別紙１

厚生労働科学研究費補助金

医療安全・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ＩＴ技術

に関する研究

平成１６～１８年度　総合研究報告書

主任研究者　　田中　博

平成１９年３月

別紙２

総合研究報告書目次

目　　次

別添３

平成 １８ 年度厚生科学研究費補助金（ 医療技術評価総合 研究事業）
総合研究報告書

医療の質の向上、効率化の為の先進的ＩＴ技術（ 16-医療--一般-029 ）に関する研究

主任研究者： 田中 博

研究要旨：平成１６年度は、以下の2項目について調査研究を行った。１）インターネットメールが医療情報流通の中心となっているため、このメールシステムを対象とし、この上で医療情報を安全に交換・流通させるための手法について考察した。２）IT利用によって遠隔医療を普及させるためには、セキュリティを確保した通信を安価に実現することが必要である。そこで、トランスポート層にて暗号化を行うTCP2技術に着目し、遠隔画像診断における有用性について調査・研究をおこなった。平成１７年度は、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について調査研究を行った。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について調査研究を行った。平成１８年度は、医療の質向上のためのネットワークシステムの一例として、医療ネットワーク上で集計された疾患分布状況を、鑑別診断のための有益な情報として提供することについての調査研究を行った。すなわち、現在の疾患分布状況をもとに鑑別診断を自動的に判定するアルゴリズムをし、試験実装を行った。

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
高田 英明、山肩 大祐

A. 研究目的

平成１６年度の研究目的は以下である。

次世代インターネットを医療に応用するためには、安全な通信を確保することが必須である。特に、次世代インターネットによる電子カルテ交換、およびIT利用による遠隔医療普及をめざすためには、安全な通信を安価に使いやすく提供することが必要である。現時点においても、安全な通信を確保する手段は技術的には存在している。しかしながら、これらの手段は種々の理由（高価、設定が複雑、使いにくい、性能が低い）により、現実には医療における普及率は低いままである。この状況を改善するために、新しい暗号化技術に着目し、その技術の医療への応用について検討することとした。

平成１７年度の研究目的は以下である。

1)セキュアな電子メールシステムに対する定量評価

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ということを示した。

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，ディ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った。

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）内視鏡動画像を，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）同様の動画像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。

平成１８年度の研究目的は以下である。医療の質向上のためのネットワークシステムの一例に、医療ネットワーク上で集計された疾患分布状況を、鑑別診断のための有益な情報として提供するシステムがある。つまり、伝染性疾患の状況を正確に迅速に把握することで、鑑別診断および治療に役立てようということである。本研究では、現在の疾患分布状況をもとに鑑別診断を自動的に判定するアルゴリズムを開発し、有効性を検証することを目的とする。

B:研究方法

平成１６年度の研究方法は以下である。

１）暗号化メールにおける手法の検討

次世代インターネットによる電子カルテ交換を実現させるにあたり、まず、現状の分析から行った。現時点においては、インターネットメールが医療情報流通の中心となっているため、現時点では、インターネットメールを安全に配送することが必要である。そこで、メールシステムを対象とし、この上で医療情報を安全に交換・流通させるための手法について考察した。具体的には、暗号メールシステムに着目し、既存の暗号メールにおける暗号鍵生成の問題点を整理し、さらに新しい暗号鍵生成手法を持つシステムと比較した。新しい暗号鍵生成手法を持つシステムとしては、IBE（Identity-Based Encryption）に着目し、その実装としてVoltageSecureMailの検討を行った。このシステムは、送信先メールアドレスを公開鍵とする事により、鍵の取得や管理が不要となり、ユーザ認証が完了すれば、すぐに暗号化通信が利用可能となる画期的なシステムである。

具体的な研究方法としては、病院内の一部にVoltageSecureMailのシステムを設置し、医療従事者が実際に利用した上で、利便性などについてのアンケートを実施し、そのアンケート結果について階層分析法を用いて解析した。本研究において用いた階層分析法モデルを下に示す。

