日医総研ワーキングペーパー

ホームページから見る都道府県・郡市区医師会の

セキュリティ動向の調査

No. 110

平成 17 年 2 月 4 日

日本医師会総合政策研究機構　　増子　厚

ホームページから見る都道府県・郡市区医師会の
セキュリティ動向の調査　　（No.110 要旨）

１．背景と目的

■通常、ホームページでの通信の内容は、“ 平文 ”と呼ばれる人間がそのまま読める文字列の状態で流れている。このため、インターネット上で通信の監視などが行われていると、通信の内容がそのまま閲覧できてしまう。
→「盗聴」「改ざん」「なりすまし」「否認」　が行われる危険性がある。

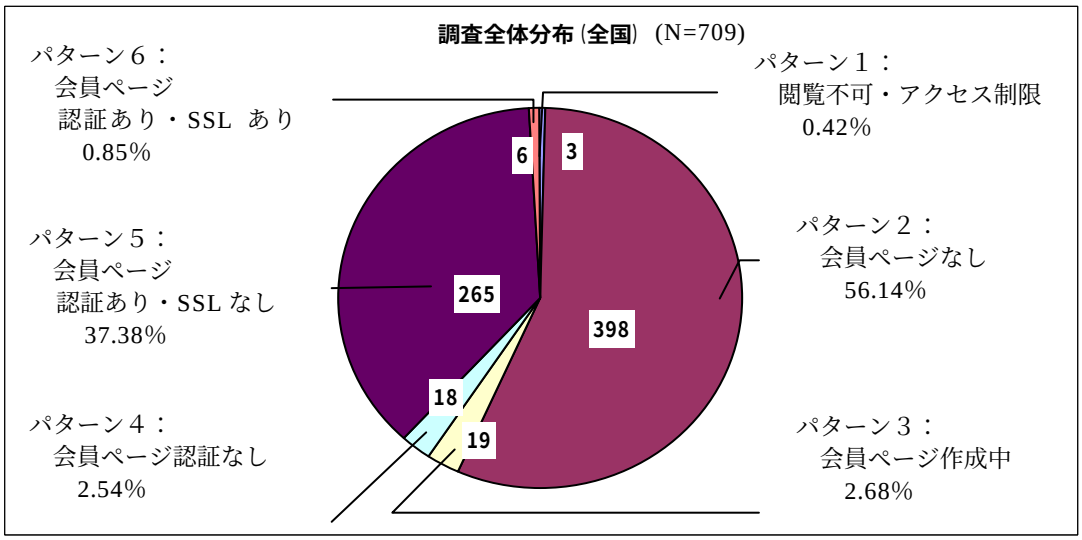
■ホームページは外部からのアクセスを直接受け付ける部分である。セキュリティ管理を確実に行っておかないと、ホームページを通じて情報の漏洩などが起こる可能性がある。

■身近な事例として医師会員の利用の多い都道府県・郡市区医師会のホームページではセキュリティ対策はどのように運営されているか調査を行った。
現在公開されている全国医師会のホームページのセキュリティ動向を把握のため認証の利用、SSL[1]というセキュリティ対策への対応状況を調査した。

２．調査

各医師会のホームページを閲覧し、調査項目を確認した。
■都道府県医師会 47 ヶ所、郡市区医師会 662 ヶ所

調査全体の分布から見ると、全対象 709 ヶ所の内、認証を用いている会員ページ（パターン５とパターン６）を運営していたのが 271 ヶ所(38.23%)、そのうち SSL を用いた運営を行っていた（パターン６）のが 6 ヶ所(0.85%)となっていた。



[1]*SSL：安全に通信するための技術。詳しくは、本稿 P8「1-3　SSL とは」にて述べている。

３．セキュリティ対策

■危険を回避するには、セキュリティ対策を確実に行う必要がある。
→「通信の暗号化」「認証」「ウィルス対策」「フィルタリング」「障害対策」

■リスク分析
ホームページで扱う情報に見合ったセキュリティ対策を行う必要がある。

→リスク低　一般向けに作られているコンテンツ：
医師会の紹介、行事予定、所属医院の紹介、コラム、公開掲示板、会誌などに掲載予定の理事会録の速報

→リスク高　会員の情報が結びつく場合：
氏名、自宅の住所、電話番号、生年月日などが識別できる会員情報。
このほかにも、ホームページ内部のコンテンツが重要でなくても、ID とパスワードが漏洩してしまうことで、別の機関で用いている認証から、会員の個人情報に結びついてしまう可能性もある。

リスクに応じて、SSL 技術などを採用することも必要になる。

４．医師会ホームページのこれから

■来年度から、個人情報保護法、e 文書法の施行など情報分野の法整備が整えられてきており、情報を持ち出した犯人だけではなく、情報を管理している立場の責任が重要視されてきている。

■近い将来、通信上で健康情報などの重要度の高い情報を扱う必要がでてくれば、SSL 等の認証や暗号化技術の導入によるセキュリティ対策が必須になる。

■SSL を使っての運用には利用料が発生する。従って、情報の重要度と運用コストのバランスを見て適切に導入の判断をする必要がある。

■SSL を提供する商用サービスも、最近では増えてきているが、日本医師会も「日医認証局」を検討しており、日医が主体となった安全で利用しやすいネットワーク環境を整えて行く予定でいる。

ホームページから見る都道府県・郡市区医師会のセキュリティ動向の調査

日本医師会総合政策研究機構　　増子　厚

キーワード

◆セキュリティ　◆ホームページ　　◆SSL　　◆認証局

ポイント

- 全国には、都道府県 47 ヶ所、郡市区 916 ヶ所の医師会があり、そのうち 73.6%が各医師会のホームページを保有していた。その中で会員ページを運営している医師会は 40.8%であった。
- セキュリティ対策として、通信中のデータを暗号化する SSL（エス・エス・エル）という技術の使用状況を調査した。
- 会員ページに SSL 等のセキュリティを施されていない場合、各会員の ID やパスワードがインターネットを平分で流れることに留意する必要がある。
- 会員ページ保有のうち、都道府県医師会では 47 ヶ所中 2 ヶ所、郡市区医師会 662 ヶ所中 4 ヶ所 SSL を用いた通信を行っていた。
- SSL の利用率はまだまだ少ないが、日医認証局などの設立が進められ、医療系ホームページにおいても利用しやすい整備が整えられてきている。
- ホームページ運営に関するセキュリティについて考える必要がある。

目次

はじめに

急速に情報化が進んできたといわれる現在、個人や会社でホームページを立ち上げ、運営を行うことが一般的になってきた。

全国には、都道府県医師会が 47 ヶ所、郡市区医師会 916 ヶ所[1]存在する。そのうち、ホームページ運営を行っている医師会が全国で約 700 ヶ所あることが確認されている。

ホームページは外部に対する広報の手段として有効である反面、外部からのアクセスを直接受け付ける部分でもある。そのため、セキュリティ管理を確実に行っておかないと、ホームページを通じて情報の漏洩などが起こる可能性がある。事実、昨今のマスコミ報道で、ホームページを通じてアンケートに回答した顧客の個人情報が漏洩したという事故が見受けられる。

これは、民間企業に限らず、ホームページを運営する医師会においても同様である。今後の展開によっては、所属会員の個人情報だけでなく、場合によっては患者の健康情報のような重要度の高い情報を取り扱う可能性も否定できない医師会では、早い段階から十分な配慮、対策を検討しておく必要があると考える。

ホームページを通じて情報を配信、収集するような場合に用いるセキュリティ対策の一つとして、通信の経路を暗号化して、外部への情報漏洩を防ぐ SSL[2]（エスエスエル）という技術が存在する。

本稿では、まず現状を把握する目的で、現在公開されている都道府県･郡市区医師会のホームページの SSL への対応状況を調査した。

これは、現状を把握するもので、ホームページを運営している各医師会に闇雲に SSL の対策を施す必要性を訴えるものではない。提供している情報、収集している情報の種類や性質によっては現在の運営形態で何ら問題がないということも十分考えられる。そこでまず、現状を把握し、その上で、今後必要となるかもしれない対策や考え方について概観したい。

本稿の構成として、第 1 章では、調査の前提となる一般的な通信の仕組みや通信に潜む危険性、それを回避するための SSL 技術について紹介した。第 2 章では、今回セキュリティ動向調査の調査対象、調査方法、調査結果を示した。第 3 章では、ホームページ上でのセキュリティの対策方法を例示した。そして、医療とネットワークを

[1] 都道府県、郡市区医師会数：2004 年 5 月日本医師会調べ。
[2] SSL：Secure Sockets Layer（セキュア・ソケット・レイヤー）の頭文字 、P8 「1-3 SSL とは」にて詳細を説明している。

取り巻く環境と、その上で、今後医師会でホームページを運営して行くにあたり必要となってくることを述べた。

本稿が、今後の都道府県・郡市区医師会のセキュリティ対策を考える上での一助となれば幸いである。

【研究協力者】　日医総研　矢野一博

1　背景

本章では、本稿の目的である医師会のホームページ運営実態の把握にあたり、前提となる一般的な通信の仕組み、通信上の危険、危険を回避するための技術等について簡単に触れておく。

1－1　一般的なホームページの現状

通常、ホームページ（以下、HP）を見る場合、ウェブブラウザ[3]といわれるものを利用する。たとえば、ウェブブラウザで日本医師会のホームページを見ると、蜘蛛の巣状に張り巡らされたインターネット網を通じて、日本医師会がホームページを提供しているサーバといわれるコンピュータに情報を取得しに行く。情報を取得する経路は様々であり、どこを経由して情報が取得されるか利用者にはわからない。

また、取得された情報が利用者のコンピュータに表示されるまでの通信の内容は、“平文”と呼ばれる形式でインターネット網を流れている。平文とは、人間が判読できる状態の文字列のことである。つまり、インターネット網上のどこかで通信の監視などが行われていると、通信の内容がそのまま閲覧できてしまう。

これは、もともとウェブブラウザ自体が通信内容を秘匿にする暗号の仕組みを持たないためである。特に設定を行っていない場合、通信にはこの平文が用いられる。

このことは、ホームページ上でやり取りを行うすべての通信データに対して言えることである。

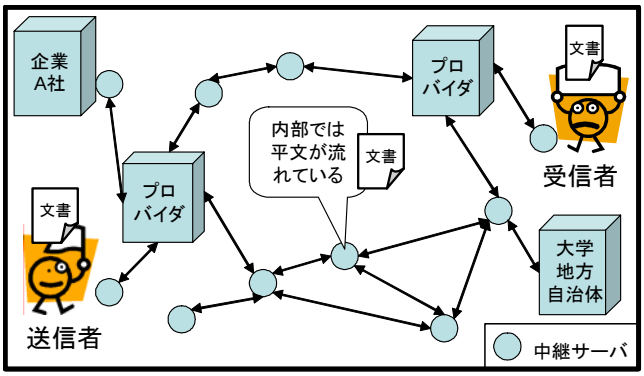


図　1-1 ネットワーク上の通信

[3] ウェブブラウザ：インターネットから HTML ファイルや画像ファイルなどをダウンロードし、閲覧するためのアプリケーションソフトのこと。Microsoft 社の Internet Explorer、Netscape Communications 社の Netscape Navigator、Mozilla.org の Mozilla、Opera Software 社の Opera などが著名なウェブブラウザである。

旧来のようにホームページから情報を取得するだけであれば、これで問題はなかったが、昨今はホームページに対して情報を送信するというケースも増えてきている。

たとえば、インターネットで買い物をする場合や、懸賞に応募する場合に、「氏名、住所、電話番号、クレジットカード番号」といった情報を送信することになる。

利用者から送信されたそれらの情報は、閲覧したときとは逆にインターネット網を経由して取引先のサーバに届くことになる。

その途中に、先ほどのような通信監視や、第 3 者による盗聴が行われていた場合、内容が平文であるため送信した情報が他人に知られてしまう可能性がある。

さらに、インターネットは物理的に遠距離のサーバにアクセスを行う場合、利用者側や取引先でデータを削除しても、中継基地を通った通信内容が残っている場合がある。それらの通信を覗かれた場合も、通信監視や盗聴と同じく利用者にとって不利益なことが起きる可能性がある。このような問題を解決するために、何らかの対策を行う必要がある。

