20112902 9A

厚生労働科学研究費補助金

地域医療基盤開発推進研究事業

病院情報システム端末からの安全なインターネット直接接続に関する研究

平成２３年度　総括・分担研究報告書

研究代表者　大山　永昭

平成２４（２０１２）年　５月

目　　次

厚生労働科学研究費補助金（地域医療基盤開発推進研究事業）
総括研究報告書

病院情報システム端末からの安全なインターネット直接接続に関する研究

研究代表者　　大山　永昭　　東京工業大学像情報工学研究所　教授

研究要旨：　医療機関内部からインターネット等を利用して外部に接続するためには、病院内に保存されている個人情報などが漏洩しないための対策をとることが極めて重要であり、そのために必要な措置を講じることが急務とされている。医療機関内の情報端末から外部ネットワークに接続する際には、端末の使用者や医療用端末の正当性を認証すること及び、その認証結果に基づき適切なネットワーク制御を行うことが重要であるが、本研究では、情報端末を認証する仕組みを導入することで、適切な利用者・端末からのみ外部接続を可能とするシステムの開発を行う。さらに、外部との接続に際しては、オンデマンドVPNの機能を拡張することで、医療機関と情報提供機関間のインターネット接続を安全におこない、不正アクセスなどを防止可能な仕組みを開発する。

研究分担者　喜多　紘一　保健医療福祉情報安全管理適合性評価協会　理事長
土屋　文人　国際医療福祉大学薬学部 教授
八幡　勝也　産業医科大学産業生態科学研究所 非常勤講師
秋山　昌範　東京大学政策ビジョン研究センター 教授
安藤　裕　放射線医学総合研究所重粒子医科学センター病院　課長
山本　隆一　東京大学大学院情報学環　准教授
小尾　高史　東京工業大学総合理工学研究科　准教授

A．研究目的

近年の情報基盤整備の進展に伴い、保健医療分野における情報化の推進が期待されているが、電子的に保健医療情報の流通を行う場合には、個人情報の保護が極めて重要であり、そのために必要となる適切な措置を講じることが急務とされている。

ここで、個人情報の安全性を確保するためには、医療データ等を使用する者の正当性を認証すること及び、通信回線上や医療機関内での医療データ等の保護を実現することが重要である。このような仕組みを実現するための指針として、厚生労働省医政局に設けられた医療情報ネットワーク基盤検討会より、医療分野の情報化を推進するために必要となる公開鍵基盤や、医療に係る文書の電子化・電子保存に対するガイドラインが示されており、この中で、医療機関内部において情報を安全に管理するための要件や、医療機関同士が接続する際に必要なネットワーク要件、外部から医療機関内部のネットワークに接続するための要件などが述べられている。また医療機関内部におけるネットワーク管理の必要性も指摘されているが、現時点では、内部端末から外部接続を許可するために必要となる具体的な技術的要件は明らかにされていない。

本研究では、医療機関内に設置された情報

端末の認証と端末利用者の認証と組み合わせることで、適切な情報端末からのみ外部接続を許可し、安全に外部情報を参照可能とするシステムの実現を目的とする。

具体的には、医療機関間を安全に接続するネットワーク基盤であるオンデマンド VPN の有する機能及び法人を含む人・物の認証機能を組み合わせ、医療情報の利活用を可能とする新たなネットワーク基盤を実現する技術的手法について具体的に研究するものであり、今後改訂される医療情報システムの安全管理に関するガイドラインに成果を反映させることを目指している。平成２２年度の研究においては、医療情報端末に搭載されたセキュアモジュールや医師などの保有する IC カードを利用して、端末及び利用者認証を行い、その結果に基づき医療機関のゲートウエイ制御をおこなう方法を検討すると共に、オンデマンド VPN を提供する事業者などが管理する外部接続用ゲートウエイを利用して安全に外部接続をおこなう方法について検討を行い、システム設計に必要となる要件をまとめた。今年度は、前年度の成果を踏まえ、提案システムの設計、プロトタイプシステムの開発を行い、その評価を行う。また、提案システムの導入、管理、運用方法についても検討する。

B．研究方法

今年度の研究では、前年度の研究成果に基づき、病院内の情報をインターネット経由で安全にやり取りするための技術要件の再整理及びプロトタイプシステムの設計を行い、実際にプロトタイプシステムを開発する。また、プロトタイプシステムについて技術的、経済的側面から評価を行い、実運用に向けた課題を明かにする。さらには、医療機関内外を含めた統一的な保健医療情報ネットワークを構築するための技術的指針を明らかにし、提言としてまとめる。

C．研究結果

(1) 医療機関からの外部情報参照を行うプロトタイプシステムの開発

(ア) システム要件の再整理

平成２２年度に行った研究で検討した、新たな医療用ネットワークシステム構成(図1)に必要となる要件は、以下の通りであった。

医療機関内のネットワーク利用については、

1. 医療機関等の院内LANに接続される端末の正当性を確保し、正当な機器（登録機器）からのみ外部接続を許可すること
2. 医療機関内部の通信の安全性を確保すること
3. 外部接続時の機器利用者を特定し、許可された利用者のみの外部接続を許可すること
4. 院外でモバイル機器を利用する際には、外部モバイル機器は院内LANに対してVPNを利用して接続されること
5. モバイル機器が院内LANに接続される際には機器及び利用者の認証をおこなうこと

