広島県立保健福祉短期大学紀要　5(1)　57－65　2000

パーソナルコンピュータを使用した医療情報保護システム構築の為の基礎的検討

羽根田　清文[*1]　小山　矩[*1]　梅田　徳男[*2]
原内　一[*3]　稲邑　清也[*3]

*1 広島県立保健福祉短期大学放射線技術科学科
*2 北里大学医療衛生学部
*3 大阪大学医学部保健学科

抄　録

これまでは医療情報システムを構築するには，専用装置の導入などが必要であった為に，費用や管理などの面から医療情報システムの構築は容易ではなかった。しかし，近年の急激なコンピュータ技術の進歩により，パーソナルコンピュータのような比較的安価でありかつ容易に入手可能な装置にても情報システムの構築が可能となってきた。しかし，医療情報のような重要な情報を利用する為には，単純な性能だけではなく，運用に関する安全性および信頼性が重要となる。そこで，我々は，パーソナルコンピュータを用いて仮医療情報システムを構築し，その安全性および信頼性を検討した。それらの結果，適切な構築を行った場合には，パーソナルコンピュータを使用した医療情報システムでも実用性に問題なく運用を行うことが可能であることがわかった。

キーワード：パーソナルコンピュータ，安全性，実用性，信頼性，遠隔医療

1．はじめに

医療情報システムを構築・運用する際に医療情報の保護及びシステムの信頼性が重要となる[1]。規模の大きな医療施設などでは，専用装置や専用に開発されたソフトウエアを使用して，医療情報システムを構築することが可能であるが，在宅医療・遠隔医療などが中心となる小規模施設や患者宅などでの使用を考えた場合には，汎用性及び費用面などの制約から専用装置などの導入・普及は困難であると考えられる。そこで我々は，医療情報システムを構成する装置として，専用装置を使用せず，汎用性があり，しかも比較的安価であるパーソナルコンピュータに注目し，パーソナルコンピュータを使用した医療情報保管・伝送システム構築の検討を行うこととした。我々はこれまでに，医療情報保護方式の1つとして，パーソナルコンピュータを使用した暗号化による医療情報保護に関して検討を行い，パーソナルコンピュータを使用した場合でも安全かつ実用的な医療情報保護が可能であることを示した[2]。また，最近は種々の医療情報システムにおいてもクライアントとしてパーソナルコンピュータが使用されてきている[3]。しかし，システムの基幹部であるサーバなどを含めたシステム全てをパーソナルコンピュータのみで構成されたシステムは殆どない。そこで今回我々は，パーソナルコンピュータのみを使用した医療情報保管・伝送モデルシステムを構築し，モデルシステム運用に対する理論値と実測値との比較を行い，医療情報保管・伝送システムとしての運用性及び実システム運用時に必要となるシステム信頼性などに関して基礎的検討を行った。

2．実験モデル

本研究の基本となる，システム構成，利用形式及び医療情報保護の為の暗号方式などについて述べる。なお，本論文中のデータ運用時の暗号方式及び暗号・復号化のようする付加時間などに関するデータは，我々が以前に行った報告[2]に基づいた値を示す。