1－2　通信上で起こりうる危険

セキュリティ対策を行っていない通信には、どのような危険が潜んでいるかまとめておく。

ネットワークを使った通信は、人と直接会って話す対話や、電話を用いての通話とは異なり、お互いに顔が見えない。電話通話による声の区別などもなく、文字情報のみでやり取りを行う特徴がある。そのため、一般的に「盗聴」「改ざん」「なりすまし」「否認」という危険を持ち合わせている。

●盗聴

通信の内容を盗み取る行為のことをいう。電話の盗聴では、会話中の音声を聴き取ることを主にしている。しかし、通信上の盗聴は、電子化されている文書や、個人を識別する ID やパスワードなどの需要なデータを丸ごと盗むことができ、すべての情報が容易に外部に流出してしまう恐れがある。

たとえば、図 1-2 のように、送信者から受信者へ送信している文書データを通信中に盗み取ることができる。盗聴は、受信者、送信者に気づかれないことが多く、知らないうちにデータが流出していることが多い。

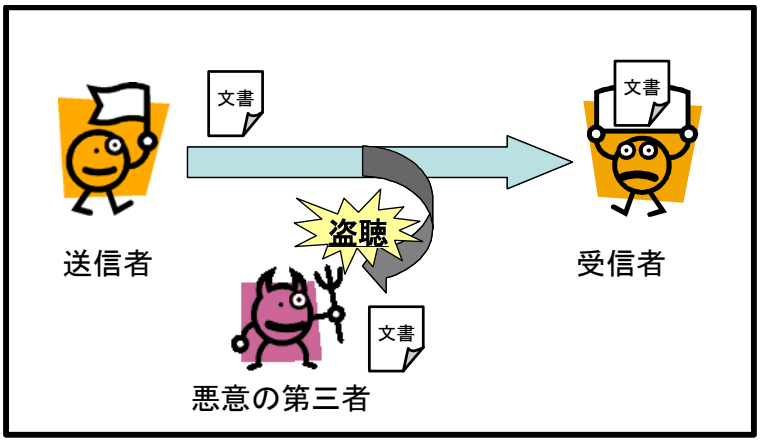


図　1-2　ネットワーク上の危険：盗聴

●改ざん

送信者からのデータを受け取り、内容に変更を加え受信者に送信する行為のことをいう。送信者からのデータは、受信者に渡る途中で書き換えられてしまうので、受信者が変更に気づかずに処理を行ってしまう可能性がある。

銀行での現金の振り込みや送金で起きた場合、金額の桁を少し変えただけでも大変な被害を受けることになる。

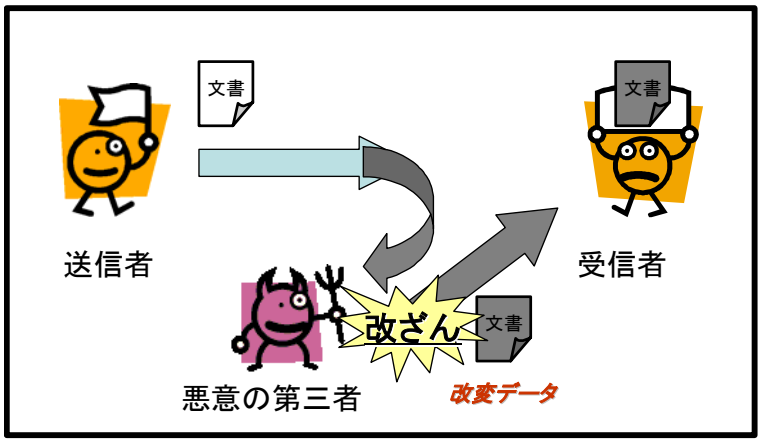


図　1-3　ネットワーク上の危険：改ざん

●なりすまし

受信者に対して、第三者が送信者として振る舞い、悪意ある行動を行う行為のことをいう。

図 1-4 の例では、第三者が、送信者になりすまして商品の注文を行い、送信者にその請求が来てしまうというものである。

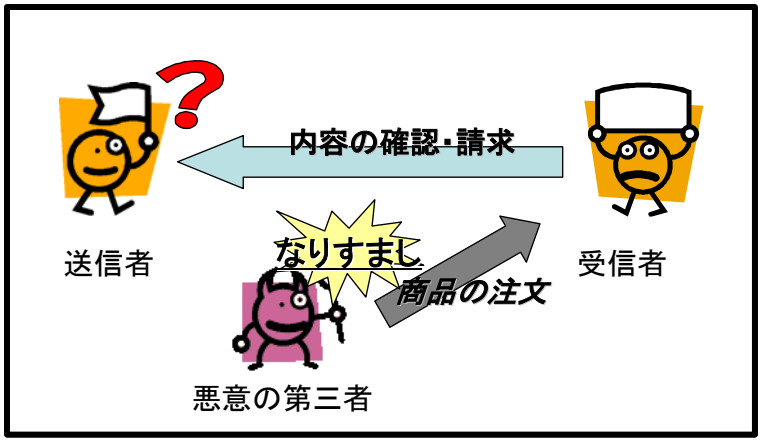


図　1-4　ネットワーク上の危険：なりすまし

●否認

実際に取引を行った本人が、本人であることを認めない行為のことをいう。インターネット上で虚偽の注文等を行って、送信者が注文した事実を認めないなどが考えられる。

もしくは、商品を一度受け取っているのに、受け取っていないと嘘をついて、2 つ目を得ようとする行為も否認のひとつと言える。

否認は、ネットワークの先にいる人物を特定できないため成り立ってしまう。

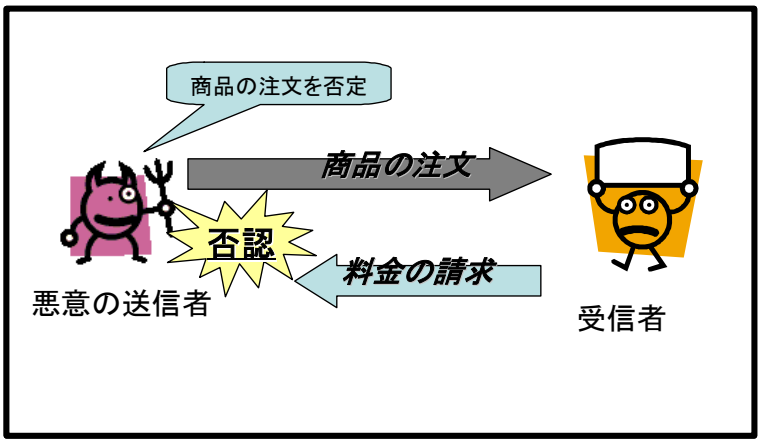


図　1-5　ネットワーク上の危険：否認

インターネットを使った通信は、このような危険を含んでいる。また、それぞれが単一で起こることは少なく、「“盗聴”によって得た ID、パスワードを使って、当人に“なりすまし”、インターネット上で買い物をする。」など、複合的に生じることが多い。

このような危険に対応するべく、利用者側も、ホームページの提供側も対策を講じる必要がある。

1－3　SSL とは

SSL （Secure Sockets Layer（セキュア・ソケット・レイヤー）の頭文字)とは、インターネット上でコンピュータ同士の通信を安全にやり取りするため、内容を暗号化して送受信する技術のことである。

インターネットに流れるデータを暗号化し、プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信するために確立された技術である。

SSL は主要な三つの機能より成り立っている。

・認証局(CA)[4]によるホームページサーバの正当性保障

・利用者側での証明書の確認

・利用者とホームページサーバ間での通信内容の暗号化

●認証局の署名の入った証明書を使ったサーバの正当性証明

ホームページの提供者は、通信する相手が取引先の本人であるか、自分（組織）の運営するホームページが確かに自分（組織）の運営しているホームページであると正当性を証明しなくてはならない場合がある。このとき、自分自身でその正当性を主張しても、不特定多数の人々が閲覧するホームページでは困難を伴う。従って、第 3 者からその正当性を認めてもらうという方法が考えられた。この正当性を認める機関が認証局と呼ばれている。いわばホームページにお墨付きを与える機関である。

ホームページ提供者は、あらかじめ認証局に公開鍵[5]と電子署名[6]を登録して、電子証明書[7]を作成してもらう。それをサーバ側に設定する。

アクセスしてきたホームページの利用者は、ページの中に埋め込まれている証明書を閲覧し、アクセスしたホームページが本物であるか判断する。この仕組みを図にすると「図 1-6 SSL 通信のしくみ（１）サーバ認証」のようになる。

---

4 認証局(Certification Authority)：ネットワーク上に存在する人間の身元や資格、組織を保証する機関のこと。現実の世界でいえば、印鑑証明を発行する役所のようなものであり、書類などの真正性を保証する公証役場と同じ役割を果たす。電子商取引などで使われる電子的な身分証明書を発行する機関。

5 公開鍵・秘密鍵 : 通信の暗号化を行うために用いる、暗号法則に基づいたデータが書かれているもの。鍵は 1 対で生成され、一般に公開されるほうが公開鍵、自ら保管する鍵が秘密鍵と呼ばれる。

6 電子署名（ディジタル署名）: ディジタル文書の正当性を保証するために付けられる暗号化された署名情報。公開鍵暗号方式の応用によって、文書の作成者を証明し、かつその文書が改ざんされていないことを保証する。

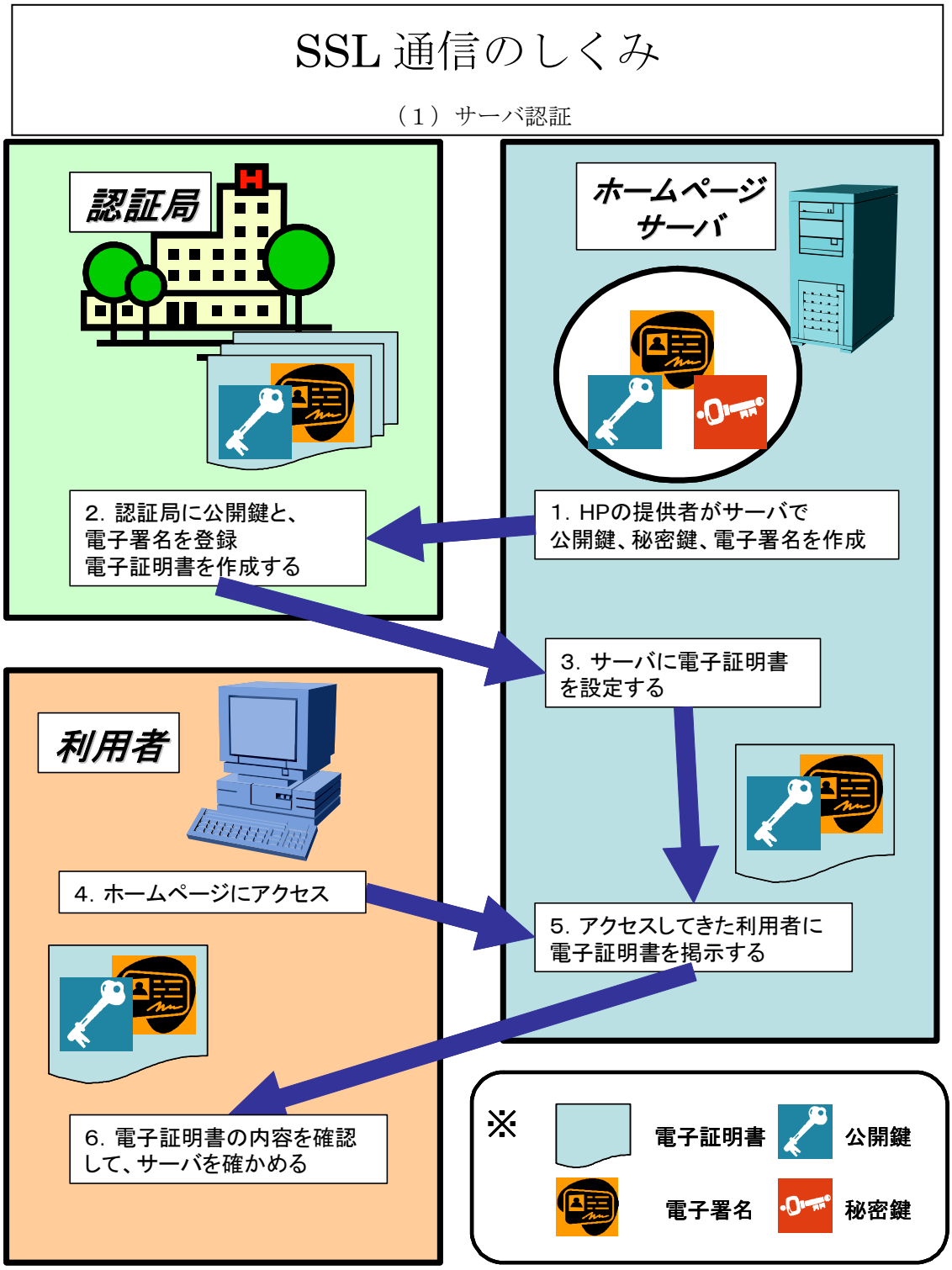


図　1-6　SSL 通信のしくみ　（1）サーバ認証

[7] 電子証明書（ディジタル証明書）：認証局が発行するディジタル署名と公開鍵が真正であることを証明するデータ。ディジタル署名単独では確認できないが、ディジタル証明書をディジタル署名に付属させることにより、データが改ざんされていないことと、データの作成者を証明することができる。

