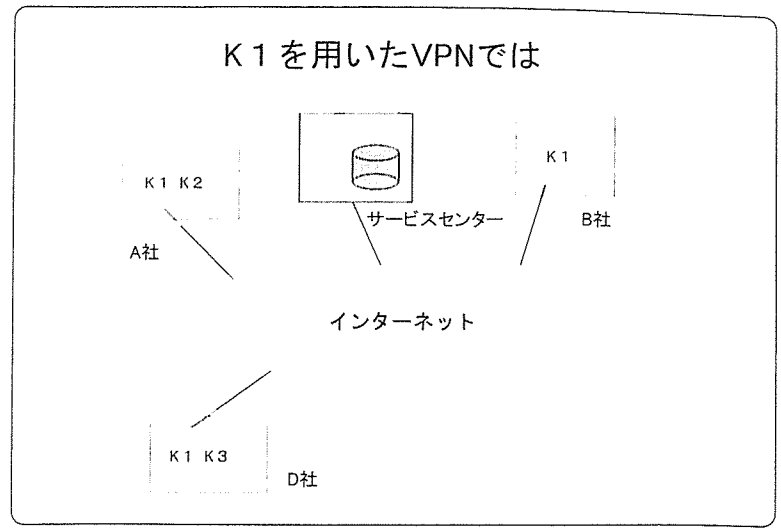
相互認証をかけます。相互認証をかけるので，ルーター側とは相手が正しいことが確認されるので，これで一種の暗号通信を開始することができます。これで，サービスセンターとD社のエッヂルーター間でセキュアなセッションが張られます。次に，同じように，センターはE社のルーターと相互認証して，セキュアなセッションを張ります。DとEの2社が相手確認をするための鍵は，当初から入っているわけではないので，相互認証用の鍵を暗号化して配送します。これがK´で，仮の鍵になっています。仮鍵は上の層，すなわち第2層に記録されます。以上で，サービスセンターとしての役目は終了です。

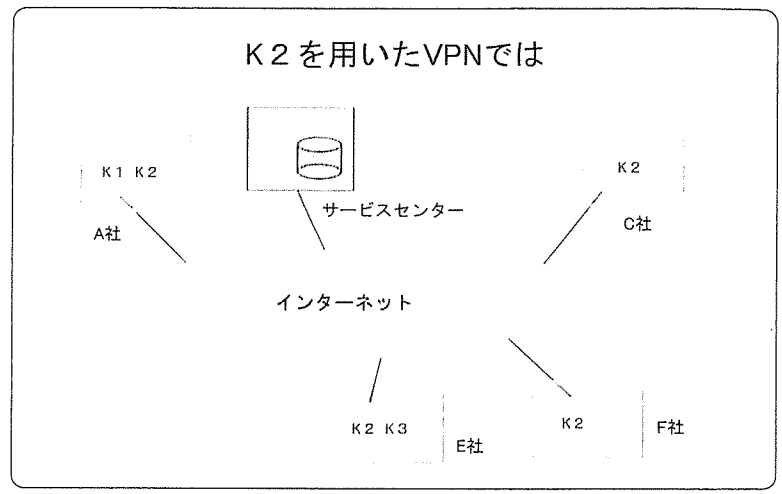
その後D社とE社は，互いに相手確認を行います。両者のルーターは相互認証して安全な通信を張ることができるので，その後，仮鍵を本番の鍵に取り替えます。こうすることで，サービスセンターは実際に用いる暗号鍵を知ることができなくなります。

以上のような手順でそれぞれのルーターに複数の認証鍵が配送されます。実際の利用場面は，例えばK1をアクティブにすると，**スライド37**の例では3社が（**スライド39**），K2を使うと4社が（**スライド40**），K3を使うと2社が（**スライド41**），論理的に異なる暗号通信ができるようになります。

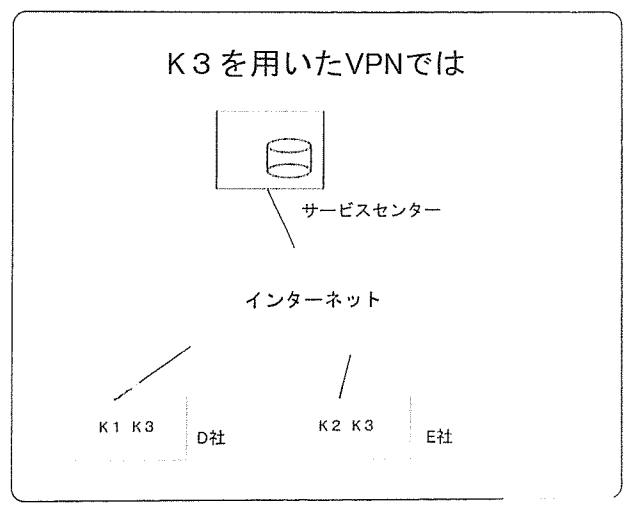
予測ではこの辺のサービスは月に2,000〜3,000円で提供できるのではないかと期待しています。ルーターは大体2万円くらいの装置で，2万円が20万カ所なので総額でも40億円です。40億円ならば，場合によっては国費で整備することも可能かもしれません。もちろんこれからの議論ですが，第2フェーズを実現するのに不可欠なセキュアなネットをつくる方法としては，可能性があるかもしれないと思います。



スライド39



スライド40



スライド41

実証実験はすでに沖縄で行っています　サービスセンターは東京に立ち上がっていますが，東工大も開発に関与しましたので，アメリカの大学と

東工大との間で実験を行っています。この暗号装置をアメリカに持っていって，日本から鍵を配送してVPNが張れることを確認しています。これは技術を開発しているものから見るとけっこう感動的でした。何しろ日本のサービスセンターから「アメリカとVPNでつながった」わけですから。それも鍵を替えればどことでもつながります。秘話通信が非常に簡単にできるようになります。このセンターのルートを日本に置ければ，ひょっとすると輸出産業としても伸びてくる可能性があるかもしれません。どうやるかはこれからですが，楽しみなことです。

まとめ

（スライド42）中途半端になりましたが，私の講演をまとめます。「インターネットの安全性確保」はこれから第2フェーズに発展するためにはどうしても必要であると思います。相互認証と暗号通信，認証鍵の安全性確保と基本的な要求は，先ほど言った住基カードのチップにより実現できます。

「医療分野の情報化」では，ご案内のとおり個人情報の保護が不可欠であること，そしてそのためには医療関連機関間のネットワーク化とHPKIの導入（これは今年から導入開始される）が有効です。このなかの1つのアプリケーションがレセプトのオンライン化になります。

近未来を考えると，「人・機器・コンテンツの認証」が次の課題になると予想されます。レセプトやカルテの開示を考えると，正当な人（間違えて他の人に見せたら大変ですから）が，安全な機器（出した途端に，例えばどこかにウィルスがあって，カルテの情報をばら撒いてしまうようなのも困るわけです）で，正しい情報（本人のカルテ情報でなければならないわけですから，そこを間違えて他の人というのもダメです）にアクセスできることが必要です。その意味で「正当な人が安全な機器で正しい情報にアクセス」できる環境を，このICTの技術を使ってどう実現するかが課題になると思います。従来は安全性と利便性というのは相反するものでした。例えば家の鍵を増やせば，安全性は増しますが，利便性は低下します。このように，物理的な空間では安全性と利便性は相反しています。ところが，電子的には両者を両立させる可能性があります。ですから，電子的な空間は，安全安心そして便利になることを徹底することが重要なのです。

少々中途半端な説明になってしまいましたが，医療分野の情報化が上手く進むためのさまざまな試みと施策を紹介しました。皆さま方のご協力をお願いいたします。

まとめ

- インターネットの安全性確保について
  - 相互認証と暗号通信の導入
  - 認証鍵の安全性確保 ⇒ Sチップの利用
- 医療分野の情報化について
  - 機微な個人情報の保護が不可欠
  - 医療関連機関間のネットワーク化とHPKIの導入
- 人・機器・コンテンツの認証について
  - 正当な人が安全な機器で正しい情報にアクセス
  - レセプトやカルテの開示、コンテンツ流通などに有効

スライド42

多機能 IC チップを利用したネットワークサービスにおける暗号技術の更新とサービスの継続利用の実現

Study on updating cryptographic mechanism on an apparatus with multi functional IC chip for cryptographic functions and continuity of the service for network connected apparatuses

押田知己[*1]　谷内田益義[*1]　鈴木裕之[*1]　小尾高史[*2]　山口雅浩[*1]　大山永昭[*1]
Tomoki Oshida, Masuyoshi Yachida, Hiroyuki Suzuki, Takashi Obi, Masahiro Ymaguchi, and Nagaaki Ohyama

東京工業大像情報工学研究施設[*1]
Imaging Science and Engineering Laboratory, Tokyo Institute of Technology

東京工業大学総合理工学研究科[*2]
Interdisciplinary Graduate School of Science and Engineering , Tokyo Institute of Technology

1．はじめに

現在、様々なシステムで用いられている暗号の強度が弱くなる、いわゆる危殆化が問題となることが想定されている。システムで用いられる暗号が近い将来危殆化するという予測がなされた場合、使用している暗号を安全性の高いものに更新する必要がある。しかし、現在の殆どのシステムでは使用している暗号方式の更新を想定して構築されていない。このため全体の安全性を低下させることなく新たな暗号方式に移行可能なシステム構築を考慮する必要がある。

