遠隔地画像診断のための医用画像の個人情報遮蔽と暗号化の試み

高　誠治郎

近畿大学医学部整形外科学教室

抄　録

インターネットを使って遠隔地画像診断を行おうとする場合，Digital Imaging and Communications in Medicine（以下DICOM）データをそのまま送信すると個人情報がインターネット上に流出してしまうおそれがある．これを防止する目的で，高価な専用機器が開発されているが，ここではそのような機器を使用しないで，全てIBM-PC/AT互換機を用い，医用画像や個人情報の第三者への漏洩を防止できるシステムの構築を試みた．

まずスタンドアロンコンピュータでDICOMデータから個人情報のみを選択的に消去するプログラムを作成した．次いでインターネットを想定した模擬回線を設定し，それに接続されたコンピュータで情報を送信し，同時に第3者を想定したコンピュータよりデータの傍受を行った．その結果，DICOMデータから個人情報を選択的に消去したデータを用いる事により個人データの漏洩がなくなることを確認した．さらに128 bit SSL暗号化機能付ファイアウォールでデータを暗号化する事により，第3者には傍受データの復元が困難な医用画像・情報の通信を行うことが可能となった．

Key words : 遠隔地画像診断，患者情報の保護，公衆回線網，医用画像

緒　言

僻地の病院に勤務する医師が手術適応や画像診断に関してセカンドオピニオンを求める時，診療録とともにX線フィルムなどの様々な画像を持って移動をするには多大な労力と時間を要する．また，当直時など病院に1人しか医師がおらず，外出できない状況で，専門分野以外の迅速な画像診断が求められ，難渋する事態も起こりうる．こういった場合，たとえば医用画像をファックスなどで送信しても鮮明な出力は得られず，小さな骨折を見逃してしまうなどの誤診をまねく恐れもある．そのような場合，インターネット等の公衆回線を使用して，画像診断機器からの画像出力をそのまま転送できれば，医師が移動せずに迅速な画像診断の依頼などが可能になる．しかし，公衆回線を使う遠隔診断の問題点として，

1）電子カルテ，またはそれに類するものを含んだ電算機をインターネットなどを含む一般公衆回線に接続出来ない通達の存在[1]．
2）遠隔診断を行う事に対して患者の同意があっても，患者の個人情報保護に留意しなければいけないという通達の存在[1]．
3）情報交換用のコンピュータを第3者から不正に操作される恐れがあり，不正使用を受けると個人情報漏洩の危険性があるためにサーバの安全性の確保のための技術が必要，などの問題点があげられる．

これまでの遠隔画像診断の歴史では，1975年に通常のアナログテレビを使った実験が米国で行われた[2]．1979年にはカナダで静止衛星を使ったX線写真とX線透視の中継が試みられた[3]．1981年にデジタル化された画像をコンピュータのディプレイに表示して診断する試みが行われた．1991年には，日本で最初の遠隔診断が，電話回線を使ってCCDカメラの映像をパソコンから転送する試みとして行われた[4]．1995年に日本初の遠隔画像診断支援サービスがセコムで開始され，転送にはISDN回線を使用した[5]．1997年に医用画像をデジタルカメラで撮影し，PGP暗号化メールで転送する試みが行われた[6]．1998年にDICOMサーバをインターネットにプロ

大阪府大阪狭山市大野東377-2（〒589-8511）
受付　平成13年8月30日，受理　平成13年12月3日

キシサーバで接続する試みが行われ，暗号化には，PGP暗号が用いられた[7]．2000年にDICOMサーバの通信を一部，Secure Socket Layer（以下SSL）で暗号化し，インターネットに接続する試みが行われた[8]．2001年，携帯電話付属のカメラで撮影した画像をメールを用いて転送し，初期治療に利用する試みが日本で行われた[9]．

テレビ中継を用いた遠隔画像診断[2,3]では，公共の電波を用いるため，個人情報の保護が十分とはいえない．アナログ電話線やISDN回線を利用したシステムでは，秘匿性は保たれるが，転送速度がインターネット回線に比べると低速であり，鮮明な画像を得るためには，転送に時間を要する．インターネット等の公衆回線を用いた遠隔画像診断については，デジタルカメラを使ったもの[6]では画像は鮮明とは言えず，小さな骨折を見逃してしまうなどの危険性がある．また，携帯電話のメール[9]は簡便だが，暗号化を行う機能がなく，個人情報の保護が十分とはいえない．また，PGP暗号化[6,7]を行うと，被依頼者クライアント側でPGP暗号解除のため，ソフトウェアのインストールが必要となり，利便性が損なわれる．

この実験では，転送速度が速く，通信経路が全て暗号化され，鮮明な画像が得られ，クライアント側で暗号解除のために特別なソフトウェアを必要としないシステムの構築を試みた．同時に，暗号化機能付きファイアウォールの作成と実装を行い，情報交換用のコンピュータの保護に努めた．また患者の個人情報の保護にも十分に留意した．システムは専用ワークステーションを用いず，出来るだけ安価に作成するよう各部に工夫を凝らした．

材料および方法

使用機材

表1，表2，表3に示す機材を使用した．これらにおいてX線CT装置以外は高価な特殊機材を使わず，一般入手が容易であるものとした．また，コンピュータは全て旧式のものを用い，実験価格が安価