が必要となることを明らかにした。また、新たに導入した外部接続管理機関については、、

6. 複数の医療機関からのパケットを分離し処理すること
7. 許可されたWebサイト（ページ）にのみ接続を許可すること
8. 院内LANに接続された機器に対して、名前解決の仕組みを提供すること

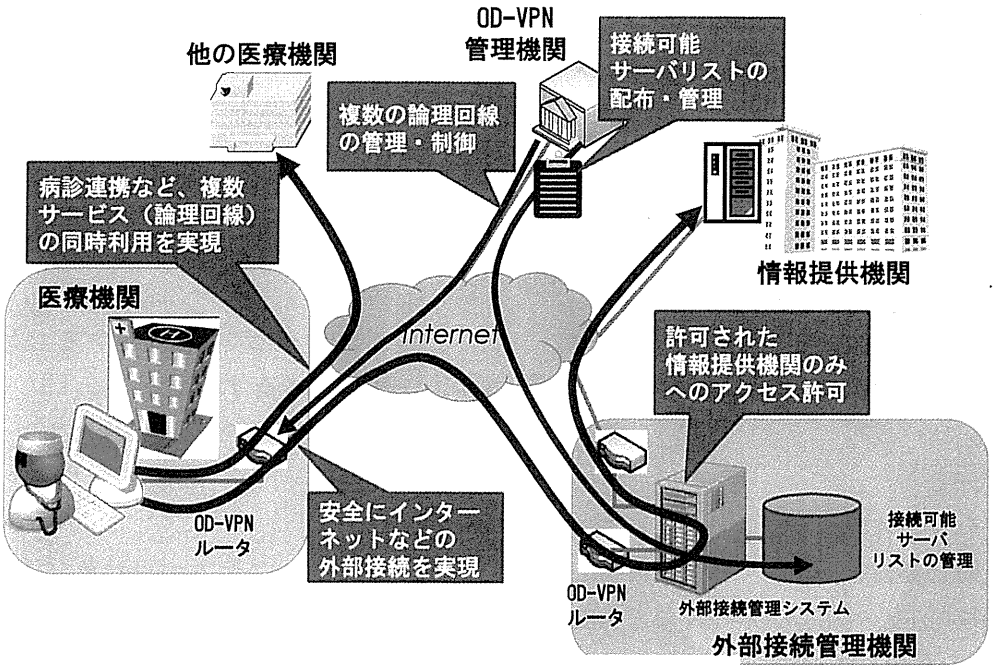

図１　提案システムの全体像

9.　証跡管理をおこなうこと

が要件になることを示した。

以上の要件を踏まえ、昨年度整理した技術的要件の概要を技術的動向や実現可能性を考慮して以下の通り再整理した。まず、要件１の院内ＬＡＮで利用する端末の正当性確保を実現する技術的要件として、

1. PCの個別認識をハードウェアで保証するために、機器に組み込まれているチップ、特定ID等を利用した認証の実施すること（例えば、vPro搭載PCの利用、イーサネットボード、CPUやチップセットの中に特定のコードを利用）
2. 不正PC接続検知防止システムを導入すること（登録外のＰＣ等が接続されたことの検知とネットワーク接続の妨害など）

を、要件２のPCなどの機器、ルータ間の通信など医療機関内部の通信の安全性を確保については、

3. 機器とルータ間の通信にはIPAHを利用したパケット改ざん防止、VLANによる通信路の仮想化をおこなうこと

と定めた。要件５のモバイル機器の接続については、

4. IEEE 802.1x（EAP-TLS,PEAP)を利用して、無線LAN利用機器の安全性確保を行うこと

が必要であるとした。

また、要件３の機器利用者の識別及びそれに基づく特定機器からの外部接続については、

5. 外部接続利用時の利用者認証を行うこと。利用者認証方法はID, Passwordの利用も可能とするが、ICカード利用を奨励する（但し院内で特定の利用者のみが使用するモバイル端末の場合には、利用者認証だけでなく、機器認証のみでの利用も可能）

6. 利用者がどの機器を利用しているかを確認する必要があるため、認証はオンデマンドVPN（OD-VPN）ルータに対して実施すること
7. OD-VPNルータ又はそれと連携する機器は、機器・利用者情報を紐づけて管理すること
8. 機器認証及び機器利用者の認証が行われている場合のみ外部接続を許可すること

を技術的要件とした。

要件６から９の外部接続管理機関の要件を満たす技術的要件として、

9. 医療機関との間はOD-VPNなどVPN技術を利用して接続すること
10. 外部接続機関内では、VLAN 技術を利用して複数の医療機関からのパケットを分離し処理すること
11. アプリケーション制御型 FW を設置し、アプリケーションレベルで、医療機関から外部接続機関に対する接続ポリシー制御を実施すること
12. ホワイトリスト方式による Web フィルタリングを実施すること
13. ホワイトリスト対象サイトの管理を行うこと
14. 院内のネットワーク機器に対して名前解決サービスを提供するためのDNS 機能を有すること
15. 接続ログを保存すること

を定めた。

(イ) プロトタイプシステムの設計及び構築

これら技術的要件を満たすためのシステムとして、図２，３に示す構成のプロトタイプシステムを構築した。プロトタイプシステムでおこなう実験的検証においては、技術的有効性を確認するための装置構成を用いているため、OD-VPN ルータの代替として、既存の VPN ルータを利用（接続先の変更管理

