

厚生科学研究費補助金

統計情報高度利用総合研究事業

**厚生統計情報の利便性の向上とその活用における
個人医療情報保護の在り方に関する研究**

平成12年度 総括・分担研究報告書

主任研究者 高石 昌弘

平成13（2001）年4月

目 次

I. 総括研究報告書

- 統計情報の利便性の向上とその活用における
個人医療情報保護の在り方に関する研究…………… 1

高石 昌弘 ((財)厚生統計協会)

- 資料1：「高度セキュリティ保健統計情報ネットワークシステム」…11
参考資料1：「用語解説」……………12
参考資料2：「代表的なオープン・ソフトウェア」……………13

II. 分担研究報告書

1. 電子媒体化された医療情報のセキュリティに関する研究
～電子化のための技術調査～……………14

山本 隆一 (大阪医科大学医学部附属病院病院医療情報部)

2. オンラインにおけるセキュリティに関する研究
～地方自治体における保健統計調査の情報化に関して～……………17

佐々木哲明 ((財)医療情報システム開発センター普及調査部)

- 資料2：「調査結果(グラフ)」……………19
参考資料3：「都道府県統計情報実態調査票」……………36
参考資料4：「指定都市統計情報実態調査票」……………45

3. 電子カルテのセキュリティに関する研究
～統計情報の高度利用における安全性とプライバシー保護に関して～……………54

坂本 憲広 (九州大学医学部附属病院医療情報部)

厚生科学研究費補助金(統計情報高度利用総合研究事業)

総括研究報告書

厚生統計情報の利便性の向上とその活用における
個人医療情報保護の在り方に関する研究

主任研究者 高石 昌弘 (財)厚生統計協会 理事

[研究要旨]

厚生統計諸調査の高度利用、効率化に資するため、医療機関、地方公共団体を対象とした情報化、オンライン化の実態調査を行い、今後の課題についての検討を行った。現在、厚生統計調査は一部が電子化されているもののほとんどは紙ベースでの処理が行われている。現在の情報通信技術水準を踏まえると、医療機関における発生源入力、地方自治体における統合データベースの構築、インターネットを利用したオンラインによる情報システムの構築が望まれる。そのためには基盤整備はもとより、個人情報保護、情報セキュリティに関して十分な配慮を行う必要がある。

分担研究者：山本 隆一

(大阪医科大学 助教授)

佐々木 哲明

((財)医療情報システム開発

センター 次長)

坂本 憲広

(九州大学医学部 講師)

ータ収集は、地方公共団体(都道府県、政令指定都市、特別区、中核市等)並びに各医療機関から紙媒体によることを原則としており、フロッピーデスクを用いたオフライン方式によるデータの提出収集も一部行われている。

本研究においては、これらの現状をオンライン化の観点から把握すると同時に、データ提出、収集並びに解析を可能にするハードウェア及びソフトウェアの整備、開発の在り方を検討した。

さらに、医療機関から収集するデータには患者個人が特定されるデータが含まれるが、患者のプライバシーの侵害に結びつく可能性を排除するため、電子媒体を経由す

A. 研究目的

医療機関を対象として行われている既存の厚生統計統計は、我が国の医療の状況を施設及び患者の両面から詳細に把握して医療の現状分析に資する一方、貴重な情報として将来の我が国の医療を検討する際の基礎資料となっている。

現在、これらの厚生統計調査におけるデ

る個人特定可能データの保護等、安全に万全を期す必要があるため、個人情報保護のためのオンラインシステムにおけるセキュリティについて、現状の技術上の水準を確認しつつ研究を進めた。

B. 研究方法

医療機関を対象とした厚生統計調査に関して以下の調査研究を行った。

(1) 電子媒体化された医療情報のセキュリティに関する研究

～電子化のための技術調査～

オンライン伝送とデータベース蓄積、およびネットワーク上からの検索を行うための安全性確保の手段を調査し、一部は実装評価を行った。伝送の安全性の確保のために、VPN (Virtual Private Network)、LDAP (Light weight Directory Access Protocol)、TLS (Transport Layer Security) について調査を行った。

(2) オンラインにおけるセキュリティに関する研究 ～地方自治体における

保健統計調査の情報化に関して～

都道府県の保健統計担当部署に対して、厚生統計調査の情報化に関する質問紙調査を行った。対象は、全47都道府県および12政令指定都市計59自治体である。調査項目は、各種保健統計調査の台帳の管理状況、国への調査結果の報告状況等である。

(3) 電子カルテのセキュリティに関する研究 ～統計情報の高度利用における安全性とプライバシー保護に関して～

厚生労働省の実施する統計調査の電子化の状況は、紙で収集した情報の集計システムにもっとも近いと考えられることから、次の段階である「紙のアンケートを電子化し、現場で電子的に入力し、それを自動集計する」段階、さらに進んだ段階である「調査集計用のプログラム(ロボット)を開発し、それをインターネットを利用して実行する」段階を実現するために必要となる手法と、患者プライバシー問題について検討した。