表1 コンピュータ用途別のハードウェア

コンピュータ用途	ハードウェア
DICOM画像変換用	INTEL TE430VX（Intel MMX-Pentium 166 MHz） Canopus TOTAL3D 64 MB SD-RAM PC66 SYMBIOS 53c875チップPCIバスSCSIカード SCSI HDD 4.3 GB SONY SMO-S501（5インチ光磁気ディスク） ELECOM EMO-2300（3.5インチ光磁気ディスク）
ファイアウォール(1)	富士通FMV-466D（Intel 486DX2 66 MHz） Realtek8019チップISAバスイーサネットカード（NE2000互換）2枚
ファイアウォール(2)	Proside LB486-50（Intel 486DX 50 MHz） Realtek8019チップISAバスイーサネットカード（NE2000互換）2枚
メールサーバ(1)	GIGABYTE technology GA-586VX（Cyrix M2-300GP） Matrox MilleniumII 32 MB 60 ns FP SIMM（2枚）IDE HDD 10 GB DEC21140-AFチップPCIバスイーサネットカード
メールサーバ(2)	ASUS Computer International P2E-M（Intel Celeron 300 A） ATI RAGE IIC 64 MB PC-100 SDRAM（2枚） IDE HDD 10 GB DEC21140-AFチップPCIバスイーサネットカード
メールクライアント(1)	富士通FMV Deskpower S165（Intel Pentium 166 MHz） DEC21140-AFチップPCIバスイーサネットカード
メールクライアント(2)	SHARP MN-8000D（Intel MMX-Pentium 200 MHz） SYMBIOS 53c875チップPCIバスSCSIカード ELECOM EMO-2300MS（3.5インチ光磁気ディスク）
通信傍受用	ACER A1G（Intel 486DX2 66 MHz） 16 MB 70 ns FP SIMM（2枚） Realtek8019チップISAバスイーサネットカード（NE2000互換）

表2　コンピュータ用途別のOSとソフトウェア

コンピュータ用途	オペレーティングシステム（以下OS）	ソフトウェア
DICOM画像変換用	Vine Linux Ver2.1.5[10]	自作データ変換ソフトウェア
ファイアウォール(1)	Vine Linux Ver2.1.5	Stone version 2.1e（接続中継ソフト） Open SSLライブラリ Ver. 0.9.6（暗号化ソフト）
ファイアウォール(2)	Vine Linux Ver 2.1.5	Stone version 2.1e（接続中継ソフト） Open SSLライブラリ Ver. 0.9.6（暗号化ソフト）
メールサーバ(1)	Solaris 8 for Intel 04/01[11]	ISC BIND Version 8.2.4[12]（DNS） Postfix rel-20010228（メール配送プログラム）
メールサーバ(2)	Solaris 8 for Intel 04/01	ISC BIND Version 8.2.4（DNS） Postfix rel-20010228[13]（メール配送プログラム）
メールクライアント(1) メールクライアント(2)	Microsoft Windows 2000 professional Microsoft Windows 2000 professional	
通信傍受用	Vine Linux Ver2.1.5	Sniffit v.0.3.5[14]（スニッファ） Nmap Ver. 2.5.4BETA24 （ネットワーク検査ツール）

表3　その他

ネットワーク機材	松下電工 NAiS Taphub-SR5（5Port 10Base-T HUB） 10Base-T category5ケーブル
X線CT装置	東芝 Xlead

になるように工夫した．さらにオペレーティングシステムとソフトウェアはWindows 2000以外は全てインターネットを通じて無料で入手したものである．

方　法

暗号化ファイアウォールおよび，復号化ファイアウォールの設定

ファイアウォールとは，ネットワークへの不正侵入や破壊行為，外部公開サーバの防御を行なうための機器のことである．まず，ファイアウォール用コンピュータにOSとしてVine Linux 2.15（FTP版）をインストールし，ネットワークの設定を行った．次いでStoneをOpen SSLライブラリと共にコンパイルし，インストールを行った．その後，不要なサービスを停止し，ファイアウォールとしての設定[15-19]を行った．ファイアウォールの動作の概要を図1に示す．

メールサーバの設定

メールサーバ用のコンピュータにSolaris 8 for Intel (04/01) をインストールし，ネットワークの設定を行った．次いで，DNS[20]とメールサーバの設定を行った．

クライアントの設定

クライアントコンピュータにMicrosoft Windows 2000をインストールし，ネットワークの設定

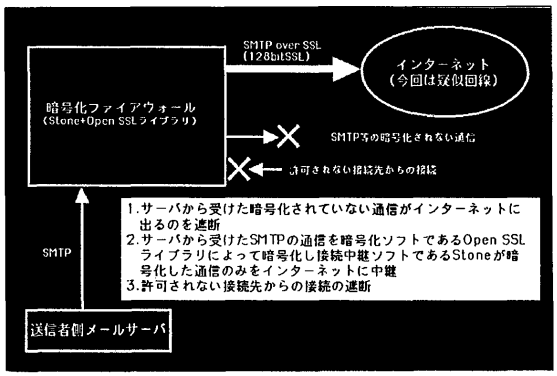

図1　作成したファイアウォールの動作について

とメールクライアントの設定を行った．また，DICOMビューアのセットアップを行い，DICOMデータを表示出来るようにした．

通信傍受用コンピュータの設定

通信傍受用コンピュータにVine Linux 2.15 (FTP版) をインストールし，ネットワークの設定を行った．次いでSniffitとNmapをインストールした．