本研究では、多機能 IC チップを利用しインターネット等のオープンな環境において安全に鍵配送を実現するネットワーク基盤である Secure e-Key Network（SeKNW）を対象として、機器に内蔵された多機能 IC チップの暗号方式の安全な更新について検討した。

具体的にはコンテンツ配信サービスを想定した応用を検討し、継続したサービス提供の可能性を検討するとともに、実験システムによりその実現可能性を検証した。

2．課題

本研究で対象とする機器には、認証等で利用する鍵などの暗号情報を格納するための多機能 IC チップが利用者端末内に取り外せない形で内蔵される。このため、認証機能で用いる暗号方式の変更が必要となった場合には、IC チップ内の暗号方式の更新も必要となる。その際には通信路上の安全性や成りすまし対策、更新する暗号ライブラリの正当性の保証といった問題以外に、機器毎に搭載する IC チップの性能が異なり新たな暗号ライブラリをモジュールとして追加可能なものと不可能なものが混在するという問題が想定される。機器毎に使用する暗号方式が異なる状況では、サービスの継続性やシステム全体の整合性を確保するための移行計画を立案する必要がある。

3. 暗号方式の更新

想定するシステム全体を新たな暗号方式へ安全に移行するために考慮しなければならない利用者端末の特性を以下に挙げる。

・　オンライン状況

機器のネットワークへの接続状況によって、更新を行うタイミングは異なってくる。STB などの常時オンラインを前提とした機器であるのか、PDA のようなモバイル端末などの常時オンラインを前提としない機器であるのかによってそれぞれ対応する必要がある。

・　多機能 IC チップに対する機能拡張が可能かどうか

チップ内の暗号機能を更新するためには、拡張用ライブラリの追加やあらかじめ移行用の暗号ライブラリを予備として備えておく等の機能が IC チップに必要となる。しかし、製造コストの面からこういった機能を有しないチップを搭載した機器が流通することも考えられる。

本研究では、表 1 のような移行パターンを想定し、公開鍵証明書の有効期間を考慮した移行スケジュールと移行方法をパターン毎に検討することで上記課題の解決を図った。

表 1：移行パターンの分類

	常時オンライン可能	常時オンライン不可能
チップ機能の拡張が可能	移行パターン①	移行パターン②
チップ機能の拡張が不可能	移行パターン③	移行パターン④

4. 実験システム

実験システムでは、利用権管理者によって IC チップ内の利用権管理機能の暗号方式を新たなものへ移行させ、新たな暗号方式によって認証とサービス（コンテンツ配信）を利用する部分を実装し検証を行った。

実験環境では暗号強度を切り替えることにより、利用権管理機能の認証、コンテンツの復号化等に用いる暗号方式の移行が行えることを確認した。

5. まとめ

本研究では、対象とする認証基盤で用いる暗号方式を新たなものに移行し、その上で提供されるコンテンツ配信サービスにおいてもコンテンツを新たな暗号方式に移行し保護することで利用者が継続的にサービスを利用できることを示した。さらに、提案モデルの一例を検証システムとして構築し、その有効性を示した。

参考文献

[1]　小尾，他：“オープンなネットワーク環境で安全な鍵配送を実現するネットワーク基盤”，電気情報通信学会 2004 総合大会予稿集，2004 年 3 月

[2]　独立行政法人 情報処理推進機構：“暗号の危殆化に関する調査報告書”，2005 年 3 月

多機能 IC チップを利用した任意多地点間 VPN における通信主体情報の秘匿

Privacy enhancement in the On-demand VPN that used a many functions IC chip

浦野雄平*　小尾高史**　大山永昭*　谷内田益義*　鈴木裕之*
Yuhei Urano*　Takashi Obi**　Nagaaki Ohyama*　Masuyoshi Yachida*　Hiroyuki Suzuki*
*東京工業大学 像情報工学研究施設, **東京工業大学 総合理工学研究科
* Imag. Sci, and Engineer. Lab., **Interdisciplinary Grad. School of Sci.and Engineer. , Tokyo Inst. of Tech.

1．はじめに

近年、インターネットを専用線と同様に利用する VPN サービスが大きな広がりを見せている。そして、現在、多機能 IC チップを搭載したルータを使用して、安全かつ動的な接続が可能なオンデマンド VPN[1]についての研究開発が行われている。ここで、多企業間における研究開発など、通信内容だけでなく、どのような組織間で通信が行われているかを秘匿したいという要求存在するが、現状のオンデマンド VPN は、一般的な VPN と同様に通信主体の匿名性を有しないため、このような用途に用いることができない。本研究では、中継ノードを用いたオンデマンド VPN における通信主体の匿名化手法の提案を行う

2．従来のオンデマンド VPN 通信

オンデマンド VPN では、暗号化プロトコルとして、IPsec を用いている。IPsec は第三層のプロトコルであり、通信パケットのヘッダを覗き見する事による通信主体の特定は容易であるため、通信主体の匿名性を有しない。

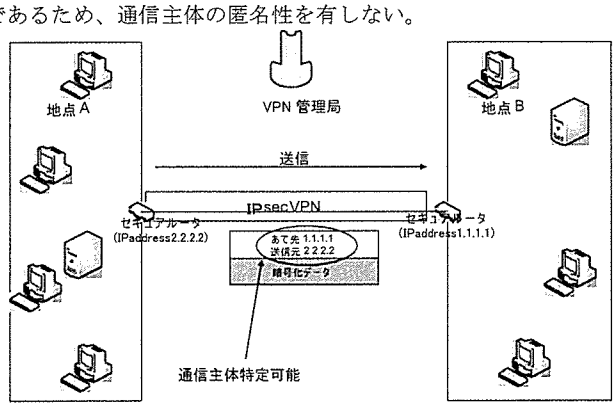


図１：現状のオンデマンド VPN

3．中継ノードを用いたオンデマンドＶＰＮ匿名通信手法

一般に、第３者を中継ノードとして用いることで、間接的な通信を行い、通信パケットのヘッダを覗き見することによる通信主体の特定を防ぐ方法がとられることが多い。しかし、中継ノードを置くだけでは、トラフィック解析の脅威、中継ノードの前後におけるパケット内容の関連付けには対応できない。そこで、提案手法では、トラフィック解析の脅威に対して、中継ノードを多数用意し、その中から使用する中継ノードをランダムに選択する事で対応し、また、選ばれた中継ノード前後でのパケットの関連付けを防ぐ為に、通信を行う２者と中継ノード間で異なるオンデマンド VPN セッションを構築する。そして、通信路上での通信の機密性を保つ為に、上記オンデマンド VPN セッションで、通信主体間のオンデマンド VPN セッションをカプセル化する。これらの方法は、オンデマンド VPN の動的な VPN 構築能力により可能となる。これにより、提案手法でオンデマンド VPN において、安全な匿名通信が実現できる。また、提案手法は、従来の匿名化手法であるオニオンルーティングや、Mix-net に対して、使用プロトコルに制限がない、中継ノードの信頼性があるという点において優位である。

以下に、提案手法による具体的な通信手順を示す。

提案システム通信手順：

① 地点 A のセキュアルータ A2 が匿名通信管理局に地点 B との匿名通信開設要求
② 匿名通信管理局において、地点 A と地点 B が匿名通信サービスを受けられるかを照合。中継ノードとして C を選択
③ 匿名通信管理局から VPN 管理局に A1、A2、B 1、B2、C の匿名通信用 SPD、ルーティングテーブル構成情報配信要求
④ 匿名通信管理局からセキュアルータ A1、B1 に C のアドレスとオンデマンド VPN 開設要求を送信
⑤ A1—C 間でのオンデマンド VPN 設立（A1－C 間でのトンネル成立）
⑥ C—B1 間でのオンデマンド VPN 設立（C－B1 間でのトンネル成立）
⑦ A1、B1 から匿名管理局に VPN 開設完了通知
⑧ 匿名通信管理局からセキュアルータ A1、B1 にオンデマンド VPN 開設要求
⑨ A2—B1 間でオンデマンド VPN 設立（A1－C 間、C－B1 間のトンネルを通す）

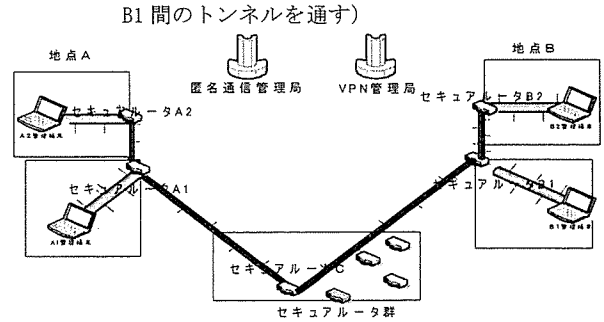


図２：提案システム図

4．実装・評価

提案システムを構築し、途中点（中継ノードの前後、セキュアルータ A2 と A1 の間、B2 と B1 の間の計４点）で、パケットをキャプチャする。そしてそれらのパケット内容による通信主体の関連付けが困難である事を確認した。

5．参考文献

[1] 高橋成文，東川淳紀，山本修一郎，小尾高史，谷内田益義，大山永昭：「２階層 PKI を用いたオンデマンド VPN システム」，情報処理学会論文誌 Vol.46 No.5 1129-1136 ページ（2005 年 5 月）

