスが重複することがあり得る。そこで、将来のことを鑑みるとIPv6によるGlobal Networkの構築が望まれる。そこで、我々はVirtual Global Networkを提案し、それを実現するための方法を検討した。

上記、2つのことを実現するためのBOXを共同研究により開発し、IPv4ネットワークにトンネル技術を用い接続し、その上にVirtualにIPv6のネットワークを構築することを試みた。

このBOXを用いることにより簡単に、どこでもIPv6のネットワーク環境を手に入れることができるようになった。そこで、各地へ出張を機会に、接続実験を行ったところ、セキュリティがしっかりしておりFireWallが完備されていると逆に使えないことが判明した。

そこで、対策として、大概の場合はWebアクセスだけは許している、port 80をつかってトンネリングすると、上記の問題はほぼ解決した。

具体的には、BizMateという電子会議システムを使い、東横インのホテルから実証実験をおこなったところ、以前は使えていたものが、セキュリティ強化と共に使えなくなっていた。そこで、VPNでできることと同じことが、このBOXをつかうことにより実現できた。さらに、VPNでは実現できなかったことも実現できるようになった。それは、FireWallの内側で利用していた環境と全く同じ環境を、そのBOXを持ち出し外部から接続することにより医学部内部と全く同じ環境で使えることが出来るということである。

ネットワークの医療応用の為の実験として、健康情報を流通させる2つの実験を行った。

1つ目は、IPv6-BOXを使った無呼吸症候群の患者のデータを取得する試みと、ホームヘルスケアの機器を利用した健康管理である。

これは健康マットと呼ばれるもので、法政大学の渡辺教授が開発したものを、IPv6で利用できるようにし、先ほどのIPv6-BOXを繋ぎ、病棟での検査を、セキュリティを守り、別の場所から観察できるようにした(図1)。

SAS (睡眠時無呼吸症候群)検査

VGN(IPv6 TAP)による検査システム

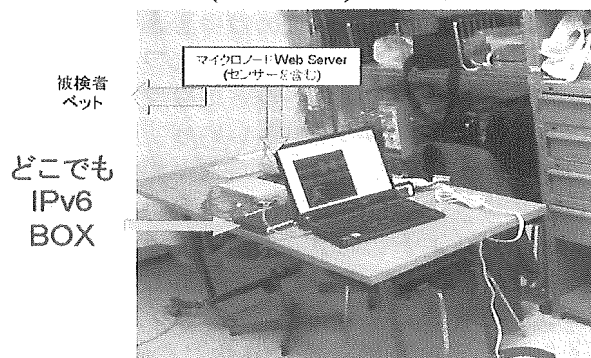


図1. VGNを使った検査システム

SAS Examination with VGN(IPv6 TAP)

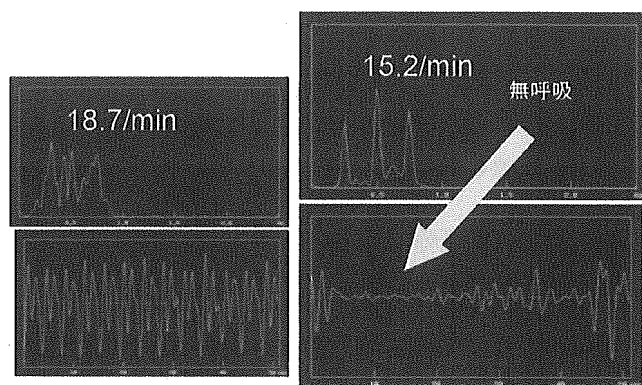


図2. エアマットセンサーによる無呼吸データ

この実験で、規則正しい呼吸のリズムが見られていたところ(図2左)、突然呼吸のリズムが見られてることが分かった(図2右)。これは、IPv6の環境のないところに、BOXを設置することにより、容易にIPv6接続でき、FireWallの内側にIPv6 Topological Addressing Policyを実現しさらに、セキュリティを守ったネットワークにてデータを観察することができた。

このシステムの発展系として、家庭で容易に得られる健康データとして、歩数計や、体重、血圧などのデータの送信を計画した。その中で、歩数計のデータをIPv6ネットワークにて送信し、Walking Marathonの実現できるシステムの構築を試みた。