DICOM画像変換用コンピュータの設定

DICOM画像変換用コンピュータにVine Linux 2.15(FTP版)をインストールし，3.5インチと5インチ光磁気ディスクを読めるようにした．次いで文献21Grevera Jら[21]を参考に筆者が作成したプログラムを用いて，内部に画像情報と文字情報を含んで

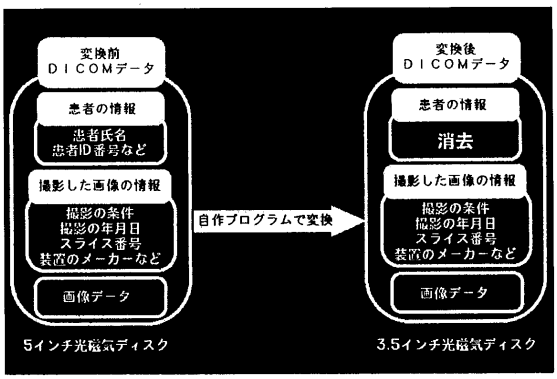

図2 DICOMデータ変換のための自作プログラムの動作について

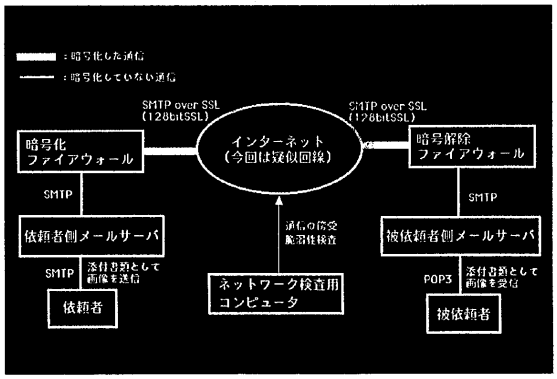

図3 暗号化付のファイアウォール付きで構築したネットワークの模式図

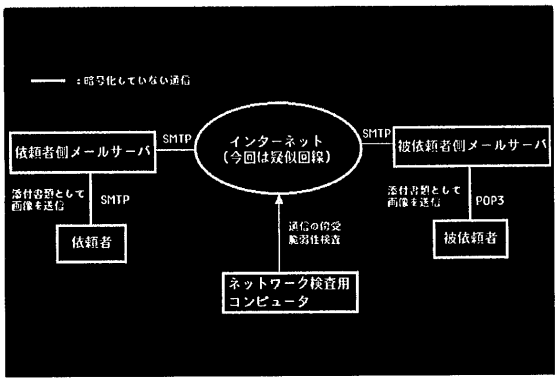

図4 図3のネットワークをファイアウォールなしで構築したネットワークの模式図

いるDICOMデータから患者情報だけが隠蔽されるように設定した．自作DICOM変換プログラムの動作を図2に示す．

ネットワーク接続

次の2つのネットワーク環境を構築した．

a）メールサーバ，ファイアウォール，通信傍受用コンピュータ，及びクライアントを集線装置（以下ハブ）を介して接続した．インターネットを想定したファイアウォール間の通信は，全て暗号化された通信となる（図3）．

b）メールサーバ，通信傍受用コンピュータ，及びクライアントをハブを介して接続した．インターネットを想定したメールサーバ間の通信は，全て暗号化されない通信となる．（図4）

DICOMデータ作成と変換

X線CT装置で撮影したデータを5インチ光磁気ディスクにDICOM形式で保存した．DICOM形式は，医用画像の汎用フォーマットであり，内部に画像データ以外にも患者個人のデータ，撮影条件などを含んでいる．3.5インチ光磁気ディスクは，あらかじめWindowsで初期化した．DICOM画像変換用コンピュータでデータを5インチ光磁気ディスクより読み込み，自作プログラムによりDICOM形式のデータのうち患者個人の情報だけを消去したDICOM形式のデータに変換を行い，3.5インチ光磁気ディスクに保存し直した．

DICOMデータの転送

変換したデータを含む3.5インチ光磁気ディスクをクライアントコンピュータで読み込み，メールの添付書類[22]として画像データを送信した．被依頼者はメールの添付書類として画像データを取り出し，DICOMビューアにて閲覧を行った．図3のインターネットを想定した回線上ではメールは暗号化された通信となり，図4のインターネットを想定した回線上ではメールは暗号化されない通信となる．

ネットワークの検証

通信傍受用コンピュータから，スニッファであるSniffitを用いて図3のインターネットを想定した回線上と図4のインターネットを想定した回線上で回線の傍受を行い，データが暗号化されているかどうかを確認した．また，ネットワーク検査用コンピュータからネットワーク検査ツールであるNmapを用いて，図3のインターネットを想定した回線上と図4のインターネットを想定した回線上で，サーバとファイアウォールに対して擬似的な攻撃を仕掛け，システムが不正な操作を受けないかを診断した．