特集1 遠隔画像診断の現況そして未来

Part 1 遠隔画像診断の現状と課題

遠隔画像診断のセキュリティと個人情報保護

東京大学大学院情報学環
山本隆一

遠隔画像診断のセキュリティ

遠隔画像診断はデジタル撮影された、またはデジタル化された画像情報をネットワークを介して遠隔地で診断することで、情報の安全管理という面では2つの組織と介在するネットワークにわけて考えなければならない。厚生労働省は平成17年3月に医療情報システムの安全管理に関するガイドラインを公表して、各医療機関に準拠を求めている。このガイドラインは主に施設内で運用される医療情報システムに関するものであり、外部との情報交換についても簡単な記載ではあるが、指針を示している。具体的には6章の9項で、(1)回線上では適切な暗号化を行い秘匿性を保つ、(2)回線の起点・終点の識別のための認証を行い、(3)リモートログインを制限する機能を持つこと、という3つの条件が示されている。(3)は機器を外部からオンラインでメインテナンスを行う際などに必要になる要件で、遠隔画像診断では(1)、(2)を確保しなければならない。いくつかの場合にわけてやや詳しく述べる。

ISDN

都会では今更の感があるISDNではあるが、わが国にはまだ比較的広い範囲のBroadband 0地帯、すなわち光ファイバーもADSLも利用できないところがある。ISDNは1対1で対向で接続されるので、電話番号さえ間違わなければ起点・終点の識別は問題ない。したがって暗号化さえしておけば大きな問題はない。むしろ回線速度が遠隔画像診断の質を制限することが問題であろう。

IP-VPN

インターネットではなくて、回線プロバイダが仮想専用回線として提供するもので、比較的大規模な情報共有基盤を作るのによく使われる。一般に高速で、DICOMサーバに直接書き込んで遠隔画像診断を行うことも可能である。専用回線と同じ感覚で使用できるので、2施設だけが接続されるのであれば起点・終点の識別は問題ないが、2施設だけでIP-VPNを用いるのは経費の面からも一般的ではない。通常は県域などの一定の範囲で複数の施設が接続される。もともと暗号化されたネットワークであるVPNなので、経路の秘匿性は問題ないが、起点・終点の識別はIP-VPNの機能としてはないので正しく行う必要がある。具体的にはアクセスする際に、正しく管理されたID・パスワードなどで不要なアクセスをさける必要がある。またIP-VPNはいわば広域に広がったLANを形成するような仕組みで、たとえば10施設が接続されている場合、そのうちの1施設がルーズな管理をすると、他の施設にも安全性の問題が生じる可能性がある。参加施設のすべてで共通の方針で安全管理を行わなければならない。

Internet-VPN

Broad Bandの使えるところではこの方法がもっとも安価で、正しく用いれば安全管理上も問題はない。しかし一般にはIP-VPNと同様の注意が必要である。最近は機器や利用者認証機能を備え、理論的には1対1接続を行うInternet-VPNサービスも出現しており、この方法を用いれば多少初期経費はかさむがそれぞれの施設の運用上の負担は軽くなる。

遠隔画像診断と個人情報保護

2005年に個人情報保護法が全面施行され、医療でもプライバシーがクローズアップされたが、プライバシーはプライベートとは似て非なる権利概念で、19世紀末に大衆新聞の出現ではじめて問題になり、20世紀後半にコンピュータとネットワークの急速な発達であらためて問題になった。つまり情報技術の進歩と密接に関連した権利であり、情報の価値や利活用手段が対話や手紙などの効率が悪く使い勝手の悪い情報伝達手段が主体であった時代では大きな問題にはならなかった概念である。対話と紙の記録という旧来の医療においては我々医療従事者は厳しい守秘義務とヒポクラテスの誓いからリスボン宣言にいたる医療倫理によ

って患者様の権利を保護し、概ね成功してきた。情報が電子化されても患者様の権利の保護のあり方が変わるはずもなく、今後もその保護に成功する必要があるし、そのことに異論はないであろう。遠隔画像診断には新たな留意点も生じる。

紙の紹介状は本人が持参することがほとんどで、フィルムもそうであった。しかし遠隔画像診断では本人と情報は乖離して他施設に送られる。わが国の個人情報保護法では他の事業者に情報を提供することに関して、かなり厳しく規制している。

委託と第三者提供

遠隔画像診断で個人情報である画像情報を診断施設に提供することになるが、個人情報保護法から見れば2つの異なる提供がある。一つは委託であり、これはあらかじめ契約した機関に本来の業務を行うために個人情報を提供するが、個人情報の管理はもともとの施設が最後まで責任を負わなければならない。検体検査を外注している場合がこの典型である。患者様の受診している施設は、委託先の施設と個人情報保護に関する契約を結び、適切に監督する義務がある。その代わり、委託先に情報を提供するにあたって患者様の同意は必要ない。

一方で第三者提供は提供した情報は相手先に管理をゆだねるもので、提供元は提供が完了した時点で提供先での情報管理に関する責任はなくなる。紹介状がこの典型である。第三者提供は患者様の同意が必要である。ただ、紹介、逆紹介や、遠隔画像診断に代表されるコンサルティングは一般には医療では必須の第三者提供とされており、黙示の同意、すなわち、掲示物等でそのような第三者提供が行われることがあること、それに対していつでも非同意の意志を示すことができることを明記した上で、患者様が非同意の意志を示さなければ同意が得られていると見なして差し支えない。つまり遠隔画像診断において同意を得るという意味では大部分の患者様では委託も第三者提供も大きな違いはない。しかし、一方では提供元の施設に管理責任があり、一方では提供先の施設に管理責任がある点はしっかりと理解して選択する必要がある。

委託契約の場合の留意点

委託契約では、情報の管理責任は委託元にある。管理責任を果たすためには一般には個人情報保護に関する事項を含めた契約を交わし、委託元が個人情報保護に関して監督をすることになる。契約内容は具体的には安全管理に努め、委託元で患者様に提示した利用目的の範囲内で使用し、当該個人情報を保持する間は定期的に委託元に管理状況を報告することがなどが含まれる。委託元は報告を受け、問題があれば適切に対処しなければならない。委託の場合、一般的には診断を行う施設では診断および報告に必要な期間だけ保持し、その後、破棄するか連結不可能な匿名化をしなければならない。連結不可能な匿名化とは完全な匿名化で、たとえば画像に独自の番号を振り、別にその番号と個人情報の対応表を保持することは含まれない。

継続して遠隔画像診断を行う場合は、画像を保存し、過去の画像として将来の診断で参照することが多いが、委託契約では当該画像の診断が終了した後の保存は慎重でなければならない。委託元から診断の都度、過去の画像も含めて送付するほうが問題がない。

第三者提供（紹介）契約の場合の留意点

この場合は、診断施設は独立した施設としてあらためて個人情報を収集することになる。したがって診断施設は利用目的を示すか公表しなければならない。また苦情の申し出先なども明示する必要がある。さらに長期間保持する場合は開示や利用の停止の手続きを定めて、明示する必要がある。遠隔画像診断の場合、患者様が診断施設にこられないことがほとんどなので、一般の医療機関のように掲示物を施設内に置くことでは明示にも公表にもならない。ホームページ等で公表しておくことに加えて、可能であれば受診医療機関で患者様にパンフレットのような形態で個別に示す。委託契約と違って利用目的の範囲内であれば診断施設が画像を保持し続けることは、安全に管理していれば、本人から利用の停止の申し出がない限り個人情報保護法上の問題はない。また提供元の立場から見れば黙示の同意の上で提供している限り、提供先の画像情報に対する管理責任はない。

終わりに

安全や個人情報保護は結果的に達成できることも重要であるが、それはいわば当たり前の大前提であり、事故が起きないこと、プライバシーが侵害されないことを事前に説明できることが求められている。遠隔画像診断ではネットワークのセキュリティ確保の方法や個人情報保護法上の取扱いに複数の方法が存在する。それらを当事者すべてがただしく認識する必要がある、我々医療従事者は診断の精度を上げ、患者様にとってもっとも良いと思われる方法をとっているのであるが、患者様からみて一体感のある対応が行われてはじめて安心感のある医療につながるといえる。遠隔画像診断自体はこれからの連携医療でおおいに推進していくべきことであるが、誤解や不安を与えないために最低限の努力は必要であろう。

電子カルテとプライバシー保護

山本隆一*

1. プライバシーは電子化情報でこそ問題になる

2005年に個人情報保護法が施行され，医療でもプライバシーがクローズアップされるようになったが，プライバシーはプライベートとは似て非なる権利概念で，19世紀末に大衆新聞の出現で初めて問題になり，20世紀後半にコンピュータとネットワークの急速な発達で改めて問題になった．つまり情報技術の進歩と密接に関連した権利であり，情報の価値や利活用手段が，対話や手紙などの効率が悪く使い勝手の悪い情報伝達が主体であった時代には，大きな問題にはならなかった概念である．

対話と紙の記録という旧来の医療においてわれわれ医療従事者は，厳しい守秘義務とヒポクラテスの誓いからリスボン宣言に至る医療倫理によって患者の権利を保護し，おおむね成功してきた．情報が電子化されても患者の権利の保護のあり方が変わるはずもなく，今後もその保護に成功する必要があるし，そのことに異論はないであろう．しかし診療情報の電子化は患者の権利保護において2つの点で問題になる．