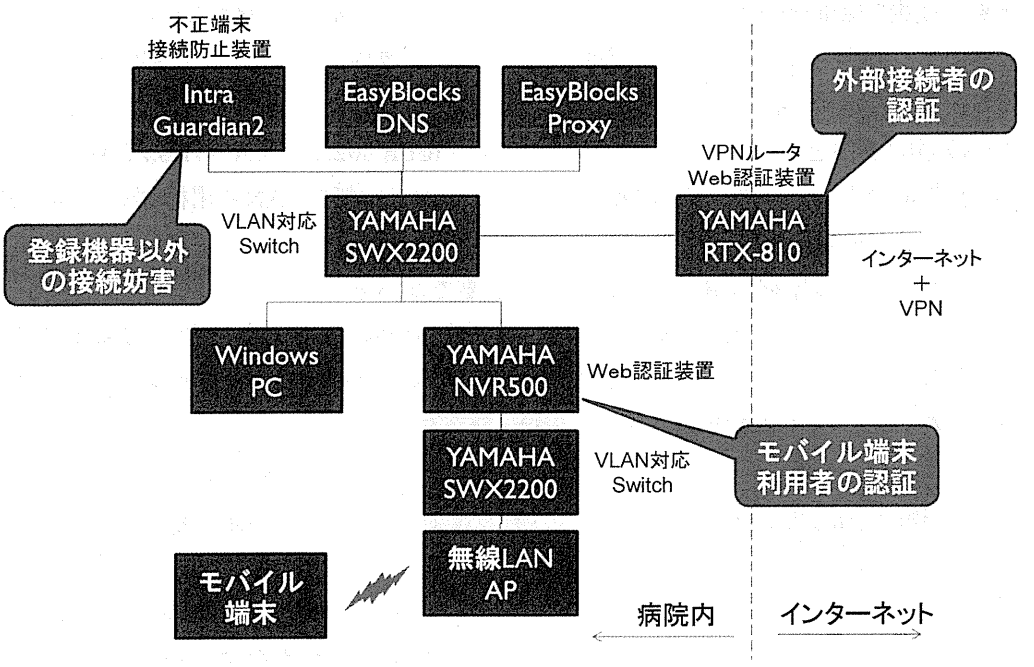

図２　プロトタイプシステムの機器構成（医療機関内）

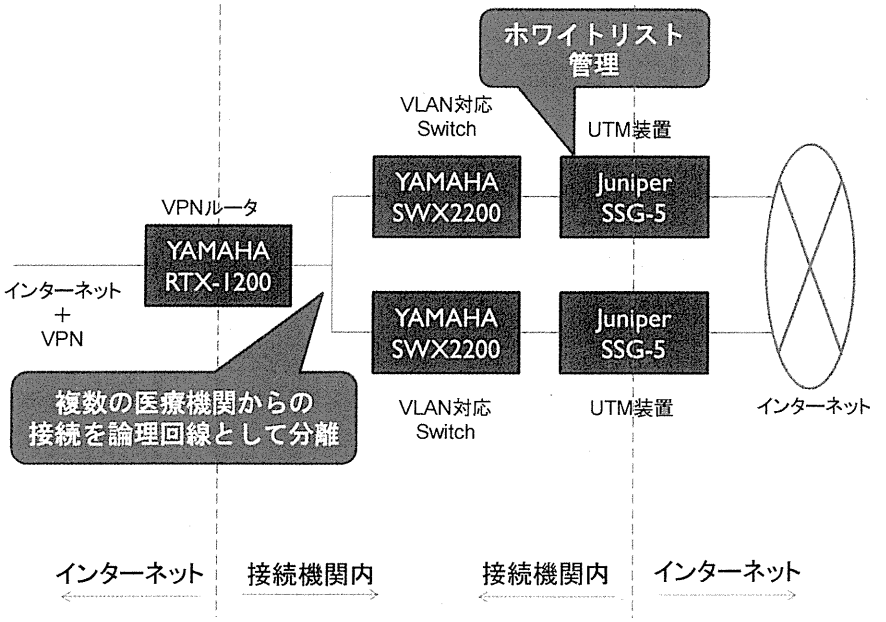

図３　プロトタイプシステムの機器構成（外部接続機関内）

は実施しない）している。

以下に技術的要件の実現方法を具体的に記載する。

- 技術要件１については、MAC アドレスを利用し、利用する機器は、すべて MAC アドレスを登録
- 技術要件２については、不正アクセス防止装置として IntraGuardian2 を導入し、MAC アドレスが登録されていない機器のネットワーク利用を防止
- 技術要件３は、外部接続時には、WindowsPC が接続された YAMAHA SWX2200 と YAMAHA RTX810 間で VLAN 接続をおこない、他の機器からの接続を禁止することで実現
- 技術要件 4 は、モバイル機器と無線 LAN アクセスポイント間で WPA2-AES を利用するとともに、YAMAHA NVR500 の Web 認証機能を利用し、モバイル機器利用者の認証をおこなうことで実現。認証が成功した場合のみ院内 LAN への接続を許可
- 技術要件 5-8 は、外部接続用の YAMAHA NVR500 の Web 認証機能を利用し、外部接続利用者の認証を実施することで実現。認証が成功した場合のみ外部接続機関への接続を許可
- 技術要件 9 は、YAMAHA NVR500、YAMAHA RTX-1200 間を IPsec/IKE で接続することで実現
- 技術要件 10 は、YAMAHA RTX-1200、YAMAHA SWX2200 間を VLAN 接続することで、異なる医療機関から RTX-1200 へ接続された通信経路を論理的に分離することで実現
- 技術要件 11-13 は、UTM(Unified Threat Management、統合脅威管理)装置 JuniperSSG-5 を利用し、外部接続時の通信ポート制御と外部接続先 Web サーバのホワイトリスト管理を実施
- 技術要件 14 は、外部接続管理機関内に設置された JuniperSSG-5 の DNS 機能と医療機関内に設置された EasyBlockDNS の DNS サーバ機能を