C. 研究結果

(1) 電子化に伴う安全対策の評価

VPNは文献的な調査にとどめたが、ここ数年で市販機器は充実し、比較的廉価で、Internet内にSecureなプライベートネットワークが構築可能である。またTLSに関してはOpenSSLと呼ばれるOpen Sourceのフリーウエアを、LDAPについてはOpen LDAPと呼ばれるOpen Sourceのフリーウエアを入手し、実装の上、一般的なデータベースをWEBインターフェイスを用いた検索を行う場合、およびHTTPで情報交換を行う場合の安全性について検討したが、RSA方式の1024bitsの公開鍵を用いる暗号化、および通信の両端の認証が可能なことを検証した。

(2) 医療機関の調査

地方自治体における保健統計の電子化の状況は、医療施設調査、病院報告が約60%と高かったものの、衛生行政報告例、地域保健・老人事業報告については約10%と低かった。その理由として、電子化にかえて時間がかかる等の理由が多かったが、一方で、電子化に対する要望も多かった。

(3) システムの構築

システムの構築のためには、(1) 項目／用語の標準化、(2) データモデルの標準化、(3) 匿名化データベースの構築、(4) 調査権限の管理が重要である。

項目および用語の標準化のために、MEDIS-DC編纂の「電子保存された診療録情報交換のための標準データ項目セット(J-MIX)」の活用が重要であるが、一部不十分な点もあり、更なる用語の標準化が必要であることが明らかになった。

データモデルに関してはHL7 RIM(Health Level Seven Reference Information Model)が標準的データモデルとして使用可能であった。

匿名化データベースについては、J-MIXの第1, 2, 6, 7章に含まれる項目を個人情報と定義したところ、個人情報を分離した匿名化データベースの構築が可能となった。

調査権限の管理については、公開鍵基盤を用いたシステムの構築が可能と考えられた。

D. 考察

(1) 電子化が困難な原因

厚生統計調査の効率化、精度向上のためには医療機関における発生源入力が望ましいが、現在、医療機関において電子化が行われていない。その原因として以下の点が挙げられる。

1) 調査項目の一部変更があること

調査年度によって調査項目の一部に変更がある。また、どのような変更がされるかが事前にわからない。このため、厚生統計調査に対応した病院情報システムを構築することは困難である。対応したシステムであっても調査項目や調査方法に変更が生じるとその都度システム改良のコストが発生し、電子化のメリットが明確にならない。

2) 報告書式が紙媒体を前提としていること

一部の調査でフロッピーディスクでの提出が可能となっているが、現状ではほとんどが紙媒体で提出されている。紙媒体を前提とした書式に出力するシステムは高コストとなり、システムの導入を妨げる一因となっている。

(2) 個人情報保護及び情報セキュリティについて

個人情報保護に関する法律が国会に上程

され、審議中となっている。ここでいう個人情報とは個人が識別できる情報であり、その情報自体では識別が困難であっても、他の情報と関連付けることによって容易に識別できる場合も含まれている。法の精神からはこのような情報は目的の明確化と目的外利用の制限、適正な取得、正確性の確保、安全性の確保、透明性の確保が求められている。公益性が高い場合、法の適応から除外されるかも知れないが、その場合でも、個人情報保護に十分な配慮が求められている。従って厚生統計調査データも個人情報が含まれる場合には慎重な対応が要求される。

厚生統計調査データには個人情報が含まれないものもあるが、母体保護統計のように患者名が含まれているものもある。患者名がなくとも住所、生年月日、性別等により一定の割合で個人が特定可能な場合などは個人情報として扱うべきであろう。また行政として一般的にセキュリティ及び個人情報保護には十分な配慮が求められていることもあり、厚生統計調査データを扱う場合、個人情報として十分な配慮で扱う必要がある。

目的の明確化については、各医療機関・保健機関で、明示したほうがよいかも知れないが、厚生行政が医療・保健の実態を正確に把握し、それを利用することはまさに公益目的であり、また自明と考えることもできる。しかし患者等にとってはそのような調査があることも知らない場合があり、

各施設で明示しない場合は何らかの広報的な方法で周知を図るべきであろう。

適正な取得については上記の目的の周知がはかられれば大きな問題はないと考えられる。

正確性の確保については統計調査の複数の段階で適切な努力がされており、電子化した場合も現在の運用を適応すれば大きな問題はない。むしろ電子化によって統計調査の各段階へのフィードバックが早くなる可能性があり、そうなれば、正確性の確保はさらに容易となる。

安全性の確保は、電子化した場合に特別な配慮が要求される。情報の電子化は一般に利用性の向上をもたらすが、利用性の向上は不正なアクセスの機会を増すことにもなり、安全性の低下につながりかねない。例えば調査データを単純な電子メールでインターネットを介して交換した場合、容易に盗み見されるし、内容を改変される可能性もある。紙の調査票を運ぶ場合も同様の危険はあるが、やはりアクセスのし易さと言う点で、電子化した場合のほうが危険と考えるべきであろう。したがって電子化に伴って十分な安全対策の強化が必要である。

透明性の確保は厚生統計調査データの場合、当該対象個人によるアクセスは原則として生じない。母体保護統計のように明示的な個人情報の場合は一次データの取得時に開示し、確認を求める用意をすればよいと考えられる。むしろ医療機関の診療情報から統計調査データを抽出する場合はもと