変換前のDICOMデータと変換後データの検証

変換前のDICOMデータと変換後のDICOMデータの個人情報の検証を行った．

転送前データと転送後データの検証

転送前と転送後のデータをファイル比較し，完全に一致しているかどうかの検証を行った．

結　果

ネットワーク傍受の結果

ファイアウォールなし（図4のネットワーク接続）の場合

図5のように，接続先のサーバの名称，転送元の

メールアドレス，転送先のメールアドレス，サーバのMTAのプログラム名とバージョン番号，メールの内容が，全て受信された．

ファイアウォールあり(図3のネットワーク接続)の場合

図6のように，通信内容は，画像も含め意味不明な文字の羅列となり，通信の内容は理解出来ない状態であった．

サーバとファイアウォールの脆弱性検査の結果

ファイアウォールなし(図4のネットワーク接続)の場合

図7のように，DNSと暗号化していないメールサービスの稼動を認めた．

ファイアウォールあり(図3のネットワーク接続)の場合

図8および図9のように，許可されたIPアドレスからはDNSと暗号化されたメールサービスの稼動を確認できるが，許可されないIPアドレスからは，サービスの稼動が判定できなかった．

変換前のDICOMデータと変換後データの検証

転送前のデータと転送後のデータをDICOMビューアで表示した結果を図10および図11に示す．転送前は患者の名前を確認出来るが，転送後は，患者の名前が匿名となっており，DICOMデータの患者情報のみが選択的に消去されている．

転送前と転送後のデータが完全に一致しているかどうかの検証

比較は，Windows 2000に含まれる“FC”コマンドを用いて行ったが転送前のDICOMデータであるct.00001.dcmと転送後のDICOMデータであるct_00001.dcmの比較は図12に示すように，完全にフ

