広島県立保健福祉短期大学紀要　5(1)　117－123　2000

パーソナルコンピュータを使用した暗号化方式による医療情報保護の基礎的検討

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

医療情報を保護する為に専用装置を用いずにパーソナルコンピュータを使用して医療情報を暗号化する方式に注目し，現在国内で比較的入手及び使用可能な装置を対象として，公開鍵暗号法を用いて医療情報を暗号化した場合の暗号処理時間及び安全性に対する有用性の検討を行う為に，暗号鍵やシステム構成などをパラメータとして検討した。それらの結果，暗号化/復号化に伴うファイル容量にたいする付加時間は22s/MB及び15s/MBであり，比較的ファイル容量の多い医療情報を暗号化する場合でも，実使用に耐えうる範囲であった。また，データ圧縮を行うことにより，暗号データのファイル容量は元データとほぼ同容量となり，保管容量・伝送時間に変化はないこと。さらに暗号化した情報は充分保護されていたことを示した。これらの結果からパーソナルコンピュータを使用して医療情報の保護を行うことは可能であることがわかった。

キーワード：公開鍵暗号法，医療情報，パーソナルコンピュータ，安全性，複数環境動作システム

1．はじめに

医療情報をデジタル情報として保管・伝送する場合に，情報の漏洩・改ざんなどから保護する必要性が指摘されている[1]。保護する方法としては，医療情報を暗号化する方法やアクセス制御をかける方法，物理的制限をかける方法などがあり，それらに対して種々のプロジェクトなどを通して様々な研究が行われている[2-3]。しかし，それらの研究には専用装置が必要であるなどの理由から，大規模施設や特定プロジェクトなどでの限られた範囲でのみ運用が可能であり，小規模施設や広範囲な在宅医療での使用を考えた場合には，汎用性や費用面などの制約により運用は困難である。そこで，本研究では，汎用性が有りしかも比較的安価なパーソナルコンピュータ（以後パソコンと称す）を使用することにより医療情報の暗号化を行うことに着目し，パソコンを使用した場合の医療情報暗号化に対する基礎的検討を行った。

2．研究対象

2.1　使用装置

研究対象とした装置及びOperation System（以後OSと称す）をTable 1に示すが，対象装置としては日本国内にて比較的容易に入手可能であり，かつ使用頻度が高い装置を対象とし，各装置に通常使用を対象としたOSとして，Macintoshシリーズ(各装置：RAM 48 MB搭載)ではMac OS，PC-98シリーズ(CPU：pentium（166 MHz），RAM 48 MB搭載）及びPC/AT互換機(CPU:pentium (133 MHz)，RAM 48 MB搭載）ではWindows 95を搭載し，システム管理などに比較的適したOSとして，Unixを使用し，Macintoshシリーズでは Mklinux，PC-98シリーズ及びPC/AT互換機ではFreeBSDを搭載し，各装置に対して計2種類のOSを搭載して研究を行った。

2.2　使用暗号

現在一般的な暗号方式としては，公開鍵暗号方式，対称鍵暗号方式及びワンタイムパッド暗号方式などがあり，各暗号法の特徴をTable 2に示す[4]。ここで，医療情報の利用形態は多数の人間による利用が行われることが多い為に，暗号鍵の運用・管理を考慮すると公開鍵暗号方式が最も適していると考えられる。そこで，本研究では暗号方式として，公開鍵暗号方式を使用した場合における基礎的検討を行うこととした。

2.3　使用ソフトウエア選定

現在インターネットなどで広く普及している公開鍵暗号方式のソフトウエアは，インターネット標準化技術であるPEM（Privacy Enhanced Mail）[5-7]の規定に対応したソフトウエア及び独自規格のソフトウエアであるが世界中で普及しているPGP（Pretty Good Privacy）[8]の2種類のソフトウエアが有名である。そこで，PEM系ソフトウエアとしてPemCATを使用し，PGPソフトウエアとしてPGP 2.6.3 iを使用して比較した結果をTable 3に示すが，PGP 2.6.3 iをPemCATと比較した場合に，暗号鍵が長い，暗号処理時間が短いとの特徴がある。ここで，医療情報は，文字データのみではなく画像データなど数10 MBものデータを扱う可能性がある為に暗号処理の高速化の観点から，暗号化ソフトウエアとして，処理時間の短いPGPを使用して検討を行った。