2. 安全管理—パラダイムシフト？

最初に明記しておきたいが，電子カルテの安全管理は決して難しいものではない．医療従事者のインテリジェンスをもって当たれば簡単とさえいえる．しかし，紙のカルテの安全管理とは全く違う対策が必要になる．つまり発想を変えなくてはならない．馬と駕籠と徒歩しかなかった江戸時代の街道の安全管理と，現在の都市の道路の安全管理は全く異なるのと同じである．

個人情報保護法への対策には過剰反応も過少反応もあったが，過少反応の代表が電子化情報の安全管理で，PCやUSBメモリの紛失事故は後を絶たない．この程度の安全管理が医療従事者にできないとは思われないが，PCやUSBメモリの紛失が診療所に厳重に保管されているカルテの紛失と同じことであるという認識が不足しているのではないだろうか．

本稿で個々の対策を述べることはできないが，厚生労働省もガイドラインを公表しており[1]，電子カルテの使用に当たっては初心に返って安全管理に当たる必要がある．

3. 利活用の高度化—自己情報のコントロール

紙にボールペンで書かれた情報は，書き写すか複写機でコピーするぐらいしか再利用の方法はない．しかし電子化情報は加工が容易で簡単にいくらでもコピーできる．コピーという動作を意識することさえない場合がある．これは重要な診療情報を最大限に活用するという意味では大変すばらしい利点といえる．しかし，容易さはしばしば安易さにつながり，情報取得時の利用目的を外れて利用することになってはプライバシーの侵害になりかねない．

電子化情報の利活用に当たっては患者に通知した利用目的の範囲内であるか，そのことを説明できるか，という点に留意する必要がある．仮にあらかじめ通知した利用目的の範囲外の利用である場合は，匿名化をしなければならない．幸い，電子化診療情報は匿名化が紙に比べれば容易であるが，単に姓名を消すだけでは，少し努力すれば本人が特定できる場合もあり，実効ある匿名化に注意する必要がある．

文　献

1) 医療情報システムの安全管理に関するガイドライン（平成17年3月），厚生労働省（http://www.mhlw.go.jp/shingi/2005/03/s0331-8.html）．

*やまもと・りゅういち：東京大学大学院情報学環助教授．昭和54年大阪医科大学卒業．主研究領域／医療情報学（個人情報保護，電子カルテ，セキュリティー）．

健康管理を支援する情報技術
健康情報化研究会
共催　日本健康科学学会

八幡 勝也[1)]　稲田 紘[2)]　梅田 勝[3)]　吉田 勝美[4)]　片山 文善[5)]　大江 和彦[6)]
名和 肇[7)]

ヒューマンメディア財団[1)]　兵庫県立大学大学院応用情報科学研究科[2)]
厚生労働省健康局[3)]　聖マリアンナ医科大学予防医学[4)]　ネクストウェア[5)]
東京大学病院中央医療情報部[6)]　東京医科大学[7)]

Information Technologies for supporting Healthcare

Yahata Katsuya[1)] Inada Hiroshi[2)] Umeda Masaru[3)] Yoshida Katsumi[4)]
Katayama Humiyoshi[5)] Ohe Kazuhiko[6)] Nawa Hajime[7)]

Humanmedia Creation Center / Kyushu[1)]
Graduate School of Applied Informatics, University of Hyogo[2)] Health Service Bureau[3)]
Department of Preventive Medicine, St. Marianna University School of Medicine[4)]
Nextware Ltd.[5)]
Department of Medical Informatics and Economics, Graduate School of Medicine, The University of Tokyo[6)]
TOKYO MEDICAL UNIVERSITY[7)]

In promoting preventive medicine, it pays attention to the digitization of the health information. Therefore there are some subjects. A health information meeting was started on JAMI, and act to solve some problems in this field.
This time, discuss it about the subject and the action to solve them in cooperation with the Japan Society of Health Sciences.

Keywords: Metsbolic Syndrome, Health Examination, Information Technologies

1. はじめに

予防医療や生涯にわたる健康管理の重要性については、以前から認識され旧労働省のTHP(Total Health Promotion)などの活動が行われていたが、所属による制度の違いや標準的管理手法の提案が遅れたため普及が遅れている。
しかし、平成17年度より、メタボリックシンドロームへの対応などを目的として厚生労働省も「標準的な健診・保健指導の在り方に関する検討会」を通じて生涯にわたる健康情報管理を検討している。その中では健康情報をデジタル化して取り扱うことで、適切な支援が効率よく行われることが期待されている。
健康情報を適切な取り扱うためには、以下の事項の整備が必要である。

・健診項目の標準化・コード化
・健診項目の基準値の標準化
・データの精度管理
・制度の違いによるデータ取り扱いの違いの整理
・データを解析利用するための精度管理
・データ利用のための倫理規定、認証方法

この様に多方面からのアプローチが必要である。本企画では行政の取り組みを中心に健康管理の推進のためにデジタル技術ではどのような事を決定し、支援していくかについて検討する。

2. プログラム

座長:名和 肇(東京医科大学:日本健康科学学会)
　　八幡勝也(ヒューマンメディア財団)

プロローグ:
・課題研究会と本セッションの意義について
　稲田　紘(兵庫県立大学大学院応用情報科学研究科)

・基調講演:「ITによる医療の構造改革
個人健康情報の生涯を通じての活用のために」
　梅田　勝(厚生労働省健康局前大臣官房参事官)

講演
(1)「健診情報のデータ管理」
　大江　和彦(東京大学病院中央医療情報部)

(2)「国民の保健医療の質を確保する情報支援」
　吉田　勝美(聖マリアンナ医科大学)

(3)「保健指導支援情報システムの構築と使用」
　片山　文善(ネクストウェア(株))

・総合討論

総説

医療分野におけるOpen Source Software活用の現状と問題点

小林慎治[*1]　八幡勝也[*2]　宮司正道[*3]　岡田昌史[*4]
中原孝洋[*5]　石原　謙[*6]

オープンソースソフトウェア（OSS；Open Source Software）は近年の情報技術の発展に貢献してきた．その多くはボランティアベースで開発されてきたが，現在では商用利用を前提として企業が主体となり開発される事例も少なくない．医療分野においてもOSSが活用される事例が増えており，コスト低減などの効果に期待が寄せられている．欧米では，1970年代から医療分野におけるOSSの応用が進められている．日本においては，日本医師会主導で医療における情報基盤をOSSとして開発するというORCAプロジェクトが注目されている．しかし，医療標準規格のライセンスがOSSライセンスと矛盾するため使用できないといった問題もある．今後，医療分野へのOSS活用を推進するためには，これらの規制を緩和していく必要がある．

■キーワード：オープンソースソフトウェア，バザールモデル，インターネット，オープンソースソフトウェアライセンス，標準化

Current Review of Open Source Software in Medicine : Kobayashi S[*1], Yahata K[*2], Goudge M[*3], Okada M[*4], Nakahara T[*5], Ishihara K[*6]

Open Source Software(OSS) has driven the revolution of information technology. Although, most of the OSSs have been developed by volunteer community, some commercial companies recently tend to proceed development of open source software for commercial use.

OSS has now been utilized in medicine. It is anticipated that has effect to cut off the high cost of medical infomation system. The development history of OSS in medicine starts from 1970 in the world. In Japan, Japan medical association has promoted their information infrastructure as OSS in the ORCA project.

Nevertheless, there are much problem on the medical use of OSS, such as medical standard license is not compatible for OSS license. For the promotion of OSS in medicine, we must going on a deregulation program on medical informatics, and contribute not only in medical use but also in a whole OSS community as a member.

Key words : Open source software, Bazaar model, Internet, Open source software license, Medical standard

[*1] 九州大学病院外来化学療法室
[*2] ヒューマンメディア財団
[*3] 医療法人財団明理会新松戸中央総合病院内科
[*4] 筑波大学人間総合科学研究科社会医学系疫学
[*5] 九州歯科大学総合教育学分野
[*6] 愛媛大学医学部医療情報部
〒812-8582　福岡市東区馬出3-1-1
E-mail : skoba@intmed1.med.kyushu-u.ac.jp
受付日：2005年11月28日

[*1] Outpatient Chemotherapy Unit of Kyushu University Hospital
[*2] Human-Media Creation Center/Kyushu
[*3] Shinmatsudo Central General Hospital
[*4] Graduate School of Comprehensive Human Sciences, University of Tsukuba
[*5] General Education, Kyushu Dental College
[*6] Medical Informatics, Ehime University
3-1-1 Maidashi, Higashi-ku, Fukuoka, 812-8582, Japan

図 1　Web server ソフトウェアのシェア [1)]

表 1　代表的な OSS 開発プロジェクト

名称	種類	URL
Linux kernel	OS kernel	http : //www.kernel.org/
FreeBSD	OS environment	http : //www.FreeBSD.org/
BIND	Berkley Internet Name Daemon	http : //www.isc.org/
sendmail	SMTP server	http : //www.sendmail.org/
Apache	Web server and its peripherals	http : //www.apache.org/
GCC	GNU Compiler Collection	http : //gcc.gnu.org/
Perl	Script language	http : //www.perl.org/
Ruby	Object oriented script language	http : //www.ruby-lang.org/
Vim	Improved VI clone	http : //www.vim.org/
Emacs	Editor, Lisp environment	http : //www.gnu.org/softwatre/emacs/
PostgreSQL	Relational database management system	http : //www.postgresql.org/
MySQL	Relational database management system	http : //www.mysql.com/
JBoss	Java2 enterprise edition container	http : //www.jboss.com/
X Window System	Graphical engine and windowing environment	http : //www.X.org/
OpenOffice. org	Office suites	http : //www.openoffice.org/