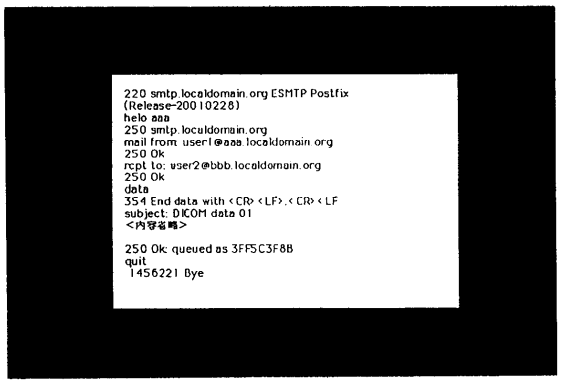

図5　図4のネットワークのインターネット上を流れた通信の傍受結果

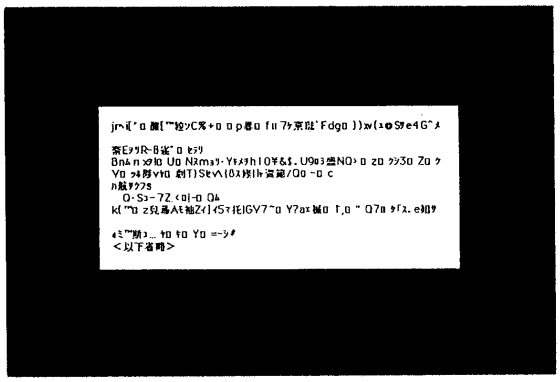

図6　図3のネットワークのインターネット上を流れた通信の傍受結果

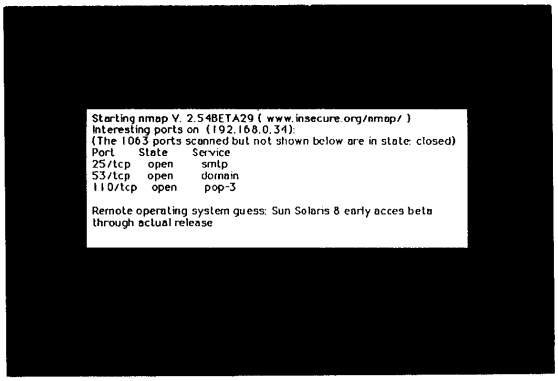

図7　図4のネットワークをインターネット上から脆弱検査を行った結果

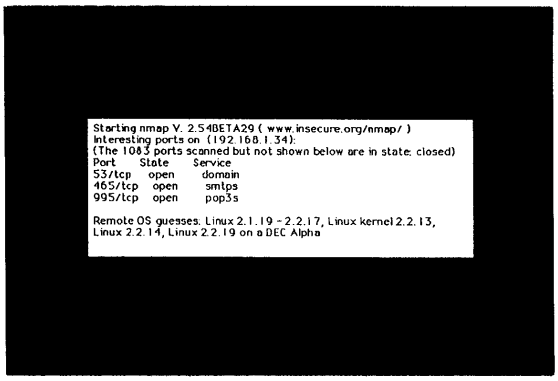

図8　図3のネットワークをインターネット上の許可されたIPアドレスから脆弱検査を行った結果

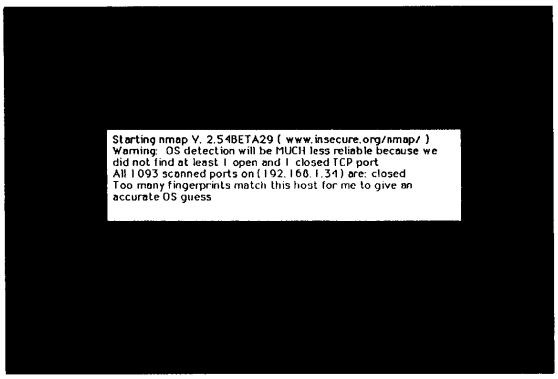

図9　図3のネットワークをインターネット上の許可されないIPアドレスから脆弱検査を行った結果

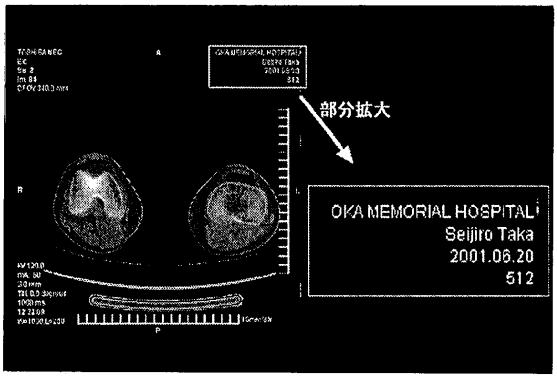

図10 自作プログラムで変換する前の生のDICOMデータをDICOMビューアで表示した結果

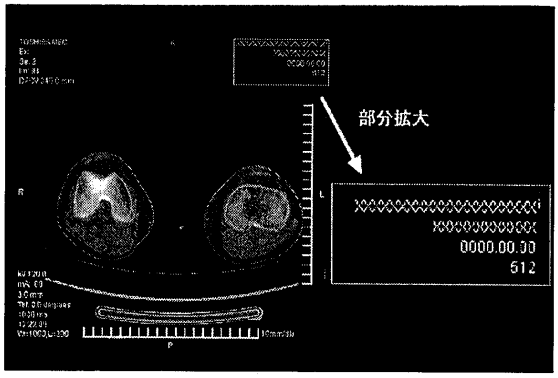

図11 自作プログラムで変換した後の加工されたDICOMデータをDICOMビューアで表示した結果

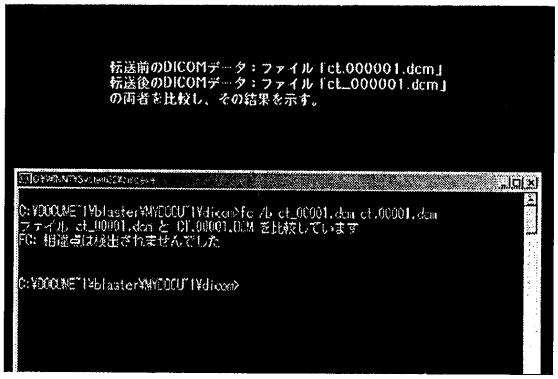

図12 転送前のファイルと転送後のファイルの比較結果

ァイルの長さと内容が一致していた．

考　　察

ネットワーク傍受の結果について

ファイアウォールを設置せず，暗号化を行わない状態では，傍受した通信の内容が平文で流れるため第3者に内容を知られる可能性があった．傍受した通信内容にはメールの送信元と送信先等のデータ，サーバのメール転送サービスの種類とバージョンが含まれているため，サーバの不正使用のきっかけを与えてしまう可能性がある[23-27]．たとえメールソフト(以下MUA)に暗号化機能があり通信内容の暗号化を行った場合[28]でも，メールの内容以外の通信は平文で行なわれるため，サーバの不正使用のきっかけを作ってしまう事になる．またMUAに暗号化機能を含むものを使って秘匿性を保とうとした場合，MUAが限られてしまい使用しづらくなってしまうなどの問題が一般に認識されている．

ファイアウォールを設置して，暗号化を行った状態で通信の内容を傍受しようとしたが，意味不明な文字の羅列となり，解読困難な状態であった．暗号化手順にNetscape社のSSLを用いた．128ビット暗号化SSLは，12.3Tflops(浮遊小数点演算を1秒間に1.23×10^{13}回実行可能）程度の速度のコンピュータを使用した場合でさえ解読に約3万年かかり[29-32]，事実上，解読は不可能である．

サーバとファイアウォールの脆弱性検査の結果について

ファイアウォールがない場合，サーバのOSが判明した．ファイアウォールがあると，サーバのプラットフォームがファイアウォールのものとして判断されるため，不正なサーバの使用のきっかけを与えにくい．これは，ファイアウォール外から見ると，サーバのTCP/IPのシーケンス番号がLinuxのものに変換されるためである[30]．サーバに用いたSolaris 8では問題にはなりにくいが，極端に古いサーバはTCP/IPのシーケンス番号を特定されやすいため，古いサーバ機を使っていた場合，特定のIPからだけサービスを許可していても，シーケンス番号を予測し騙すことで特定のIPアドレスになりすまし，本来許可していないホストからの接続を許してしまう事がある[23-27]．しかし，ファイアウォール設置によってIPのなりすましがある程度防止されるものと思われる．またファイアウォールがある状態では，ファイアウォールを突破されない限り，たとえサーバ上で不要なサービスが稼動していても，ファイアウォール外からはそのサービスの存在を特定されにくい[23-27]．

