データベースシステム 105－2
（１９９５．１０．２６）

World Wide Webのセキュリティの検討

山本隆一* 山本大助**
yamamoto@art.osaka-med.ac.jp*
center@art.osaka-med.ac.jp**
大阪医科大学中央検査部病理*
大阪医科大学医学情報処理センター**

医療の広報型情報提供の方法としてインターネット上のWWWの利用は有望であり、実験的運用が始まっているが、通常のWWWではセキュリティに問題があり、特にデータ改竄となりすましは深刻な影響を与える可能性がある。これらの問題は暗号技術を用いることで解決可能で、この機能を持ったSecure WWW serverが開発されている。我々はこのサーバを実験的に導入し評価をおこなった。我々が評価したサーバは使いやすく、医療で広報型情報提供に用いる限りは十分なセキュリティ機能を持つと考えられた。しかしWWWが本来可能である双方向の情報交換にはセキュリティは不十分と考えられた。また公証制度がわが国で整備されていないことも実用化の障害になると考えられた。

Evaluation of the security of World Wide Web

Ryuichi Yamamoto*, Daisuke Yamamoto**
Department of Laboratory Medicine, Division of Pathology, Osaka Medical College*
Biomedical Computation Center, Osaka Medical College**

World Wide Web (WWW) is fairly developed infosystem of the internet and many Medical servers are carried even in Japan. Distributing medical information with WWW is convenient in the social health care, especially in disaster such as earthquake. But WWW itself has not security and certification ability which prevents unconvincing or misleading information. So we evaluated a secure WWW server with SSL protocol for the purpose of medical communication, and revealed that has enough ability for certification for providing medical information, but fair reliability for secure medical bi-directional communication. And also we suggested that the lack of organized certification system in Japan may disturb the development of secure medical communication with the internet.

医療とインターネット

インターネットは140以上の国が参加し、5000万人以上の利用者がいる世界最大のコンピュータネットワークで、研究目的で発展してきたネットワークであるが、マルチメディア通信の最初の実用例と言えるWorld Wide Webの普及と商用利用への解放で、現在でも爆発的に利用者が増加している。今後、これだけの規模のネットワークをインターネットと独立に構築することは、経済的にも、すでに存在する利用者の利便性からも不可能に近い。もちろん技術の発展とともにネットワークも変貌していくものであるが、インターネットは出発当初から自己改革を繰り返して発展しており、歴史的に新技術の提案・実装・評価・標準化のサイクルの取り扱いに優れており、今後もインターネットをベースに大規模ネットワークが発展していくことが予想される。

医療は本来、患者と医療サイドの契約に基づくサービス行為で、個々の医療に広域ネットワークの関与する必然性は小さい。しかし以下に述べる理由から医療も広域ネットワークと関わらざるを得ないと考えられる。

1　医療が高度化し、一人の医師、単一の医療チーム、単一の医療機関ではすべての医療シーンに対応することが困難になりつつある。多数の医療機関での連携が必要であり、しかも迅速な対応が要求される。現在の高度に情報化された医療では広域ネットワークの利用は避けられない。

2　医療のバックグラウンドである医学は集学的色彩が強く、しかも新技術の速やかな適応が要求される分野であり、効率のよい研究促進のためには広域ネットワークの利用はきわめて有効である。実際、計算機科学をのぞくとインターネットの学術利用がもっとも盛んなのは医学・生物学の分野である。

3　医療自体も変貌しつつあり、保健・福祉などとの連携が強化される傾向にある。つまり1人の患者を対象とする医療だけでなく、多数を対象とする医療サービスの提供も要求される。このような医療サービスを必要とする人は社会にまばらに存在し、集中型のサービス提供には限界があり、大規模なネットワークの利用が有効と考えられる。

4　阪神大震災の例に見るように、大規模な災害の初期では、平時のような秩序ある広報は期待できない。医療に関する情報はこのような場合、もっとも重要な情報であり、医療機関も独自で責任ある情報を発信できる能力を持つことが期待される。コンピュータネットワークは専用回線を用いている部分が多く、単位時間に搬送できる情報量も多いために、災害時に強い情報伝送経路であることは阪神大震災でも実証されている。