2.4　暗号処理過程

暗号処理過程をFig .1に示すが，本研究での処理過程としては，次に記すように大きく3段階に分けることが出来る。・暗号化を行う為の暗号鍵の作成（但し，この暗号鍵は暗号処理の度に作成する必要はなく，1度暗号鍵を作成すれば以後の暗号処理では同じ暗号鍵を繰り返し使用可能である)。・通常データに対し可逆的圧縮処理を行い圧縮データに変換する。・圧縮データに対し暗号化を行い暗号データに変換する。また，以後使用する用語として，通常データから暗号データに変換するまでに要した時間を暗号化時間，及び暗号データを通常データに変換するまでに要した時間を復号化時間とする。

Table 1　Structure of Machine and Operation System

Machines	Operating System	
	Proper OS	Unix
Macintosh Series (APPLE)	Mac OS	Mklinux
PC - 98 Series (NEC)	Windows95	Free BSD
PC / AT Compatible	Windows95	Free BSD

Table 2　Comparison Cryptosystem Attributes

Cryptosystem	Attribute Description	Number of Secret Keys (in case of 500 users)
Public Key Encryption	Easy to genetate and distribute key Low Speed Encryption	500
Symmetric Key Encryption	High Speed Encryption Difficult to control Crypt-Key Need to transit Secret Key	124,750
One Time Pad	Impossible of code breaking Need to transit Secret Key Must create crypt key everytime	124,750/time

Table 3　Comparison between Pretty Good Privacy and Praivacy Enhanced Mail

tested software : PGP (PGP2.6.3i), PEM(PemCAT)

	Software Type & Product	Crypt Speed (sec) CT Image Data Size (512KB)	Key Length (bit)
Pretty Good Privacy	Individual Software PGP2.6.3i etc	12	2,048
Privacy Enhanced Mail	Internet Standard PemCAT FJPEM etc	256	512

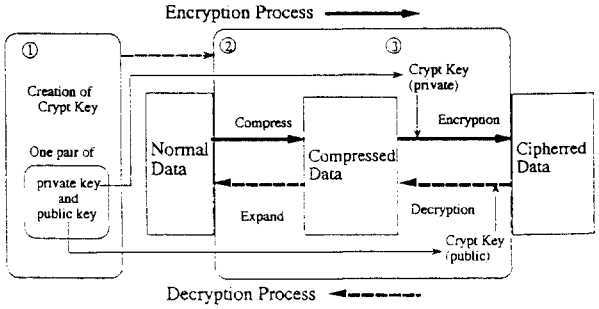

Fig.1　Flow chart of Encryption and Decryption with Pretty Good Privacy

3．結果

3.1　暗号鍵に関して

暗号鍵についてMac OS（ver 7.5.5）を搭載したMacintosh 7500/100を使用して，鍵長512 bit，1,024 bit，2,048 bitの3種類の暗号鍵を作成する際の鍵作成時間及び暗号鍵解読困難度に関して比較した結果をTable 4に示した。Table 4より鍵作成時間は，鍵長512 bitの時は8秒，1,024 bitの時は76秒，2,048 bitの時は1,032秒となり，鍵長2,048 bitの鍵作成時間は512 bitと比較して，129倍必要となった。このように鍵長が増すとともに鍵作成時間は，指数関数的に増加した。また，暗号鍵を解読する場合の困難度であるが，現在可能な暗号鍵解読方法は素因数分解を繰り返し行う方式である[9]。その為に素因数分解の繰り返し回数が暗号鍵解読の困難度となる。よって，各鍵長に対する素因数分解の繰り返し回数を一般数体ふるい法により求める為の数式として(1)式を使用して求めた値[10]をTable 4に示すが，鍵長512 bitでは1.61×10^{19}回，1,024 bitでは1.18×10^{26}回，2,048 bitでは1.32×10^{35}回必要となった。

$$A(n) = \exp(1.92(\ln(n)^{1/3}\ln(\ln(n)^{2/3})) \quad (1)式$$

n: 鍵長（bit）

Table 4　Comparison of Crypt Key with creating key times and Instruction Speed

Key Length (bit)	Creating Key Time (sec)	Instruction Speed of factorization into prime factors (times)
512	8	1.61×10^{19}
1,024	76	1.18×10^{26}
2,048	1,032	1.32×10^{35}