の診療情報の透明性が問題になる可能性を考え、医療全体での透明性の向上に努めるべきであろう。

(3) 目指すべきシステムの概要

現在の情報通信技術を前提にすると厚生統計調査の高度化、効率化、精度向上のために以下のようなシステムの構築が求められる(図1)。

1) 医療機関・保健機関における発生源入力

調査データは、その発生源である医療機関において入力されるべきである。また、病名等医師が入力すべき情報は医師が入力できるシステムが求められる。これにより、効率化だけでなく、転記による誤記入が減少しデータ精度が向上する。もっとも多忙な医療現場で医師と医事課職員などが分担して入力するとなるとデータを完全なものにするための労力が多大になる可能性がある。幸い大規模・中規模の病院ではオーダエントリシステムの普及が進んでおり、それ以外でも医事請求のためのコンピュータシステム(レセコン)は広く普及している。したがってこれらのシステムから厚生統計調査に必要な項目を簡単に抽出できるような仕組みが存在すれば、調査データの収集は容易で確実なものとなる。中期的には各方面との協力でこのような仕組みを目指す必要がある。

2) オンラインによるデータ送受信

現在は電子化された統計調査データもフロッピーディスク等によるオフラインのデータ送受信が行われているに過ぎないが、オフラインの送受信は両端で手作業が生じる上に、安全性も低い。さらに媒体の管理の手間も無視はできない。十分な安全性の確保を前提にインターネットを利用したオンラインによるデータの送受信を行うべきである。オンラインで送受信を行うことにより、安全性・確実性が増すとともに、すぐに集計できるようにデータベースに直接入力することが可能となり、データの整合性などのチェックもリアルタイムに行うことが可能となる。安全性の確保は後述するように現在の技術で十分に達成できる。

3) 自治体における統合データベースの構築

厚生統計調査のみでなく医療監視、各種医療法上の提出書類等の統合データベースが各自治体に構築されるべきである。これらのデータのうち、多くは発生源である医療機関で入力される。これらのデータは互いに関連のあるものが多く、包括的に管理することにより、調査データの整合性が容易になる。ただしこのような包括的な管理を行う場合、個人情報保護やデータベースの安全管理はきわめて重要であり、後述の配慮が必須である。

4) 個人情報保護、情報セキュリティ対策

個人情報保護、情報セキュリティ対策には運用面とシステム面の2面から考える必要がある。また具体的に考えなければいけない要素はシステムの安全性確保、情報操作者の認証、通信経路の安全性確保、および情報の分離である。さらに統計調査にあたる組織全体を対象とするポリシーやそれに基づく運用規程も必要である。厚生統計調査の場合、大部分は公務員が情報操作にあたるために、守秘義務や安全性確保に特別にポリシーを定める必要はないように見えるが、データの発生源では各種身分法による守秘義務が規程されていない人が操作する可能性がある。また、統計処理やシステムのメンテナンスを外注する可能性もあり、包括的なポリシーとそれに基づく運用規程は定めるべきであろう。

システムの安全性確保には物理的な安全性確保とネットワーク的な安全性確保がある。物理的な安全性とは、漏水、浸水などによるシステム障害をさけることや、不法な侵入を防止するための入退室管理などが挙げられる。ネットワーク的な安全確保は一般にファイアウォールと呼ばれている技術を利用することで達成される。ファイアウォールは種々の方面で利用されており、技術的にも完成度は高い。従って運用に留意すれば一般的なものを導入することで十分安全性は確保される。

情報操作者の認証には十分留意する必要がある。よく用いられる認証手段として、IDとパスワード、IC-Cardによる認証、生体

計測認証がある。現在もっとも広く用いられているのはIDとパスワードによる認証で、パスワードを知っているのはその人だけである、という仮定に基づいている。パスワードは当然ながら記憶しなければならないが、短いパスワードや総当たりで容易に破られるし、長くても電話番号のように類推可能なものは容易に破られる。連想しにくくて長い文字列は記憶することが難しく、IDとパスワードによる認証は本研究の対象のようなセンシティブな情報では現実性を失いつつある。IC-Cardによる認証は現状ではもっとも合理的な認証方法と言える。政府のIT戦略で住民基本台帳カードなども計画されており、入手が容易で、かつ確実に安全な認証が可能である。後述する経路の安全性の確保のための公開鍵基盤にも対応が容易である。ただし印鑑と同様で、IC-Card紛失の危険はある。そのためにIC-Cardと本人を結びつける必要があるが、これにはパスワードや生体計測認証が用いられている。パスワードだけの認証は現実性を失いつつあるとしたが、この場合はIC-Cardを入手しない限り、パスワードを破っても意味がなく、IC-Cardの管理に十分留意している限り、安全性は高い。生体計測認証は指紋、声紋、虹彩のような、個別性の高い身体の一部を用いて認証するもので、所持情報の一種と考えられるが、IC-Cardのように紛失の危険性はない。理論的にはもっとも安全で確実な方法であるが、計測精度の高いものは高価であり、また身体の一部を認証機器に接