5　インターネットは商業利用の導入にともなって急速に社会に浸透しており、営利・非営利サービスの充実にも目を見張るものがある。社会の要請としてインターネット上の医療サービス情報の提供が求められるようになるのは自明である。

これらの理由により医療が今後、インターネットに何らかの形で関与していかなければならないことは明白である。しかし現状のインターネットをそのまま利用する場合にはいくつかの問題点がある。わが国の現状でもっとも大きな問題は、インフラストラクチャの整備の遅れである。ハードウエアとしての回線設備の整備の遅れも重大であるが、回線使用料金が諸外国に比べて高額であることも無視できない。医療サービスを必要とする社会的弱者の利用を促進するためには上下水道のように公共性に配慮したインフラストラクチャの整備が望まれる。

つぎに問題としてあげられるのは安全性であ

る。一般にネットワークの安全性には多種の問題が含まれるが、ここでは医療サービスから見た安全性について述べる。

医療サービスは一定の基準を満たした状態で常に利用可能なことが最優先される。つまりネットワークの長期間の機能停止や大幅な機能低下は許されない。また盗聴、改竄、なりすまし、という不正情報操作は患者のプライバシー保護にかかわるだけでなく、不正情報が社会に流れた場合の影響の大きさからも十分に配慮されなければならない。

現在のインターネットはこれらの問題点について、ある程度の信頼性は期待できるが、決して完全とは言えない。特にネットワークが常時、健康な状態で使用できるかという面については、わが国のインターネットを支えるバックボーンでさえ、一部で実験的色彩が払拭しきれていない状態であり、関係者の努力が期待される。また不正情報操作については使用者のモラルに依存している部分が大きい。プライバシーに関わる患者情報を計画的にインターネットを利用して交換している例はまだないと思われるが、その他の情報はすでに活発に交換されている。また阪神大震災のボランティアグループのメーリングリストのように、多数を対象にした医療情報の提供もすでに行われている。したがってこれらの安全性の対策は急がなければならない。ネットワークはメディアであり、医療サービスでも様々な状況での利用が考えられる。求められる安全性も状況によって異なる。今回我々は1対多数の広報型情報提供をインターネットを利用して行う場合の安全性について導入事例を紹介するとともに、有効性について考察を加えたい。

World Wide Webとそのリスク

インターネットを利用した広報型情報提供にはWorld Wide Web、GopherなどのInfosystemが使用されることが多い。中でもWorld Wide Web（以下WWW）は汎用の文書記述言語であるSGMLから派生したHTMLをネットワーク上で交換するInfosystemで、交換手法はhttpと呼ばれるプロトコールを使用している。画像、音声、動画を含めたマルチメディア表現が可能な点とURLと呼ばれる従来のインターネットのリソースの大部分を包含できる標準記法を持っていて、柔軟で汎用性に