3.2　暗号処理時間

暗号鍵作成と同様の装置構成にて，通常データの暗号処理を行った場合に必要な時間をFig .2に示した。Fig .2（a）は，鍵長として1,024 bitの暗号化時間及び2,048 bitの暗号化時間を示したが，鍵長の違いによる処理時間の違いは殆ど認められなかった。Fig .2(b)は，鍵長2,048 bitを使用してデータを暗号化及び復号化した場合の各ファイル容量に対するそれぞれの所用時間を示したが，暗号化を行う場合のファイル容量と暗号化時間は22 s / MBの関係となり，復号化を行う場合は15 s / MB（但し，オーバーヘッドタイム30 s有り）となった。Fig .2（c）は，ファイルの変換に伴う処理時間の比較として，圧縮のみ行う，圧縮＋暗号化を行う，暗号化のみ行う場合の各処理時間を示した。Fig .2（c）より圧縮処理＋暗号化を行う場合の処理時間を100 %とした場合に，圧縮のみ行う場合の処理時間は40 %であり，暗号化のみ行う場合は70 %となった。

3.3　データサイズの変化

Fig .3は，通常データに対して，圧縮のみ行う，圧縮＋暗号化を行う，暗号化のみ行う場合のファイル容量の増減を示した。Fig .3より，通常データのデータサイズを100 %とした場合に圧縮のみは60 %，圧縮＋暗号化は90 %，暗号化のみは150 %となった。

3.4　装置・OS別処理時間変化

Fig .4は，装置の性能と処理時間との関係を比較する為にMac OS（ver 7.5.5）にて各Macintosh装置で暗号化した場合のファイル容量と暗号化時間の関係を示した。これより装置の性能と暗号化時間は装置の性能に依存することが解る。また，Table 5は，使用OSと処理時間との関係を比較する為に同一装置にて使用OSを変えた場合の暗号化時間の違いを示した。これより，同一装置であっても使用OSの違いにより暗号化時間の違いが認められ，特にMacintoshの場合にはMac OSとMklinuxとを比較した場合にMklinuxの処理時間は約半分に短縮した。

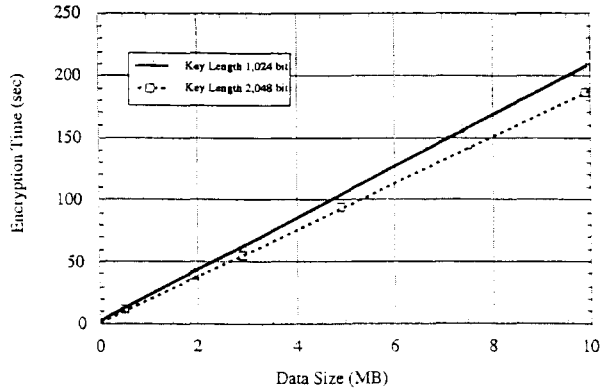

Fig.2(a)

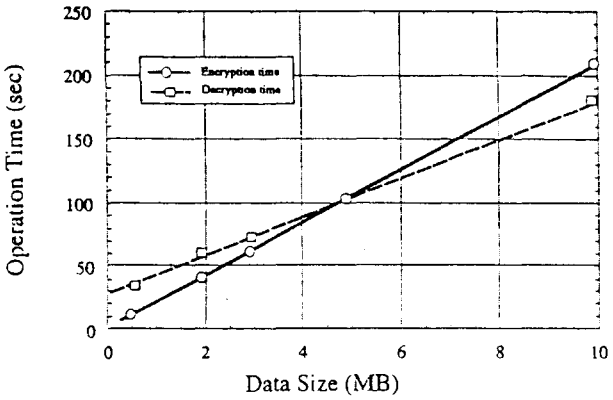

Fig.2(b)