触させるものが多く、感染症伝播などの問題がある。実用的に使われている例もあるが、本調査研究の対象に単独で用いるのは時期尚早であろう。IC-Cardなどと組み合わせて用いる場合はそれほど高い精度は不必要で、実用性がある。

通信経路の安全性対策には経路全体の安全性を確保と個々の情報の安全性確保の2つが存在する。経路全体の安全性確保は他からアクセス不可能な閉じたネットワークを形成することで、物理的に専用の閉じたネットワークを使う方法、スイッチング技術（電話交換機の原理を情報ネットワークに応用したもの）による論理的な閉じたネットワークを構成する方法、および暗号化と両端の機器を認証することによるVPNがある。物理的に専用のネットワークを構築することはかなり高価であり、また広域になればなるほど、ネットワークの監視が難しくなる。本調査研究ではネットワークの末端は個々の医療機関・保健機関であり、現実的ではない。スイッチングにより論理閉域ネットワークは地域により利用可能で、比較的安価であるが、全国規模では十分整備されているとはいいがたく、また通信業者が管理するために、ポリシーの統一の問題もある。いずれにしても全国を対象とする厚生統計調査ではすべてで利用することはできない。これらに比べてVPNは基本的にはソフトウェアで仮想の閉域ネットワークを構成するもので、既存のインターネットを利用することができる。機器も安価で

あり、安全性も高い。もっとも現実的な選択と考えてよい。

経路上で個々の情報の安全性を確保する手段は暗号化と電子認証によるもので、TLSが標準化された規格の1つである。またメールだけでよければPGPやS-MIMEと呼ばれる規格も利用することができる。これらはいずれもPKI（Public Key Infrastructure 公開鍵基盤）に基づくもので、現在もっとも広く使われている。本調査研究でもOpenSSLとOpenLDAPを用いて検証を行ったが、容易に構築可能であり、安全性を確保できる。VPNのような経路全体の安全性確保とTLSのような個々の情報の安全性確保の関係であるが、原則として両方を併用することが望ましい。VPNはネットワーク全体を安全に運用することができ、DoS攻撃（Denial of Service attack サーバに対して膨大な接続要求を出すことで利用不可能にする攻撃）にも抵抗性があるが、そのネットワーク内では個々に安全性のレベルを変えることができない。それにくらべてTLSやS-MIMEはクライアントの認証を個々に行うために、必要に応じた安全性を確保できる。しかしTLSやS-MIMEは外見上は通常のインターネットの規格の1つであり、DoS攻撃に抵抗性がない。したがって理想的にはこれら2つを組み合わせる運用することが望ましいが、いずれも安全性は高く、例えば個々の医療機関・保健機関と地方自治体の間はTLSやS-MIMEだけにし、自治体と厚生労働省の間は併用すると言った運用でも可能と考えられ

る。

情報の分離は収集された情報をできるだけ早く、個人識別不可能にすることで、個人識別可能な情報と個人識別不可能な情報に分離して管理することにより達成される。目的が統計調査なので、大部分の調査においては最終的に個人識別可能な情報は含まれる必要がない。個人識別が可能な情報が必要な理由はデータの整合性のチェックなどに用いるためであり、目的を達した時点で速やかに個人識別不可能な状態にすることが望ましい。ただ調査項目によっては個々の項目では個人識別が不可能であっても組み合わせることで、強く限定される場合もあり、この処理は慎重に行う必要がある。後述する「電子保存された診療情報交換のためのデータ項目セット」のような標準的な見出し項目を用いてデータを収集することが、情報分離を容易にする可能性が高い。

(4) オンライン化のための提言

上記システムの構築のために以下の点の対策や検討が必要である。

1) 病院情報システム化のための方策

a) データ（調査）項目の明確化

長期にわたり不変の調査項目と各調査ごとに変更される項目を分け、これらのデータ型、コード等を公表すべきである。また、項目の変更を行う場合にはなるべく早く変更点等を広報すべきである。

b) 電子媒体を考慮した書式

電子媒体による提出を考慮した提出書式にすべきである。現在の情報通信技術を踏まえるとXML(eXtensible Markup Language)形式を検討すべきである。

2) 「データ項目セット」の拡張

厚生統計を利用目的として「データ項目セット」を拡張すべきである。また、医療機関名、医療機関住所、病床数等を含む「医療機関データ項目セット」を新たに作る必要がある。

3) データモデルの標準化

HL7 RIMを用いたデータモデルの構築が重要である。

4) 個人情報保護、情報セキュリティ対策

セキュリティポリシーの明確化、暗号化、ファイアウォール設置・運用、アクセス権設定、ログ監視、関係者の教育等の個人情報保護、情報セキュリティ対策を行う必要がある。

5) 電子メールでのデータ送信の禁止

インターネットでは通信経路の情報セキュリティは確保されていないこと、宛名の入力ミスにより誤送が起りえること等から電子メールでのデータ送信は行うべきでない。メールによるデータ送信を行う場合は、送受信者の確認、暗号化等の対策を