連携させることで実現
- 技術要件 15 については、下記機器のログ機能を利用して実現

(ウ) プロトタイプシステムの動作実験

以上のプロトタイプシステムを利用して、施設内における機器等の安全性向上に関する機能の検証として、

- 登録外機器を医療機関内 LAN に接続し、通信がおこなえないこと
- 外部接続時の院内機器、ルータ間の通信が、他の院内機器から傍受できないこと
- 登録された利用者のみが外部接続許を行えること
- 正当な手順を実施した場合、医療機関内の PC に対してから医療情報提供サーバの URL を入力することで、接続が可能なこと
- 外部接続機関内で複数の医療機関からの回線が論理的に分離できていること
- 容易に接続可能リストの管理と接続制御が行えること

を確認した。

(2) 提案システムの評価と今後の課題

現在大学病院などでは、研究等に利用するネットワーク（研究系ネットワーク）は Firewall を介してインターネットに接続していることが多いが、診療系のネットワークは、研究系ネットワークとの物理的な接続を遮断しているのが一般的であり、このようなネットワーク構成とすることでインターネットからの情報漏えいや外部からの攻撃などのリスクを取り除いている。しかし、このようなネットワーク構成では、患者紹介時における治療サマリー等のインターネットを経由した送付、CT、MRI 等の医療機器や電子カルテなどのリモートメンテナンス等のサービスが利用できない。また、今回の分担研究の調査によると、一部に安全性に配慮しつつ診療系ネットワークのインターネット接続を許可している大学病院もあり、このような医療機関では、Twitter や Facebook 等、潜在的には情報漏えいの危険性のあるサービスが利用されていることが明らかになっている。現在のところ大きな問題は起こっていないが、今回の調査対象となっていない医療機関においても同様のケースがあると想定されることから、一律に医療機関の診療系ネットワークのインターネット接続を行うことは危険である。さらに、安全性の高い情報ネットワークシステムを導入して技術的に安全性を確保する場合には、運用するための費用や専門的知識が要求されるなどの負担が大きく、運用ルールの徹底やセキュリティ教育だけでは十分な安全性を確保できないことから、特に規模の小さな医療機関における外部接続は容易ではない。

このような状況を踏まえると、本研究で提案したネットワーク構成は、外部情報の参照だけではなく、さまざまな分野における利用が期待できる上に、レセプトオンライン請求に利用するためのネットワークとして普及が進みつつある OD-VPN を利用した仕組みであり、また安全性を保証するためのシステム管理は外部接続機関によって行われることから、医療機関での新たなシステム導入は必要なく、小規模の医療機関でも導入及び運用は比較的容易であると考えられる。

以上の検討を踏まえると、本研究で示したインターネット接続の方式は、本国における

医療機関で利用する外部接続のための仕組みとして有用であることは明らかである。よって今後は、本研究の成果を厚労省医の定める「医療情報システムの安全管理に関するガイドライン」に反映させ、我が国の方策として実現されるよう推進活動を行っていく予定である。

今回我々が行った実験では、機器等の設定をオフラインで実施し、接続管理機関内でのネットワークの論理的分離についてL2スイッチを用いたVLANを利用しているため、これらの設定をOD-VPNの管理者等が実施できる仕組みを整えることが課題となる。これについてはOpenFlowと呼ばれ、現在は主なネットワーク機器メーカにより設立されたOpen Networking Foundationにより標準化作業が実施されているネットワーク技術の利用が想定される。OpenFlowは、ネットワーク層L1からL4の要素を利用してフローを制御するものであり、今回手動で設定を行った、VLAN対応Switching HUBなどの設定を自動化することが可能になると考えられるが、ルータ管理手法を持たないため、OD-VPN技術で培ったルータ管理手法をOpenFlowに対して融合させることで、安全安心な医療情報の連携・流通を可能とするネットワーク基盤である次世代OD-VPN（図４）を構築していくことが今後必要になると考える。

また、2007年の第五次医療法改正等で、完治していない患者も在宅通院するよう制度改正されたことから、近年在宅医療や介護の重要性が高まっている。今回の研究で想定したように医師等が利用する小型端末を常に病院内LANにVPN接続して利用する場合には、同様のネットワークを利用することは可能であるが、分担研究で報告されているように、在宅医療介護においては、さまざまな利用形態が想定され、常に今回検討した仕組みがそのまま適用できるとは限らない。今後は、このような在宅医療介護に特化した要件の整理を進め、このような利用も含めたシステムの設計を進めることも今後の検討課題である。