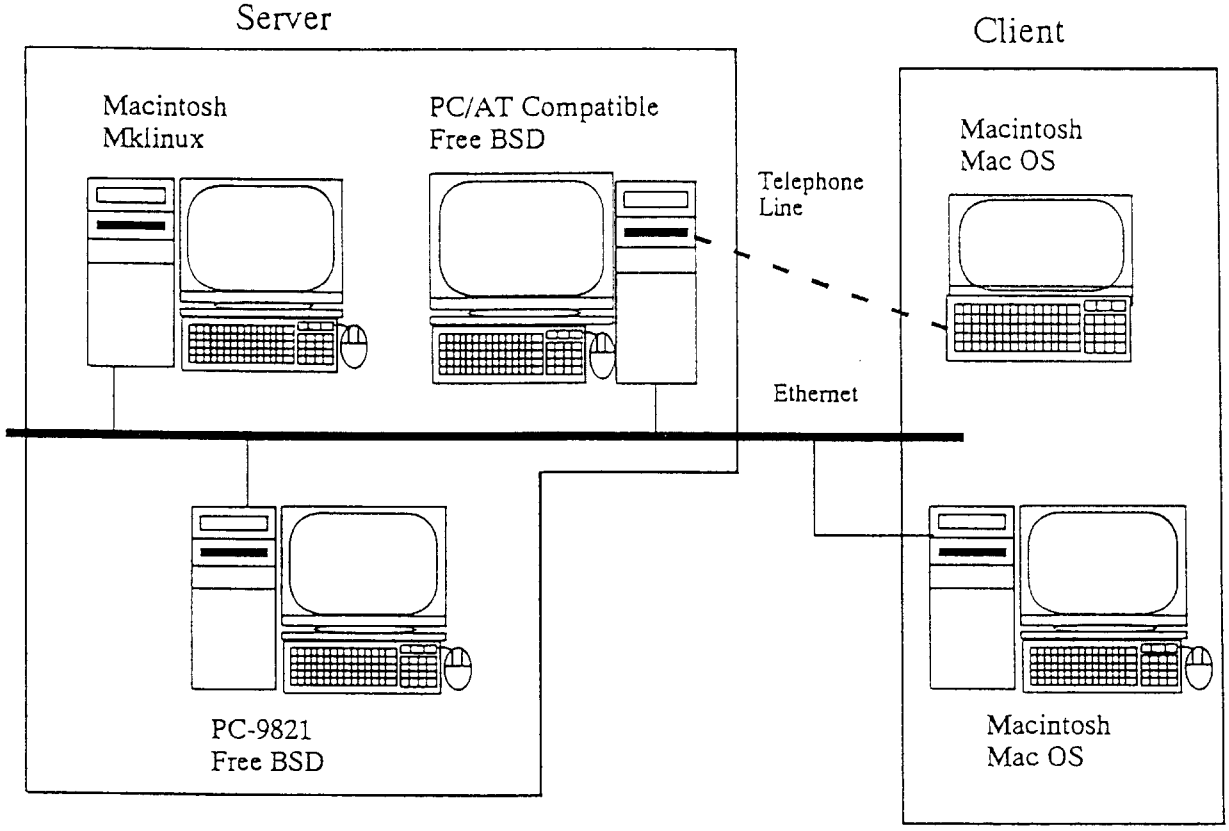

Fig.1　System configuration of Medical Information Transmission and Storage System