構築したシステムを稼動させたところ特に致命的な脆弱性は見つからず，DNSと暗号化したメールサービスの稼働を認めるのみであった．

自作DICOM変換プログラムについて

全体の動作アルゴリズムは，ファイル読み込み後，DICOMファイルかどうか，DICOMファイルでも，コピーに失敗したデータかどうかのチェックを行う．チェックが問題なければ，ファイルの解析を行う．ファイルの解析では，①検査日付②画像時刻③

施設名④主治医⑤患者の名前⑥患者のID番号⑦患者の生年月日⑧患者の性別⑨患者の身長⑩患者の体重を含む領域を検索し，その領域が存在すれば，その部分を書き換え，ファイルに出力し，画面に書き換える前の患者データを出力する．患者情報が1つも見つからなかった場合，匿名化ファイルを作成せずに終了する．

DICOMヘッダは①タグ（4バイト）②データのタイプを示すVR（2バイト）③データの長さ（通常2バイト）④タグで示される内容データの連続で成っている．自作プログラムは，タグとVRを検索し，その位置を記憶する．タグの形式としては，リトルエンディアン形式（タグの上位1バイトと下位1バイトが逆順に並ぶ形式）と呼ばれるタイプのものにしか対応していないが，ビッグエンディアン形式（タグの上位1バイトと下位1バイトが順番に並ぶもの）にも，少しのプログラム改変で対応し得る．DICOM形式にそぐわずに，メーカー独自のヘッダの拡張を行っているものについては，経験がないため，不明である．使用されるDICOMデータの形式は，同一の機器では，同一の形式であるため，最初にプログラムの設定を行えば，以後は再設定を必要としない．自作プログラムは個人情報を消去したDICOMデータを作成するが，既往歴や家族歴などの情報が必要な場合は，DICOM画像を添付するメール本文で言及可能である．また，自作プログラムはデータ変換時に患者情報を出力するので，必要な場合は，患者情報の出力をテキストファイルに変換し，それの全部または一部をメール本文に利用すれば，被依頼者側で画像と分離した状態で個人情報の交換が可能である．

DICOMデータの検証について

変換前のDICOMデータ中には名前等の個人情報が含まれているのが確認出来る．変換後は，図11のように名前が匿名（anonymous）となっており正しく個人情報が消去されている事が解る．しかし再現された画像に特殊な人工関節が入っている場合などはCT画像そのものが個人を特定し得ることになる[33-35]．

転送前と転送後のデータの考察

転送後のデータは，1文字も違わず転送前データに完全に一致した．画像データの精度は転送前と同じ精度であり，転送による劣化は認められなかった．この方法と比較し，デジタルカメラやスキャナで取り込んだ画像の場合さまざまな問題点がある（図13）．しかし，この実験で転送した画像データの場合，無料で入手可能なScion Image release beta4.0.2[36]を用いて図14のような詳細な3D画像を再構築することも可能であった．このようにデータ利用の自由度が非常に広がる．しかしディスプレィで写る画像はモニタの発色によって差が出るため完全に転送元と転送先で同じ画像を得るためにはモニタの写り具合の調節が必要である．

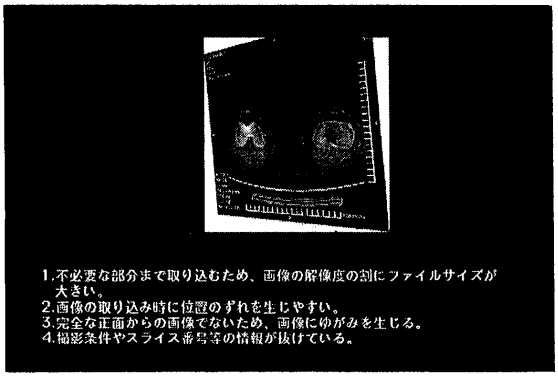

図13　デジタルカメラで医用画像を取り込んだ時の問題点

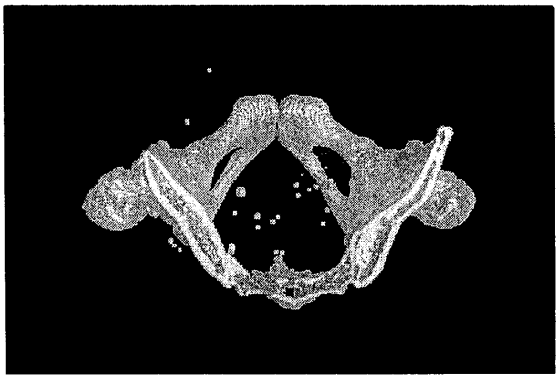

図14　転送したDICOMデータを用いて骨盤の3次元画像を作成しproximalより観察した結果

低コスト化と安全上の問題点に関する考察

低コストでシステムを作成するため，自作を含むAT互換機を用いた．AT互換機はワークステーションと比べると広範囲に使用されているため，悪意のある者が不正な使用を行おうとする可能性がある．しかし，

1）フロッピーディスクから悪意のあるプログラムを起動しないように，設定の変更を行う．
2）権限のない者が設定を変更しないように，設定変更にパスワードを設ける．
3）特定の権限を持った人しか出入り出来ない部屋にコンピュータを設置する．
4）持ち去られ，筐体を開けられないように，コンピュータにキーチェーンをつける．