●利用者側での証明書の確認

利用者は、閲覧しているホームページが正しい証明を受けているか、暗号通信が可能かをウェブブラウザに表示させて確認することができる。

「SSL 利用の見分け方」

ホームページに SSL 技術が使われているかを見分けるには、インターネットの住所であるアドレスを確認することにより可能である。

・ SSL が使われているホームページは、通常 http://～で始まるアドレスが、https://～と「s」が付いている。

・ ブラウザの下に錠前のマークが表示される。
ブラウザによって多少異なるが、図 1-7 のようにブラウザの下に錠前のマークが表示されるようになっている。これにより、SSL 技術が使われているか見分けることも可能である。

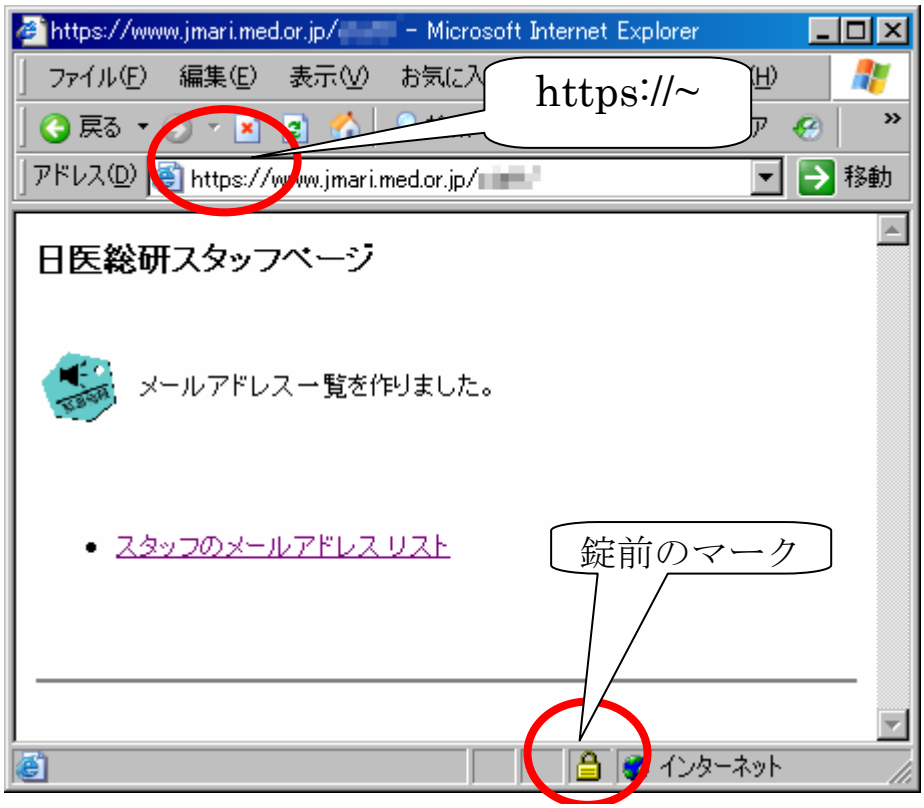


図 1-7 SSL 利用の見分け方

●利用者とホームページサーバ間での通信内容の暗号化

電子証明書により、サーバが正当な取引相手であると認められたのち、暗号化通信が開始される。これにより通信中は内容が暗号化されるので、盗聴などの脅威から回避できる。

具体的な通信のやり取りは「図 1-8　SSL 通信の仕組み（２）暗号化通信」のようになる。

このように SSL を用いることで、会員専用ページにセキュリティ対策を行い、盗聴や改ざん、なりすましなどの通信上の脅威から情報を守ることができる。

サーバ側には鍵の登録、公開、更新作業が必要になるが、主要なウェブブラウザが SSL 技術に対応しているため、利用者は特別な設定をせずに利用することができる。

SSL 通信のしくみ

（２）暗号化通信

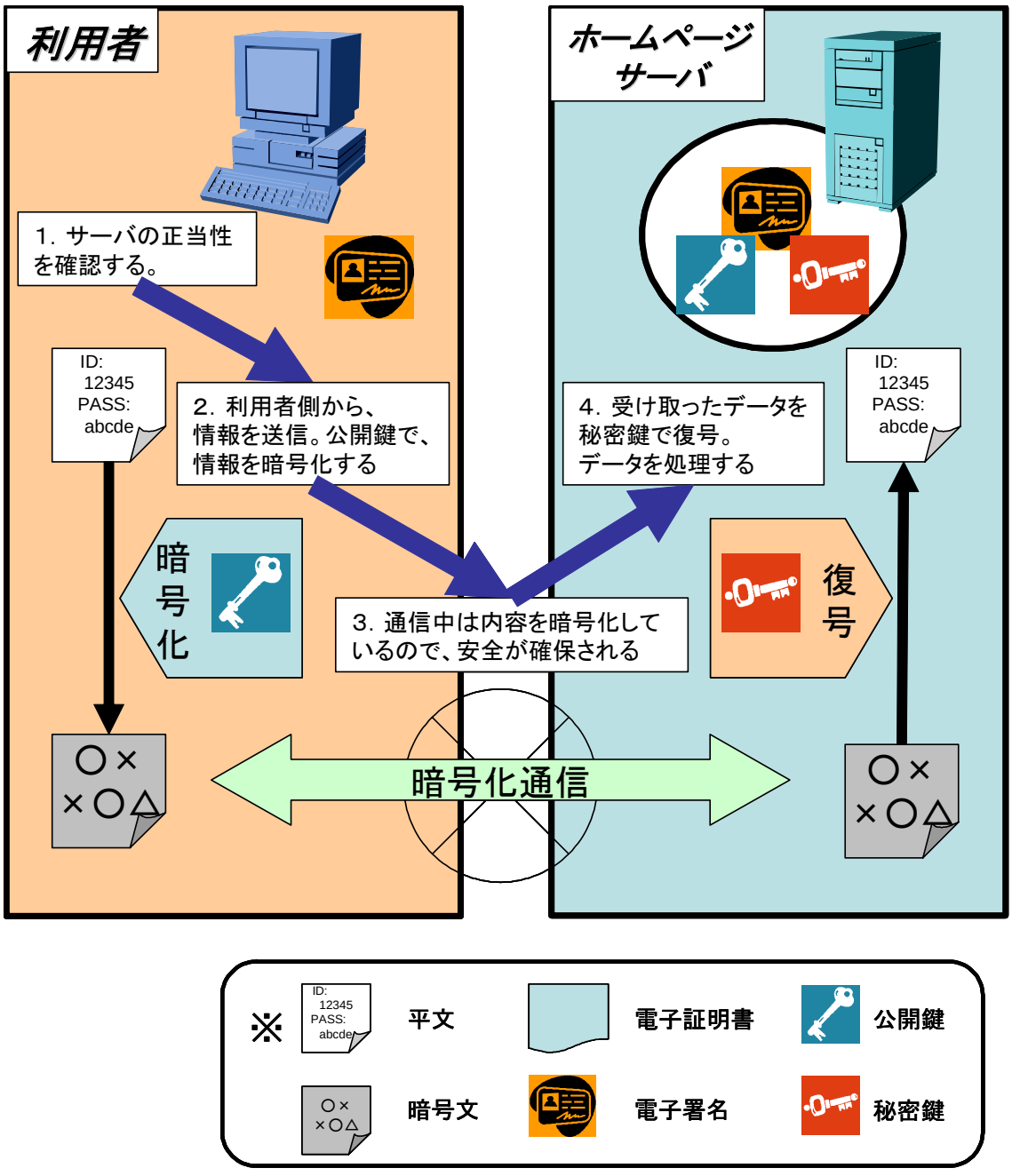


図　1-8　SSL 通信の仕組み（２）　暗号化通信

１－４　会員ページの認証

ホームページセキュリティの中での実装として、一般的に用いられている方法として“パスワード認証”というものがある。

これは、セキュリティ対策のひとつである、“認証”にあたる。本人を確認する方法はいくつかあり、ホームページ上で利用されている認証（本人確認）の方法のひとつに“パスワード認証”というものがある。

●パスワード認証とは

サーバ側は、予め利用者別に決められたユーザ名を配布し、利用者本人にしかわからない文字列で構成するパスワードを入力させる。

この場合、ユーザ名自体は一意に決められているが、パスワードに関しては本人しか知りえないものを用いるので、２つの組み合わせによって本人認証を行い、なりすましを防ぐ方法である。

ユーザ名	：	利用者別に一意に決められた文字列
パスワード	：	ユーザによって生成、変更が可能

図　1-9　ユーザ名とパスワード

これを用いることで、確かに本人であると証明することができる。ただし、パスワードは他人に知られないように記憶し、保管しておく必要がある。

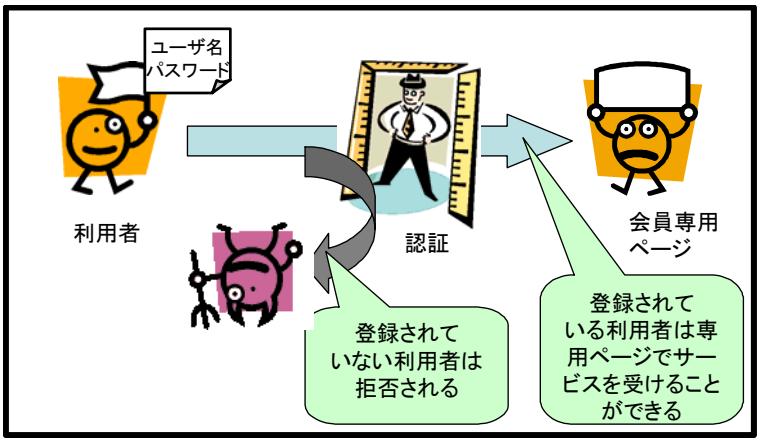


図　1-10　認証の役割

しかし、問題となるのは、「1-2 通信上で起こりうる危険」でも触れた通り、通信上の経路では、ユーザ名とパスワードが平文で送受信されていることである。この状態で通信を盗聴されると、ユーザ情報が容易に漏洩してしまい、大変危険である。

それが悪意のある第三者に渡った場合、盗聴したユーザ情報を用いて、その利用者になりすまし、認証を抜けることが可能になってしまう。

認証を抜けてしまえば、会員ページにある重要な情報を盗むことや、内容を改変することもできる。

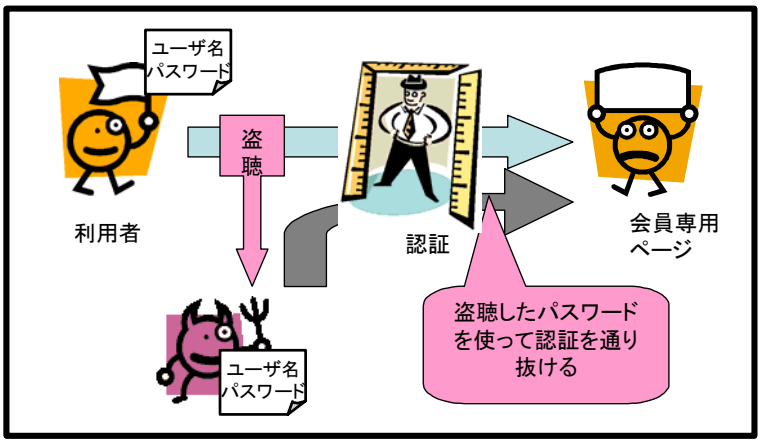


図 1-11 盗聴による認証のすり抜け

このような問題を解決するひとつの方法として SSL がある。この技術を用いることにより、盗聴による、なりすましのような脅威から通信を保護することができる。

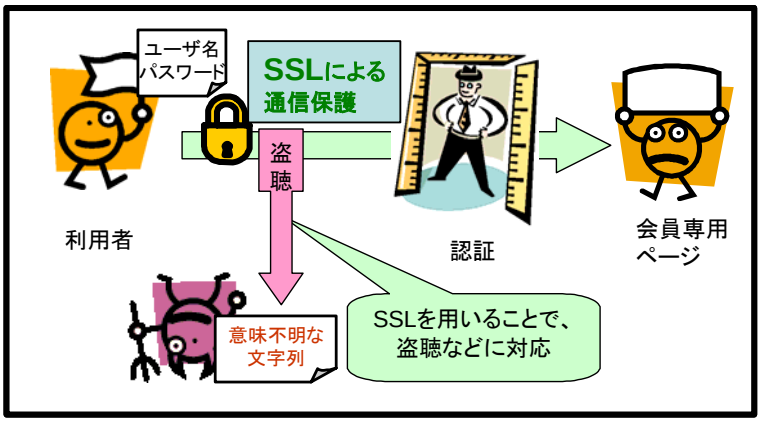


図 1-12 SSL の利用による通信保護

2　調査

2-1　調査目的

前章まで、ネットワーク通信に潜む脅威について説明してきた。ホームページを公開・運用している以上、一般企業などと同様に医師会が運営しているホームページもセキュリティ対策を常に意識する必要がある。