２）暗号化通信を用いた動画像転送の検討

IT利用によって遠隔医療を普及させるためには、安全な医療情報ネットワークの構築が必須である。そのためには、セキュリティを確保した通信を安価に実現することが必要である。そこで、トランスポート層にて暗号化を行うTCP2技術に着目し、遠隔画像診断における有用性について調査・研究をおこなった。具体的には、TCP2技術の性能を技術的に評価するとともに実証実験を行った。　技術評価としては、以下の方法で行った。TCP２をインストールしたWindowsXPマシン（Pentium4 3.0G 1MHSA, メモリ1024Mbyte）を用い、暗号アルゴリズムはAES（128bit）を採用した。TCP2コアのプロトコルスタックソケット、TCP、UDP、IP、ARPの下にループバックの試験プログラムを実装した。またTCP2コアのプロトコルスタックの上位に試験プログラムを実装した。試験プログラムは、10220バイトのデータを送信し、ループバックにより折り返してきたデータを受信するものである。これを10000秒間繰り返し、ループバックで折り返したTCP及びUDPのペイロードデータのバイト数をカウントした。

平成１７年度の研究方法は以下である。

１）　セキュアな電子メールシステムに対する定量評価

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うだけで、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対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、一対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、一対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像(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像信号と受信した動画像信号を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像と送信先の動画像を，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。

平成１８年度の研究方法は以下である。

現在の疾患分布状況をもとに鑑別診断を自動的に判定するアルゴリズムを開発し、試験実装を行った。さらに、実際に医師に使ってもらい、評価を行った。

（倫理面への配慮）

平成１６年度においては、１）暗号化メールにおける手法の検討、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）暗号化通信を用いた動画像転送の検討、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。

平成１７年度においては、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。

平成１８年度においては、アルゴリズムの開発・実装を行うにあたり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

平成16年度の研究結果は以下である。

１）暗号化メールにおける手法の検討

病院内の一部にVoltageSecureMailのシステムを設置し、医療従事者が実際に利用した上で、利便性などについてのアンケートを実施し、そのアンケート結果について階層分析法を用いて解析した。その結果、医療関係者の利用満足度が、新しい暗号鍵生成手（VoltageSecureMail）では既存の手法に比べて高いことが判明した。しかし、各心理因子のウエイトおよび総合評価の結果からは、受信のやりやすさに難点があることも判明した。

2)暗号化通信を用いた動画像転送の検討

技術評価において、DVTSとDVTSにTCP2を実装した場合の画像の品質および、ネットワーク品質を比較した。両者ともパケットロスはなく、フレーム落ちも観察されなかった。またTCP2を実装したDVTSでの送信映像と受信映像での画像品質に差はみられず、受信映像は送信DV映像と同等であった。動きへの追従性も問題なくスムーズに表示され、パケットロスが発生することはなかった。音声も途切れる事なく、十分に伝送できた。利用帯域については約35Mbpsであり両者間の差は見られなかった。

実証実験においては、内視鏡画像を実際に転送し、臨床診断に十分な品質を持つことを確認した。

平成17年度の研究結果は以下である。

１）セキュアな電子メールシステムに対する定量評価

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。

平成18年度の研究結果は以下である。

鑑別診断アルゴリズムの試験実装は、通常のPCの上で軽快に動作し、実用上問題のない処理速度を確認することができた。また、医師による評価結果では臨床において使える可能性があるとの評価を得た。ただし、鑑別診断アルゴリズムにはまだ一部に不十分なところがあるため、アルゴリズムの改良および基礎データの収集が今後の課題である。

D:考察

平成１６年度の研究結果に対する考察は以下である。

１）暗号化メールにおける手法の検討

本研究グループの研究成果により、IBE（Identity-Based Encryption）を用いた暗号鍵生成システムが医療に対して親和性が高く、利用者がその利便性を意識していることが判明した。しかしながら、「受信のやりやすさ」などいくつかの点に関して満足度が低く、更なる改良が必要であることが判明した。