行うべきである。

6) 電子認証について

平成13年4月の電子署名法の施行を踏まえ、高度な個人情報保護、情報セキュリティの実現のために電子認証のあり方について検討すべきである。

7) 標準的かつオープンな規格の採用

安価で効率的なシステム構築のために標準的かつオープンな規格を最大限活用すべきである。例えば、TCP/IP、HTTP、XML、CSV、X.509等が挙げられる。

8) オープンソースソフトの活用

オープンソースソフトの活用により、安価で応用性の高いシステムが構築可能である。また、オープンソースソフトの方が市販のソースコードを公開していないソフトよりもセキュリティ上安全だと言われている。そのため、システム構築に当たっては、オープンソースソフトを活用すべきである。現在、OS、Webサーバ、セキュリティ通信、データベース、アプリケーションサーバ、ディレクトリサービス等多くのジャンルでオープンソースソフトの利用が可能である。

(5) 情報システムの機能要件

情報システムが最低限備えるべき機能要件を以下に示す。

1) 病院情報システムの機能要件

- ・ 特定日の受診患者のID、氏名、生年月日、性別、病名、入院・外来の別等を出力できること。

- ・ 患者には、健診、正常分娩目的等保険適用外の者も含まれること。

- ・ データ項目のデータ型、コードは指定のものをを用いること。

- ・ 出力形式はCSVまたはXML形式であること。

- ・ XML形式の場合は、タグ名に「データ項目セット」名を用いること。

2) 自治体システムの機能要件

a) データチェック機能

- ・ 前年度データとの比較ができること。

- ・ 性別、年齢別データ等の集計ができ、チェック用に利用できること。

- ・ 相互に関連したデータを同時表示等により表示できること。

例：

- ・ 医療監視データ、医療法上の各種提出書類等のデータを参照できること。

b) 利便性のための機能

Excel、Access等の表計算/データベースソフトとの連携が図れること。

3) 情報セキュリティ機能

医療機関、自治体、政府のシステムいづれにおいても情報セキュリティ機能は重要である。

- ・ 個人情報を扱う場合と同等のセキュリテ

ィ機能を有すること。

例：SSLまたはISCLによる通信等

E. 結論

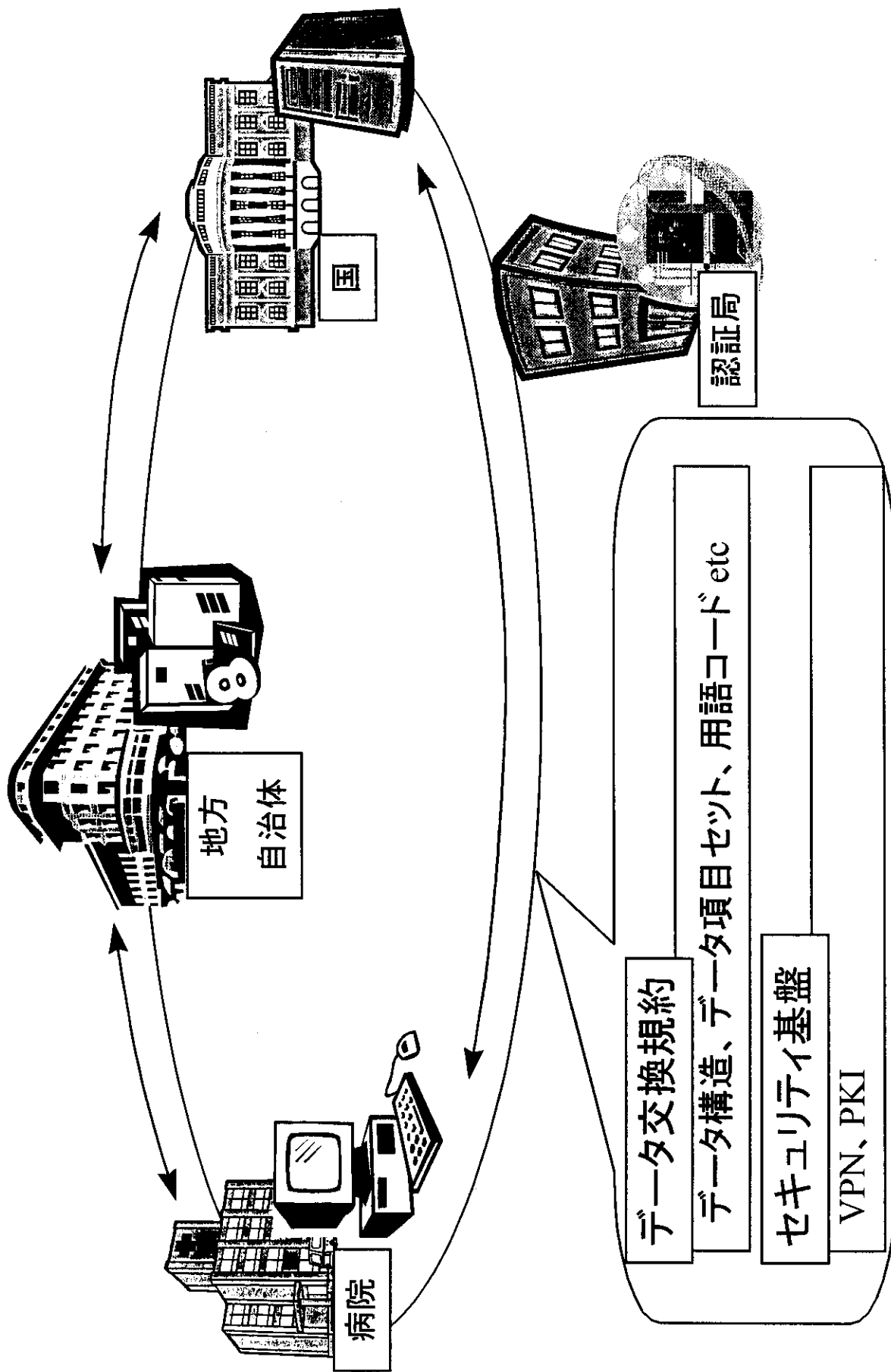
厚生統計諸調査の高度利用、効率化のため、情報化の現状調査を行った。現在の厚生統計調査は一部電子化されているもののほとんどは紙ベースの処理が行われている。これを改善するためには、医療機関における発生源入力システム、自治体における統合データベースの構築、オンライン化が求められる。また、個人情報保護、情報セキュリティに関して十分な配慮を行う必要がある。