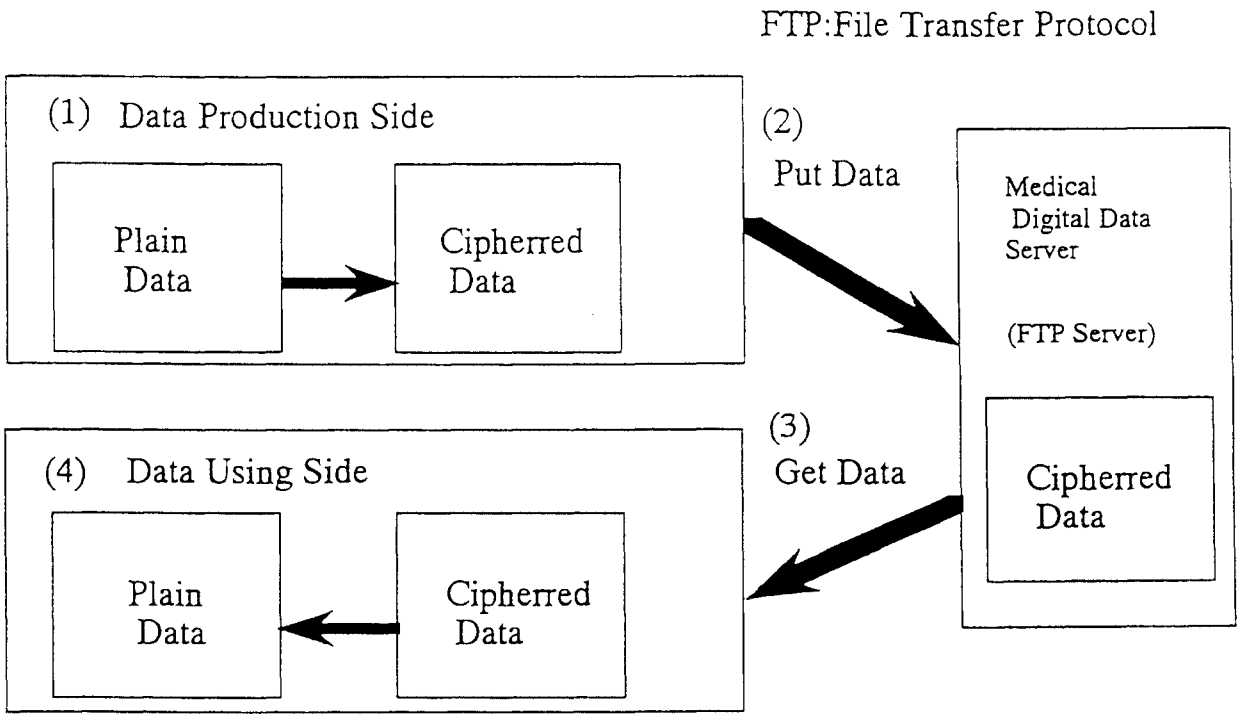

Fig.2　Flow chart of Medical Digital Data using Fig.1

2.1 モデルシステムの構成

Fig. 1に本研究にて構築したシステムを示す。Fig. 1より構築システムは，小規模施設での運用を想定したモデルシステムとし，全てをパーソナルコンピュータのみによるクライアント/サーバシステムとした。また，通信プロトコルとしてTCP/IP(ver 4)[4]を利用し，各種サーバ及びクライアントを同一施設内では，イーサネット（10baseT）にて接続し，施設外との接続は，モデム（33.6Kbit）を使用したPPP（Point to Point Protocol）[5]における一般電話回線での接続とした。各種管理を行う為のサーバOSには，UNIXを使用し，医療情報保管用サーバ(FTP:File Transfer Protocol Server)としてMacintosh (Power Macintosh8500/120,RAM:48MB) にてMklinux（ver2.1）を使用し，PC/AT互換機（pentium（133MHz），RAM:48MB）及びPC9821（pentium（166MHz），RAM:48MB）では，FreeBSD（ver2.1.5）を使用して，メールサーバ，ネームサーバ，DHCPサーバ及びPPPサーバなどシステムを運用する為の各種サーバとしてシステムを構築した。一方，医療情報を利用するクライアントには，施設内外共にMac OS（ver7.5.5)を搭載したMacintoshを使用して接続した。

2.2 システム利用形式

Fig. 2にFig. 1にて構築したモデルシステム利用形式を示す。Fig. 2に示すように利用形式は(1)医療情報作成側にて医療情報に対して暗号化を行う，(2)FTPにより暗号データを医療情報保管用サーバに転送・保管する，(3)必要時に暗号データをFTPなどを利用して取り出す，(4)医療情報利用側にて復号化を行う，との4行程に分かれる形式とした。

2.3 医療情報暗号化方式

医療情報保護に用いた暗号化方式に関して説明を行う。本研究では公開鍵暗号化方式を利用したPGP(Pretty Good Privacy)ソフトウエア[6]により，ファイルの暗号化による医療情報保護を行う。そこで，通常情報に対して，圧縮処理のみ行う場合及び圧縮＋暗号化処理を行う場合の2種類の処理を行った場合の処理時間及び処理後のファイルサイズ変化について示す。なお，処理時間の相対値及びファイルサイズの変化割合は，装置・OSに関係なくほぼ一定であった。