D: 考察

インターネットを医療系で活用するためにセキュリティを確保しながら、簡単にIPv6ネットワークを構築する方法を考えた。その実現の方法がVGN(Virtual Global Network)である。この実現の為のBOXには2つの利点がある。

1つ目は、VPNをソフト的に利用する場合は、もしパスワードが盗まれると、悪用されることがある。パスワードの管理の難しさは、盗まれても

物が無くなるわけではないので、分からないということである。一方、BOXタイプの場合は、このBOXがないと使えないので、BOXが盗まれるとすぐ分かり、VGN接続の対抗の口をふさぐと不正利用は防ぐことができる。また、2つ目の利点として、VGN接続する端末への新たなソフトのインストールも、接続の為の手順もいらず、配線を繋ぐだけで、すぐに使えるので、我々が提案しているゼロクリック（出来るだけ手間をかけず、複雑でなく簡単にすること）に近い方法である。

医療系においては安全性を確保しながら、利便性も維持することが必要で、この2点において我々のIPv6利用環境構築の為のこのBOXは合格といえる。

さらに、医療系ネットワークにおいては、高速性だけではなく、安定性が重要になる。即ち、インターネットの場合は、上流の回線は選べても、最終目的地までの経路を制御することはできない。そこで、ネットワークの安定性を増強するために、End to End MultiHomeをIPv6で実現することを実験してきたが、今後、このBOXにより実現できる方法を検討し、現在、さらに研究を進めている。

また、現在のところは対一の対向のBOXの設置ではあるが、今後対Nのシステム構築を考えている。さらにこれに拡張性、発展性をもたせるためにも、対Nの効率のよい全国規模のネットワーク構築も必要になり、おそらく各プロバイダーに接点を持つ全国的なNOCの効率のよい分散計画が必要になるものと考えられる。

E：結論

いままで、IPv6の医療応用が叫ばれていたが、現状では、IPv6の普及は非常に覚束なく、現実的でなかった。このBOXを活用することにより、大きな障害なく容易にIPv6の接続環境が手に入った。具体的なこのようなBOXの利用現場を想定して、開発・実証実験を繰り返すことにより、汎用的で使えるシステムの実現が可能ではないかと考えている。

まだ、IPv6化は実現されていないが、マイクロソフトの協力を得て、SQLサーバとInfoPathをつかった簡易電子カルテシステム（検査データの参照システム）を構築し、今後、これらのネットワークの上に稼働させ問題点を解明していく予定である。

また、遠隔医療の一部として、地域医療支援のTV会議の活用や、遠隔医療講義の実験なども行い、今後の実験の基礎構築が出来たところである。

さらに、基礎医学研究用のシステムとして、1D,2D,3D,4Dのデータ共有システム及び知的生産活動支援環境及び共同研究を推進するための知

的フィールドの構築を考え、その基礎システムの構築を行った。

F：研究発表

1. 論文発表

- (1) 辰巳治之、新見隆彦、中村正弘、高橋正昇、明石浩史、戸倉一、大西浩文、村井純、南政樹、三谷博明、田中博.ITとATを活用した情報薬の開発. 医療情報学 25.Suppl, 2005, 766-767
- (2) 戸倉一、明石浩史、大西浩文、新見隆彦、西城一翼、山口徳蔵、西陰研治、辰巳治之、今井浩三. End to End Multihome解説. Proceedings of NORTH Internet Symposium 2005 (ISSN 1345-0247), Pp19-20 (2005)
- (3) 辰巳治之、新見隆彦、中村正弘、高橋正昇、明石浩史、戸倉一、村井純、南政樹、三谷博明、田中博. 情報薬とゼロクリック-戦略的防衛医療構想を支えるもの:ITとATのフル利活用. Proceedings of NORTH Internet Symposium 2005 (ISSN 1345-0247), Pp33-42 (2005)
- (4) Akashi H, Tokura H, Ohnishi H, Nishikage K, Yamaguchi T, Saijo K, Shimmi T, Nakamura M, Nakayama M, Tatsumi H. Establishment and Assessment of Wide Area Medical Information Network System in Hokkaido. Lecture Notes in Computer Science. 2005, 3597:179-189.
- (5) 明石浩史、中村正弘、戸倉一、大西浩文、西城一翼、山口徳蔵、新見隆彦、西陰研治、木村眞司、佐々木茂、澤田いずみ、今野美紀、片寄正樹、仙石泰仁、相馬仁、小海康夫、丸山知子、辰巳治之、今井浩三. 各種ビデオ会議システムによる遠隔地教育支援の実際と評価. 医療情報学 25.Suppl, 2005, 1046-1047.
- (6) 戸倉一、藤川健二、明石浩史、大西浩文、西城一翼、山口徳蔵、新見隆彦、西陰研治、中山正志、辰巳治之、今井浩三. エンドツーエンドマルチホーミング技術を使用した医療施設間通信. 医療情報学 25.Suppl, 2005, 877-878