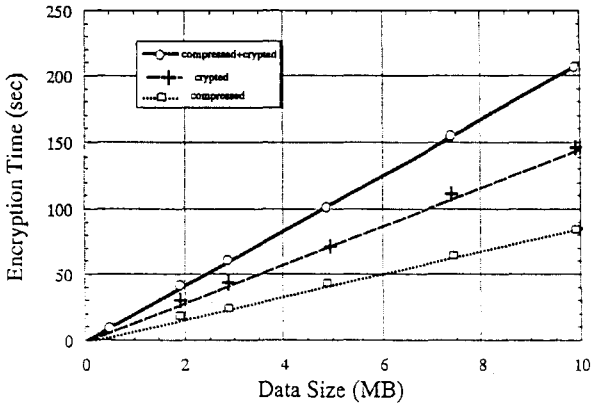

Fig.2(c)

Fig.2 Relation of Data Size and Operation Time for changing some parameter by Macintosh 7500/100 & Mac OS(ver 7.5.5), (a) is result of the comparison for Key Length 1,024 bit and 2,048 bit, (b) is result of the comparison for Encryption and decryption, (c) is result of the comparison for Three data coding formats (a) compress data, (b) compress crypt data, and (c) crypt data.

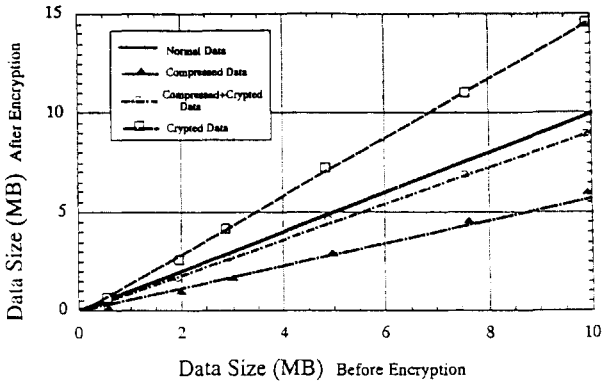

Fig.3 Relation of Data Size and data coding formats, (a) normal data, (b) compress data, (c) compress crypt data, (d) crypt data.

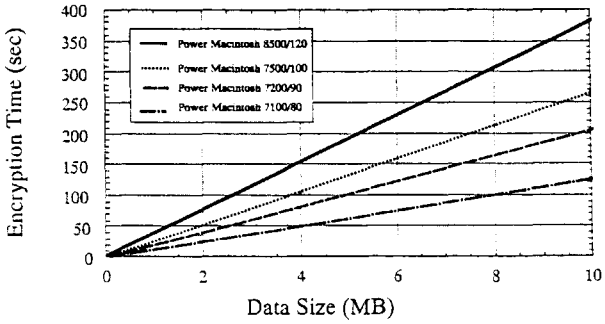

Fig.4 Relation of Data Size and Operation Time for each machines on Mac OS.

Table 5 Comparison of encryption time between Operation System by Same Machine

Machine	Operating System	Encryption Time (sec)
Macintosh Series (APPLE)	Mac OS	126.2
	Mklinux	59.3
PC - 98 Series (NEC)	Windows95	79.8
	Free BSD	69.7
PC / AT Compatible	Windows95	74.9
	Free BSD	72.9

4．考察

4.1　使用暗号の安全性

Table 4で求めた暗号鍵解読に必要な演算回数と暗号鍵解読時間との関係をFig .5に示した。Fig .5は，横軸をコンピュータが1年間に行える演算回数（MIPS）とし，縦軸を演算終了に必要な年数とし，Table 4で求めた各鍵長における必要演算回数を当てはめたものである。ここで，医療情報を保護すべき年数を人間の寿命の10倍と想定し，約1,000年とした場合に暗号解読に必要な処理能力は，鍵長1,024 bit の場合では3.8×10^{9} MIPS（鍵長2,048 bit の場合には4.2×10^{18} MIPS）必要となる。これは100 MIPS 相当のコンピュータを同時に3.8×10^{7}台使用して暗号鍵解読を行う場合に演算に必要な年数が1,000年であることを示している。また，鍵長512 bit の繰り返し回数は1.61×10^{19}回であり，MIPS年に換算すると5.1×10^{5} MIPS年となる。これは100 MIPS相当のコンピュータが5,100台有れば1年で暗号鍵の解読が可能であり，現在のコンピュータ技術にて不可能ではない。その為，鍵長512 bit を使用している PemCAT での暗号化は医療情報の保護に適しているとはいいがたい。