2.3.1 処理時間

Fig. 3に圧縮及び圧縮＋暗号化処理を行う場合のファイルサイズと処理時間との関係を示した。Fig. 3に示

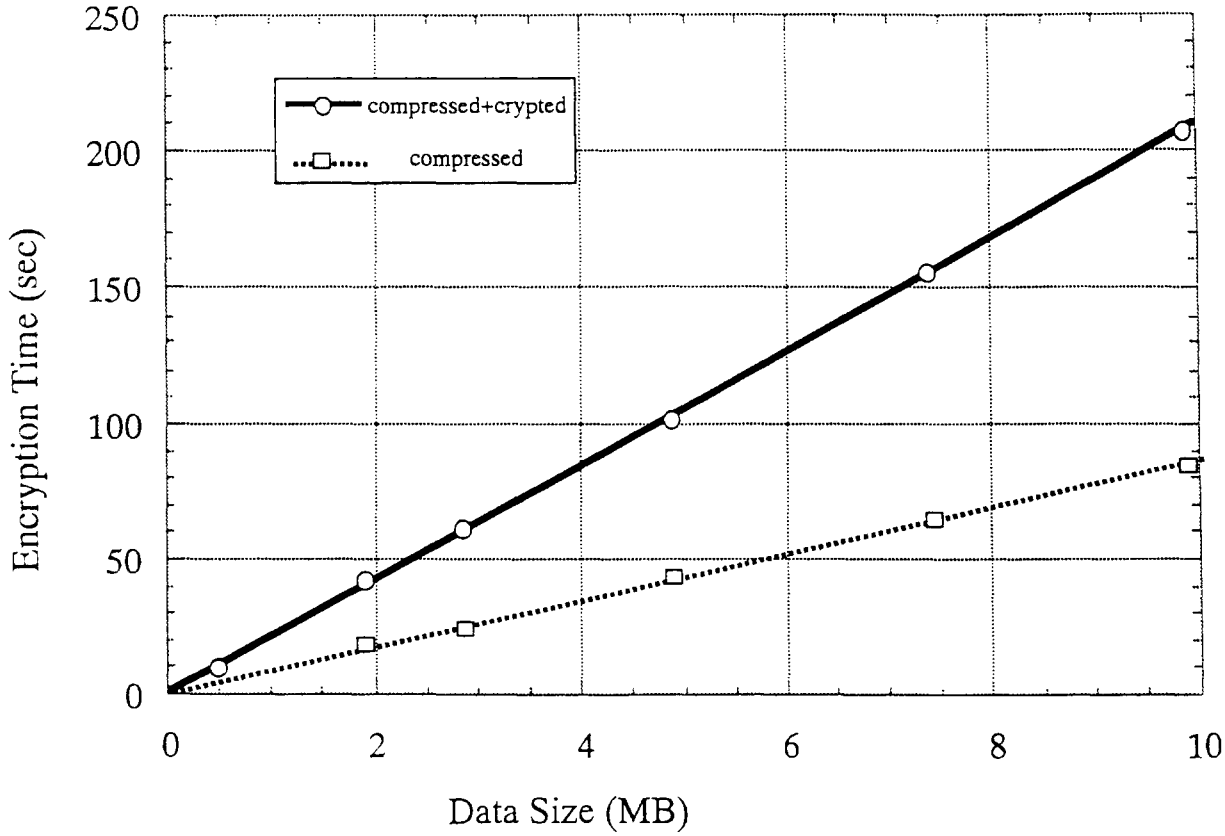

Fig.3 Comparison Data Coding Formats
：compressed data and compressed+crypted data.

すように圧縮＋暗号化処理を行う場合の処理時間を100%とした場合に，圧縮処理のみは40%の処理時間となる。ここで，利用者が操作を簡単に実施することを考え，操作が比較的容易であるMac OSを搭載したMacintosh 7500/100を使用して，通常データを各種ファイル形式に変換する場合の処理時間を求めると，ファイルサイズと処理時間との関係は，圧縮＋暗号化処理では22秒/MBとなり，圧縮処理のみは8秒/MBとなった。

2.3.2 ファイルサイズ

Fig. 4に圧縮及び圧縮＋暗号化処理を行う場合の処理前後のファイルサイズ変化割合を示した。Fig. 4より，処理前の通常データのファイルサイズを100%とした場合に，圧縮処理のみ行う場合は60%となり，圧縮＋暗号化処理を行う場合は90%となる。

2.4 伝送帯域

本研究では，伝送帯域を求める計算を容易とする為に，１ノード（２台の装置間でのみ通信）通信として計算を行った。イーサネットにてTCP/IPを使用する場合は，１ノードによる通信であっても１パケットにて伝送可能なデータ量は制限されている。その為に，データは複数のパケットに分割され伝送されることになり，伝送帯域は(1)式にて表される。

実伝送帯域＝N/（N＋38）×物理伝送帯域（bit）(1)

N: 1パケットのデータ量（byte）

但し，データ量は46～1,500（bytes）の範囲である。

一般に伝送帯域はBitで表されるのに対して，ファイルサイズはbyteにて表され，単位換算の必要がある。ここで，1 byte＝8 bitsの為，イーサネットは，10Mbits＝1.25Mbytesとなる。以下，本論文の記述では特に断りのない限り使用単位はbyteを使用することとし，単位表示でのMB or KBなどのBはbyteとする。

ここで，Ethernet及びモデムでの実伝送帯域を求めると，イーサネット10baseTの物理伝送帯域は10Mbitsであるため(1)式より，実伝送帯域は最高9.8Mbits，最低5.5Mbits（中央値7.8Mbits）となる。また，PPPの場合には上記の制限よりも効率よく転送可能であるが，本構築システムでは施設外からの利用の場合でもPPPサーバから医療情報保管用サーバまでイーサネットを利用する為，モデム使用時の伝送帯域においても伝送効率の低いイーサネットの制限を受けると考え，モデムの物理伝送帯域は33.6Kbitsである為に，実伝送帯域