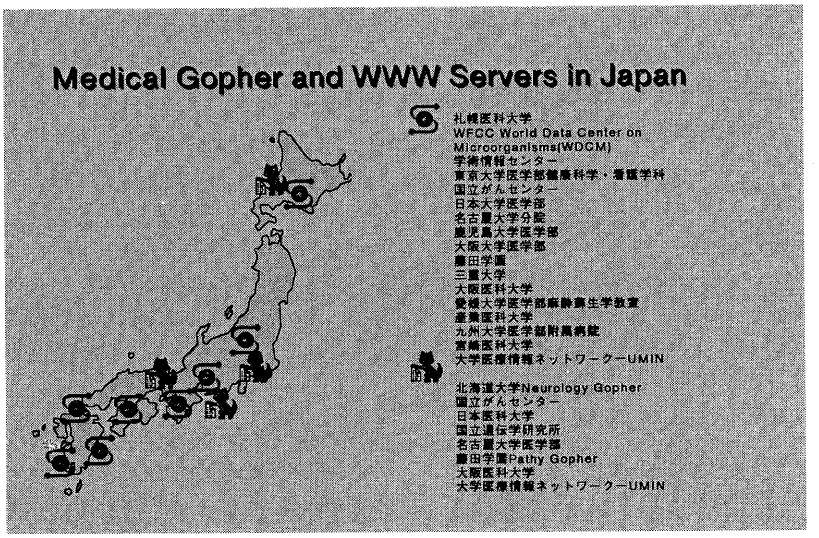

図1　日本の医学関係のWWWサーバとGopherサーバの一部

富む仕組みである。WWWはサーバ・クライアント型のネットワークアプリケーションで、サーバ、クライアントともに数種類のソフトウエアが存在する。クライアントはいずれもユーザフレンドリなインターフェイスを持ち、安価である。サーバはフリーウエアも存在し、インストールは簡単で、データの構築も容易である。　図1は現在わが国で運営されている医療関係のWWWサーバおよびGopherサーバの一部である。これらのサイトでは有益な情報提供が行われているが、学術的な紹介や、セキュリティ上の問題が生じない医学データが中心である。しかしながら、今後は社会的な医療サービス情報や診療情報の提供なども安全性が確保されれば行われる可能性が高い。そこでまず広報型情報提供に求められる安全性について考察したい。

本来だれでもアクセスできる情報である広報型情報では、盗聴防止は積極的な意味はない。一方で、情報が書き換えられることは大きな問題となる。身分を詐称して情報を発信することも影響が大きい。つまり改竄となりすましの防止が安全確保の主目的となる。データの改竄はネットワークでなくても可能であり、ネットワーク上で不正操作を行うためには、かなりの技術力が要求されるので、ネットワークが特に危険というわけではないが、ネットワーク上の不正操作は組織的・継続的に行われる可能性がある。また公開性の高いインターネット上で情報の改竄そのものを防止することは極めて困難である。しかし改竄を検出することはそれほど難しい事ではない。そして改竄が確実に検出できれば改竄そのものの意味を失わせることができる。つぎに「なりすまし」についてであるが、インターネットでは、特にネットワークの知識に乏しい人相手では、「なりすまし」は簡単に行い得る。WWWサーバの最初に表示される画面（ホームページと呼ばれている）に「○○医科大学」と書いてあればサイト名がそれらしくなくても詐称に気づかない人もいるかも知れない。このような行為を防止することはできないが、身元の確認をネットワーク上で行う方法は存在する。これを用いれば、情報にアクセスするユーザは常に情報発信元の身元を確認することが可能であり、表面的な詐称は意味を失う。

暗号化通信

これらの危険の防止には暗号化技術が用いられる。暗号化には単一の鍵で暗号化と復号を行う秘密鍵暗号化方式と、二つの相補的な鍵を用いて、一方で暗号化し他方で復号する公開鍵暗号化方式がある。改竄の検出と身分の確認はどちらも公開鍵暗号の技術を応用することで達成できる。公開鍵暗号は数学的に特殊な関係にある秘密鍵と公開鍵という二つの暗号鍵を用いる暗号で、秘密鍵は安全な場所に保管し、公開鍵は広く公開しておく。二つの鍵は相補的で、一方で暗号化した文書はもう一方でしか復号できないようになっている。情報発信者のAが、秘密鍵で暗号化してBに送ると、Bは公開されているAの公開鍵で自由に復号することができる。もちろんB以外の人も復号することができるので秘密保持の意味はないが、この文書を暗号化できたのは秘密鍵を持っているA以外にはありえない。したがってこの暗号化はAが発信者である証拠になる。これは電子署名と呼ばれている。秘密保持が目的ではないので、実際には文書全体を暗号化する必要はない。名前と住所などの短いデータを暗号化したものを添付するだけで十分である。さらに文書全体から計算されるチェックサムのような情報も添えて暗号化して送ると、受け取り手は復号したチェックサムと実際に文書から計算したチェックサムを比較することで改竄があったかどうかも検出できる。これで広報型情報提供の安全性の問題の多くは解決されるが、実際はまだ不十分である。それはAの身元の確認で、AがAであることの証明はこの方法ではできない。これを解決するためには公証制度の導入が有効である。公証制度は信頼性の高い組織（公証局と呼ぶ）が、まずAを慎重に身元確認する。AがAであることを確認できたら、Aの公開鍵に公証局の公証情報を添付して公

証局の電子署名を付けて（公証書と呼ぶ）発行する。Aは電子署名に公証書を添付して使用する。送られた文書の電子署名を公証書を利用して復号する。復号したデータが公証書の内容と一致していれば、公証局が保証したAであることが確認できる。このような仕組みを取り入れる事で広報型情報提供の安全性は確保できる。