そこで、身近な事例として医師会員の利用の多い都道府県・郡市区医師会のホームページの調査を行った。

都道府県・郡市区医師会の場合、各医師会に所属している会員向けに作成された会員専用ページを用意していることが多い。このことから会員ページを調査することで、ホームページのセキュリティ状況やセキュリティ技術の普及度合いを把握することを目的として実施した。

ただし、会員ページ内のコンテンツに関しては、直接調査することができないので、今回は主に、ホームページでの会員ページの運営と、SSL の利用について動向調査を行った。

2-2　調査対象

日本医師会が運営している「日本医師会ホームページ[8]」にあるリンクから辿れる各医師会のホームページを調査対象としている。

ホームページ内の「各地の医師会へのリンク[9]」より、都道府県・郡市区医師会のホームページの所有数は、2004 年 9 月現在以下の通りであった。

都道府県医師会……全国 47 ヶ所中 47 ヶ所（100.0%）
郡市区医師会……全国 916 ヶ所中 662 ヶ所（72.3%）

[8] 日本医師会ホームページ　http://www.med.or.jp
[9] 日本医師会ホームページ内、各地の医師会へのリンク http://www.med.or.jp/kakuti/kakuti/link.html

全体から見ると７割以上(73.6%)の医師会がホームページを運営していることになる。

予備調査をしていた 2004 年 4 月の時点で郡市区医師会のホームページ数は、633 ヶ所であったので、医師会サイトの開設数は約半年で 29 ヶ所(4.37%)増えたことになる。

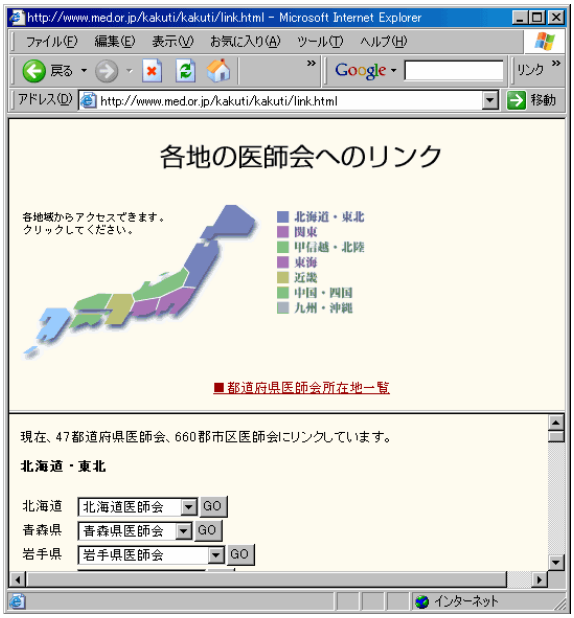


図　２-１　各地の医師会へのリンク

２－３　調査方法

調査環境は、一般的に用いられるパソコンとし、以下の環境で実施した。

- OS：　Microsoft Windows XP　(Professional Service Pack1)
- ウェブブラウザ：　Internet Explorer(Ver.6)

ホームページのリンクより、各医師会のホームページを閲覧し、「２－4　調査項目」に従って全てのリンク先のページで確認した。

2－4　調査項目

各医師会のホームページを閲覧した際に、以下の点を調査し、集計を行う。

・ホームページの閲覧（できる・できない）

リンクで判断できるのが、対象のホームページが「閲覧できる状態にあるかどうか」である。

閲覧できない場合でも、調査実施時にホームページの更新を行っていて、一時的にファイルがない状態になっていることが考えられる。この場合は数日置いた後に再調査を行った。

他には別の場所にホームページが移動しており、移動した旨を案内している場合などがあげられる。移動を行っている場合は、その移動先を対象に調査を行った。

・会員ページの存在（あり・なし・作成中）

閲覧できたホームページが会員専用のページを作成しているかどうかを調べる。それぞれを見分ける方法は次のように行った。

『あり』

ホームページの内部に、「会員ページ」、「会員専用」などが書かれていて、そのリンクの先にデータがあるホームページ。

『なし』

会員ページなどの表記がないホームページ。

『作成中』

会員ページ作成中と表示されているもの。もしくは、会員専用ページなどの表記がされていても、その先にデータが無いホームページ。

・会員ページに認証が必要（あり・なし）

会員専用ページが存在していて、会員ページの内容を閲覧する際に認証が必要になるかどうかを調べる。

この場合用いられる認証方法は、パスワード認証である事が多く、他に方法がある場合は別途記録する。

・認証に SSL を利用しているか（あり・なし）

認証が必要なページの中で、SSL 通信が設定されているかどうかを調べる。SSL を見分ける方法については、“1-3 SSL とは　●利用者側での証明書の確認”に記述してある方法で判別した。

SSL 通信を用いている場合は、どこの認証局を用いているかを記録していた。

調査手順のフローは、「図 2-2　ホームページ分類フロー」のようになる。

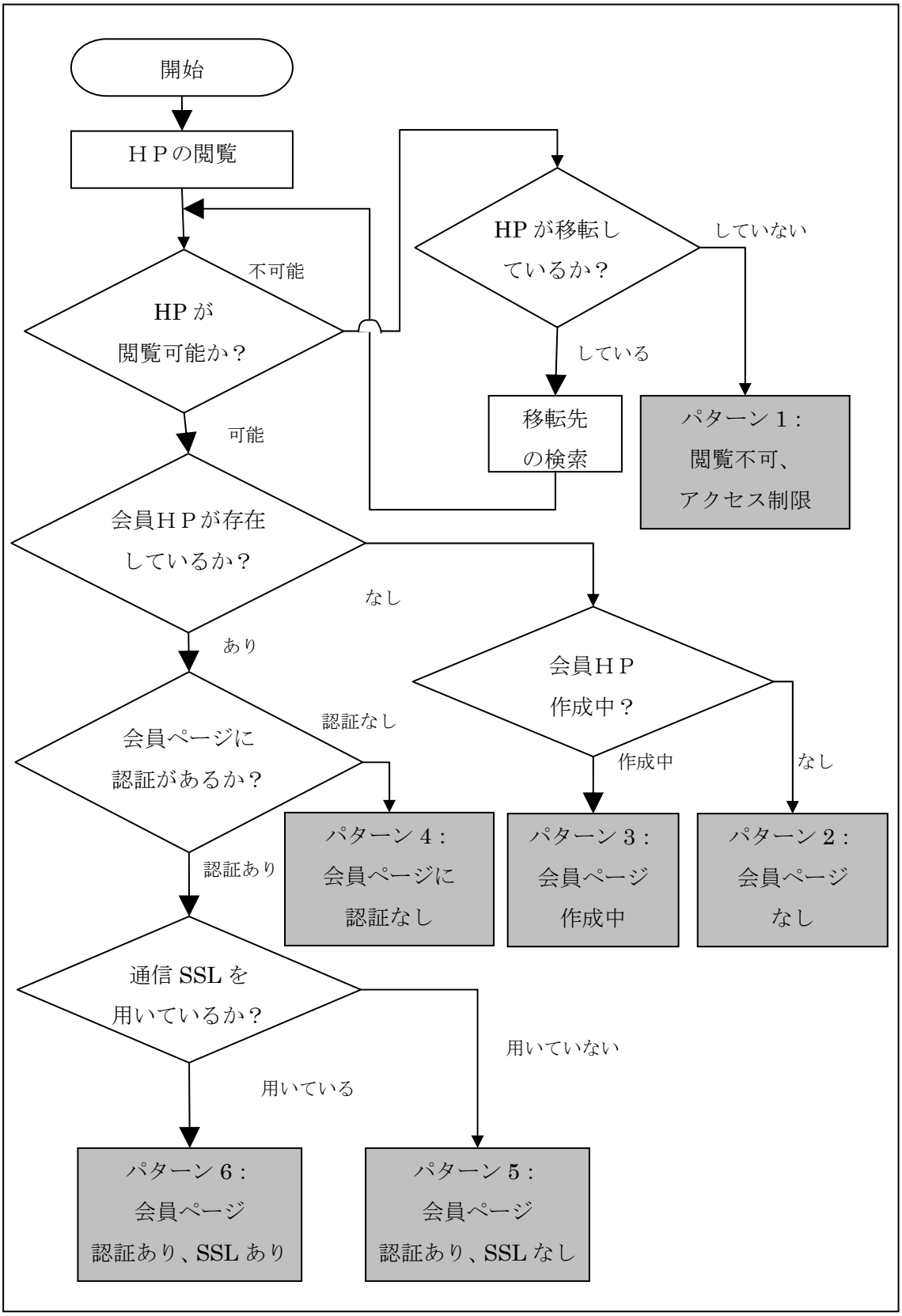


図 2-2　ホームページ分類フロー

このフローを元に調査を進めると、ホームページは以下の 6 つに分類することができる。

表 1　ホームページの分類

パターン1	閲覧不可、アクセス制限
ホームページ自体が作成途中で表示できない。 ホームページのアドレスが内部にしか公開されていない。	
パターン2	会員ページなし
公開はされているが、会員向けページが存在していない。	
パターン3	会員ページ作成中
ホームページに会員ページの項目が存在しているが、 （正常に）稼動していない。 または、作成中と明記されている。	
パターン4	会員ページ認証なし
会員ページが存在するが、認証する機能はなく、 一般からアクセスしてきた人でも閲覧できる。	
パターン5	会員ページ認証あり、SSLなし
会員ページを見る際に、 パスワードによるログインは必要になるが、 SSLやそのほかの通信を暗号化する機能などはない。	
パターン6	会員ページ認証あり、SSLあり
ログイン画面に、SSLを用いて通信を暗号化している。	

・ホームページアドレスの調査

ホームページを閲覧する場合、インターネット上の住所と呼ばれるホームページアドレスが必要となる。

日本医師会のホームページアドレスは、 http://www.med.or.jp/ である。その中にある、http://の部分は「ホームページを表す決まり」、www の部分は「管理しているコンピュータ」、med.or.jp の部分は「日本医師会」を指している。その中の or.jp[10]の部分は「非営利組織」などに与えられるアドレスであり、その中の jp 部分は「日本専用ドメイン」であることを示している。これらのようなアドレスは、JPNIC[11]という機関から割り振られている。

このようにドメインを見ることで、そのアドレスの提供者が分かる仕組みになっている。

日本医師会(med.or.jp)が都道府県医師会にアドレスを提供する場合、ホームページのアドレスは、「http://www.都道府県名.med.or.jp/」となる。

さらに、都道府県医師会が郡市区医師会にアドレスの提供する場合、「http://www.郡市区.都道府県.med.or.jp/」となる。

また、より上位のアドレス管理組織からアドレスの提供を受けて構成されるドメインのことをサブドメインと呼ぶ。医師会の場合、都道府県医師会のドメインは日本医師会のサブドメインになり、群市区医師会のドメインは都道府県医師会のサブドメインになる。

一方、都道府県医師会がホームページの一部を郡市区医師会に貸し出して運営する形態も見られる。この場合、アドレスは「http://www.都道府県.med.or.jp/郡市区/」のようになり、サブドメインとは呼ばない。