医療情報を安全に交換・配送するための技術については、現時点においても複数の手法が提案されて実装されている。しかしながら、それらのいずれもが種々の理由（高価、設定が複雑、使いにくい、性能が低い）から現実の医療においてはほとんど使用されていないのが実状である。今回の研究で用いた、IBE（Identity-Based Encryption）を用いた暗号鍵生成システムは既存の手法の問題点を解決する手法であり、今後、更なる改良を加えることにより、医療現場において暗号化メールシステムが一般的に用いられることを期待するものである。

2)暗号化通信を用いた動画像転送の検討

TCP2の性能評価実験、およびDVTSへのTCP2実装実験より、本技術は動画伝送でのセキュリティ技術として十分な要件を満たしており、インターネット上での利用が可能であると判明した。また他のセキュリティ技術とも比較した結果、セキュアなDVTSを実現するためには最適な技術であることが確認できた。

平成１７年度の研究結果に対する考察は以下である。

１）セキュアな電子メールシステムに対する定量評価

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、利用の際に若干分かりにくい箇所があったためで、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「送付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に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考える。

平成１８年度の研究結果に対する考察は以下である。鑑別アルゴリズムの一部に不十分な箇所があり、その箇所の改良が今後の課題である。また、アルゴリズムの開発および検証には、疾患に関する基礎データが必要であり、それらの収集を加速させることも今後の課題である。

E、結論

平成16年度の本分担研究における結論は以下の2項目である。

１）暗号メールシステムに着目し、既存の暗号メールにおける暗号鍵生成の問題点を整理し、さらに新しい暗号鍵生成手法を持つシステムと比較した。この新しい暗号鍵生成手法は、IBE（Identity-Based Encryption）を用いるものであり、実装としてはVoltageSecureMailを用いた。システムの比較方法としては、医療関係者にアンケートを行い、その結果について階層分析法を用いて解析した。その結果、医療関係者の利用満足度が、新しい暗号鍵生成手法(IBE)では既存の手法に比べて高いことが判明した。

２）セキュリティを確保した通信を安価に実現するために、トランスポート層にて暗号化を行うTCP2技術に着目し、遠隔画像診断における有用性について調査・研究をおこなった。具体的には、TCP2技術の性能を技術的に評価するとともに実証実験を行った。技術評価においては良好なパフォーマンスを示し、実証実験においては、内視鏡画像を実際に転送して臨床診断に十分な品質を持つことを確認した。

平成17年度の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。

平成18年度の本分担研究における結論は以下である。

医療の質向上のためのネットワークシステムの一例として、医療ネットワーク上で集計された疾患分布状況を、鑑別診断のための有益な情報として提供することについての調査研究を行った。すなわち、現在の疾患分布状況をもとに鑑別診断を自動的に判定するアルゴリズムを開発し、試験実装を行った。

アルゴリズムの試験実装は、通常のPCの上で軽快に動作し、実用上問題のない処理速度を確認することができた。また、医師による評価結果では臨床において使える可能性があるとの評価を得た。ただし、鑑別診断アルゴリズムにはまだ一部に不十分なところがあるため、アルゴリズムの改良および基礎データの収集が今後の課題である。

F、健康危険情報

なし

G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
4)Hideaki Takata, Hiroki Nogawa, Hiroshi Nagata, Yuichiro Gomi, Hiroshi Tanaka. IMPLEMENTATION OF MEDICAL DIAGNOISTIC SYSTEM BASED ON EPIDEMIOLOGICAL DATA. CJK 2006, Cheju (Korea), pp. 129-131, Nov 2006

2.学会発表

1)大橋　久美子,五味　悠一郎,田中　博; IBE(Identity-Based Encryption)によるセキュアメールの医療への応用;第８回遠隔医療研究会,2004

2)大橋　久美子,五味悠一郎,水島　洋, 田中　博; TCP2 を利用した医療セキュアネットワークの構築;第 24 回医療情報学連合大会,2004

3)五味 悠一郎,大橋 久美子,田中 博; IBE を用いた暗号メールシステムの医療機関における有効性の検証;第 24 回医療情報学連合大会,2004

4)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

5)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

6)高田英明、野川裕記、永田宏、田中博. 疾患頻度情報に基づく診断支援システム. 医療情報学, Vol. 26(Suppl.), pp.149 ,Nov 2006