Secure WWW server

このような仕組みを内蔵したWWWサーバが米国のNetscape comunications社からNetsite commerce serverとして発売されている。我々はインターネットでの広報型情報提供の安全性の検討のために実験的に導入した。なおクライアントは同社のNetscape Navigatorを用いなければならない。

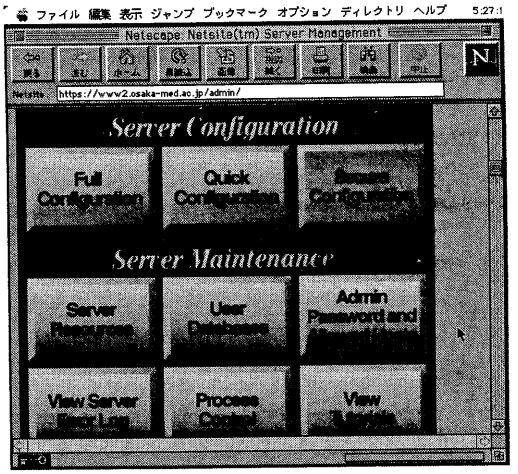

図２　NCSの管理ページ

Netsite commerce serverはソースの提供はなく、数種のプラットフォーム用のコンパイルされたシステムとして提供される。改変はできないが、インストールは非常に単純である。CD-ROMから適当なディレクトリに展開し、まずインストール用のミニサーバを起動する。ここまではプラットフォーム上で行う必要があるが、あとはこのミニサーバにNetscape Navigatorでアクセスして行う。図２に管理用のページを示す。このページを利用し、マニュアルに従ってセットアップすれば通常のWWWサーバとしてインストールは数分で終わる。

このままではNetscape社のセキュリティ機能のないサーバであるNetsite Communication serverと同等の機能で動作する。セキュリティ機能のセットアップをする必要があるが、まずNetsite Commerce Server（以下NCS）のセキュリティの仕組みについて述べる。NCSは公開鍵暗号とセッションキーと呼ばれる秘密鍵暗号方式を組み合わせて使用している。クライアントがNCSにアクセスすると、まずサーバはサーバの電子署名と公証書をクライアントに送る。クライアントは公証書サーバの身元を確認することができる。次にクライアントはセッション鍵をと呼ばれる秘密鍵を作成する。そしてその鍵のコピーをサーバの公開鍵で暗号化し、サーバに送る。このセッション鍵はサーバの秘密鍵でしか復号できないために盗聴はされない。これ以後は交換されたセッション鍵を使って秘密鍵暗号化方式で暗号化してHTMLを交換する。このように２つの暗号化を組み合わせて用いるのは、一般に公開鍵暗号化方式は秘密鍵暗号化方式に比べて暗号化／復号に時間がかかるためと、現状ではすべてのクライアントに公開鍵暗号化機能を付加するのは現実的でないからである。

公開鍵暗号化方式にもいくつかの種類があるが、NCSで用いられているのは二つの大きな素数の積を計算するのは簡単だが、もとの素数に素因数分解することは著しく難しいという整数論の現状での限界に基づいたもので、Ron Rivest, Adi Shamir, およびLeonard Adlemanの３人が1977年に開発したRSA暗号化方式と呼ばれているものである。この暗号の安全性は二つの素数の積の大きさに依存している。大きければ大きいほど安全であるが、NCSでは512ビットを採用している。これは150桁程度の10進数に相当する。512ビットRSAの鍵の解読はスーパーコンピュータを用いても１年以上かかり、軍事用には不十分かも知れないが、医療情報の流通には十分な安全性があると思

われる。

秘密鍵暗号化方式にも多数の種類があるが、NCSで用いられているのはRon Rivestの開発したRC4と呼ばれる可変長鍵の暗号化である。秘密鍵が直接漏洩しない限りはRC4の安全性は鍵の長さに依存する。米国外で使用できるNetscape Navigatorは40ビットのRC4を用いている。40ビットのRC4の鍵は高速なワークステーションを用いれば７～１０日程度で解析可能である。NCSはRC4をセッション鍵として用いている。つまりセッション毎に鍵は変更されるので、１つのセッションは破られる可能性はあるが、継続的な暗号破りは事実上は不可能である。特に広報型情報提供の手段として用いる場合は十分な安全性があると考えられる。ただしNetscape Navigator 1.1以前のバージョンではセッション鍵の生成アルゴリズムに問題があった。すでに改善されているが、この問題点を知っているものならパソコンで１分程度で鍵の解析が可能であった。