G. 健康危険情報 なし。

H. 研究発表 論文に発表予定。

I. 知的財産権の出願・登録状況 なし。

高度セキュリティ保健統計情報ネットワークシステム



用語解説

Virtual Private Network (VPN) : 仮想専用線

暗号化等を用いてインターネット上で仮想的な専用線を構築する技術。

Public Key Infrastructure (PKI) : 公開鍵暗号基盤

公開鍵を用いた暗号方式。電子署名の基礎技術。

Transport Layer Security(TLS) :

TLとはISO (Open System Interconnection, OSI)通信 7層モデルの第4層。トランスポート層。各ノード上で実行されている2つのプロセス間で、仮想的な通信路を実現するためのプロトコル層。インターネット (TCP/IP) のTCP層に相当する。

TLSとはTL層において暗号化等でセキュリティを確保する方法のこと。

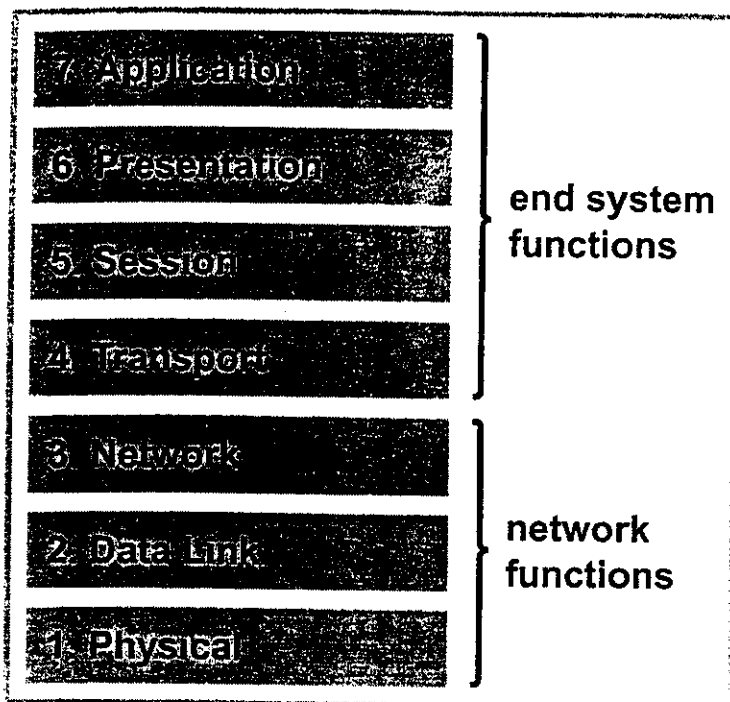


Fig.
The ISO/OSI
Reference
Model

代表的なオープンソース・ソフトウェア

Operating System: Linux, FreeBSD, Darwin, HURD

Window System: Xfree86 + GNOME or KDE

Database: PostgreSQL, MySQL

Directory Services: openLDAP, NetInfo

Domain Name Services: BIND

Mail Server: sendmail, Postfix, qmail

List Server: Majordomo, fml

Web Server: Apache

CGI: Perl, Ruby, PHP

Streaming Server: Darwin Streaming Server

Web Browser: Mozilla

電子媒体化された医療情報のセキュリティに関する研究

～電子化のための技術調査～

分担研究者 山本 隆一 大阪医科大学 病院医療情報部 助教授

[研究要旨]

厚生労働省のおこなう統計調査をより合理的で利用性の高いものにするためには電子化が必要なことは論を待たない。しかし電子化を実施するためには安全性の確保とプライバシーの保護が必要である。本研究では電子化することを前提に安全性の確保とプライバシー保護に用いられる技術要素を検討し、現時点で経済的にも効果の面でも十分実用的に使用できることを証明した。またその実現のために必要な証明書発行局の整備について提言した。

A. 研究目的

厚生労働省が実施している様々な統計調査はわが国の医療の実態や患者動向を把握、分析する上できわめて有用な調査であり、大いに活用されることが望まれる。しかし、現時点ではほとんど電子化されていないために、都道府県、保険所、各医療機関での記入は合理的と言いがたく、統計処理やその結果のフィードバック、さらには分析や報告などにかかなりの時間を要している。IT革命の自体にあって医療行政の迅速な対応に支障をきたす可能性も否定はできない。