1. はじめに

ソフトウェア開発において OSS を活用し，開発効率を向上させコストを低減していくことはいまや常識となりつつある．普及が進んでいるとされる OSS であるが，その性質上，流通を直接把握することができないため，正確な導入実数を商用ソフトウェアと比較検討することは困難である．しかし，Netcraft 社による調査では，Web server のシェアで OSS である Apache が約 70% を占めていて，事実上の標準となっている（図 1）[1)]．これは，OSS の普及を示唆する一つの証拠であるといえる．

OSS 運動（Open Source Software Movement）は 2000 年前後より世界的に活況を呈しており，開発プロジェクトも日々増加している．OSS の開発を支援するサイト SourceForge[2)] に登録されている OSS プロジェクトは既に 10 万を超えており，そこに登録している開発者も 100 万人を超えている．SourceForge に登録していない OSS プロジェクトや開発者もいるため，実数はそれよりも多いと考えると少なくとも OSS に関心を持

つ開発者人口は世界中で数百万にものぼると考えられる．OSS 開発の対象は OS の kernel やインターネットサーバソフトウェア，コンピュータ言語やエディタ，データベース，Window システムからオフィススイートに至るまで多岐にわたっている（表 1）．

OSS は主にボランティアベースで開発が進められていることや，利用に際して原則として無保証であることから，安全性や可用性について疑問視されることもあった．しかし，近年では大規模システムや基幹システムにも OSS を導入する事例も増えている．ソースコードを隠蔽したソフトウェアよりもむしろ，ソースコードが公開されていることで，より多数の開発者がソースコードを検証できるため，品質が向上するとされている[3]．その傍証として，Linux kernel のソースコードを解析した結果，一般的な商用ソフトウェアでみられる頻度よりもバグが少ないという報告[4]や商用の Unix ソフトウェアと比較して OSS 由来のツールの方が可用性や信頼性が高いという報告がある[5,6]．さらに，セキュリティバグに対する修正パッチのリリースが商用ソフトウェアよりも OSS の方が早いという調査結果もある[7]．OSS の利用は原則として自己責任，無保証ではあるが，現在は有償でビジネス用途で利用される OSS についてサポートを行う会社も多数あり，サポート面での不安は解消されつつある．

OSS はソースコードが公開されていることから，いわゆる「車輪の再発明」を避けることができ，効率のよい開発を行うことができるとされる．近年のインターネットビジネスにおいては，提案から実現までのスピードが何よりも価値を生み出すことから，低コスト，短納期でのソフトウェア開発を実現するため，OSS の積極的活用が進められている．このような分野では従来ではメインフレームが必要とされていた高負荷条件で安定運用が要求されるような場面でも，OSS が利用されている．従来，商用ソフトウェアの独壇場であった中規模から大規模システムにおいても OSS が利用されており，基幹業務システムの構築において OSS を利用することでコスト低減などの効果があったという報告がなされている[8]．なにより，OSS には特定のベンダーが持つ技術に拘束されるベンダーロックインを回避し，ユーザーがより強い交渉権を持てるという魅力がある．

前述の SourceForge には 168 の “medical” に関連したプロジェクトが登録されている（2005 年 5 月現在）．日本では 2000 年に日本医師会が中心となり，OSS での医事会計システム開発を中核とする ORCA Project[9] を発足させ，現在は普及期に入っている．

このような状況を踏まえて，医療分野においても OSS の導入が積極的に試みられるようになってきた．さまざまな成果があげられている一方で，問題が生じているケースもある．そこで本稿では，OSS に関して概説を行うとともに，医療情報システムの問題点と医療分野での OSS 開発に関する問題点について相互に考察を試みる．

2. OSS 概論

まず，OSS についてその成立過程とその定義，そして OSS ライセンスについて概説する．OSS の歴史は現在も進行しているのであり，その定義やライセンスポリシーについては常に議論の中心であり変遷している．したがって，以下の内容は 2005 年現在のものであり，今後変更されることもあることを了承いただきたい．

1) OSS 小史

ソフトウェアが，ハードウェアの付属物であった 1960 年代には，すべてのソースコードは開発者や研究者の間で共有されていたとされる．1969 年に Ken Thompson と Dennis Ritchie らによってベル研究所で開発された Unix は，優れた OS（Operating System）として人気を集めた．その理由の一つとして誰でも自由にソースコードを参照して，状況に応じて改変することができたことがあったとされている．

しかし，1980 年代に商用ライセンスの元，Unix はソースコードが非公開となった．そのソースコードを利用するには高額のライセンス料を支払わなくてはならなくなった上に制約も多くなった．これが，1980 年代に Richard Stallman を中心として Free Software 運動が起こる契機となった[10,12]．ここでいう “Free” とは，「無料」という

意味ではなく，制限のない「自由」な状態を意味している[13]．彼らが推進している GNU Project（GNU ; GNU is Not Unix の略とされる）は，彼らが提唱する "GNU General Public License"（GNU GPL ; GNU 一般許諾契約）[14] に基づき，Unix 互換の自由な OS 環境を実現することにある．

GNU Project はコンパイラやライブラリ，エディタなど優れた成果物を生み出してきたが，OS の kernel だけは実装が遅れていた．Unix のライセンスを所有していた AT&T 社と 1980 年代より独自の Unix 互換環境を実装して配布していた BSD（Birkley Software Distribution）との間の泥沼の法廷闘争は 1993 年まで続き，混乱と停滞が生じていた．それを補完するかのように 1991 年に Unix 互換の教育用環境 Minix を参考にした Unix 互換 kernel が Linus Torvals により発表されると，当時普及しはじめた Internet を通じて衆目を集めることとなった．Linux と名付けられたこの Unix 互換 kernel は短期間のうちに飛躍的な進歩を遂げ，現在も進化し続けている．

1995年にEric Raymond が "The Cathedral and the Bazaar"（邦題「伽藍とバザール」）[3] という小論文にて，Linux kernel において短期間で高品質なソフトウェア開発を成し遂げた背景とその手法を考察している．Linux の開発モデルは，従来行われてきた階層的な組織のもとで厳密な設計書や仕様書に基づいて進められてきたソフトウェア開発モデル（伽藍モデル）とは全く異なり，インターネットを介したコミュニティにより同時多発的に行われている．伽藍モデルに対して，一見無秩序に見えるこの開発モデルを彼はバザールモデルと名付けた．バザールモデルでは，多様なアイデアや実装の中から優れたものが広く普及していくという進化論的な発展が大きな力を生み出している．このバザールモデルがソフトウェア開発をいかに強力に推進するかを自ら fetchmail というソフト開発プロジェクトをバザールモデルで立ち上げることにより証明している．1998 年に Bruce Perens と Eric Raymond は商用利用も視野に入れて，ソースコードの改編と再配布を許諾したこの「自由な」ソフトウェアを Open Source Software として再定義[15] し，用語として定着させていくこととした．これは Free software 運動が教条的に過ぎるという批判に基づくものでもある[16]．以後，OSS はインターネットを支えるソフトウェアとして開発が進められると同時に，インターネットを介して流通し，開発コミュニティも拡大している．インターネットを拡大すると同時に自らも拡大するという好循環により OSS は発展を続けている．多様なシステムを相互接続する Internet において，参考となる実装例がソースコードレベルで公開されていることが，プロトコルの標準化に関する何よりも詳細な仕様書であり，Internet の進歩に重要であったとされる．2000 年前後には Yahoo や Amazon といった OSS を活用してサービスを提供するインターネットベンチャーが株式市場を席巻して話題となった[10]．IBM は Linux を中心とした OSS に 2001 年だけで約 1,200 億円を投資するなど大企業も積極的に OSS ビジネスに乗り出すようになった[17]．現在では名立たる大企業の多くが OSS 開発やサポートビジネスに取り組んでいる．このようにソフトウェア開発の手法として誕生した OSS 運動は，経済分野にもインパクトを与えている．

OSS 運動は，政治へも波及している．アジアおよびヨーロッパ諸国では，OSS のさらなる発展を促すため，政策による OSS 振興支援が行われている．日本でも 2002 年より情報処理推進機構を中心に OSS 開発および普及支援が開始された．日中韓共同による OSS フォーラムが結成されるなど，国境を超えた取り組みも行われている．欧米やアジアで OSS を振興する背景には米国産の商用ソフトウェアによる市場支配に対する安全保障という意図もあるとされる．経済基盤が脆弱な低開発諸国では商用ソフトウェアの高額なライセンスを支払うことができないため，代替として OSS の普及が進められているという切実な状況もある．

2) OSS ライセンス

よく誤解されているが OSS は PDS（Public Domain Software）ではない．PDS が著作権を放棄したソフトウェアであるのに対して，OSS は著作権者が自己の著作物が自由に流通されるために

表2 GPL incompatible OSS licenses[47]

Name	Reason
Original BSD License	advertising clause
Common Public License (CPL)	patent license requirement
Mozilla Public License (MPL)	cannot link GPL modules with MPL modules
	legally because of some complex restrictions
The PHP License	practical problems like original BSD license
Common Developmont and Distribution License (CDDL)	unfortunatelly they use term "intellectual property"