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

別添３

平成 １８ 年度厚生科学研究費補助金（ 医療技術評価総合 研究事業）
総合研究報告書

医療の質の向上、効率化の為の先進的ＩＴ技術（ 16-医療--一般-029 ）に関する研究

分担研究者： 村井 純

研究要旨：
平成16年から18年度に渡り、人々の健康増進や生活習慣病予防を支援するための情報技術の応用について研究を行った。初年度は、家庭用運動器具をIPv6によってインターネットに接続し、運動処方の専門家が任意に介入できる「インターネットトレーニング環境」の構築を行った。二年度目は、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。これは「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。三年度目は、予防医学的な観点から、健康を維持するための習慣づけ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展開する。昨年度の成果をさらに発展させ、APIを提供することで、健康情報を任意の専門家と効率的に共有することを目指した。

研究協力者
南 政樹

A. 研究目的

生活習慣病をはじめとする多くの疾患の予防と治療には、健康のためによいとされている行動をとり、それを維持することが大切である。しかし、そのような行動を習慣として定着させ維持することは、全ての人にとって容易なことではなく、場合によっては何らかの助けが必要である。その助けとして、健康に関する行動変容と維持について長年の研究に基づいた健康行動理論と呼ばれる手法が用いられている。

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、そのためには運動時に顔を合わせなければならず、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た客観的なデータの計測と、それに基づいた外部からの介入を支援することで、先にあげた時間と場所に関する問題の解決を目指す。具体的には、家庭用運動機器などを含む計測機器によって客観的なデータをデジタル化すること、そしてそれらから得られた情報を長期間・安全に蓄積する情報システムの構築、そしてWebサービス型の連携が容易に行えるAPIの提供の３つを柱にした研究を進める。

B:研究方法

初年度は市販されている家庭用運動器具（自転車エルゴメーター）を対象に、これらをインターネット接続できるようにした。この際、運動情報の送受信を行うためのプロトコルおよびXMLによるデータ形式を設計・実装した。

図 1　インターネット化した家庭用健康機器

二年度目は、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。

また、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。

三年度目は、健康行動理論に則った予防や治療を実践するために、個人を単位として健康に関する行動や生体情報などを継続的に記録するとともに、適切な手続きによって本人や家族、あるいはサービス提供者と情報を共有し、健康行動への変容を支援する情報システムの構築を目指した。

これらの目的を検討し、本システムの機能要件を以下のようにまとめた。

1. 個人主体の情報システムであること
2. 管理母体が変わっても対象者に関するデータが連続して蓄積されること
3. 任意の地点から参照できること
4. 様々なセンサーノードに対応できること
5. 対象者のプライバシーを守れること

これらの要件を満たすモデルとして、個人が情報蓄積サービスを提供するパーソナルアーカイブモデルを提案した。このモデルでは、健康に関する行動や生体情報が全てパーソナルアーカイブに記録され、情報を利用する際には、適切な手続きを介してアクセスすることとなる。また、個人に関する情報と記録された情報を分離して格納し、アクセス方法も分離することで、プライバシーを守ることができる。

これらのプロトタイプに対して、神奈川県藤沢市内在住の40～60歳代の健康な男女10名に対して、機器を配布し実際に使用してもらった。

実証実験は、全ての被験者にアンケートによる意識調査を行うところから始まった。

また、同時に体力や健康度、意識の変化を数値的に比較するために、体力テストとインタビュー調査を行った。なお、実験への参加は被験者の自由意志に基づくものとし、その間、どの程度本システムが利用されたのかを、積極的に介入する場合とそうでない場合とに分けて行った。

（倫理面への配慮）

特に必要なし。

C：研究結果

初年度は家庭用運動器具を使った実験であった。事前調査の結果、被験者の属性として「運動を継続的に行うことに興味がある」人は、10名中7名であり非常に高いことが分かった。また、5名が既に何らかの取り組みを行っていることも分かった。実証実験期間中の利用者の行動については、1ヶ月間のシステムの利用回数は99回であった。そのうち、通信異常で途中終了したケースが3回観測された。これは、被験者が途中で利用を止め電源を切るなどしたことが考えられる。図２は利用頻度を縦軸に累積度数、横軸に日付を取り表したものである。