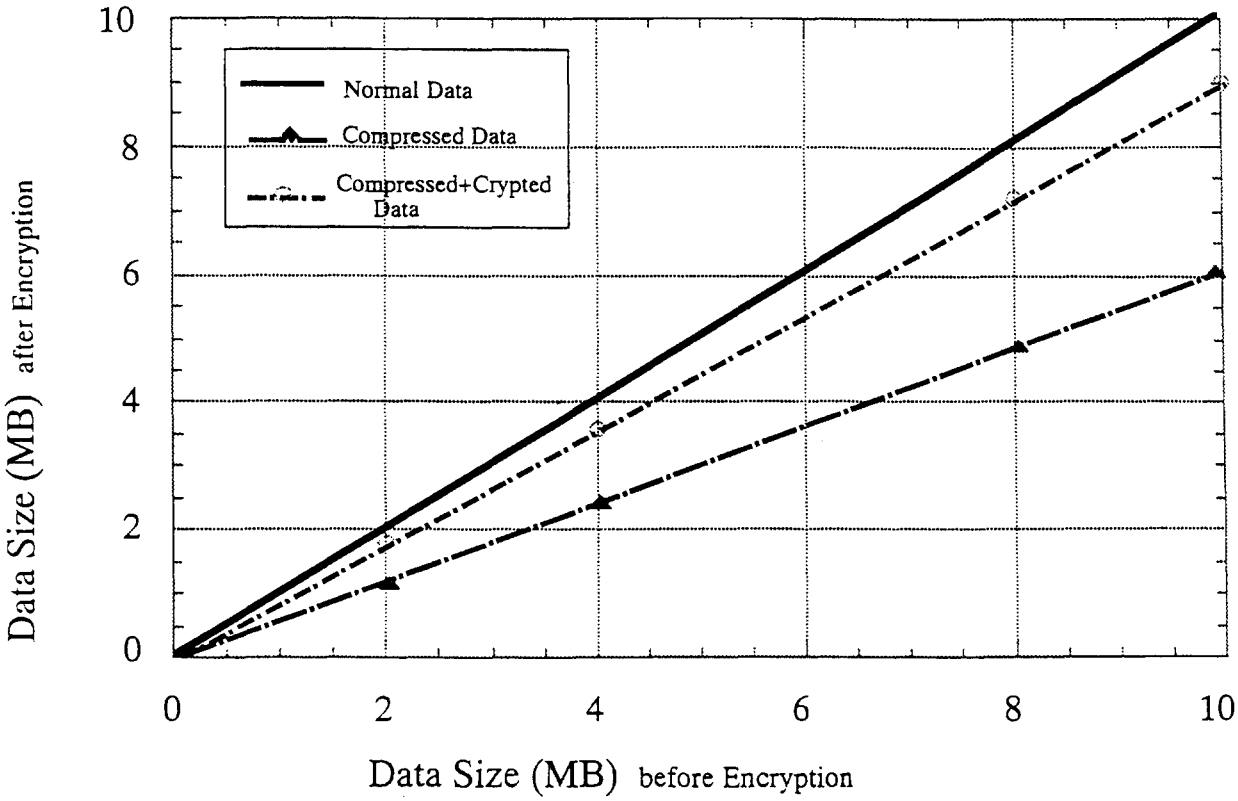

Fig.4 Relation of Data Size after Encryption versus Data Size before Encryption in different the data coding formats : normal data, compressed data, and compressed+crypted data.

は最高32.8Kbits，最低18.4Kbits（中央値25.6Kbits）とする。なお本論文では，通信線のみの伝送容量を伝送帯域とし，装置の動作に伴うオーバーヘッドなどを含めたファイル伝送割合を伝送速度として区別する。

3．実　験

構築したモデルシステムにおける医療情報伝送時間及びシステム運用時の信頼性について施設内外より運用を行うことにより実測値を求める。

3.1 医療情報伝送時間に対する検討

医療情報を施設内からはイーサネット，施設外からは一般電話回線を利用して伝送する場合の各ファイルサイズに対する伝送速度を求めた。測定環境は，医療情報保管用サーバ１台に対してクライアントを１台～６台まで変化させた伝送試験とした。Fig. ５はサーバ，クライアントとも各１台（１ノード）の施設内及び施設外からFTPコマンドを使用してファイルを取得する場合のファイルサイズと所用時間との関係を示す。Fig. ５に示すように施設内及び施設外ともにファイルサイズと伝送時間とはほぼ比例関係となり，それぞれの伝送速度を求めると施設内は870KB/秒であり，施設外は3.1KB/秒であった。但し，施設内伝送の場合には伝送速度が早く装置のオーバヘッド（約８秒）による影響が生じた為にその値を差し引いた。

Table １は施設内にてのクライアントの台数を１台～６台（１ノード～６ノード）まで変化させた時の平均伝送速度であるが，１ノード～６ノードの値はそれぞれ853.3KB/秒，520KB/秒，323.3KB/秒，246.7KB/秒，146.7KB/秒，80KB/秒となった。