一方でIT技術の進歩はめざましく、統計調査を電子的に行うことは技術的には難しくはなくなっている。また経費の面からも収集データをあらためて入力していることと比較すれば発生源入力を実現できれば有利であることも確実と言える。しかしこのような電子統計を実施する場合、収集データのプライバシー保護や、処理途中の改ざんに留意する必要がある。一般に情報を電子化すれば利用性や処理の容易さは飛躍的

に向上するが、何も対策を講じなければ安全性は多少とも低下する。したがって適切な安全対策を講じる必要がある。本研究では統計調査およびその結果の利用方法の電子化にあたり採用されうる安全対策を調査し、適切な方法を提言することを目的とした。

B. 方法

1 発生源入力を前提とし、入力まで、収集後の統計処理中を対象外として、入力データの蓄積と伝送および処理結果の伝送と公開の安全性とプライバシー保護を対象とした。

2 伝送の安全性とプライバシー保護について

Virtual Private Network (VPN) と Public Key Infrastructure (PKI) を利用した Transport Layer Security (TLS) を検討対象とし、蓄積データの安全性とプライバシー保護についてはデータベースそのものの安全性については時間的な関係で今回は対

象とせず、システム全体の保護について利用者認証とファイアウォールによるシステム保護について調査した。

C. 結果

VPNに関しては統計調査に参加するすべての施設にVPN専用機器を配置することは困難と考え、大阪医大に季節のVPNコンセントレータとWindows にインストール可能なVPNクライアントソフトウェアを用いて堅牢性と使いやすさを検討した。コンセントレータとしてContivity Extranet Switch (ノータル社製)を用いたが、通常のインターネットを介して容易にVPN接続をすることが可能で、例えば患者調査などで発生源入力を行う場合でも十分実用になることが判明した。このコンセントレータのクライアントソフトウェアは無制限ライセンスであり、費用面からも問題はなかった。

PKIによる暗号化基盤であるTLSはOpenSSLを中心としたFreewareのソフトウェアを使用し、サーバはDOS/V上のLinuxで構築し、クライアントとしてはWindows 2000とInternet Explorerを用いて実験を行った。また統計情報の公開を考慮しApacheを用いてWEBサーバを構築し、TLSを使用した暗号化と利用者認証を試みた。いずれも堅牢性は暗号化の確認しただけであるが、ただし処理されており、問題ないと考えられた。またWEBサーバでの利用者認証も電子証明書の発行さえたたく行われていれば確実に問題はなかった。

利用者認証単独の実験は指紋パターンによる生体計測認証(三菱製FPR DtmkII)とIC-Cardをシュミレートしたフロッピーディスクによる認証を比較検討した。パスワード認証は常識的に運用可能な長さのパスワードでは安全性に問題があることは明らかで、対象に含めなかった。指紋パターン認証は利用者がなにも管理しなくて良いという点で利便性が高いが、高価であり、また10%程度の確率で読み取りができず、アクセスが拒否された。統計調査に用いる場合、誤認識によるアクセス拒否が大きな問題になることはないが、医療現場での発生源入力などの場合、わずらわしさはできる

だけ避けるべきであり、問題がある。サーバ管理などには有用であろう。フロッピーディスクによる認証は特に問題を発見できなかった。ただ実際にIC-Cardを用いる場合は生体計測認証に比べれば安価ではあるが、費用面で問題が生じる可能性がある。

D. 考察と提言

厚生労働省が実施している統計調査を電子化するためには安全性の確保とプライバシーの保護が必須であるが、本研究では比較的広く用いられている方法で安価にこれらの課題を克服できる可能性があることを示した。もちろん本研究は技術的な面からの検討を行っただけであり、その意味では十分な解を得たとは言えない。入力現場や統計処理現場まで考慮に入れると技術面だけで安全やプライバシー保護を確保することは不可能で、運用規則やポリシーに依存せざるを得ない。運用規則やポリシーが必要な以上は技術的な対策はそれと相補の関係にあり、本来は一体として論ずるべきものであり、それは総括報告の提言として別途論じられている。

伝送の安全性に関してはVPN、TLSのいずれでも十分確保できることが証明されたが、安全性を確保するためにはフェイルセーフも重要であり、併用することも考慮する価値がある。この2つの技術はまったく独立しており、併用も何ら問題を引き起こさない。ただいずれの場合も全国レベルでの調査のような多数のクライアントを扱う場合、PKIによる電子証明書を用いることが必要である。実験レベルでは証明書の発行は難しくはないが、実用に用いるとなると、少なくとも電子証明書発行局の整然とした整備は不可欠である。統計調査だけでなく、今後医療全体としてもIT化は避けられない状況であり、PKIはその重要な基盤と考えられている。しかしながら現時点では医療ドメインでの証明書発行局の整備は手をつけられておらず、このままではIT化の足を引っ張る可能性も否定できない。早期の整備が必要であり、厚生労働省の積極的な働きかけを期待したい。