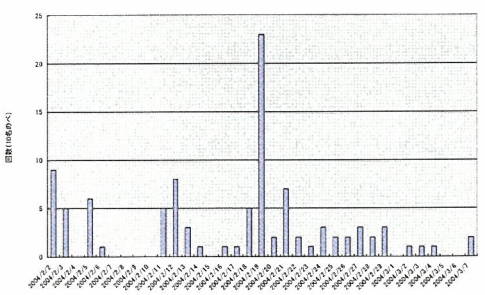


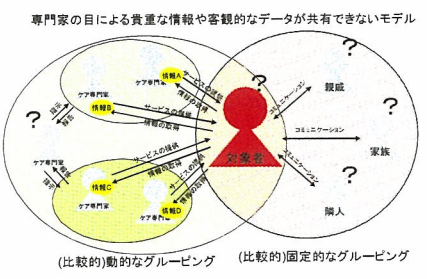
図 2　1ヶ月間の利用頻度の累積度数

継続的に利用されたことを確認するために1ヶ月を十日ごとに三等分し、それぞれの頻度の平均値を求めた。ただし、突出しているデータはトレーナーからの呼びかけにより、促されたものである。その結果、一日平均のアクセス数は、最初の十日間は３．１回、次の十日間は４．３回、最後の十日間は２．２回であった。利用時間帯で分布を見ると、当初予想した夕方～夜の時間帯のうち、18:00～19:00が２９回と多かったが、一方で、10:00～11:00と13:00～14:00の二つの時間帯がその次に多い結果となった。

続いて、事後調査の結果、本システムを主観的に「運動の支援に役立つ」と考えている人は10人中7名であった。同様に、「運動の継続に役立つ」と考えた人は10人中8名であった。その理由として、「専門家の指導による安心感」と「時間を気にせずにできる」が挙げられている。逆に否定的な考えを答えた人からは「時間がとれず十分に試す前に期間が終わった」「やる気の助けになる仕組みが欲しかった」と言った意見が挙げられた。

体力測定をした結果、事前と事後を比較してレベルの上昇が見られた被験者は10名中3名であった。これは、事前アンケートの結果からも分かるように、普段から何かしらの運動に取り組んでいる人が多かったことから、さらに厳密な測定が必要であることを示していると考えられる。

二年度目は、システム全体の見直しを行った。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。

外部の介入を前提とした場合に、現状の情報共有は図１に示すように、分散したのち本人からはたどりにくい構造であることが分かった。

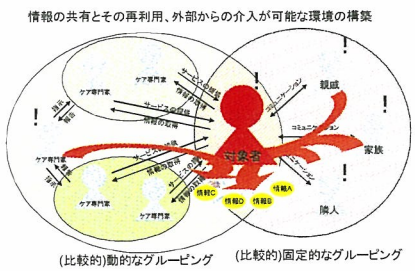


図 2　現状の情報伝播モデル

保健師、運動指導員、医師らとの議論の結果、適切な介入を行うためには、図２で示すような関係性が必要であると結論付けた。

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。

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)には開示した方が良い場合がある。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。

三年度目では、初年度・二年度目の成果を元に、プライバシーを考慮しつつ自由に専門家と情報が共有できる情報システムの構築を目指した。そのため、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）匿名性通信技術の応用　3）Webアプリケーションとしてのパーソナルアーカイブによる実現、４）　情報保持者の検索機能　の４つの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

三年間の成果から、インターネットを経由した行動変容に向けた外部からの介入の実現可能性を示すことができた。初年度に

取り組んだ運動指導では、行動変容を誘発するという点で、一定の結果を見ることができた。特に利用者の利便性と運動指導者の利便性を考えるとさらに多くの機器が接続され、多くの施設で同様の仕組みが利用されることで大きな成果が期待できる。

二年度目は、初年度の結果を受け、行動変容を支援するため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、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、このことがスムース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。