その著作権を行使している．したがって，OSSにおける「公開」や「自由」の範囲は各著作権者が定めるライセンスに限定されるものである．そもそも，著作権法では，他人の著作物を改編して再配布することは許されていない．つまり，ソースコードを単に「公開」するだけではOSSたりえず，オープンソースライセンスを伴ってはじめてOSSたりうるのである．なお，日本では著作者人格権を放棄することができないため，PDSとしてソフトウェアを公開することはできない．

また，OSSはソースコードの再配布に制限がなければ，配布のために実費を請求しても構わないとされている[18]．ソフトウェアの導入や使用法の解説，利用に際してのサポート料などの付加的サービスに関しては有償で行ってよいとされ，OSSビジネスはここに立脚しているものが多い．

Open Source Initiative（OSI）は，以下の10カ条に亘るOSSの定義[15]を示しており，その定義を満たすライセンスをOSSライセンスと認定している．この定義では，ソースコードの入手，改変，再配布が自由にできるようにライセンスを規定していることが求められている．この自由を実現するために，ライセンスが特定の領域や個人，集団に差別をしないこと，特定の製品やソフトウェアに限定したものではないこと，技術的に中立であることが求められている．

(1) Free redistribution
(2) Source code
(3) Derivered works
(4) Integrity of the author's source code
(5) No discrimination against persons of groups
(6) No discrimination against fields of endeavor
(7) Distribution of license
(8) License must not be specific to a product
(9) License must not be restrict other software
(10) License must be technology-neutral

この定義を満たす代表的なOSSライセンスとして，GNU GPLとBSDライセンス（およびその派生物）がある．GPLは改編，再配布した二次著作物やその機能を利用するソフトウェアに対してもGPLを適用することを義務づけていることが特徴である．一方，BSDライセンス[19]では原著作権者（古典的BSDライセンス[20]ではBarkley Software Distributionの広告も）を表示し，ライセンス文書を同時に配布すればよいという制約の少ないライセンスである．その他，IBMが策定したCPL(Common Public License)[21]やArtistic license[22]，MPL（Mozilla Public License)[23]などがOSIにより認定されたOSSライセンスである[24]．GPLに準拠したOSSは，その派生物もOSSでなくてはならないため，開発者や開発コミュニティに必ずフィードバックされることから開発者にとって最もインセンティブの高いライセンスである．GPLを採用しているOSSはSouceforge.netに登録されているプロジェクトの約43%を占めている[2]．

MPLやCPLはビジネス用途での使用を意識して作成されたライセンスであり，特許や知的財産権についても言及されている．しかし，そのため規定が複雑なものとなっており敬遠される傾向にある．

OSSはそれぞれのライセンスに従えば，自由にソフトウェアを改編・再配布することができる．しかし，そこで問題となるのが，ライセンスの異なるソフトウェアを組み合わせて使う場合である．独占的(proprietary)ライセンスのソフトウェアとGPLのソフトウェアとを組合せて利用することはできない．OSSライセンスであっても，それぞれのライセンスが矛盾を来たすことがあるの

表 3　OSS ライセンス違反事例

Product	Violation	Result
MP3 encoder/decoder	LAME(GPL) のソースコードを使用して販売	販売停止
Full text search tool	全文検索エンジン namazu(GPL) を組み込んで販売	販売停止．会社倒産
Broadband router	Linux kernel(GPL) を使用	不買運動の後ソースコード公開
Netfilter /firewall	iptables/ipchains(GPL) を流用	ドイツで敗訴
Medical accounting	GPL を改編したライセンスとその適用範囲が問題となる	ライセンスの範囲を明示
Printer driver	国際対応のため gettext(GPL) を盗用	事後の誠実な対応で好評価

で注意が必要である．特に GPL は他のライセンスとの衝突を起こすことが多いことで知られている（表 2）．

GPL に関しては商用利用が難しいと考えられていたが，GPL の例外規定を利用して GPL と商用ライセンスの 2 つのライセンスを選択できるようにしているものもある．商用サポートが必要な場合（ビジネス用途）や，関連するソフトウェアのソースコードを公開することができない場合には商用ライセンスを選択することもできる．一方で，開発コミュニティには GPL により最大限の自由とフィードバックが提供される．JBoss や MySQL はこのようなライセンス形態をとっている．

OSS ライセンスが法的有効性を持つ文書であるかに関しては議論があるが，OSS ライセンスが著作権に立脚したものである以上，ライセンス違反は著作権法に反することになると一般に解釈されている．ドイツで GPL の法的有効性について争われた裁判では，GPL 違反をした製品の出荷停止命令と GPL を遵守するように勧告がなされた[25]．このように OSS の普及に伴いライセンス違反が露呈する事例も増えており，コンプライアンスの悪い企業によるライセンス違反事例がインターネット掲示板等で糾弾される事例が頻発している[26]（表 3）．

ライセンス違反が発覚した後に，誠実な対応をしたことで評価を高める事例もあるため，違反の事実よりもむしろ開発者の姿勢が問題視されているといえる．

3. 医療情報システムの諸問題と OSS

医療分野への情報技術の導入は安全で効率のよい医療を提供すると期待され，各国で進められている．生体情報モニタ，生化学をはじめとした各種検査，放射線画像や薬剤管理，医事会計などの各部門システムと，それらを統合するオーダーエントリーシステムやいわゆる電子カルテに至る診療支援システムまでさまざまなシステムが開発されている．

一方，情報システムを導入することによる間接コストの増大も問題となっている．電子カルテの導入コストは 1 床あたり 80 ～ 120 万円かかるとされている．

日本医師会の試算では全国の病院に電子カルテを導入した場合にかかるコストは 10 年間で約 18 兆円としている[27]．この電子化コストを年間 30 兆円の日本の医療経済から支出することは事実上不可能であり，普及のためにはコストを低減させなければならない．OSS を活用することはコスト低減のための有力な手段の一つであると考えられている．

医療情報システムが高コストになる要因の一つに，各部門システム間の統合がある．システム間連携のために，さまざまな標準規格やコード体系が提案されている．しかし，代表的な医療情報分野での標準規格である HL-7 や MML はデータ形式を規定しているものの，システム間の通信手順を規定していない．

多様なシステム間の接続においては，通信手順の開発およびその検証作業に難渋し，膨大なコストがかかることが少なくない．多様なネットワークを相互に接続するインターネットの標準化に OSS が貢献したように，医療情報分野においても OSS は通信手順の標準化に貢献すると期待される．

日本においては医療情報システムは少数ベンダーによる寡占状態にある．その結果，競争が生

じ難い状況にあり,高コスト体質を助長している.診療情報は病院が所有するものでありながら,データを抽出して経営判断を行うこともできないデータロックイン問題や,内部がブラックボックスであるため他のベンダーのシステムに切替えることができないというベンダーロックイン問題も発生している.OSSは内部仕様が明らかであるため,このようにロックインされる状態を回避するために有効である[8].また,医療分野でのOSS資産が増えていけば,新規参入に関する障壁が少なくなる.寡占の解除により競争が活性化されれば,多様性が創出されることにもつながりうる.医療機関の業務形態は,さまざまであり独自の運用に基づいた開発が求められることも多く,コスト高の原因ともなっていた.しかし,提供されるシステムが多様化すれば,このような医療機関にも対応しうると期待される.

患者に関するプライバシーを扱う医療情報システムは,高度なセキュリティ要件を満たす必要がある.OSSは第三者によるコードレビューが可能であることから,より安全なシステムを構築することができるとされている[7].したがって,セキュリティが重視される医療分野では透明性と安全性を担保する手段としてOSSを積極的に利用するべきであると考える.

4. 国内外の動向

このように,医療分野においてもOSSを活用することは,有意義であり多大な期待が寄せれらている.医療分野でのOSSの誕生は,OSSという概念が成立する以前の1970年代にG.Oct BarnettがCOSTAR(COmputer-STored Ambulatory Record)のソースコードを無償配布した時点であるとされている[28].そのほか,欧米ではVistA[29]やFreeMed[30],OpenEMR[31]といった診療支援システムがOSSとして開発されている.OpenEMRは最も注目されているプロジェクトの一つであり,中小規模の病院を対象にIBMが導入支援サービスを提供している.LinuxMednews(http://www.linuxmednews.com/)というニュースサイトでは医療分野でのOSS活用について配信を行っており,一般からの投稿も受け付けている.2003年にはIMIA/AMIAでOSSに関するワーキンググループが結成されており[32],OSSに関する研究が医療情報学の一分野として認知されるに至っている.

日本国内では,やはり2000年の日医IT化宣言[33]とORCAプロジェクトが話題の中心となる.一般的にOSSの開発はエンジニアが主体となることが多いが,このプロジェクトでは医師会が中心となりプロジェクトを推進していることが特徴である.成果物をOSSと指定することで,特定のベンダーや技術に依存することなく,医師会会員にとって有益な情報基盤を形成しようとしている.

医療だけでなく,他の業種においてもこのような開発事例は少なく,先進的なプロジェクトとして評価されている.日医標準レセプトソフトはMONTSUQIと呼ばれるミドルウェアと100万行に亘るCOBOLソースからなるものであり,それらを0から開発し,成果物として公開している.このプロジェクトの派生物である,OpenCOBOLプロジェクト[34]は国際的な広がりを見せており現在も継続して開発されており,バージョンアップを重ねている.汎用機で培われたCOBOLソースをLinuxベースのPCにダウンサイジングして利用するなどの事例も報告されている[35].こうしたORCAプロジェクトの成果物と連携するソフトウェアについて研究・開発を進めようと2004年4月に有志により医療オープンソースソフトウェア協議会が発足し,第1回のセミナーが開催された.同年,日本医療情報学会では課題別研究会として医療オープンソースソフトウェア研究会を発足させた.