3.2 医療情報保管・伝送システム運用時に必要な基本的信頼性の検討

医療情報システムでは，システム障害が生死に関わる可能性が生ずる。その為に運用の信頼性が重要とな

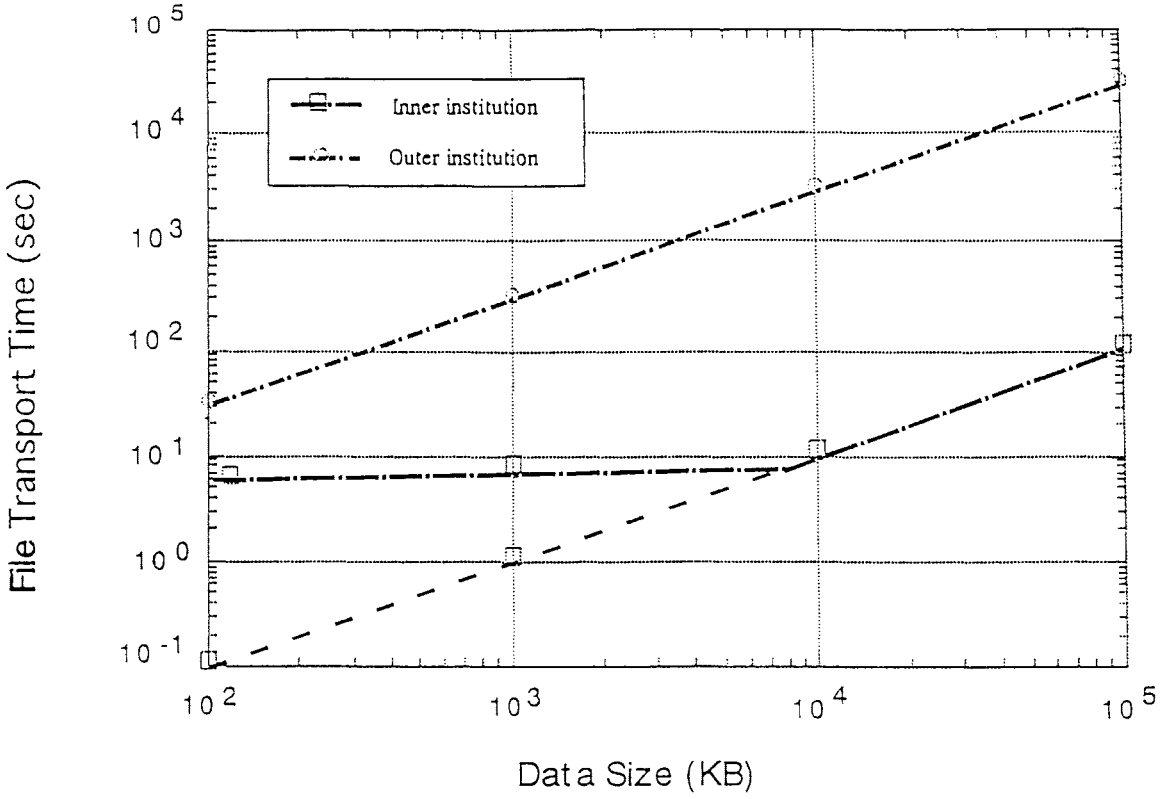

Fig.5 Comparison of File Transport Time
Route or Channel
: inner institution and outer institution

Table 1　System Operation Time in Medical Information

(overhead time 8sec)

		Encryption Time (sec)	Post Data Size (MB)	File Transfer Time (sec)		Total time (sec)	
				MODEM	Ethernet	MODEM	Ethernet
Patient information (0.5MB)	compressed +crypted	11	0.45	145	8.0 (0.52)	156	19.0 (11.52)
Chest X-ray	compressed +crypted	176	7.2	2,323	8.28	2,499	184
(8MB)	compressed	64	4.8	1,548	8.0 (5.52)	1,612	72.0 (69.5)
CT or MRI Image	compressed +crypted	11	0.45	145	8.0 (0.52)	156	19.0 (11.52)
(0.5MB)	compressed	4	0.3	97	8.0 (0.34)	101	12.0 (4.34)

る。また，運用上の問題として，システム利用は診療時間内だけではなく，診療時間外にもあり，利用時間帯も不定期である為にシステムとしては常時稼働する必要がある。また，医療情報は電子カルテなどの文書情報だけではなく，医用画像などファイルサイズが大きい情報もあり，システムとしては大きなファイルの保管・伝送が安定して行える必要がある。以上の内容を考慮して，下記の条件により医療情報保管・伝送システムを構成するサーバとしてパーソナルコンピュータを使用した場合の基礎的信頼性の検討を行う。

3.2.1 連続運転試験

システムの連続運転に関しては，システムを四半期に一度点検を行うと仮定し，その間常時システムを稼働させることとし，１月～３月及び５月～７月の２期間についてサーバを常時稼働させ連続運転に対する信頼性に関して，定期的なファイル伝送による動作確認及びシステム動作記録の確認により調査した結果，２期間ともに動作異常は認められず正常に連続運転を行えた。