4.2　使用暗号鍵長

暗号鍵の特徴として，①鍵長が長いほど暗号解読が困難である，②暗号鍵作成時間は鍵長に比例して指数的に増加する，③暗号処理時間はほとんど鍵長に影響されない，のような特徴がある。また，暗号鍵は，一度作成すればよく，実際の暗号処理過程において鍵長は暗号化時間に対してほとんど影響しない。以上の理由から暗号の安全性を考慮して可能な限り長い暗号鍵を使用することが望ましいことが解る。

4.3　ファイル暗号形式

今回は，全医療情報に対して暗号化を行うことを想定して研究を行ったが，実際の運用では全医療情報を暗号化する必要はなく，患者情報など一部を暗号化すれば良い可能性もある。そこで，3.2及び3.3で得られた結果をもとに医療情報として，患者情報0.5 MB＋医用画像3 MB（CT 画像 6 枚相当）を使用する場合に，暗号処理を行うデータを分割した場合のファイル容量変化及び暗号化時間を Table 6に示した。このように保護必要情報（暗号化必要）と不必要情報（暗号化不要）とを分割することにより，ファイル容量及び処理時間が減少し効率的な運用が可能である。また，処理時間は圧縮処理を実施しない場合には約70％の短縮が可能となる為に，情報を保存する必要がない場合や伝送速度が速い場合においては圧縮処理を行わないほうが効率的な場合もある。

4.4　装置による処理時間変化

Table 7に，3.4で使用した装置の性能を示した。ここで，Table 7の装置性能と Fig .3における10 MB データの暗号化時間との関係を求めると，装置性能と暗号化時間との関係は，演算回数に影響を与えるクロック周波数ではなく演算速度とディスクの読み書き速度の積に比例した関係となり，その場合の装置性能と暗号時間の関係を Fig .6示した。また，Fig .6では，縦軸の値が下にくるほど暗号化時間が短くなるために性能が良いことになる。

4.5　医療情報に対する処理時間

Fig .2（b）にて求めたファイル容量に対する暗号化時間を医用画像のファイル容量に対応させた場合，1画像として，最もデータサイズの大きい胸部単純写真（8 MB: 2,048×2,048×12）を暗号化する場合でも 3 分以内にて暗号化を行えることが解る。また，この処理時間は今回の装置構成が高性能な為にこの程度の時間となった訳ではなく，現在日本で通常に使用されているコンピュータを使用した場合には，本研究結果と同程度かあるいはそれ以上の時間にて暗号処理を行うことが可能である。

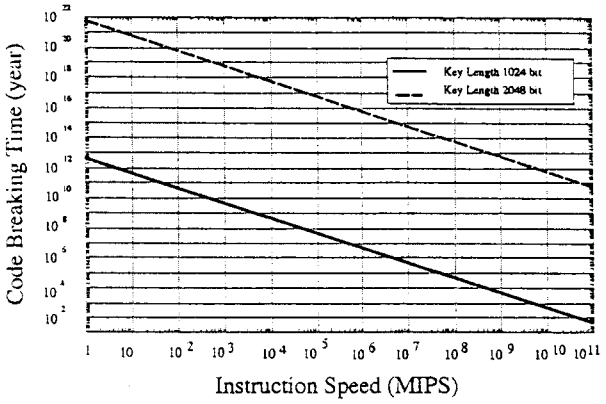

Fig.5　Relation of Instruction Speed and Code Breaking Time

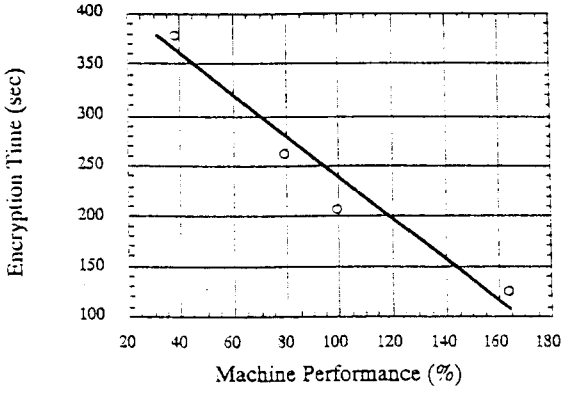

Fig.6　Relation of machine performance and Data Encryption Time　(10 MB)

Table 6　Comparison of Data Format Patarn on Medical Information.