医学生物学分野では既にOSS運動は大きな潮流となっている.バイオインフォマティクス領域では,Perlをはじめとしたさまざまなコンピュータ言語に対応したバイオ研究用のライブラリがOSSとして整備されている.ヒトゲノム計画においてPerlは大きく貢献したとされ,その過程で生み出されたCGI.pmが広く一般にも利用されている[36].学術誌でも開発事例が多数報告されており,バイオインフォマティクス領域では生物学者が率先してOSS運動を展開している[37].バ

イオインフォマティクスから疫学，医学統計学に亘るデータサイエンスツールとして，強力な行列演算とグラフィックツールを兼ね備えたOSSの統計環境“R”[38]が広く利用されている．また，公衆衛生分野における調査とデータ収集の支援ツールをOSSとして開発しているNetEpiプロジェクトも注目を集めている[39]．数理学的解析においては計算過程やそのロジックに関する透明性が重要であることから，OSSは適していると考えられている[40]．

5. 医療OSSの問題点

このように，医療分野におけるOSS活用にはさまざまな効果が期待されており，一部では成功しつつある．しかし，解決すべき課題も多い．OSS開発を推進するバザールモデルでは，さまざまなアイデアや技術を持つ開発者が多数集まることで力を発揮する．有力なOSSプロジェクトは国際的な開発コミュニティが形成されている．一方で，医療においては制度が各国で異なるため，単に言語を翻訳するだけでは実用にならないこともあり，国境を超えて展開しているプロジェクトは少ない．しかし，医療画像に関しては言語や制度への依存度が低いことから国際的に利用されるソフトウェアもある[41~43]．現代の医療では，診察から検査，治療といった診療方式の差に国家間の差はあまりないため，国際的に共通のシステムを使うことは不可能ではない．共通利用できるシステムを中核として国際的なプロジェクトとして開発し，各国で差の大きい部分（会計システムなど）を切り分けて，連携部分を標準化していくことが，今後医療分野でOSSプロジェクトを国際展開する上で検討していく必要がある．

しかし，既存の医療標準規格には問題がある．規格そのものをパブリックドメインとしておきながら，実装や事業化においてはその規格を制定している団体に所属することが義務づけられているものが多い．日本においては，代表的な医療情報の標準規格であるHL-7とMMLは規格自体に著作権を主張し，再配布を認めていない上に，実装するにはそれぞれの団体の会員になるように義務づけている[44, 45]．この点がOSSの定義である再配布の自由と矛盾してしまうため，OSSとして実装して公開することができない．この状態には法律上の問題もある．日本の著作権法においては著作者人格権を放棄することができないため，そもそもパブリックドメインにすることはできない．さらに著作権法第10条ではコンピュータプログラムに著作権を認めているが，コンピュータ言語やその規格に著作権を認めていない．したがって，上記団体は日本の著作権法で認められていない権利を主張しているものである．したがって，HL-7とMMLには国内法に準拠した使用ライセンスを適用していただくべきであり，広く普及させていくためにも自由な開発を促すように利用条件を見直していただきたい．財団法人医療情報システム開発センターもまた，標準マスターの再配布を原則として認めていない[46]．同財団は税金を財源とする公的機関であり，公共の福祉のために成果物は広く国民に利用されるべきである．こうした方針はOSSを推進するという国の政策に矛盾している．

これまでは医療情報システムに関しては医療の独自性を根拠に制約や規制を設けることにより品質の高い医療情報システムを開発を促すという伽藍モデルに近いアプローチがなされてきた．しかし，医療情報システムの問題を解決するためにOSS活用を推進するためには，バザールモデルへ転換していかなければならない．OSS開発者が医療情報システムを手軽に開発ができるように規制を排除していくべきである．

これらの問題を解決し，医療情報分野でのOSS活用を推進していくことは，医療において低コストで信頼性の高いソフトウェアを供給し，広く医療一般に貢献するだけではなくOSS界全体にとっても有益な資産を増やしていくことになる．OSS界全体の資産が大きくなることにより，医療分野も恩恵を受けることができるという好循環につながりうる．そのためには，既存のOSSを医療分野のみで利用していくことだけを追求するのではなく，開発成果や運用事例を広く公開し，OSS界全体に貢献していく姿勢が重要であると考えられる．

6. まとめ

医療分野でのOSS活用には，開発費の低減を始め有益な効果が期待される．国際的なOSS運動の高まりのもと，医療分野においても積極的なOSS活用が進められている．しかし，医療標準規格のライセンスとの整合性やOSS全体での位置づけといった問題点もある．発展させていくためには医療のためだけという姿勢ではなく，広くOSS界全体に貢献していく必要がある．

参 考 文 献

1) Netcraft.Market Share for Top Servers Across All Domains August 1995-May 2005.http：//news.netcraft.com/archives/web_server_survey.html,2005

2) SourceForge. http：//www.sourceforge.net

3) ERic R. The Cathedral and the Bazaar. http：//www.catb.org/~esr/writings/cathedral-bazaar/, 1997

4) Coverity Inc. Analysis of Linux kernel. http：//linuxbugs.coverity.com/linuxbugs.htm, 2004

5) Barton M, Lars F, Bryan S. An empirical study of the reliability of UNIX utilities. *Communications of the Association for Computing Machinery* **33** (12)：32-44, 1990

6) Barton M, David K, CjinPheow L, Vivekananda M, Ravi M, Ajitkumar N, Jeff S. Fuzz revisited：A reexamination of the reliability of UNIX utilities and services. Technical report,1995

7) David W. Why Open Source Software / Free Software (OSS/FS) ?
Look at the Numbers! http：//www.dwheeler.com/oss_fs_why.html

8) Devid B. Rockin' on without Microsoft.Technical report, CNET news, 2003

9) Japan Medical Association.ORCA Project. http：//www.orca.med.or.jp/,2000

10) Glyn M. Rebel Code.Perseus Books Group, Jan 2001

11) Peter S. A Quarter Century of Unix. Addison Welsy, 1994

12) Sam W. Free As in Freedom：Richard Stallman's Crusade for Free software.Oreilly and associates Inc,October 2002

13) Free Software Foundation. Free Software Definition. "http：//www.gnu.org/philosophy/free-sw.html", 1996

14) Free Software Foundation.GNU General Public License, Version 2.0.http：//www.gnu.org/copyleft/gpl.html,June 1991

15) Open Source Initiative.The open source definition.http：//www. opensource.org/docs/definition_plain.php, 1997-2005

16) Eric R. Goodbye, "free software" ; hello, "open source". http：//www.catb.org/~esr/open-source.html, 1998

17) Gerstner : IBM To Place Billion-Dollar Bet Linux Could Overtake NT. http：//linuxtoday.com/news_story.php3?ltsn=2000-12-13-007-06-PS-BZ, 2000

18) GNU Project.Frequently Asked Questions about the GNU GPL. http：//www.gnu.org/licenses/gpl-faq.html

19) The BSD License. http：//www.opensource.org/licenses/bsd-license.php

20) Berkley Software Distribution.The Original BSD License. http：//www.xfree86.org/3.3.6/COPYRIGHT2.html#6,1993

21) Common Public License, v 1.0.http：//www.eclipse.org/legal/cpl-v10.html

22) The Artistic License, Version 2.0. http：//dev.perl.org/perl6/rfc/346.html

23) Mozilla Public License, Version 1.1.http：//www.mozilla.org/MPL/MPL-1.1.txt

24) Open Source Initiative. The Approved Licenses. http：//www. opensource.org/licenses/

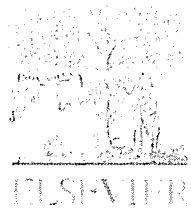
25) gpl-violation.org. gpl-violations. org project was granted a preliminary injunction against Fortinet UK Ltd http：//gpl-violations.org/news/20050414-fortinet-injunction.html, 2005