3.2.2 ファイル伝送

ファイル伝送に関しては，3.2.1にて約0.5MBのファイル転送を行ったが異常は認められなかった為に，医用画像伝送時などの比較的大きなファイル伝送に関して検討を行うこととした。施設内での伝送は，１検査での最大転送ファイルサイズを400MBと仮定し，それに安全性を加味して1.5倍とし，伝送容量600MBの伝送（出し入れ）を各20回/日を20日（計800回）行い，3.2.1と同様に装置動作及びシステム動作記録の確認を行った結果，800回全て動作異常なしに伝送を行えた。一方，施設外への伝送は，伝送速度が遅いことなどから夜間の伝送であると考え，その伝送時間を８時間と仮定し，それに安全性を加味して1.5倍とし，伝送時間約12時間（約117MBのファイル取得）の転送を20回行い，装置動作及びシステムログの確認を行った結果，データ伝送試験20回中５回伝送に失敗し，成功率75%となった。但しこれは，サーバ側の動作異常ではなく，クライアント側のコンピュータが停止した為の転送失敗であり，サーバ側の動作異常による転送失敗は１度も認められなかった。また，施設外への伝送試験においてクライアントとしてもUNIXを使用してファイル伝送を５回行ったが，全て問題なく伝送が行えた。

4．検　討

4.1 データ送信速度における理論時間と実測時間との比較

装置の性能以外の要因を排除する為に，１ノードの場合に関して考えると3.1より施設内外ともに転送速度は2.4にて求めた実伝送帯域の範囲内におさまった。但し，施設内の伝送速度は実伝送帯域の中央値と比較して10%程度早くなったのに対し，施設外の伝送速度は実伝送帯域の中央値と比較して３%程度遅くなった。これは本研究では施設内の測定時に装置間に他装置を介在せず直接接続されており，なおかつ比較的大きなファイルを使用した為に１パケットの転送効率が高い状態にて測定を行えた結果このようになったと考えられる。一方，施設外への伝送の場合には，モデム独自の誤信号確認機能及び，PPPサーバを経由してファイルの転送を行っている為にPPPサーバを情報が経由する分，伝送速度が遅くなったと考えられる。伝送帯域は，１ノード間の通信であっても計算上ですでに伝送帯域は1.8倍もの差がある為に転送速度が実伝送帯域内に収まっていたとしても，本システムにて求めた実測値がどの程度の速度なのかを考える。ここで，笹生らの報告[7]によると医療情報に関する規格であるDICOMにおけるイーサネットでの最大伝送帯域は813～950KBであり，本研究にて得られた値とも近い値であることから，パーソナルコンピュータのみのシステム構成でも伝送速度は通常の医療情報システムと同程度の性能を得られると考えられる。

また，サーバに対してのクライアントの接続台数を１～６台と変化させた時の伝送容量を求めると１～５台までは伝送容量は730～1040KBに収まっているが，クライアントの台数を６台とすると480KBとなり著しく伝送容量を小さくなった。これは，トラフィックの増大によるコリュージョンによる為と考えられる。この結果より大容量データなどを常時利用する場合には，クライアントの台数が６台以上では，伝送システムの容量によっては極端に効率が悪くなるので注意する必要があると考えられる。

4.2 伝送容量及び時間

Table １に１ノードでの各種処理時間及び伝送速度をもとにした場合の代表的な医療情報ファイルの処理時間及び暗号化データの伝送時間を示した。Table １より，まず各ファイルの処理時間は圧縮＋暗号処理を行う場合，患者情報及びCT，MRIなどの場合には11秒，胸部X-rayの場合には176秒が必要となり，処理後にファイル伝送を行う場合，施設内の伝送時間はそれぞれ8.0秒及び8.28秒となる。この為，ファイル処理時間と伝送時間との合計時間は，患者情報及びCT，MRIなどの場合には19秒，胸部X-rayの場合には184秒が必要となる。一方，施設外への伝送の場合のファイル処理時間と伝送時間との合計時間は患者情報及びCT，MRIなどの場合には156秒，胸部X-rayの場合には2，499秒が必要となる。このように施設内の伝送は，１画像として最

大ファイルサイズである胸部X-ray（8MB）画像を暗号処理後伝送する場合でも184秒にて処理・転送可能であり，小規模施設内などでの運用においては所用時間はそれほど問題がないと考えられる。一方，施設外への伝送には，患者情報（CT,MRI画像も同じ）及び胸部X-ray写真を暗号処理後転送するのにそれぞれ2.5分及び42分必要となり，施設外へ医療情報の伝送は所要時間の面から実運用時には，利用可能なファイル容量が限定される。ここで，情報を保護する為に患者情報に対しては暗号化を行う必要があるが，医用画像は必ずしも暗号処理を行う必要はない。そこで，医用画像の圧縮処理のみを行う場合の合計時間はCT,MRIの場合には101秒，胸部X-rayの場合には1,612秒となり，暗号化を行う場合の約64%に所用時間が短縮される。このように，伝送速度が遅い回線を利用する場合などには，保護必要情報（暗号化必要）と不必要情報（暗号化不要）とを分割などして，効率的な運用を行う必要がある。