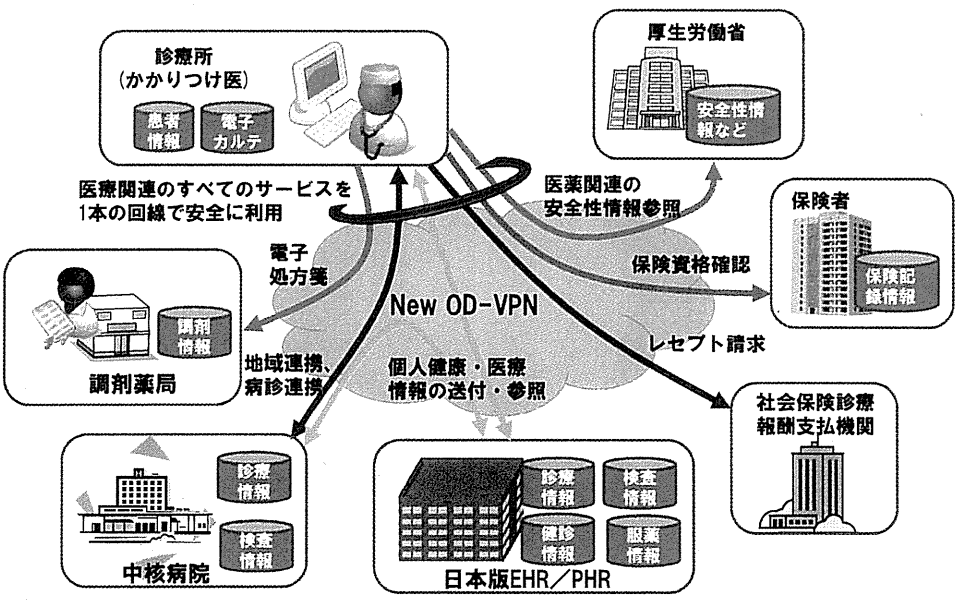

図４　次世代 OD-VPN の将来像

D．結論

本研究では、病院内部の医療情報をインターネット経由で外部接続可能な仕組みを提案し、システムの要件や技術的な実現方法を示した上で、今後の課題を明らかにした。

現在、医療機関などではレセプトのオンライン請求を実現するための手段としてOD-VPN が利用されており、今後様々なサービスへの応用が期待されていることからも、本研究の成果は、医用機関の内部・外部を問わず統一的なネットワーク管理・運用に必要な仕組みを提供するための標準技術として電子的な医療情報の流通促進に大いに寄与することになると考えている。

E．健康危険情報

該当なし

F．研究発表

- 小尾高史, 大山永昭：シームレスなサービス利用を可能とするセキュアネットワーク基盤の実現に向けて, 月間基金, 52 巻, 5 号, pp. 2-4 (2011) .
- 大山永昭：年金業務の改善とマイポータル, 年金時代, 40 巻, 14 号, p. 13 (2011) .

厚生労働科学研究費補助金（地域医療基盤開発推進研究事業）
分担研究報告書
医療情報を利用するサービス提供事業者、医療機関における運用方法の検討、
国際的な医療情報保護の取り組みとの整合性の調査に関する研究
研究分担者　喜多紘一
保健医療福祉情報安全管理適合性評価協会　理事長

研究要旨　本研究は「病院情報システム端末からの安全なインターネット直接接続に関する研究」の分担研究としてサービス提供事業者、医療機関において外部医療情報を参照し、利用する場面を想定し、その結果に基づいて、医療機関内の情報端末からの利用シーケンスを調査するものである。本年度は、医療で独自なHPKI認証局等「特殊サービス局」利用のユースケースとして「じん肺健康診断結果証明書」を取り上げた。本証明書は本文に異なった医師が４名署名した部分結果報告書を集合し、全体を通して医師が総合判定後署名する形式である。エックス線写真やシェーマもリンクして添付する必要があり、様々な要素を含み、ユースケースとして最適である。これを例として、施設内の端末で書類を作成、統合化あるいは提出された証明書を施設内で参照する場合のシーケンス検討を行った。

記名押印に替わって、電子署名およびタイムスタンプを行う場合、署名者自身のＨＰＫＩ証明書の有効性は予め確認してあれば、毎回署名時に確認の必要はないが、タイムスタンプはリクエストの発行およびレスポンス受信をインターネット等のネットワーク経由で行わなくてはならないので、結局PC端末と外部接続は必要となる。また、電子署名およびタイムスタンプの検証はタイムスタンプサービス局のタイムスタンプ署名用の証明書の有効性があらかじめ確認されていれば毎回確認の必要がなく、インターネットとの接続は毎回確認の必要がない。「じん肺健康診断結果証明書」の署名用の証明書の関連施設は同一であることが多く、医師も一連の健診機関では同じになることが多いので一連の受診者毎に毎回、確認する必要がなく、確認済みフラグなどの証明書のステイタスを示すイエローページを置いて利用するようにすれば外部と接続する回数を減らすことが出来る。

また、こうした「特殊サービス局」がオンデマンドVPN接続経由でサービスを提供するか、オンデマンドVPNのサービスプロバイダーが「特殊サービス局」との中継サービスを行う場合には、医療機関はインターネットとの直接接続を行う必要がない。
こうした検討は国際標準であるRFC3161、RFC3275やHL7 CDA R2等に基づいて行なった。

A. 研究目的

本研究では「病院情報システム端末からの安全なインターネット直接接続に関する研究」の分担研究として「医療情報を利用するサービス提供事業者、医療機関における運用方法の検討、国際的な医療情報保護の取り組みとの整合性の調査・検討」を行う。