26) gpl-violation.org project.http：//gpl-violations.org/

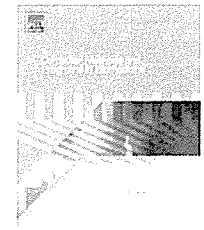
27) 内閣府総合規制改革会議．第9回総合規制改革

会議資料 , 2004
28) McDonald CJ, Schadow G, Barnes M, Dexter P, Overhage JM, Mamlin B, McCoy JM.Open source software in medical informatics.why, how and what. *Int J Med Inform* **69**：175-184, 2003
29) Veterans Health Administration.Veterans Health Information Systems and Technology Architecture（VISTA）.http：//www.va.gov/vista_monograph/
30) FreeMED Project. FreeMED.http：//www.freemed.org/
31) OpenEMR Project. OpenEMR. http：//www.openemr. net/
32) The Open Source Health Informatics Working Group. http：//www. chirad.info/imiaoswg
33) Japan Medical Association.JMA IT Declearation. http：//www.orca.med.or.jp/orca/sengen/declaration.html,2001
34) The OpenCOBOL Project.OpenCOBOL.http：//www. OpenCOBOL.org/
35) Glenn F, Andrew H, David K, Kiem-Phong Vo. Migrating an mvs mainframe application to a pc. In USENIX'04 Technical Paper. USENIX, 2004
36) Lincoln S. How Perl Saved the Human Genome Project.http：//www. bioperl. org/GetStarted/tpj_ls_bio.html,February 1996
37) Carina D. Biologists launch 'open-source movement'. *Nature* **431**：494, 2004
38) R Development Core Team. R：A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria, 2005. ISBN 3-900051-07-0
39) The NetEpi Project. Netepi. http：//www.netepi.org/
40) Sandrine D, Robert G , John Q. Open source software for the analysis of microarray data. *Bio Techiques* **34**：S45-S51, March 2003
41) Antoine R, Lucca S, Osman R. Osirix：an open-source software for navigating in multidimensional dicom images. *J Digit Imaging* **17**：205-216,2004
42) NIH. ImageJ. http：//rsb.info.nih.gov/ij/
43) Erik N. XMedCon-An open-source medical image conversion toolkit. *European Journal of Nuclear Medicine* **30**（suppl.2）：S246, 2003
44) HL7 Japan. HL7 FAQ. http：//www.hl7.jp/whatis/faq1. html
45) MedXML Consortium. MML Version 3.0 Specification. http：//www. medxml. net/mml30/default. html, 2003
46) 財団法人医療情報開発センター . MEDIS 標準マスターの概要 . http：//www.medis.or.jp/4_hyojyun/medis-master/overview/index.html
47) Free Software Foundation.Various Licenses and Comments about Them. http：//www.gnu.org/licenses/license-list.html,1999-2005

COMPUTER METHODS AND PROGRAMS IN BIOMEDICINE 81 (2006) 197–202



journal homepage: www.intl.elsevierhealth.com/journals/cmpb



Design and development of a secure DICOM-Network Attached Server

Hidenobu Tachibana, Masahiko Omatsu, Ko Higuchi, Tokuo Umeda*

Medical Image Engineering, Kitasato University, Graduate School of Medical Sciences, 1-15-1 Kitasato, Sagamihara, Kanagawa 228-8555, Japan

ARTICLE INFO

Article history:
Received 1 November 2003
Received in revised form 6 June 2004
Accepted 22 October 2004

Keywords:
Teleradiology
Web-based system
DICOM
INTERNET
DICOM-NAS

ABSTRACT

It is not easy to connect a web-based server with an existing DICOM server, and using a web-based server on the INTERNET has risks. In this study, we designed and developed the secure DICOM-Network Attached Server (DICOM-NAS) through which the DICOM server in a hospital-Local Area Network (LAN) was connected to the INTERNET. After receiving a Client's image export request, the DICOM-NAS sent it to the DICOM server with DICOM protocol. The server then provided DICOM images to the DICOM-NAS, which transferred them to the Client using HTTP. The DICOM-NAS plays an important role between DICOM protocol and HTTP, and only temporarily stores the requested images. The DICOM server keeps all of the original DICOM images. When unwanted outsiders attempt to get into the DICOM-NAS, they cannot access any medical images because these images are not stored in the DICOM-NAS. Therefore, the DICOM-NAS does not require large storage, but can greatly improve information security.

1. Introduction

In recent years, many hospitals have installed high-tech medical equipment, including Computed Radiology (CR), Computed Tomography (CT), and Magnetic Resonance Imaging (MRI) [1]. Researchers and developers have attempted to combine this equipment with information technology (IT) to improve the quality of medical care. Web-based servers, which have enabled us to display patients' medical images on computers using Internet Explorer, have been especially developed. This allows medical physicians and other researchers to easily share and view these medical images anywhere when needed. However, the use of web-based servers also brings many problems [2–13].

Since most servers were originally designed for vender-customized DICOM servers, their versatilities are not very good. Therefore, users must install a web-based server combined with a particular DICOM server for medical use. This is sometimes not feasible because of technical and financial reasons. On the other hand, in order to distribute the medical images, patients' information must be stored in the servers at all times. Therefore, the misusage risk of patients' information becomes higher.

The present study developed a web-based server called the DICOM-Network Attached Server (DICOM-NAS), which can be easily installed and adjusted to DICOM protocol and HTTP. The DICOM servers in a hospital-LAN are connected to the INTERNET through the DICOM-NAS, and the patients' medical images and information are only kept temporarily in the DICOM-NAS when eligible Clients need them. Since the patients' medical images are not stored there at all times, it greatly improves information security.

* *Corresponding author.* Tel.: +81 42 778 9565; fax: +81 42 778 9565.
E-mail address: tatibana@umeken3.ahs.kitasato-u.ac.jp (H. Tachibana).
0169-2607/$ – see front matter © 2006 Published by Elsevier Ireland Ltd.
doi:10.1016/j.cmpb.2005.11.015

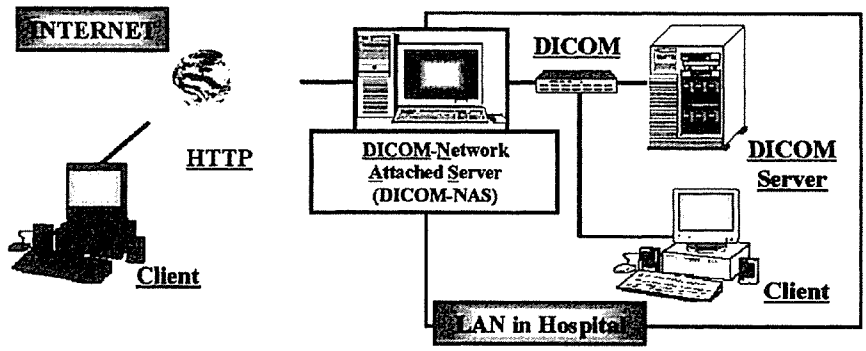


Fig. 1 – Scheme of DICOM-Network Attached Server.

2. DICOM-Network Attached Server

2.1. *Scheme of DICOM-NAS*

The DICOM-NAS scheme is illustrated in Fig. 1. It communicates with the DICOM server by using the DICOM protocol when it is attached to the Local Area Network (LAN). An IP address, AE title, host name, and port number were assigned to the DICOM-NAS. In order to view the DICOM images, the Client can use the browser in any computer to connect to the LAN, the INTERNET, and then to the DICOM-NAS.

2.2. *System configuration of DICOM-NAS and data flow*

Fig. 2 demonstrates the system configuration of the DICOM-NAS and the data flow. The DICOM-NAS can work with Internet Information Server (IIS) 5.0 on Microsoft Windows 2000 or XP and consists of Java Applets, Java Servlets, and DCMTK. The Java Servlets work with application servers Tomcat 4.0.1 and IIS 5.0 to provide a highly reliable, manageable, and scalable web application infrastructure for all versions of Windows 2000 and XP. The IIS can increase website and application availability and lower the system administration costs. Java Servlets provide a component-based and platform-independent method for building web-based applications without CGI program performance limitations. Java Servlets can access the entire Java API family, including JDBC API, to access enterprise databases and a library of HTTP-specific calls. They have all of the benefits of mature Java language, including portability, performance, reusability, and crash protection. Tomcat 4.0.1 is the servlet container that can improve performance and memory efficiency. DCMTK [14] is a collection of libraries and applications that implement large parts of the DICOM standard. It includes software for examining, constructing, and converting DICOM image files, as well as sending and receiving images over a network connection.

In this DICOM-NAS system, the Java Applets are the interfaces between the Client and the Java Servlets. The Java Servlets communicate with the DCMTK and the Diagnosis report database based on the information obtained from the Java Applets. The DICOM-NAS communicates with the DICOM servers using two applications, including DCMTK, which has the C-FIND and C-MOVE functions.

When a Client wishes to access the medical images of a patient, the Client should first connect to the DICOM-NAS using Internet Explorer and request a patient name or a patient name list, which is stored in the DICOM server. After receiving the request, the DICOM-NAS generates query keys related to the request and sends them to the DICOM server

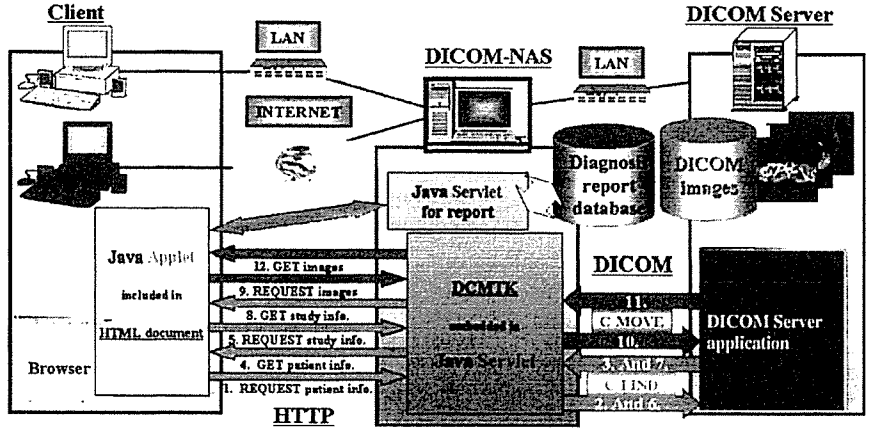


Fig. 2 – System configuration of DICOM-NAS, and data flow after downloading Java Applet that have the functions of Query/Retrieve and display of DICOM images from DICOM-NAS.