などの対策を施せば不正な使用を回避できる．

Linuxは無料で入手できるOSだが市販のものと

比較しても，何ら遜色がない．有利な点は，

1）プログラムのソースコードが入手できるため，不具合があっても，即座の修正が可能であり，市販のOSのようにセキュリティパッチを待つ必要がない．また，修正部分の入手は，小さなファイルでの入手が可能である．

2）Graphical User Interface（以下GUI）での動作も可能だが，軽快なCharacter User Interface（以下CUI）も可能である．CUIで動かせばメモリの占有量も少なく，Central Processing Unitの単位時間あたりの処理能力が低い旧型機種での動作も可能である．

3）堅牢なマルチタスクOSであり，ユーザー毎の管理が容易である．

4）設定はやや難解だが，操作体系が不変．

などがあげられる．

市販のOSを使わなくても堅牢なシステムを低コストで構築することが出来た．この実験に使用した機材は，新品のコンピュータを新規に購入しても1台あたり4万円未満で入手可能であり，使用したソフトウェアはWindows2000以外は全て無料で入手可能である．すなわち十分に低コストで安全に留意したシステムを作ることが出来たと考えられる．

SSLを使った他のシステムとの比較

医療分野でSSLを使った報告を渉猟すると，DICOMサーバの通信を一部暗号化し，インターネットに接続する試み[8]があったが，全ての通信を暗号化していない．これは，DICOM規格のプロトコルはアソーシエーション情報と呼ばれる各種設定を事前に行ったものだけが接続を許されるため，アソーシエーション折衝を利用して暗号化を一部省略しているためである．アソーシエーション情報を推測することは不可能であるが，snifferを設置し，アソシエーション情報を入手出来れば，悪意の第3者に接続を許す可能性が存在する．また，内視鏡の画像データを暗号化Webサービスで閲覧出来るようにした遠隔診断システム[37]や診療録システム[38]の報告がある．暗号化Webサービスで同様の機能を実現しているものに比べて，本システムは，サーバへのデータの登録が簡便である．さらに，メールを使用しているため，被依頼者がメールを受け取ると，既読のメールはメールサーバから消去されるように設定可能なので，被依頼者がメールチェックを行っている限りはサーバにデータが蓄積せず，サーバは小さな外部記憶装置で動作可能である．また，特定の被依頼者を対象にしているため，データが長期間，サーバに存在する可能性は低く抑えられ，不特定多数を相手にするWebサービスと比較すると，安全である．

本システムの利点と欠点について

本システムは，完全に病院内のDICOMサーバと隔離して動作するため，被依頼者は，遠隔画像診断を行う患者データ以外にアクセスする事は出来ない仕組みになっている．これは，厚生労働省の通達の要求事項を満たしている．また，不正使用を受ける可能性は極めて低く，たとえ，不正使用を受けても，患者情報が流出する可能性は，極めて低い．高いセキュリティを有するが，依頼者側に，データ変換と言う少し煩雑な手続きを要求する．安全性と利便性のバランスを考え，依頼者側の手続きを簡略化する事が今後の課題である．

遠隔地診断全体に対する考察

他病院の医療従事者に画像診断のコンサルトをする場合，必ず患者本人の同意を得る必要がある，画像は筆者自身の画像データを使用し，回線は一般公衆回線でなく模擬回線を使用した．近年，インターネットの回線速度が向上し，近畿大学でも従来の回線速度に比較して20倍を超える1.5 Mbpsの回線処理速度となったため，医用画像のようにテキストで送るメールよりも容量が極端に大きく，暗号化を行う場合でも対応し得ると思われる．本システムをそのまま，近畿大学のインターネットに接続すれば，医用情報のやりとりを，本院と分院で行えるが，データの往来量は未知であるため，導入に当たっては，さらに回線の使用状況等についての調査や設備投資が必要であると思われる．また，本システムを用いて，学外と医用情報のやりとりを行うためには，大学に設置しているファイアウォールの設定のため，この設定では通信不可能となる．しかし，ファイアウォールの設定を変更するか，自作ファイアウォールプログラムを一部変更する事で対応可能と思われる．

まとめと今後の展望

患者の個人情報を保護した状態でインターネット遠隔画像診断が可能なシステムを構築することができた．また使用料の不要なソフトを多く利用したことにより市販のシステムを導入するのに比べておよそ百分の一のコストで構築が可能であった．将来は大学と関連病院で行われるインターネットによる症例検討が，さらに転送・再構築が困難なリアルタイムの動画により行われる可能性も展望される．