4.3 システム信頼性

パーソナルコンピュータのみを使用して医療情報保管・伝送システムを構築・運用した場合，3.2にて示したようにサーバとして運用したとしても連続運転・ファイル伝送ともにシステム信頼性が問題となるような実証的データは得られなかった。一方，クライアントとして運用する場合，短時間でのファイル伝送時にはファイルサイズが大きくとも異常は発生しなかったが，施設外からなどの長時間のファイル伝送における信頼性の問題について検証を加えた結果，一般的なOSを使用して長時間のファイル伝送を行うと信頼性が低くなるとのデータが得られた。また，本研究では，パーソナルコンピュータにて医療情報システムを構築する為に装置本体に通信用基盤の増設や，サーバとしての運用の為にOSとしてUNIXを搭載させるなどしてシステム構築を行ったが，PC/AT互換機などの場合には，同一メーカー，同一名称の装置であっても（規格に準じていても）ハードウエア間やOSとの相性の問題が生ずる場合があり，現状では全ての組み合わせにおいて信頼性のある運用が行えるとはいいがたい。しかし，本研究にて示したように，システムが一旦安定稼働すればパーソナルコンピュータのみを用いたシステム構成でも，信頼性のある運用が可能である。

5．結　論

現在一般に使用されているパーソナルコンピュータのみを使用して医療情報保管・伝送システムを構築し，システム運用での運用性・信頼性に対する基礎的検討を行ったが，システム全てにたいしてパーソナルコンピュータを使用した場合でも信頼性があり，かつ実用的な運用が行えるシステム構築が可能であることを示した。

今後の課題として，今回の構築システムは装置間における運用性及び信頼性の基礎的検討を行う為に構築したモデルシステムであり，ファイル伝送をFTPでの伝送としている。その為に，本システムの操作を行う為にはFTPコマンドなどの知識が必要であり操作性がよくない。そこで，今後は実使用を考えWWWサーバとデータベースサーバを連携させることなどにより，利用性を考慮したシステム構成とし，また，セキュリティ対策としてもファイルの暗号化のみによる情報保護のみではなく，ファイル及び構築システムへのアクセス制限などシステム全体としての安全性についても検討するつもりである。

文　献

1）厚生省健康政策局総務課医療技術開発室監修．医用画像情報の電子保存のあらまし．東京，医療情報システム開発センター，1994
2）羽根田清文，梅田徳男ほか．公開鍵暗号法を利用したデジタル医療情報の暗号化による付加時間の評価．Medical Imaging Technology, 447-448, 1997
3）Lemke, H. U., Vannier, M. W. et al. Computer assisted radiology and surgery. (CAR'97) 1997
4）Comer, D. TCP/IPによるネットワーク構築 (Vol.1)．東京，共立出版，1996
5）Lynch, D. C, Rose, M. T. インターネットシステムハンドブック．東京，インプレス, 617-618, 1996
6）Zimmermann, P. Z. PGP User's guide copyright 1990-1994. ©1994
7）笹生篤二，夏住茂夫ほか．LANによる双方向通信の検討．日本放射線技術学会雑誌，53：176，1997

広島県立保健福祉短期大学紀要　5(1)　57－65　2000

Evaluation of prototype medical digital data archive and transition system using personal computer

Kiyofumi HANEDA*1, Tadashi KOYAMA*1, Tokuo UMEDA*2,
Hajime HARAUCHI*3, Kiyonari INAMURA*3

*1 Department of Radiological Sciences and Technology, Hiroshima Prefectural College of Health and Welfare
*2 School of Allied Health Sciences, Kitasato University
*3 School of Allied Health Sciences, Faculty of Medicine, Osaka University

Abstract

Medical information security and reliability are strongly required. Large medical institution could construct an exclusive medical information system, but at small medical institution and patient's home (most of telemedical users) it was difficult to construct such an exclusive system. Therefore, we tried to develop medical information protection system with personal computer. The practicability and the system performance of the system were examined. The system was operated for 80 days running, no error occurred in operation. Data transfer test was done 800 times by the inner communication using 600 MB data, that proved successful. In the system performance, encryption speed was 22 s/MB, or transfer speed of the inner communication was 870 KB/s, and that of the outer communication was 3.1 KB/s (except overhead time). For example, total time (encryption + transfer) of CT image(512 KB) of the inner communication was 19 s, and that of the outer communication was 156 s. In concluding, we should note that it is possible to utilize personal computer for medical information system.

Key words : personal computer, security, reliability, practicability, telemedicine