- (7) 明石浩史、竹原孝治、河合修吾、中村正弘、重田光雄、戸倉一、大西浩文、西城一翼、山口徳蔵、新見隆彦、西陰研治、馬場啓好、山口千寿、木村眞司、佐々木茂、澤田いづみ、今野美紀、片寄正樹、仙石泰仁、相馬仁、丸山知子、辰巳治之、今井浩三. 札幌医科大学附属情報センターにおける教育支援のとりくみ. *Proceedings of NORTH Internet Symposium 2005* (ISSN1345-0247),2005, 11:106-113.
- (8) Tatsumi H, Shimmi T, Nakamura M, Ninomiya T, Ichikawa R, Kikuchi S, Akashi H, Tokura H, Takaoki E, Matsumoto T. A Challenge to Three-Dimensional Reconstruction System Development. 第141回日本獣医学会学術集会講演要旨集. p 131(2006) ISSN1347-8621
2. 講演・学会発表
- (1) 辰巳治之. 「ユビキタス健康管理と情報薬-戦略的防衛医療構想を支えるもの-ICTとATのフル利活用」H17年4月23日 第一回ユビキタス医療シンポジウム (一橋記念講堂)
- (2) 辰巳治之, 「楽しみながらやる生活習慣病予防: ICTとATのフル利活用」総務省: 情報通信月間 H17年5月10日NORTH健康セミナー
- (3) 辰巳治之, ユビキタス健康管理と情報薬 「戦略的防衛医療構想」H17年5月20日 新社会システム総合研究所 セミナー(虎ノ門パストラル)
- (4) 辰巳治之, 究極の代替医療 情報薬による戦略的防衛医療構想.H17年5月25日 第12回PML研究会(大阪薬業年金会館)
- (5) 辰巳治之. ICTとATによるユビキタス健康管理情報薬を実現する:戦略的防衛医療構想を支えるもの: H17年5月26日 ITRC研究会 (名古屋)
- (6) 辰巳治之 IPv6ユビキタス医療ネットワーク 戦略的防衛医療構想実現に向けて. H17年6月11日 和歌山地域医療ネットワーク協議会 (アバローム紀の国)
- (7) 辰巳治之. ICTとATによるユビキタス健康管理情報薬による代替医療の可能性:戦略的防衛医療構想を支えるもの. H17年6月30日 JIMAシンポジウム(市ヶ谷アルカディア)
- (8) 辰巳治之. NORTHの歴史を振り返って21世紀を考える. 平成17年度 NORTH定期総会記念フォーラム札幌医科大学50周年記念ホール (H17.7.6)
- (9) 辰巳治之. 生命科学からの発想による 情報科学の医療応用:戦略的防衛医療構想. H17年9月8日 FIT2005 中央大学.
- (10) 辰巳治之. 知(先)見性の科学を解剖学する. H17年9月10-12日 (伊豆 大仁ホテル) JST異分野融合ワークショップ「知見性の科学一経験、類推、発見と適応」
- (11) 辰巳治之. 生命科学からの発想による システム(社会)安全についての考察. H17年10月6日 JAXAシステム安全研修 (東京)
- (12) 辰巳治之. ITで変わる!地域医療? 戦略的防衛医療構想, ICTフル利活用による情報薬の開発. H17年10月21日 鶴岡医師会
- (13) 辰巳治之. End Userから見た医療ネットワークの理想. HEASNET 保健・医療・福祉情報セキュリティネットワーク基盤普及促進コンソーシアム 第5回利用促進部会. H17年10月28日 (東京)
- (14) 辰巳治之. IPv6-VGNへの期待と医療応用:情報薬の開発応用. ITRC研究会. H17年10月24日(天人閣)
- (15) 辰巳治之. 高度情報化社会における形而上学的諸問題の解明:個人情報保護・セキュリティ. H17年11月2日第5回 個人情報保護対策セミナー, 主催: JAMINA, 共催: NORTH (札幌)
- (16) 辰巳治之. 生活習慣病克服への挑戦. H17年11月5日 京都きづ川病院文化月間行事&創立25周年 (文化パルク城陽)
- (17) 辰巳治之. NORTHについて. H17年11月8日 JPNIC セキュリティセミナー in 札幌
- (18) 辰巳治之. CTとATによるユビキタス健康管