これらを図として、表すと「図 2-3 ドメインの構成」のようになる。

これらを郡市区医師会のホームページアドレスから、それぞれのホームページ提供元がどのように分布しているか数を調査した。また、医師会ドメインに関しては、都道府県医師会から提供を受けたサブドメインとして運営しているか、都道府県医師会ホームページの一部（間借り）であるかを分けて表にした。

10 JP-NIC「ドメインの種類」: http://www.nic.ad.jp/ja/dom/types.html
11 JP-NIC(JaPan Network Information Center) : http://www.nic.ad.jp/

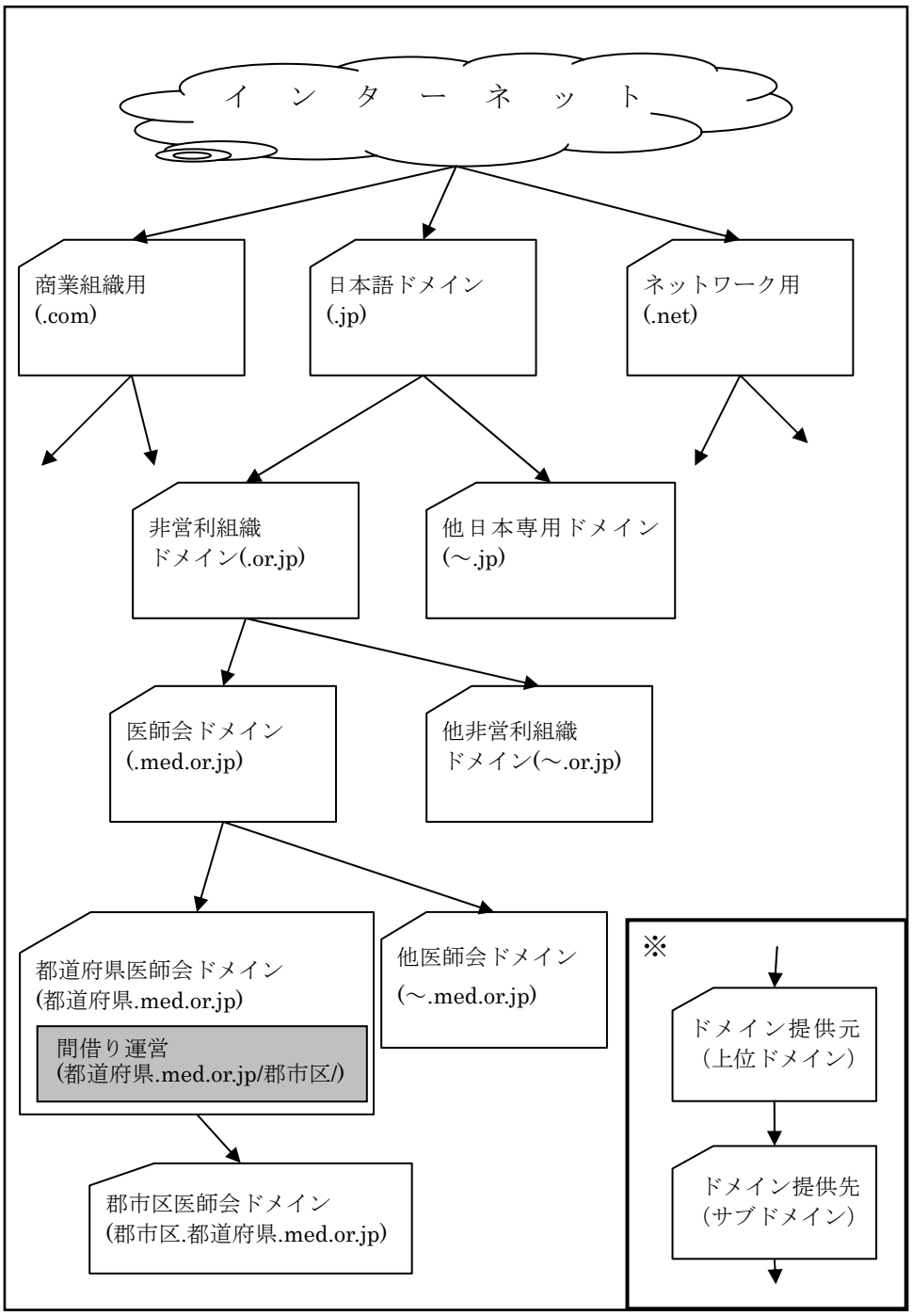

イ　ン　タ　ー　ネ　ッ　ト
商業組織用
(.com)
日本語ドメイン
(.jp)
ネットワーク用
(.net)
非営利組織
ドメイン(.or.jp)
他日本専用ドメイン
(～.jp)
医師会ドメイン
(.med.or.jp)
他非営利組織
ドメイン(～.or.jp)
都道府県医師会ドメイン
(都道府県.med.or.jp)
間借り運営
(都道府県.med.or.jp/郡市区/)
他医師会ドメイン
(～.med.or.jp)
郡市区医師会ドメイン
(郡市区.都道府県.med.or.jp)
※
ドメイン提供元
（上位ドメイン）
ドメイン提供先
（サブドメイン）

図　2-3　ドメインの構成

２－５　調査結果

調査項目に従い分類したホームページ数より、都道府県、郡市区医師会別に調査結果を示す。

（１）全体分布

都道府県および郡市区医師会全体で見ると、会員ページなし（パターン 2）が 398 ヶ所(56.14%)となり、会員ページを運営している医師会（パターン５とパターン 6）は 271 ヶ所（38.22%）となる。また、会員ページの中で、SSL なし会員ページ（パターン 5）が 265 ヶ所、SSL 認証つき（パターン 6）は 6 ヶ所となった。

都道府県では、認証あり会員ページ（パターン５とパターン６）が全体で 31 ヶ所（65.60%）確認された。その内、SSL なし会員ページ（パターン５）が 29 ヶ所にのぼり、SSL 認証あり会員ページ（パターン６）は 2 件に留まっている。ついで会員ページがないもの（パターン２）が 12 ヶ所（25.53%）と続く。

郡市区医師会では、認証あり会員ページ（パターン５とパターン６）が全体で 240 ヶ所（36.25%）確認された。その内、SSL なし会員ページ（パターン５）が 236 ヶ所、SSL あり会員ページ（パターン６）は 4 ヶ所となっている。ただし、郡市区医師会は、会員ページがないところ（パターン２）が 386 ヶ所(58.31%)と最も多いという結果であった。

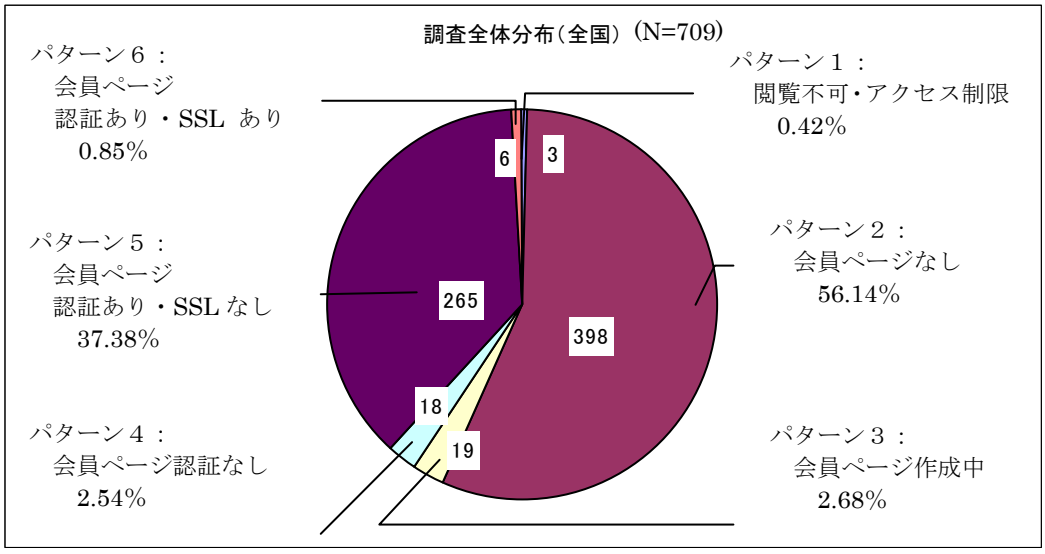


図　2-4　調査全体分布（全国）分布状況

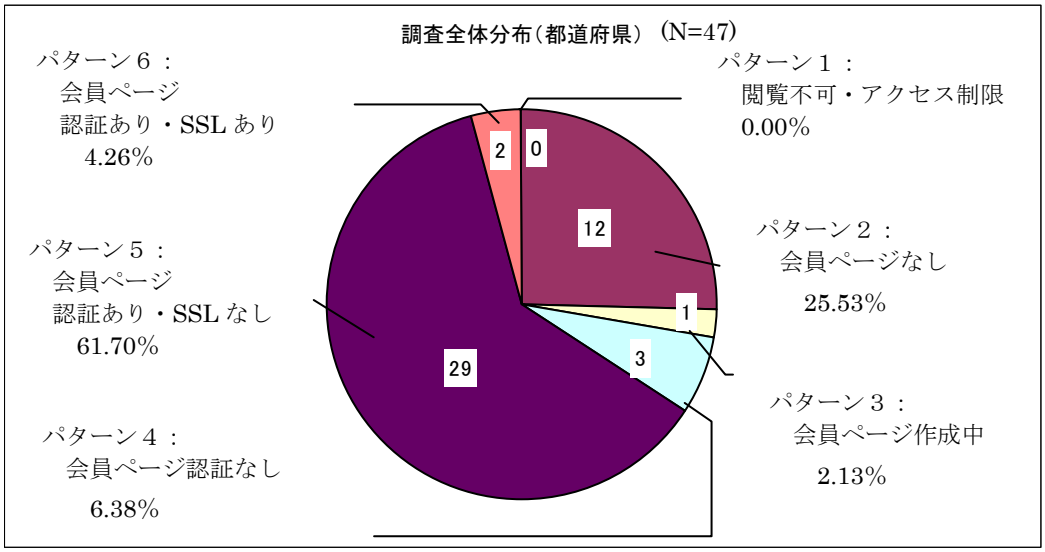


図 2-5　調査全体分布（都道府県）分布状況

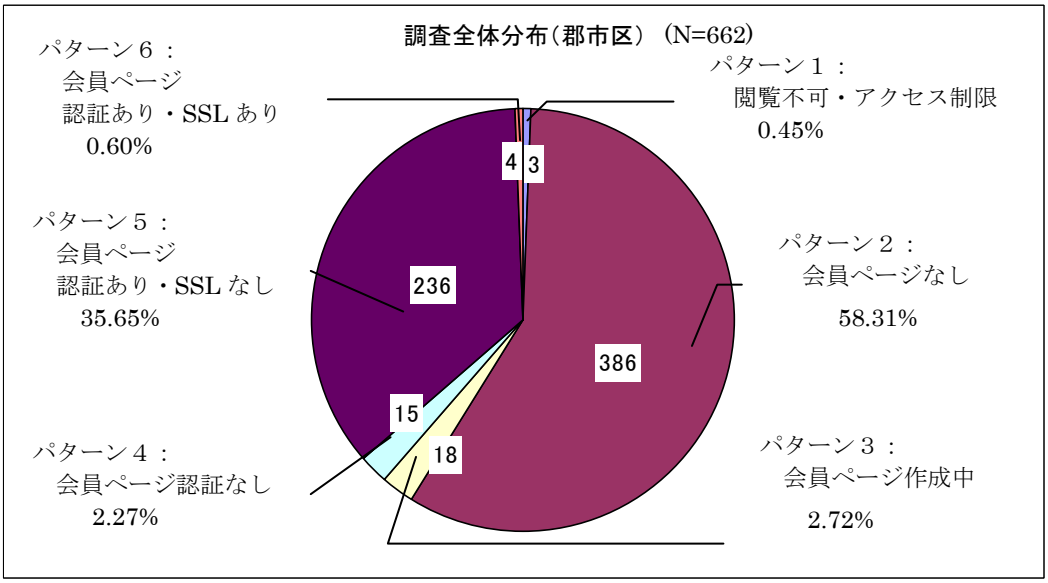


図 2-6　調査全体分布（郡市区）分布状況

（2）ホームページアドレス

ホームページアドレスから調査した、各医師会のアドレス提供元の割合を表 2 に示す。

郡市区医師会 662 ヶ所中、med.or.jp から提供を受けたアドレスとして登録されているのが 311 ヶ所(47.0%)、県医師会から間借りしているのが 147 ヶ所(22.2%)であった。県医師会のサブドメインとして存在しているのが 164 ヶ所(21.0%)、さらに 25 ヶ所（3.8%）はいくつかの地域をまとめてサブドメインの提供を受けて共同運営を行っている。