分担研究としてサービス提供事業者、医療機関において外部医療情報を参照し、利用する場面を想定し、その結果に基づいて、医療機関内の情報端末からの利用シーケンスを調査する。

本年度は医療機関内の情報端末から外部にアクセスする例として、労働安全衛生法により管理が義務付けられている「じん肺健康診断結果証明書」を現在は紙ベースで実施されているものを、デジタル化して施設内で作成および参照する場合をユースケースとして取り上げて考察する。「じん肺健康診断結果証明書」は、図１に示すように各種の検査結果の集合により構成されている。更に、図中、印のマークがあるように、エ

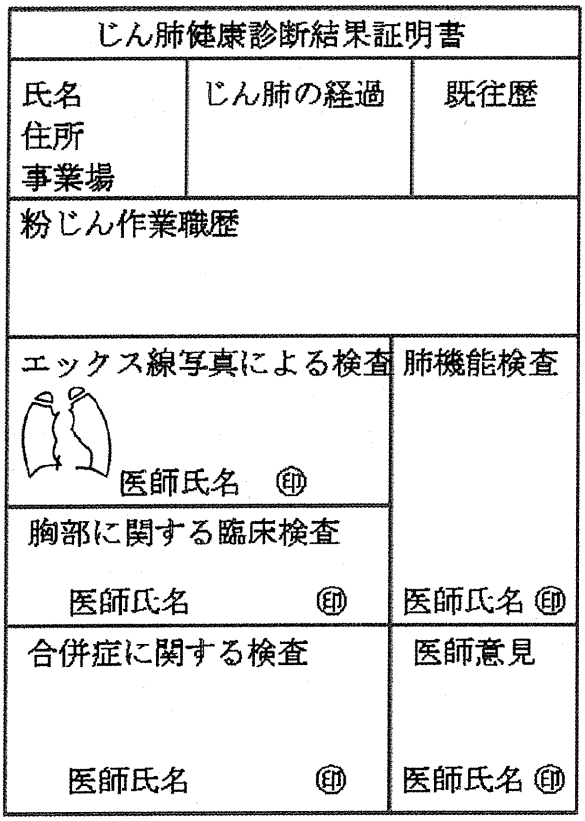

図１　じん肺健康診断結果証明書

ックス線写真による検査、肺機能検査、胸部に関する臨床検査、合併症に関する検査、医師意見の報告に対しては医師の記名・押印が要求されている。つまり、５名の異なる医師が記名・押印することになる。

これに対しては５名の医師による電子署名を行うシーンを検討する。また、エックス線写真による検査ではシェーマによる報告が求められている。ここではシェーマの添付およびエックス線写真もデジタルとして添付出来るフォーマットを検討する。

B．研究方法

１．「じん肺健康診断結果証明書」のデジタルフォーマット概要

全体の基本構成はＣＤＡ　Ｒ２に準じたフォーマットとする。ＣＤＡ　Ｒ２フォーマットは電子化された診療情報提供書[1]にも使用されているフォーマットで、基本的患者やドキュメントに関する属性を示すヘッダーと具体的な検査内容等を示すボディ部からなる。ここではボディ部を各検査毎にセクションに分け、記名押印が必要な検査は独立したＣＤＡ　Ｒ２形式の文章として作成し、診療情報提供への署名[2]と同様な形式で電子署名を行いセクション部へリンクさせることとした。また、エックス線写真による検査はシェーマがあり、更にデジタル化の特徴として撮影されたデジタル画像も添付することとした。これはエックス線写真検査の独立した報告書にさらに、シェーマと画像をリンクさせるフォーマットとした。

サンプルフォーマットの検討は昨年、同研究で検討した「HPKI署名付き医療情報パッケージ作成・参照プログラム」を修正して動作を１部シミュレートしシーケンス検討を行った。署名付与に使用する証明書の発行および失効処理はフリーソフトの「EasyCert」を用いて行なった。またICカードへの証明書の書き込み処理は「SafeSign」（G&D製）を使用した。

２．　階層化された文書への署名

２．１　階層構造の概要

階層構造を図２に示す。医療情報を交換する為には医療情報をパッケージ化して提供し、参照する必要がある。その為にＩＨＥで規約が出されているＰＤＩ方式[3]を参考に構造化をおこなった。基本部分はルートディレクトリーの下にＤＩＣＯＭ、ＨＬ７ＣＤＡフォルダーおよびＯＴＨＥＲフォルダーを置いた。ＣＤＡフォルダーには基本部分のＣＤＡ　Ｒ２に従ったＸＭＬファイルを置き、ＯＴＨＥＲファイルには基本部に結合される各検査結果報告書をリンクした。

エックス線写真による検査は更に画像とシェーマを含む為、ＯＴＨＥＲフォルダーの中にさらに「エックス線写真による検査結果報告部フォルダー」を置き、他の結果報告部のＸＭＬファイルはＯＴＨＥＲファイルに直接ファイルした。「エックス線写真による検査結果報告部フォルダー」の下には基本部分と同じようにＤＩＣＯＭ、ＨＬ７ＣＤＡフォルダーおよびＯＴＨＥＲフォルダーを置いた。ＤＩＣＯＭフォルダーにはじん肺の検査の撮影画像をファイルし、ＯＴＨＥＲファイルにはシェーマをファイルした。検査結果を示す本文はＨＬ７ＣＤＡフォルダーへファイルした。