理情報薬による代替医療の可能性:戦略的防衛医療構想を支えるもの. H17年11月9日 BB-Consortium Japan (東京)

なし。
3. その他
なし。

(19) 辰巳治之. ITの医療応用としての戦略的防衛医療構想ゼロクリックによる逆ナースコールと情報薬の開発.H17年11月12日 よくわかるIPv6セミナー・CSIインターネット利用研究会 広島県情報プラザ

(20) 辰巳治之. u-Japanに向けて全国へのフィールドの拡大と情報端末の多様化を行う工業系高等学校等に於けるIPv6を用いたユビキタス社会実験研究の展開. H17年11月26日 uJapan研究会

(21) 辰巳治之. ITとATを活用した情報薬の開発. H17年11月26日 日本医療情報学会 (横浜)

(22) 辰巳治之. ネットワーク社会における医療情報とは. H17年12月14日 JIMAフォーラム (東京)

(23) 辰巳治之. ITの医療応用と感性工学への期待:生活習慣病克服への挑戦. 2006年2月3日 感性工学会 (北海道大学)

(24) 辰巳治之. ICTフル利活用による戦略的防衛医療構想:情報薬の開発とリハビリへの応用.H18年3月11日山形県臨床整形外科医会春季総会

(25) 辰巳治之. 戦略的防衛医療構想の第一歩:生体情報収集による超予防医療実現を目指して. H18年3月17日NORTH Internet Symposium 2006

(26) H. Tatsumi, T. Shimmi, M. Nakamura, T. Ninomiya, R. Ichikawa, S. Kikuchi, H. Akashi, H. Tokura, E. Takaoki, T. Matsumoto. A Challenge to Three-Dimensional Reconstruction System Development. H18年3月21日 日本獣医解剖学会 シンポジウム つくば国際会議場

G: 知的財産権の出願・登録状況
(予定を含む)

1. 特許取得
なし。
2. 実用新案取得

電子カルテ交換及び A-net での検証

分担研究者： 秋山 昌範 国立国際医療センター医療情報システム開発 研究部長

研究要旨： 医療機関相互の連携を行うために必要な医療機関内部における医療情報管理の実施形態を検討し、医療情報ネットワークによる電子カルテ連携実現に必要なとされる要件を明らかにする。ネットワーク型電子カルテを使った臨床研究応用の方策は、病院間の診療連携のみならず多施設診療研究にも応用できると考えられる。情報技術の進歩は急速であるが、ハッカーやクラッカーの技術進歩も速く、両者は颯ごっこの状況であり、情報技術の進歩に伴いながら継続して個人情報保護法を踏まえた技術開発を研究する必要がある。そこで、異なったメーカー間のシステムを接続するための技術的検討を行い、どの病院においても検査システム等のデータが A-net に自動取り込みできることが望ましい。実際に、検査システム等より A-net に自動データ取り込みシステムの運用している病院では、キーボードから入力している施設よりも、利用率が高いことが分かった。したがって、検査データ等の連携を自動的に可能にするシステムの開発や普及、特に実装が重要で、それらが実現することで医療機関相互の連携を推進すると考えられた。

一方、近年インフォームドコンセントが当たり前のこととなり、診療情報の患者への開示が進んできた。その結果、診療は医師任せにするのではなく、患者も治療に参加するという姿勢に変わりつつあるようである。HIV 疾患では特にウイルス量や肝機能などの検査情報が重要とされているが、それらを患者にもデジタル情報として渡して欲しいという要求が生まれてきた。これは、従来の「お任せ医療」から「患者参加型医療」への大きな転換といえる。したがって、今後の医療機関内部における個人情報管理に関する考え方は、医療機関内部のみでなく連携医療機関、さらに患者との情報共有まで考慮した管理モデル構築が望まれる。