これより、172 ヶ所(26.0%)の郡市区医師会では、共同運営か都道府県医師会より借り受ける形でホームページを運用していることが判明した。

このほかにも、日本国内の一般のネットワークサービス提供者より借り受けて運営しているホームページの（ne.jp）アドレスが 98 件(14.8%)あった。

なお、都道府県医師会については、47 ヶ所すべてが、med.or.jp から提供を受けて、各自のホームページを運営していた。

表 2　郡市区医師会のホームページアドレス

郡市区医師会　ホームページ提供元割合（n=662）

1．提供者ドメイン

種類	医師会数	割合
日本専用ドメイン(.jp)	628	94.9%
商業組織用(.com)	21	3.2%
ネットワーク用(.net)	7	1.1%
非営利組織用(.org)	3	0.5%
他ドメイン	3	0.5%
郡市区医師会　合計	662	100.0%

2．日本専用ドメイン

種類	医師会数	割合
非営利組織(.or.jp)	492	74.3%
ネットワークサービス提供者(.ne.jp)	98	14.8%
株式会社・各種会社(.co.jp)	9	1.4%
学校法人(.ac.jp)	4	0.6%
医師会独自(～-med.jp)	10	1.5%
医師会独自(～ishikai.jp)	4	0.6%
他.jp	11	1.7%
日本専用ドメイン　合計	628	94.9%

3.非営利組織ドメイン

種類	医師会数	割合
医師会ドメイン(.med.or.jp)	311	47.0%
医師会独自(～-med.or.jp)	110	16.6%
医師会独自(～ishikai.or.jp)	12	1.8%
他or.jp	59	8.9%
非営利組織ドメイン　合計	492	74.3%

4．医師会ドメイン

種類	運営方法	医師会数	割合
都道府県ドメイン	間借り運営	147	22.2%
郡市区ドメイン	共同運営	25	3.8%
	独自運営	139	21.0%
医師会ドメイン(.med.or.jp)　合計		311	47.0%

（3）会員ページ運営率

調査結果から、都道府県医師会では、会員ページの運営率が 72.3%にのぼり高い水準を示していることが分かった。一方で、郡市区医師会の運営率は 38.7%であった。

「（2）ホームページのアドレスの調査」で間借り運営、共同運営をしている 172 ヶ所では、都道府県医師会が運営しているホームページの一部を郡市区医師会に貸し出して運営している箇所が多く見受けられた。そのほとんどのページは 1 ページ程度の紹介文であった。

この間借り運営の状態では、郡市区医師会側が独自でホームページを運営しているわけではないので、独自の会員ページも開設しにくい。

そのようなところでは、会員ページの運用は都道府県に任せているという状況が伺えた。

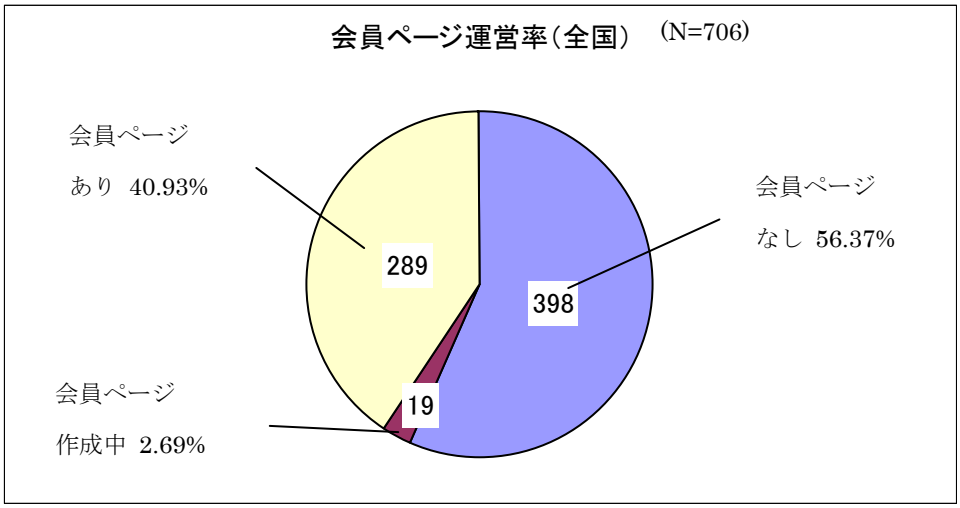


図 2-7　会員ページ運営状況（全国）

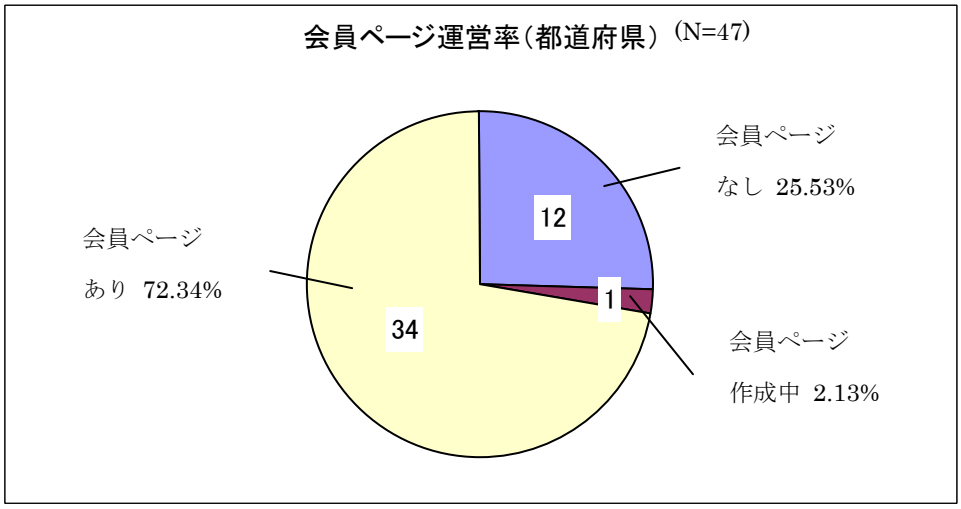


図 2-8 会員ページ運営状況（都道府県）

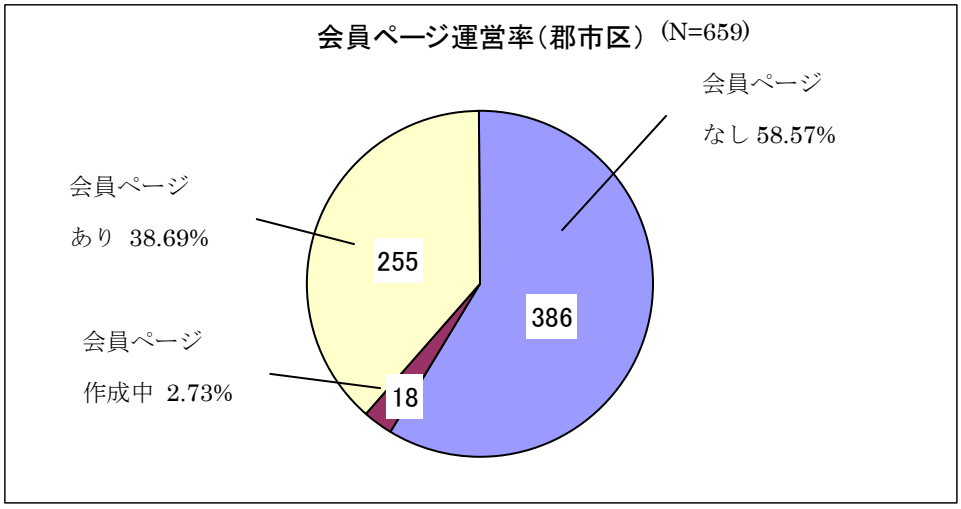


図 2－9 会員ページ運営状況（郡市区）

（4）会員ページを運営中で、会員認証を利用している割合

会員ページを運営しているサイトの中で、会員専用ページにログインする際に認証を用いていたホームページの割合は、都道府県医師会、郡市区医師会共に、9 割を超えていた。

全体で見ると、289 ヶ所の会員専用ページに対して、271 ヶ所のページにおいて認証が要求されていた。都道府県医師会では 34 ヶ所中 31 ヶ所、郡市区医師会では 255 ヶ所中 240 ヶ所であった。

ホームページの運用に際して、会員ページでは会員のみに対して情報を開示して利用者を制限するという方法が浸透しており、利用者を制限していないページでは、会員向けの行事予定等の情報を掲載しているところが多い。