謝　辞

稿を終えるにあたり，御指導，御校閲を賜りました濱西千秋教授に深く感謝いたします．また，本研究に御協力いただいた教室の方々に心から感謝致します．

文　献

1. 厚生省健康政策局長 厚生省医薬安全局長厚生省保険局長,診療録等の電子媒体による保存について. 政発第517号 医薬発第587号 保発第82号, 平成11年4月22日
2. Andrus S, Dreyfuss R, Jaffer F, Bird T (1975) Interpretation of roentgenograms via interactive television. Radiology 116: 25-31
3. Carey S, Russell S, Johnson E, Wilkins W (1979) Radiologic consultation to a remote Canadian hospital using Hermes spacecraft. J Can Assoc Radiol 30: 12-20
4. Odagiri K, Nakamae H, Ohkoshi T, Andoh K, Kinno Y, Hyodo Y, Chiyasu S, Ano K. (1991) Clinical evaluation of a teleradiology system utilizing personal computers and public telephone line. Nippon Igaku Hoshasen Gakkai Zasshi 51: 1359-1365
5. セコム株式会社 Hospi-net 推進プロジェクト(1997)セコム株式会社による遠隔画像診断支援サービス Hospi-net. INNERVISION 2　7：86-89
6. 田中直樹(1997)患者プライバシーを守る画像電子メールの暗号化 インターネット経由の症例コンサルテーション. 医療情報学 (0289-8055) 17　1：37-40
7. 櫻井康介, 有澤　淳, 松下正樹, 岸本陽督, 青木佳子, 小山光博(1998)公開鍵暗号方式を用いたDICOMファイル転送の検討. 日放線医会誌. 58 (supol)：273-273
8. Bernarding J, Thiel A, Tolxdorff T (2000) Realization of security concepts for DICOM-based distributed medical services. Methods Inf Med 39: 348-352
9. 平田哲朗, 日下義章, 塚原隆司, 今泉佳宣, 山田実貴人(2001) 整形外科における携帯電話を利用した医療画像転送. 中部整災誌　44：76-76
10. 野村　直編. Vine Linux 2.1システム管理ブック. 東京：アスキー, 2001
11. 臼田昭司編. SOLARIS8 UNIX超入門. 東京：小学館, 2000
12. 国安和廣編. フリーUNIXで作るネットワークサーバ構築ガイド. 東京：秀和システム, 1998
13. ぱぱんだ編. 怒涛のLinuxネットワーク. 東京：エーアイ出版, 2000
14. 小高知宏編. 基礎からわかるTCP/IPアナライザ作成とパケット解析. 東京：オーム社, 2001
15. 久米原栄編. LINUXネットワーク ファイアウォール管理者ガイド. 東京：ソフトバンク, 2001
16. W Cheswick, S Bellovin, eds. Firewalls and Internet Security. Boston: Addison-Wesley, 1994
17. 一條　博編. フリーソフトで出来るネットワークセキュリティ ファイアウォール構築ガイド. 東京：株式会社テクノプレス, 1999
18. 村嶋修一編. ルータ&パケットフィルタリング, 東京：株式会社情報管理, 1999
19. まえだひさこ編. PC-UNIXサーバのためのクラッカー撃退計画. 東京：翔泳社, 1999
20. Albitz P, Liu C, ads. DNS and BIND 3rd Edition. Cambridge: O'Reilly, 1998
21. Grevera J, Feingold E, Horri C (1996) A WWW to DICOM interface. Proc SPIE 2711: 109-117
22. 大東文化大学学園総合情報センター編. インターネットリテラシー. 東京：株式会社昭晃堂, 1998
23. Ryan R, ed: Hack Proofing Your Network-Internet Tradecraft. Rockland: Syngress Media, 2000
24. Anonymous (SE編集部 訳編)：クラッキング対策ファイナルガイド, 東京：翔泳社, 1999
25. チャーリー カウフマン, ラディア・パール, マイク・スペシナー編(石橋啓一郎, 菊池浩明, 松井　綾, 土井祐介訳). ネットワークセキュリティ. 東京：プレンティスホール出版, 2000
26. Stuart M, George K, Joel S, ads. (宇野みれ, ㈲ハラパン・メディアテック 訳). クラッキング防衛大全 第2版, 東京：翔泳社, 2001
27. Anonymous(SE編集部 訳編). Linux版クラッカー迎撃完全ガイド, 東京：翔泳社, 2000
28. Bruce S, ed. (力武健次, 道下宣博 訳). E-mailセキュリティ. 東京：オーム社, 1995
29. 松井甲子雄編. コンピュータによる暗号解読法入門, 東京：森北出版株式会社, 1990
30. 辻井重男編. 暗号と情報セキュリティ, 東京：株式会社昭晃堂, 1990
31. 岡本栄司編. 暗号理論入門. 東京：共立出版, 1993
32. Alfred J M, Paul C V, Scott A V. Handbook of Applied Cryptography. Florida: CRC Press, 1997
33. 郵政省編. 通信白書 平成11年版. 東京：ぎょうせい, 1999
34. 郵政省編. 通信白書 平成12年版. 東京：ぎょうせい, 2000
35. 藤原宏高編. サイバースペースと法規制. 東京：日本経済新聞社, 1997年
36. 小島清嗣編, 岡本洋一. まるごと実践！画像解析テキストNIHImage新講座. 東京：羊土社, 1997
37. Hashiba M, Matsuto T, Arai F, Yamakawa T, Akazawa K (2000) Accessing endoscopic images for remote conference and diagnosis using WWW server with a secure socket layer. J Med Syst 24: 333-338
38. Wang SS, Starren J (2000) A Web-based, secure, light weight clinical multimedia data capture and display system. Proc AMIA Symp: 898-902