A：研究目的

医療機関相互の連携を行うために必要な医療機関内部における医療情報管理の実施形態を検討し、医療情報ネットワークによる電子カルテ連携実現に必要なとされる要件を明らかにする。また、IT による電子認証等を用いて、医療情報へのアクセスコントロールを実施するにあたっての課題を HIV 診療支援ネットワークシステム（通称：A-net）を中心に検討する。

B：研究方法

IT による電子認証等を用いて、今後整備される医療情報ネットワーク基盤を用いて、医療機関において必要となる課題を明らかにする。昨年は A-net を例にとり、各医療機関における運用実態を調査したが、今年度も A-net を例にとり、引き続き運用状況と個人情報保護法施行を踏まえた運用実績と問題点を調査した。

C：研究結果

1) 現状の A-net の問題点

1-1) アプリケーションサーバの問題

A-net のソフトを格納・配信するサービスの中心となるサーバであるが、老朽化により以下の問題が生じている。

①H9 年度の補正予算を基に構築されたサーバで有る為、ハードウェア自体の保守廃止時期が近い将来訪れると予想される。既に一部分であるが、保守廃止対象となった機器も存在している。

②同様に導入されているソフトウェアについてもサポート契約が廃止されており、ソフトウェアに何らかの障害が起きた際には対応することができない状況である。

③近年の技術革新によりハードウェアの性能が現時点のものと比べて劣っている。この為、ユーザからのパフォーマンスアップに対する要望が強い。

1-2) Virtual Private Network (VPN：仮想専用線網) 関連の問題

現在では、VPN の技術を用いてインターネットを介した安全な情報基盤の技術は既に確立されたが、A-net はわが国最初の導入であり、現在の標準的技術より、前のものとなっている。そこで、以下の問題点が生じている。

①H15 年度より新規参加施設募集を休止

<経緯>

①H10 年度より国立病院(現国立病院機構)以外の施設に導入を開始する。当時、全国規模としては世界初の事例であった。以後、VPN が世間に普及する事により、業界標準化統一への流れとなる。業界標準普及に伴い、H12 年度をもって現行使用している IBM トンネリング方式の VPN ソフトウェアライセンスの販売を停止している。しかし、H13 年度～H14 年度については IBM 内での例外処理により、特別にライセンス供給された。この2年間の間に、新しい仕組への移行について厚生労働省疾病対策課等で検討されたが結果的に移行はされず H15 年度より新規参加施設募集の休止となった。

②アプリケーションサーバと同様に H10 年

度より導入したハードウェアの為、保守廃止時期が近い将来訪れると予想される。

③同様に導入されているソフトウェアについてもサポート契約が廃止されており、ソフトウェアに何らかの障害が起きた際には対応することができない状況である。

④H10 年度より導入を開始したが、当時はインターネットのインフラ環境が現在のようになかった為、殆どの施設がナローバンド接続(128Kb 以下の回線接続)を行っている。このため、ユーザからのパフォーマンスアップに対する要望が強い。

【参考】VPN サーバ導入年度別施設数

H10 年度	5 5 施設
H11 年度	1 9 施設
H12 年度	6 施設
H13 年度	5 施設
H14 年度	3 施設
合計	8 8 施設

2) データのシステム間連携実装

A-net 利用促進を図るため、病院オーダリングシステムや電子カルテ等の病院情報システムに集積されている検査データの活用が有効であるが、A-net と別メーカーのシステムとを接続することは技術的に困難であることが分かった。そこで、異なったメーカー間のシステムを接続するための技術的検討を行い、どの病院においても検査システム等のデータが A-net に自動取り込みできるように開発する必要がある、国立国際医療センター以外に、国立病院機構大阪医療センター、同九州医療センターでの検査システム等のデータの A-net に自動取り込みシステムを開発している。

利用実績を見ると、データ自動取り込み施設の方が利用頻度が高いことが判明した。

3) 物理的なセキュリティに代わる認証鍵のかからない部屋でも端末の安全性を担保するためのセキュリティソフトを開発している。この運用方法についても、システム部会で検討されている。