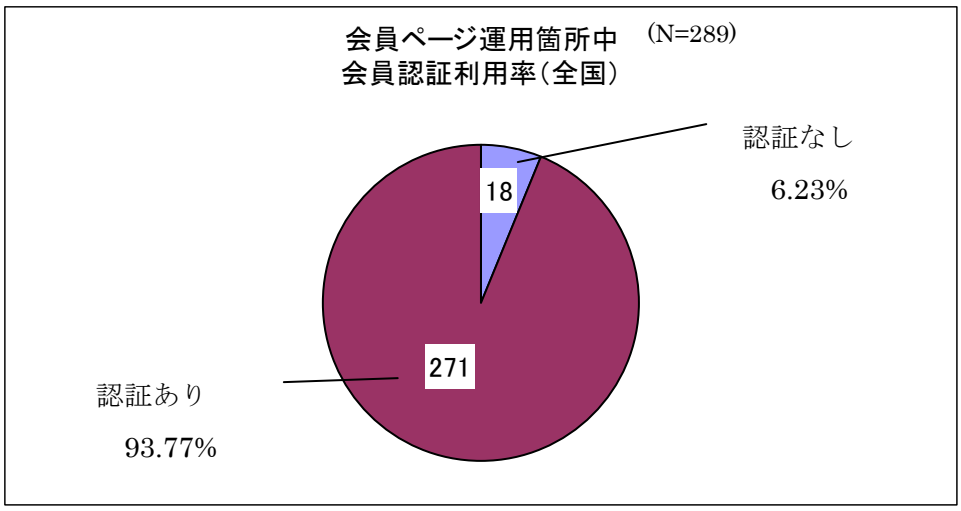


図 2-１０　会員ページ内　認証利用状況（全国）

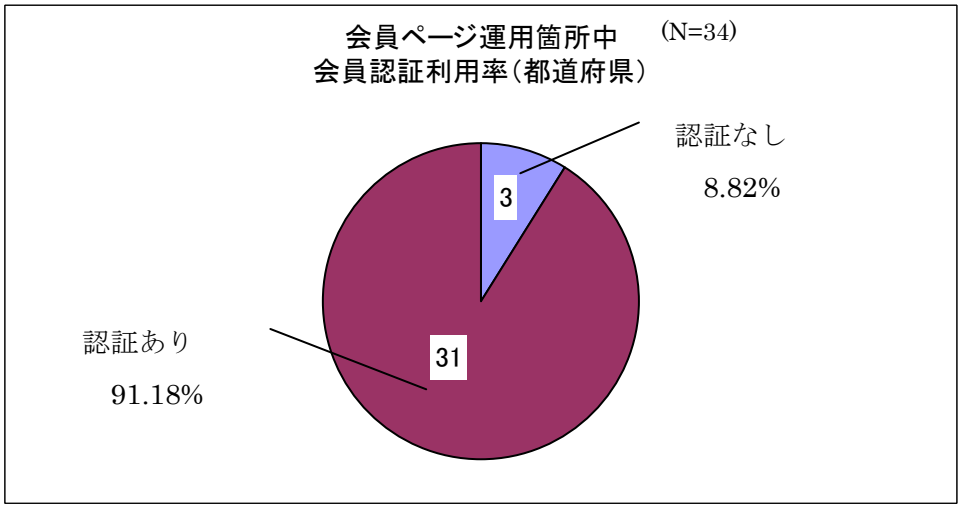


図　2-１１　会員ページ内　認証利用状況（都道府県）

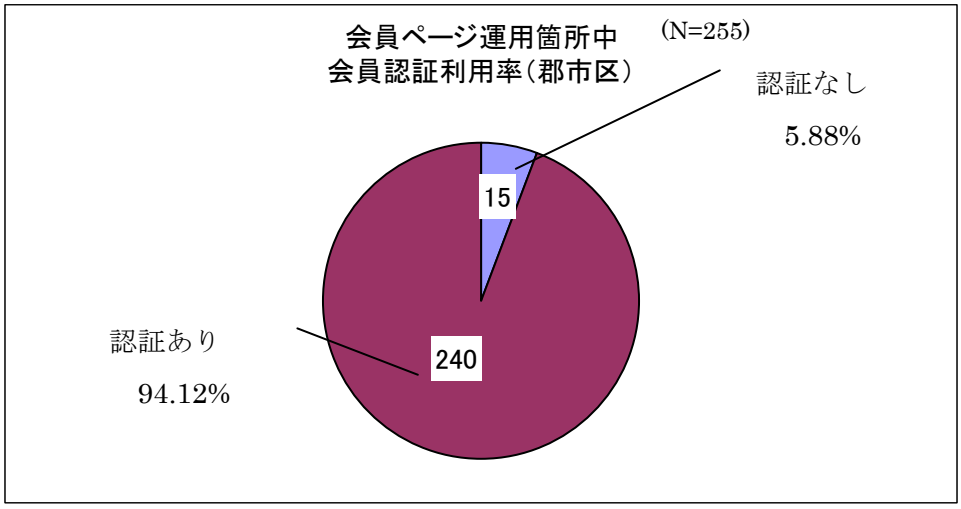


図　2-１２　会員ページ内　認証利用状況（郡市区）

（５）会員認証が必要なサイトの中での SSL 利用率

会員ページに認証を用いているサイトで SSL を利用している割合は、都道府県医師会、郡市区医師会共に 1 割に満たないことが分かった。

先ほどの「（４）会員ページを運営中で、会員認証を利用している割合」の中で、全体で 271 ヶ所のホームページで会員認証が必要であったにも関わらず、その中で SSL を利用しているのは 6 ヶ所しか存在しない。都道府県医師会、郡市区医師会別に見ても、都道府県医師会で 31 ヶ所中 2 ヶ所（利用率：6.45%）、郡市区医師会で 240 ヶ所中 4 ヶ所（同：1.67%）となっている。

調査結果から見ると、SSL 技術は医師会が運用しているホームページにほとんど普及していない。

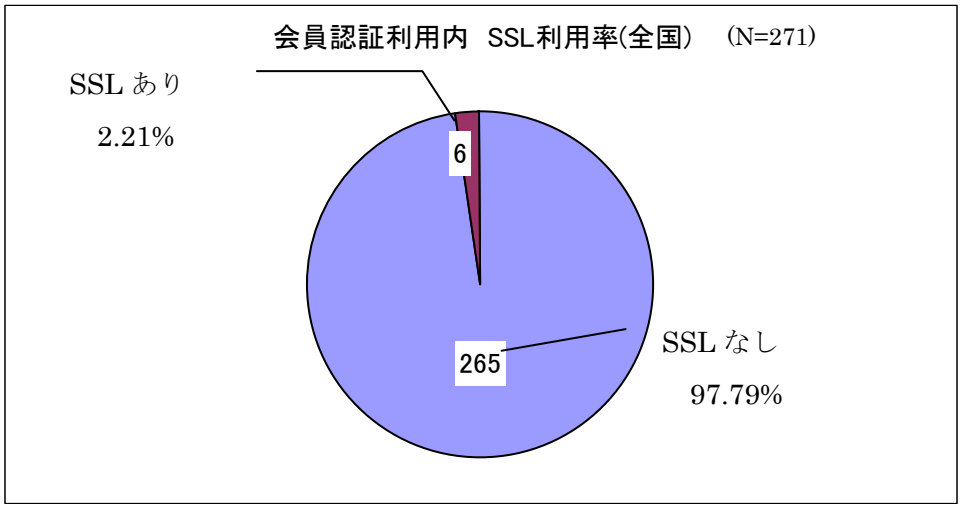


図　2-１３　会員認証　SSL 利用率状況（全国）

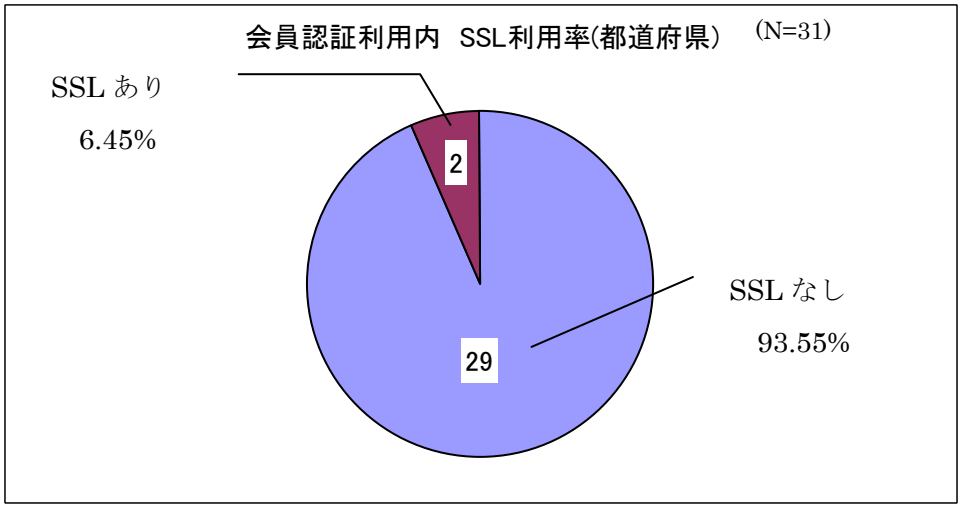


図　2-１４　会員認証　SSL 利用率状況（都道府県）

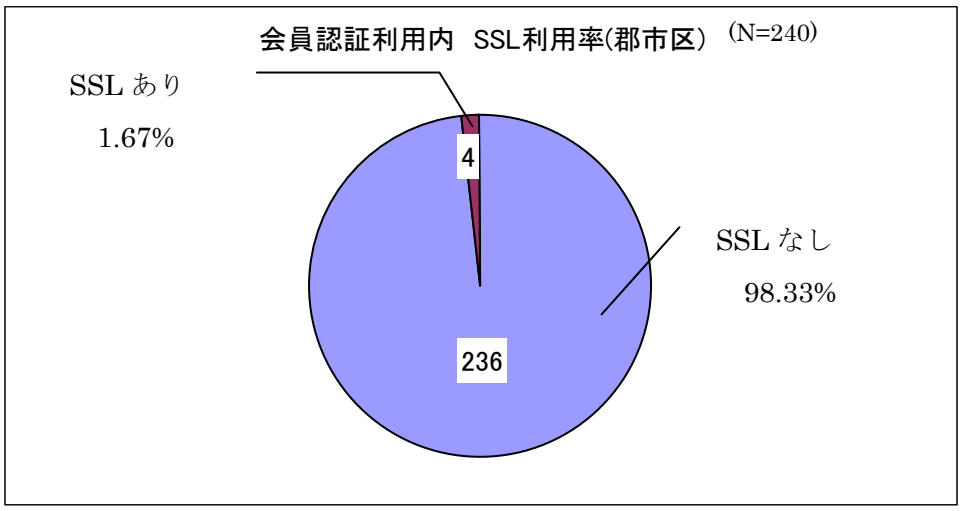


図　2-１５　会員認証　SSL 利用率状況（郡市区）

（6）利用している SSL サービス提供者名

実数は少ないが、調査対象の中で SSL を利用している場合、どこの SSL サービスを利用しているか、そのサービス提供者名と数を調べた。

SSL サービス提供企業は、都道府県医師会では、日本ベリサイン㈱社が 1 ヶ所、Thawte-Japan が 1 ヶ所、郡市区医師会では、日本ベリサイン㈱社が 3 ヶ所、医師会独自が 1 ヶ所であった。

今回は SSL の利用箇所数が少ないので、統計とは言えないが、SSL サービス事業を古くから行っている日本ベリサイン社の利用率が大部分を占めていた。SSL 事業を行う企業は増加してきているので、今後多種多様なサービスが望めるであろう。

今回独自としている箇所は、一般・商用の SSL サービスではなく、郡市区医師会単独で証明書を発行している。これには OpenSSL[12]などの SSL を行うソフトを用いて、独自の証明書を作成する方法がある。

表 3　SSL 利用分布

SSL利用箇所中　利用認証局名（全体）

	都道府県		郡市区		全体	
調査項目	調査数	割合(%)	調査数	割合(%)	調査数	割合(%)
日本ベリサイン社	1	50.00%	3	75.00%	4	66.67%
Thawte-japan社	1	50.00%	0	0.00%	1	16.67%
独自	0	0.00%	1	25.00%	1	16.67%
全体	2	100.00%	4	100.00%	6	100.00%

[12] OpenSSL：本サイト　http://www.openssl.org/
日本語サイト　http://www.infoscience.co.jp/technical/openssl/

2-6　調査のまとめ

今回の調査では、日本全国に約 1000 箇所の医師会がある中で、その約 7 割がホームページを運営し、さらにその内、約 4 割強が何らかの会員ページを所有していることが分かった。特に、都道府県医師会では、会員ページ運営率が 72.3%にも上っていた。しかし、会員ページを運営していて、SSL 技術のような何らかのセキュリティ対策を施している医師会は、全体で見ても 6 箇所と 1 割に満たないことも判明した。

今回の調査では、医師会が運営しているホームページが SSL 技術をどれくらい利用しているかのみを調査した。当然、会員専用ページに入るための ID やパスワードは調査実施側には分からない。従って、会員専用ページに置かれている情報が何かということは把握できない。このため、現在のホームページの運営形態であれば、提供する情報や会員から集めた情報そのものに、特に守秘性がないことも十分に考えられる。しかしながら、ID やパスワードは、複数のシーンで使い回す個人も多いため、銀行口座などの個人特定のできるデータベースに結びつくような場合、立派な個人情報であると言える。そのため、SSL 技術等のセキュリティが施されていない場合、各会員自身の ID やパスワードがインターネット上を平文で流れる点に留意しなければならない。

なお、SSL を利用するサイトとして目立つのが、直接お金を扱うようなネットバンクやネットショッピングなどである。このことから、SSL 技術利用のイメージが医師などの会員情報等を守ることに結びつかないケースも想定される。

このように、セキュリティに対しては、ホームページを運営する側のネットワーク上の危険へ対する感覚の違いが存在していることは否定できない。

また、単純な技術的な問題が存在するケースも考えられる。ホームページのサーバを自身で保有しておらず、外部にあるレンタルしたサーバで運営しており、レンタル会社が SSL に対応できない場合などが当てはまる。この技術的問題が考えられるホームページは、ネットワーク提供者(ne.jp)、株式会社・各種会社(co.jp)、商業組織(com)のアドレスを取得しているところで 128 ヶ所(19.3%)にも上る。また、SSL 導入に際し、別途費用がかかるため導入できないなどの経費の問題も考えられる。

しかし、このような様々なケースが想定されるにしても、例えば 2005 年 4 月から完全施行される個人情報保護法など、個人情報の取扱い、それに伴う利用者のセキュリティ意識の高まりなどの情勢を考えると、会員ページ内の情報の守秘性の洗い出し、会員個人の ID やパスワードの管理方法を合わせて対策しておくことが望ましい。また、技術的問題であったとしても、必要であれば SSL に対応できるサーバに移動し

たり、経費をかけることも考えなくてはならない。

セキュリティというものは、導入したからといって目に見えて、その成果が現れるというものではない。また、このようにしていれば安全という一定のルールが存在している訳でもない。そのため、費用対効果が明確に計算できなかったり、どのように対策を立てればよいか分からない場合もある。ところが、一旦セキュリティ侵害や、個人情報の漏洩などが起きれば、その被害は甚大なものになる危険性をはらんでいる。そのためには、ホームページを提供する医師会が、セキュリティに対する正しい認識を持つ必要があると考える。

３　セキュリティ対策のために必要な知識

ホームページを運営し、ID やパスワードなど、何らかの情報を扱う限り、セキュリティのことを常に意識しておく必要がある。しかし、セキュリティ侵害を恐れ、闇雲にセキュリティの対策を施すというだけでは、本当の意味でのセキュリティ対策とは言えない。「２－６　調査のまとめ」でも述べたように、まずはセキュリティに対する正しい認識や知識を持つ必要がある。