	Patient Information Data (PID)		Medical Image Data (MID)		Total	
	Data Size (MB)	Time (sec)	Data Size (MB)	Time (sec)	Data Size (MB)	Time (sec)
Normal Data	0.5	0	3.0	0	3.5	0
All Data : Compressed+ Encrypted	0.45	11.0	2.7	66.0	3.15	77.0
PID : Compressed+Encrypted MID : Normal	0.45	11.0	3.0	0	3.45	11.0
PID : Compressed+Encrypted MID : Compressed	0.45	11.0	1.8	26.4	2.25	37.4
PID : Encrypted MID : Normal	0.75	7.7	3.0	0	3.75	7.7
All Data : Encrypt ed	0.75	7.7	4.5	46.2	5.25	53.9

Table 7　Relation of Medical Image Size and Encryption / Decryption time

	CPU clock Frequency		Calculation speed		Disk read/write speed	
	(MHz)	(%)	(sec)	(%)	(sec)	(%)
Power Macintosh 7100/80	80	80	479	67	95	57
Power Macintosh 7200/90	90	90	660	92	141	85
Power Macintosh 7500/100	100	100	714	100	166	100
Power Macintosh 8500/120	120	120	1,155	162	168	101

5．おわりに

医療情報の保護を行う為にパーソナルコンピュータを使用して医療情報の暗号化を行った場合でも，暗号処理時間は実用範囲内にて可能であり，また，暗号データに関しても解読・改ざんが現実的にはほぼ不可能であることも示した。これらより，小規模施設や在宅医療などで暗号化による医療情報保護を行う場合でも専用装置を使用しなくともパーソナルコンピュータを使用した低価格な装置構成でも医療情報を安全に保管・伝送することが可能でありることが解った。

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，(財) 医療情報システム開発センター，1994

2）第36回画像部会シンポジューム．日本放射線技術学会雑誌，51：1281-1296，1995

3）亀山敦之，遠藤晃ほか．医師と患者に対する医療用ICカードのアンケート調査－知名度と経費負担についてー．医療情報学，17：367-371，1997

4）山口英 訳．コンピュータセキュリティの基礎．東京，アスキー出版局，208-229，1994

5）Linn, J. Privacy enhancement for internet electronic mail part : Message encryption and authentication procedures. RFC1421, February, 1993

6）Kent, S. Privacy enhancement for internet electronic mail part : Certificate-based key management. RFC1422, February, 1993

7）Balenson, D. Privacy enhancement for internet electronic mail part : Algorithms, modes, and identifiers. RFC 1423, February, 1993

8）Zimmerman, P. R. PGP user's guide copyright 1990-1994

9）足立暁生訳．公開鍵暗号系．東京，東京電機大学出版局，169-216，1992

10) Lenstra, A. K., Lenstra Jr., H.W. et al. The factorization of the ninth format number. Mathmatics of Computation, 61 : 319-350, 1993

広島県立保健福祉短期大学紀要　5(1)　117－123　2000

Investigation of medical information using the public key cryptosystem on personal computer

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

We developed a system where medical information is enciphered and decode employing public key cryptography to protect medical information from being leaked, tampered or falsified, and practicability and the security of the system was examined. Pretty Good Privacy (PGP) and Privacy Enhanced Mail (PEM) tested in multi operation system. Encryption and decryption of 8MB data size took 176 sec. and 150 sec. respectively. PGP is capable of reversible data compression before encryption, so that 10% reduction of data size was realized without loss of information. Simulation of the security proved that an instruction time needed more than 1.321035times in case of 2,048 bits key length.

Key words : public key cryptosystem, medical information, personal computer, security, multi operation system