各ＸＭＬファイルはEnveloping 方式で署名され、

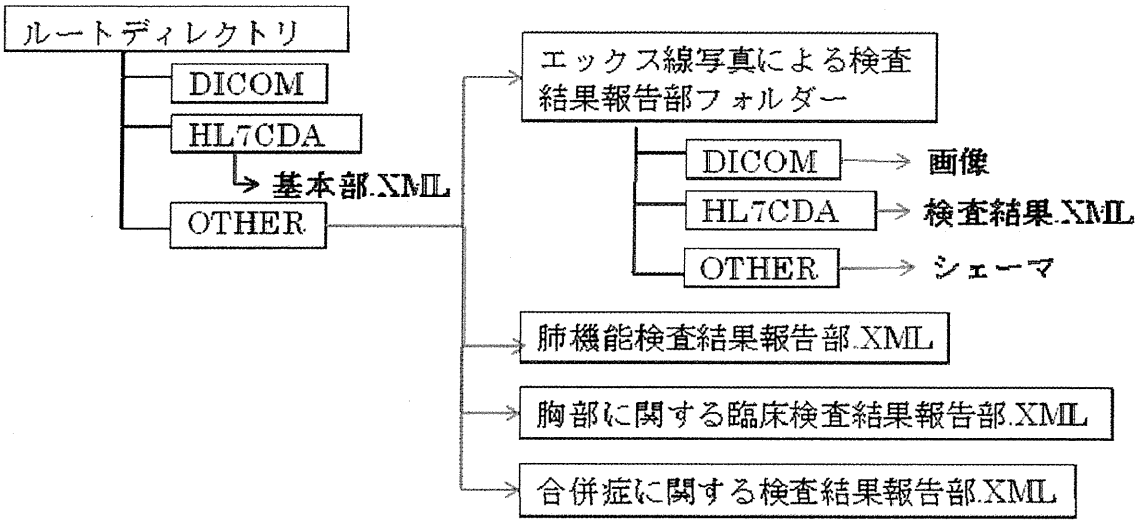

図2　階層化された「じん肺健康診断結果証明書」の文書構造

基本部XMLファイルの相当するセクションからリンクされている。また、「エックス線写真による検査」の画像およびシェーマは「エックス線写真による検査」の検査結果XMLからリンクされている。

2．2　部分報告書の共通ヘッダー

部分報告書もCDA R2形式に従って記述した。これにより基本部分と同じ署名及び検証プログラムを用いることが出来る。CDAのボディ部は検査目的により異なるがヘッダーは報告書の名称を除き同じに作成することが出来る。CDA R2の標準的なスキーマの必須項目を配慮すると図3のようなXML記述となる。この中には最低限の要素として「部分検査報告書名称」「患者名」「医師名」「医師が判定した年月日」「検査年月日」が記述できるようになっている。

C．研究結果

1．部分結果報告への署名とタイムスタンプ

基本部分で全体の判定を行う前に部分検査結果報告書が作成され且、医師により判定され電子署名がなされる必要がある。これは各検査施設で行われる事が望ましく、報告書のデジタル化により、紙媒体で結果を転記して記名押印するより運用の自由度が増すことが期待できる。

「エックス線写真による検査」結果報告書部は画像やシェーマをリンクしていて、検査結果XMLではそのハッシュ値が相当する部分のタグとして記述され、署名の時にそれを含めてハッシュをとる。従って各部分結果報告書ともXMLファイルに署名を行えばよい。署名はHPKI証明書を用いて行い、次にタイムスタンプを行う。

各結果報告書で署名を行う場合はHPKI証明書の有効性を確認する必要がある。その為には証明書を発行した認証局証明書およびその上の厚生労働省のルート証明書の有効性と自己の証明書の有効性を確認する必要がある。その為には各認証局のCRLを確認する必要があり、通常CRLは施設外にあるので、施設からネットワークを経由して外部施設へ接続する必要が発生する。

それ以外に証明書の有効期限や証明書の改ざんをチェックするがこれは施設内のソフトウエアで該当項目をチェックすれば良いので、外部施設とは接続する必要はない。

次のステップとしてタイムスタンプを行う。タイムスタンプは電子署名を行ったXMLファイル全体のハッシュをとり、それをタイムスタンプ局へ送付して署名をしてもらったものを送り返してもらい、それを所定のXMLのタグの値として保存する。

```
<!—以上はＣＤＡ　Ｒ２の固有ヘッダー記述-->
<code code="1001" codeSystem="1.2.392.200119.6.5007.2.3.4"
codeSystemName="じん肺健康診断部分報告書コード表"
 displayName="エックス線写真による検査"/>
  <title>エックス線写真による検査</title>
  <effectiveTime nullFlavor="NI"/>
  <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"/>
  <recordTarget>
        <!—患者名-->
  </recordTarget>
  <author>
    <time value="201003011020"/>
    <!—医師が署名した年月日-->
    <assignedAuthor>
      <id nullFlavor="NI "/>
      <assignedPerson>
        <!—医師の名前-->
      </assignedPerson>
    </assignedAuthor>
  </author>
  <custodian>
        <assignedCustodian>
          <representedCustodianOrganization>
            <id nullFlavor="NI"/>
          </representedCustodianOrganization>
        </assignedCustodian>
  </custodian>
  <documentationOf>
        <serviceEvent><effectiveTime value="20120519"/></serviceEvent>
       <!—健診年月日-->
   </documentationOf>
    <!—以下本文-->
```