本章では、ホームページの運営という観点に限定して、どのようなセキュリティ対策が考えられるのか、その方策を挙げてみる。

３-１　セキュリティ対策の分類

危険を極力回避するには、セキュリティ対策を確実に行う必要がある。しかし、セキュリティの対策を実施するには、何に対してどの程度のセキュリティ対策を実施する必要があるのか知らなくてはならい。

そこで、最初にセキュリティ対策の分類をする。一般に、セキュリティ対策を方法別に分類すると次の５つに分類できる。

●通信の暗号化

インターネットなどを通じて情報をやり取りする際に、通信の当事者間でしか分からない、ある決まった規則に従ってデータを変換してやり取りすること。

暗号化を行うことで、通信途中で第三者に盗聴された場合でも、内容を見ることができないため、改ざんを防ぐことができる。

●認証

コンピュータを利用しようとしている人が、利用するための正当な権利を保持しているか確認したり、利用者が名乗っている本人かどうかを確認すること。

たとえば、ユーザ名とパスワードの組み合わせを使って、利用者を識別することで利用者ごとに異なるサービスを提供する場合に用いる。

最近では、ID パスワードの代わりに個人の生体情報（手の指紋や眼の網膜パターンなど人によって異なる部分）をあらかじめ登録しておき認証するバイオメトリクスと呼ばれる方法もある。

●ウィルス対策

コンピュータウィルスから利用者を守ること。

最近は、感染したコンピュータに対して破壊活動をするものや、外部からアクセスできるように設定を変更してしまうもの、ウィルスそのものを広めるものなどさまざまなウィルスが発生している。

感染経路も、電子メールからの感染やホームページを閲覧するだけで感染するウィルスなど多岐に渡り、気づかないうちに自分のコンピュータがウィルスの感染源となっていることもある。

このようなことにならないように、ウィルス対策ソフトの導入、セキュリティホール対策などを実施する。また、常に最新の情報を得るように心がけ、対策ソフトを常に最新の状態にしておくなどの必要がある。後述するフィルタリングなどの技術もその一つである。

●フィルタリング

通信に対して一定の法則を定め、情報の仕分けを行うこと。

ホームページサーバのような、外部からアクセスがある危険な部分には、外部からアクセスできないような設定を実施しておく。

大量のアクセスがくる場合には、権限を持った者のみが内部にアクセスできるように設定するなど、状況にあった設定が必要となる。

会員ページのように、一部の利用者のみがアクセスできるように設定をするのはフィルタリングの一つである。

また、フィルタリングソフトと呼ばれるものも存在する。内容の良し悪しの分別が付かない子供たちに、暴力的なページやアダルトサイトのようなものを見せないために保護者の判断によって閲覧するページの取捨選択をするものである。これも、情報の仕分けを行うためのものなので、フィルタリングの一種だといえる。

●障害対策

機械の物理的な故障や、通信経路のトラブル、災害などを避けるために行う対策。

高級な機材を使って故障率を下げることや、複数台で同じ作業をさせることによって、ひとつが壊れても、そのほかの機器で補えるような構成を作る。

サーバを停電が起こらず 365 日 24 時間監視ができるデータセンタなどに設置するのもひとつの対策方法となる。

以上のことを表にまとめるとこのようになる。

表 4　脅威に対応する技術

対策技術	キーワード	対応脅威
通信の暗号化	公開鍵暗号、秘密鍵暗号	盗聴、改ざん
認証	本人確認、認証局	なりすまし、否認
ウィルス対策	コンピュータウィルス	
フィルタリング	利用制限	盗聴、なりすまし
障害対策	保守、メンテナンス	

3-2　リスク分析

セキュリティ対策の分類を知ったからといって、これら全てに必ず対応しなくてはならないということではない。　セキュリティ対策の分類を知った上で、次にそれぞれの組織に見合った対策を実施して行く必要がある。そのために必要となってくるのがリスク分析といわれるものである。

例えば、運営しているホームページで会員専用ページを開設し、理事会録など会員限定の情報を提供している。ただし、この情報は、後に会報など、何らかの紙媒体で後に郵送する内容を速報としてホームページに掲載しているというケースを考える。

この場合、情報の守秘性から考えると、それほど重要な情報とは考えにくく、また万が一サーバが停止して情報にアクセスできなくなったとしても、それほどの緊急性は見受けられない。

そこで、障害対策については最低限の電源対策を施し、ID とパスワードの管理についても、利用する会員に定期的にパスワードを変更するようにお願いをする程度の対策で十分という判断もできる。ただし、この ID とパスワードが何らかの別の情報と結びつけることで、会員個人の氏名や住所、生年月日などを識別できる状態で管理されているのであれば、通信上の盗聴に対する何らかの対策として SSL 技術を採用するという判断をしなくてはならない。

医師会のホームページには様々なコンテンツが存在する。一般向けには、医師会の紹介や活動報告、所属会員の診療所などの案内、病気などの医療に関するコラムなどを公表しているところも存在する。そのほかに、コミュニケーションの一環として、電子掲示板（BBS)、病院の利用状況の確認や電子会議室などで医療相談を行っているところもある。

医師会の会員ページの内部で公開されているものでは、行政通知、委員会議事録、会員用掲示板（雑談、連絡事項）等が挙げられる。また、医師会内部のデータベースとホームページの会員情報が直結しているような場合も考えられる。

このような様々なコンテンツ、運営形態が考えられることから、セキュリティ対策、情報漏洩時のリスクの程度は、運営形態毎にことなると言っても過言ではない。

従って、セキュリティ対策に対する分類を認識した上で、次は自組織が、どのような情報を、どの程度の守秘性を持ち提供しているのか、その情報が漏洩した場合のリスクの程度を洗い出した上で、必要な対策を実施して行かなくてはならない。

さいごに

本稿では、通信上で起こりうる脅威について記した。その情報を守る手段として、SSL 技術に代表されるような暗号技術を用いることの有用性にも言及した。そして医師会のホームページとして、扱う情報、内容とその重要性についても述べた。SSL を提供する商用サービスも、最近では増えてきているが、日本医師会が主導で行っている認証局プロジェクト「日医認証局」の設立により、医療分野のホームページにおいても、より安全に利用しやすい環境が整えられて行く方向にある。

しかし、利用者が会員だけの場合や、あまり重要でない内容を開示するシステムを構築するのであれば、SSL は必ずしも必要では無い。利用者の安心を得る反面、SSL を利用するには、サーバ運営費の他に SSL 利用料として毎年の支払いが発生する。会員の個人情報など、一度外部に漏洩してしまうと、取り返しの付かない場合など、内部に設置している情報の重要度と運用コストのバランスを見て導入を決める必要がある。そのためにリスク分析が必要であることにも触れている。

ただし、昨今の情報化の進展に伴う、セキュリティ対策の重要性、個人情報の保護に対する利用者の意識の高まりなどには十分な備えと注意をしておく必要がある。個人情報保護法の成立はその代表例とも言える。

個人情報保護法は、特に医療に限った法令ではないが、医療分野も含め個人情報取得事業者が規定され、その義務などを定めている。多くの会員情報を取り扱う医師会では、個人情報取得事業者として、法令に従って会員の個人情報を扱わなくてはならないケースも想定される。

例えば、本稿で述べてきたように、会員限定のホームページを使って、ID・パスワードを配布するような場合、ID から会員個人が特定でき、ID 数がある一定の数を超えるのであれば、何らかの対策が必要になる。

ちなみに、医療機関については、厚生労働省において、「医療機関等における個人情報保護のあり方に関する検討会」が設置され、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」という形で、その扱いについて平成１６年１２月に通知が行われた。その中で、電子化された診療録など、電子的な健康情報の取扱いについては、別途、厚生労働省内に設置されている、「医療情報ネットワーク基盤検討会」で作成されるガイドランを参照することとされており、それらの動向にも注意する必要がある。

個人情報保護法の完全施行も含め、医師会でも対策を実施しなくてはならないことも少なからず出てきている。つまり、情報は持ち出した当人の責任というだけでなく、情報を管理している立場の責任も重要視されてきている。近い将来、通信上でカルテやレセプトなどの重要度の高い情報を扱う必要がでてくれば、SSL 等の認証・暗号化技術の導入や利用が余儀なくされるであろう。そのような時、医師会として何らかの役割を果たすことになれば、情報を管理する立場として、その責任を問われることも十分に考えられる。

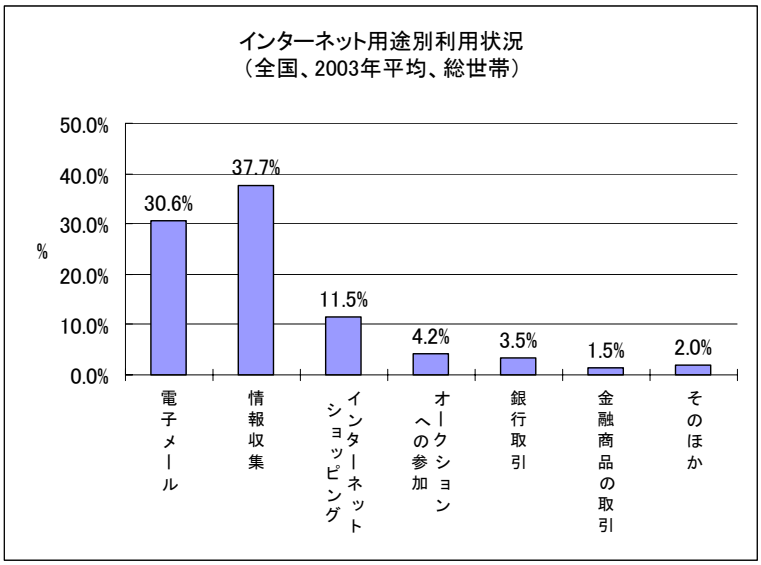
本調査は、各医師会のホームページの運営形態の把握のために、会員ページの有無、そこにかかるセキュリティ対策の一環としての SSL 技術の動向調査を行ったものである。しかし、単純に SSL 技術の動向調査のみでなく、各医師会へ向けてのセキュリティに対するより一層の意識向上を呼びかけるきっかけになることを期待している。本稿が、各医師会において運営しているホームページのセキュリティ対策を今一度、考え直してもらえる機会となれば幸いである。

なお、今回の調査は、2004 年 9 月時点のものである。今後、定期的に調査を実施することで、医師会におけるセキュリティ意識、対策の動向を継続的に観察して行こうと考えている。

参考　SSL の利用実態

インターネットが一般家庭に普及しはじめたのは、90 年代中ごろのことになる。ウェブブラウザ技術に並行する形で、SSL 技術も普及・進歩した。

現在のインターネットの利用用途は、図のようになっている。



図（参考）　インターネット用途別利用状況 [13]

図を見ると、電子メール、情報収集の利用用途が他に比べて多い。これは、携帯電話による電子メールの利用など、主に携帯端末の普及によるものだと思われる。

それ以外の、インターネットショッピング、オークション、銀行、金融取引などの利用用途で扱う情報には、金銭に結びつきが強いクレジットカード番号や銀行の口座番号が含まれている可能性が高い。従って、このような用途を持つホームページのほとんどは、SSL を利用してサービスが提供されている。

SSL 技術の利用は、提供者と利用者、双方のセキュリティ意識によって成り立っている。

[13]総務省「家計消費状況調査」 http://www.stat.go.jp/data/joukyou/index.htm

また、SSL を用いた通信は、金銭的な対策だけではなく、以下のような実用例もある。

・電子メールでの通信の暗号化を施した送受信(POP over SSL/TLS)
・専用線のようなリモートアクセスの実現(SSL-VPN)
・オンライン講座の通信(講座のでの通信暗号)
・セキュリティルームへ出入りするための認証（指紋データの暗号伝送）
・ソフトウェアを用いた、勤怠管理ソフト（Web クライアントの暗号化）

SSL を利用したサービスを提供するためには、サーバの証明を行う認証局への登録が必要となる。その場合、サーバ管理者が、登録の際に必要になる暗号鍵を作る必要があり、暗号についてある程度の知識を必要とされる。そのほかに SSL サーバ認証のサービスの利用には登録料として、年間 2~10 万円の費用がかかる。

現在は商用サービスとして、日本ベリサイン株式会社、セコムトラストネット株式会社、Thawte-Japan、日本ジオトラスト株式会社などが SSL サーバ証明書サービスを行っている。

日本医師会においても、医療系に特化した認証局“日医認証局”の開設をするべく現在試験運用中である。