三年度目は、パーソナルアーカイブを軸とした情報蓄積システムのプロトタイプを行った。このシステムを、慶應義塾大学内で試験的に運用し、問題点を明らかにした。

成果として、健康行動理論に基づく健康によいとされる行動を定着・維持するための情報流通が可能となった。また、パーソナルアーカイブがアプリケーションとして動作することで、センサーネットワークやセンサーノードとの親和性を高めることができた。その一方で、これまでは晒されることのなかった情報がインターネット上で提供されることになり、セキュリティに関する懸念が大きくなった。秘密分散技術を用いた暗号化を提案したが、システムだけでプライバシーを維持することは限界があり、運用方法について検討しなければならないことが明らかになった。

E、結論

健康行動理論を実践する一つの方法として、外部からの介入を、インターネットを利用した支援システムを構築した。特にセキュリティやプライバシーへの配慮が必要であり、また連続的にデータが蓄積されることに大きな特徴を持つシステムとなった。

三年間にわたるプロトタイピングと実証実験の結果、良好な結果を得ることができたと共に、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。

一方で、専門家とのコミュニケーションをより多く求めることも確認された。システムに対して、より自然でかつ利用者が満足できるコミュニケーションシステムを付加し、システム作りと同時にこのシステムを利用し健康指導の方法論を固めることが非常に重要であることもわかった。今後は、インターネットを通じた健康指導・予防医学・ケアサービス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

1) インターネットトレーニングシステムの構築と評価」
橋本和樹、谷隆三郎、南政樹、村井純、電子情報通信学会
モバイルマルティメディア通信研究会
(MoMuC 2004) P43-48

2. 学会発表
特記事項なし

H. 知的財産権の出願、登録状況

1. 特許取得：特記事項なし
2. 実用新案登録：特記事項なし
3. その他：特記事項なし

別添３

平成 16-18 年度厚生科学研究費補助金（ 医療技術評価総合 研究事業）
総合研究報告書

医療の質の向上、効率化の為の先進的ＩＴ技術（ 16-医療-一般-029 ）に関する研究

分担研究者： 辰巳 治之・三谷 博明・木内 貴弘

研究要旨：
医療の質向上、効率化の為の先進的IT応用に関し、基礎のネットワーク構築実験から医療現場で実際役に立つものを想定しながら、医療に適した次世代インターネットの要件定義、医療におけるIPv6、セキュリティ技術等個別技術の評価と利用、次世代インターネットによる健康情報収集、IT利用による遠隔医療の普及および地域医療における諸問題解決への糸口、先進的ITを利用した新健康サービス産業などの創造の可能性、医療系ASP/IDC用ネットワーク要件定義、設計、セキュリティ評価などを行い、VGN、IPv6 Topological Addressing Policy、End to End Multihome, ゼロクリック、 どこでも逆ナースコールなどによる解決策を提案し、実証実験を行い、「戦略的防衛医療構想」を提案する。

研究協力者
新見隆彦、明石浩史、戸倉一、
西城一翼、山口徳蔵、石田朗
榊房子、岡部寿男、藤川賢治
太田昌孝

A.研究目的

先進的ITをフル利活用することにより、どのように医療の質、効率化を達成することができるかを、基盤情報技術から、基礎医学および臨床医学への高度応用の両方の観点から研究を進め、実証実験から先進的IT活用における問題点を解明し解決策を追及するのが目的である。

B:研究方法

今後のインターネットの医療系応用においてIPv6の活用は必須のものであると考えられていながら、その普及は覚束ない。そこでIPv6が使えるネットワークを構築しながら、医療系において必要な基本要素を洗い出し、基礎技術の応用を行う。そしてネットワークを利用した健康情報をどのように収集し、どのように活用することが良いのかを検討しながら、具体的なデータを収集し、医療の質、効率化を達成するための方策を検討する。

（倫理面への配慮）

今回の通信実験などにおいては実際に患者の情報を用いることはなく、また、個人情報に関わる場合はニックネームを使ったり、連結可能な匿名化を行うとともに、NEDOの実証実験と連携して行っている部分は、