セキュリティ機能のセットアップ

NCSにセキュリティ機能のセットアップを行うためには公証局にサーバの公証書の発行を依頼する必要がある。RSAの公証局は米国にいくつか存在するが、我々は米国のRSA Data Security社に公証を依頼した。公証を行うためにはまずサーバの秘密鍵と公開鍵を作成する必要があるが、これは図２のNCSの保守画面から簡単に行える。さらに公証の申し込みに必要な項目を聞いて自動的に公証局に申し込みメールを送ってくれる。申し込みを行うと１～２日でRSA Data Security社から、公証のための書類送付の依頼が来る。公証に必要なものは（１）サーバの管理者がその組織の継続的なメンバーであることを組織の代表者が保証した手紙、（２）その組織の存在を公に証明する書類のコピー、の２つである。手紙には代表者の自筆サインとその組織の公式な便箋および封筒を用いることが要求されている。私立大学の場合、組織の存在を公に証明する書類は文部省の認可書であるが、我々の場合、古い上に日本語でかかれているために不適と判断し、大学が発行している英文雑誌の一冊をかわりに用いた。これに加えて登録料金として年間290ドルが必要であった。

これら書類をファクシミリおよび郵送で送り、数日で公証書が電子メールで送付される。電子メールの一部はサーバの公開鍵で暗号化されているために、他の機関に盗用される危険はない。あとは電子メールの本文をサーバからアクセス可能なディレクトリに置いて保守画面から操作するだけでセキュリティセットアップは完了する。通常のWWWサーバはポート番号80を使用するが、セキュリティ機能を付加したNCSはデフォウルトでは443を用いる。これは変更可能であるが、混同を避けるために80は使用しないほうが良い。

一旦セキュリティ機能を付加したNCSは立ち上げ時にパスワードを要求する。したがって何らかの理由でプラットフォームを再起動した場合にはマニュアルで起動する必要がある。またWWWのプロトコールであるhttpではアクセスできない。かわりにhttpsというプロトコールを用いる。httpsはセキュリティ機能以外はhttpと共通であるが、セキュリティ機能はセッションのすべてに影響するためにhttpsを扱えないクライアントではまったくアクセスできない。しかしNetscape社はセキュリティ機能をhttpより低位のSocket層で実現しSSL（Secure Socket Layer）として仕様をインターネットドラフトとして公開している。したがって将来は他のクライアントもSSLをサポートする可能性も高い。Socket層で実現したことにより、この層を用いる他のインターネットアプリケーション（Telnet, FTP, Gopher, NNTPなど広範に及ぶ）でも利用が可能であり、すでにいくつかは実験が開始されている。

サーバデータの構築は一般のWWWサーバと基本的には同じである。ただし、秘密鍵の保持には十分に注意しなければならない。秘密鍵そのものは一つのファイルに過ぎないので、これは結局はサーバのあるプラットフォームのセキュリティレベルを高く維持するしかない。Netscape社は

WWWに独自の拡張をほどこしたり、他のサーバにないインターフェイスの拡張をおこなっている。これらの追加機能は同社のクライアントであるNetscape Navigator以外では利用できないものが多く、通常のサーバでは多用しないほうが望ましい。しかし、NCSは現状ではNetscape Navigaotor以外からはアクセスできないので、これらの機能を多用しても問題は少ない。またサーバデータのアクセス制限はホスト別やユーザ別に自由に設定することが可能で、図2の保守画面から極めて簡単に行うことができる。全体にCERNやNCSAのサーバに比べて保守に要する労力は大幅に小さいと考えられる。