利用者の認証も統計調査にかぎらず医療

のIT化の基本的な課題である。本研究でIC-Cardのような所持情報による認証が十分機能することを証明できたが、これも統計調査のためだけに導入すれば費用面で若干の問題を生じる可能性がある。幸い住民基本台帳カードのように他分野でのIC-Cardの導入が広範囲で検討されており、それらの動きをうまく利用することで、問題は大部分解消できる可能性がある。この面でも厚生労働省の積極的な働きかけが期待される。

E. 結論

厚生労働省の統計調査の電子化に際して問題となる安全性とプライバシー保護の確保に関して、技術的には十分対応可能なことを示した。その一方で統計調査だけでなく、医療のIT化に必要な基盤整備であることを示し、整備を急がなければならないことを提言した。

F. 発表

山本隆一、他；「診療情報の無名性の定量化に関する研究」；第20回医療情報学会連合大会；浜松；2000

山本隆一；「電子保存された診療録情報交換のための標準データ項目セット」；第20回医療情報学会連合大会；浜松；2000

厚生科学研究費補助金(統計情報高度利用総合研究事業)

分担研究報告書

オンラインにおけるセキュリティに関する研究

～地方自治体における保健統計調査の情報化に関して～

分担研究者 佐々木哲明 (財)医療情報システム開発センター 次長

[研究要旨]

厚生統計の高度利用、特にオンライン化のため、地方自治体(47都道府県、12政令指定都市)における保健統計調査の情報化の現状とその問題点に関する質問紙調査を行った。その結果、医療施設調査、病院報告の約60%、衛生行政報告例、地域保健・老人事業報告の約10%がそれぞれ電子化されていた。電子化に対する関心は高いと考えられ、地方自治体にメリットのあるシステム構築が望まれる。

A. 研究目的

厚生統計の高度利用のためには情報化が不可欠である。本研究では、都道府県等地方自治体における保健統計調査の情報化の現状とその問題点を把握する目的で質問紙調査を行った。

B. 研究方法

都道府県および政令指定都市の保健統計主管部局に対して、厚生統計調査の情報化の現状および問題点に関する質問紙調査を行った。対象は、全47都道府県および12政令指定都市(札幌、仙台、千葉、横浜、川崎、名古屋、京都、大阪、神戸、広島、北九州、福岡)計59自治体(以下、「自治体」略す)である。

調査項目は、各種統計調査の台帳の管理

状況、医療機関や保健所からの報告状況、国への報告状況等である(参考資料2)。

調査は平成13年3月に実施した。全国保健統計協議会事務局の協力を得て、調査票を配付・回収した。回収率は100%であった。

なお、調査票作成に先立って、佐賀県に対してヒアリングを行った。医療機関を対象とした厚生統計調査に関して以下の調査研究を行った。

C. 研究結果

(1) 医療施設調査、病院報告の台帳管理状況等

医療施設調査、病院報告に関しては、病院台帳、診療所台帳とも約60%の自治体がエクセル、アクセス等の表計算/データ

ベースソフトを利用して管理していたが（図1(2)）、厚生労働省へ電子媒体での報告は4自治体(7%)に過ぎなかった（図2）。また、医務担当データと統計担当データを一元化しているのは6自治体(11%)に過ぎなかった（図1(3)）。電子媒体で提出しない理由としては「かえって時間がかかる」との回答が多かった（図4）。

(2) 衛生行政報告例の台帳管理状況等

衛生行政報告例に関しては、表計算/データベースソフトを利用している自治体は10%以下であり、ほとんどがワープロや手書きで処理していた（図8）。

(3) 地域保健・老人保健事業報告の台帳管理状況等

地域保健・老人保健事業報告に関しては、電子媒体で提出している自治体は6カ所(10%)だった（図13）。

D. 考察

地方自治体における保健統計の電子化の状況は、医療施設調査、病院報告が約60%と高かったものの、衛生行政報告例、地域保健・老人事業報告については約10%と低かった。その理由として、電子化にかえって時間がかかる等の理由が多かったが、一方で、電子化に対する要望も多く、電子化への関心は高いと考えられた。

そのため、業務分析等を行い、電子化のメリットが得られるようなシステムが構築

されれば、電子化は促進されると考えられた。

データベースの一元化による二重入力の解消、エクセル、アクセス等の表計算/データベースソフトとの連携、データチェック機能（特に前年度データとの比較機能）の付加、1枚のFDに複数施設のデータが入るような様式への変更等により業務の効率化やデータの高精度化等のメリットが得られると考えられた。

E. まとめ

地方自治体における情報化の現状とその問題点に関する質問紙調査を行った。その結果、医療施設調査、病院報告の約60%、衛生行政報告例、地域保健・老人事業報告の約10%がそれぞれ電子化されていた。自治体における電子化に対する関心は高いと考えられ、地方自治体にメリットのあるシステム構築が望まれる。

謝辞：本調査票の配付・回収をしていただきました全国保健統計協議会事務局（群馬県）、回答していただきました各都道府県等保健統計担当部署の方、また、本調査に先立ってヒアリングをさせていただいた佐賀県医務課衛生統計係の方に深謝致します。