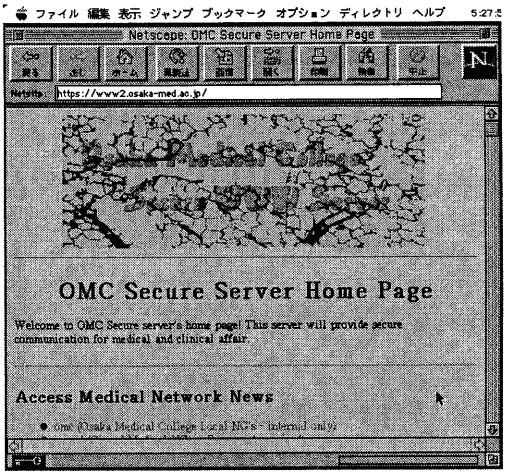

図3　NCSのページ。画面左下に鍵のマークが表示される。

図3はNetscape Navigator1.1JでNCSにアクセスした画面で、ロケーションボックスの下に青い線が入り、画面左下の鍵のマークが変化することで、NCSかどうか判定できる。また図4はファイルメニューから文書情報を選択したところで、公証書データが表示される。

Secure WWW serverの評価と問題点

Netscape Commerce Serverは全体として我々の目的である広報型情報の安全な提供が可能な使いやすいWWWサーバということができる。保守はCERNやNCSAのサーバに比べて簡単で、複雑な設定も容易に行える。しかしいくつかの問題点も明らかになった。

まず、輸出仕様のSSLの安全性についてであるが、現在日本で使用できるバージョンでは米国国内向けの製品にくらべて、暗号鍵の長さが短い。これは最近まで行われていた米国の輸出制限の影響である。輸出制限は95年9月末に大幅な緩和が発表されたので、まもなく改善されると思われるが、現在の製品では暗号鍵の長さが不十分なことが問題点として上げることができる。今回の我々の評価目的は医療サイドが広報型情報を発信する場合の安全性であったが、その点では十分なレベルであると考えられる。しかしWWWは本来、双方向の情報交換が可能であり、図5のようなFORMを用いた入力画面を用意すればクライアントからも情報を送ることができる。従って理論的には健康相談や簡単な問診表の記入程度は可能である。現状の医療にそのまま持ち込むのは法的にも問題があるが、医療機関にかかるほどではないが健康上の問題をかかえているといった例は高齢化に従って増加してくることが考えられる。このような場合に一種のプレ医療としてこのような仕組みの利用も検討の価値がある。また大震災のような非常時にも情報収集機能は利用される可能性が高い。このような双方向の利用法ではクライアント側からの情報には秘密保持が必要なデータが含まれる可能性がある。現状の40ビットRC4のセッション鍵では僅かではあるが盗聴の可能性を否定しきれない。なお米国国内仕様では128ビットのセッション鍵を使用することができるものが使われている。

しかしもっとも大きな問題点は公証局が国内にない点である。公証は本来目的に応じた厳格な審査が必要で、しかも実用化を目指すためには効率的に行われなければならない。外国の組織を公証を依頼していることには限界がある。また図4に示したように現状では表示される公証情報は英語

図4　公証情報の表示画面。インターフェイスは日本語化されているが、公証情報そのものは英語である。

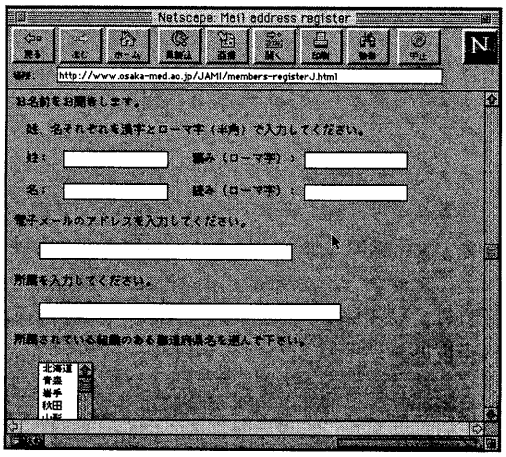

図5　WWWの入力ページの例

であり、高齢者などを対象とするには問題がある。公証機構は今回取り上げた広報型の情報提供だけでなく、医療の情報交換のすべての分野において必要になると考えられる。他国と互換性を維持した国内での系統的な公証制度の確立が検討されなければならないと考える。

Netscape社のクライアントしか使用できない点も問題点として上げることができる。現状ではずばぬけた技術力を持つ同社が先行するのはやむを得ないとしても早い時期に健全な競走が行われることを期待したい。