図３　部分報告書用の共通ヘッダー記述

この場合、ハッシュ値をタイムスタンプ局へ送付する必要があるので、外部との接続が必要になる。通常。タイムスタンプは各施設が予め定めたタイムスタンプ局と契約してそこへ送るので固定された外部施設との接続となる。

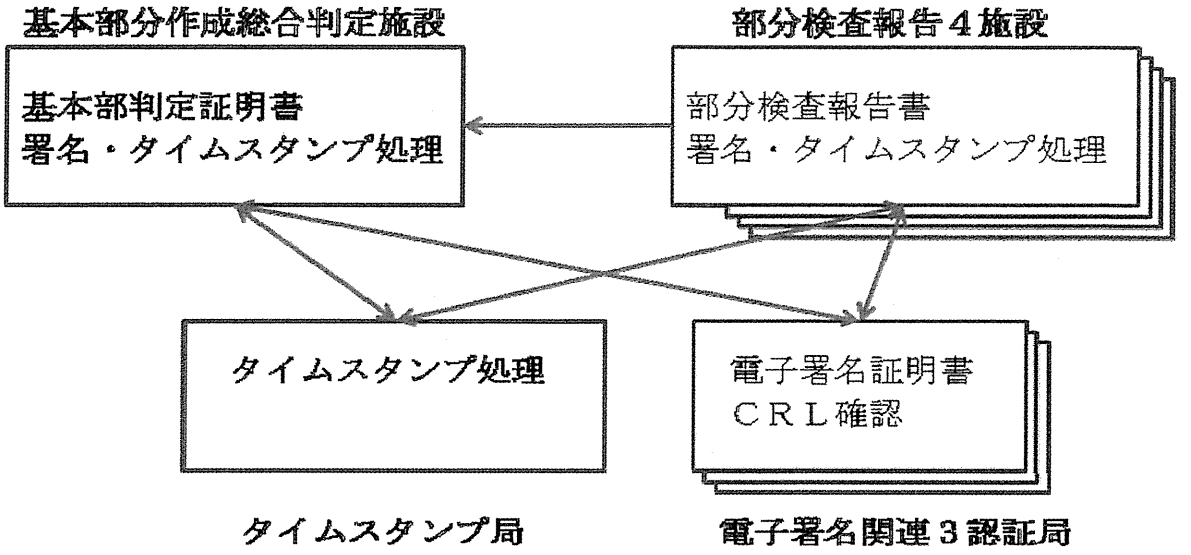

図４　電子署名及びタイムスタンプ処理時の各施設の接続関係

２．基本部分作成の為の電子署名とタイムスタンプ

基本部分に判定結果を記述して記名押印する為には、部分結果報告書として「エックス線写真による検査」、「肺機能検査」、「胸部に関する臨床検査」および「合併症に関する検査」の部分結果報告書に署名およびタイムスタンプを全部揃え、それに基本部分で入力する項目を加えて判定する必要がある。

その為には部分報告書が外部よりネットワークを通じて送られてくるのであればこれらの検査施設との間の接続が必要になる。

さらに、部分報告書の署名に使われている証明書の有効性を確認する必要がある。その為には各認証局のＣＲＬを確認する為に外部と接続する必要がある。この関係を図４に示す。

３．「じん肺健康診断結果証明書」参照時の電子署名およびタイムスタンプの確認

「じん肺健康診断結果証明書」を電子的に受け取った所は電子証明書やタイムスタンプを確認する必要がある。しかし、労働安全衛生法により実施される事が多いので、受け取ったデータは従業員が変わっても同一施設からのデータであることが多い。従って定期的に関連医師の証明書の有効性を確認しておけば毎回、外部と接続する必要はなくなる。

Ｄ．考察

１．署名時および署名検証時のシーケンス

診療情報提供書に署名を行う時あるいは検証を行う時はHPKI証明書の有効確認の為に失効確認リスト(CRL)を見に行く為にインターネットを経由して現在は日本医師会あるいはMEDIS-DCが管理する認証局のCRLサイトおよび厚生労働省のCRLサイトへ接続する必要がある。

但し署名時に自分の証明書が有効であることが何らかの手段で予め確認できていれば、署名時に毎回、失効確認をする為にインターネットとの接続は必要がなくなる。例えば１日１回、特別な確認サーバを経由して確認しておく等の方法がある。

２．タイムスタンプ使用時のシーケンス

タイムスタンプはデータのハッシュをとり、そのハッシュをタイムスタンプ局へリクウエストとして送り、タイムスタンプ局は時刻や証明書情報等を付加しタイムスタンプ局の秘密鍵で署名を行って、トークンとして応答を返す[4]。また、リクエストおよびレスポンスを授受するにはあらかじめ、ＰＣからＩＤ，パスワード等により、ログオンしておく必要がある。

タイムスタンプを行う場合には医療機関内にタイムスタンプ局を置かない限りは、毎回インターネットに接続する必要がある。

３．タイムスタンプ検証時のシーケンス

タイムスタンプの検証を行う為にはタイムスタンプサービス局のタイムスタンプ署名用の証明書の有効性を確認する必要があり、インターネットと接続する必要がある。

但し、タイムスタンプ局の証明書はタイムスタンプ局の数しかなく、その数が少なく、繰り返し同じ証明書が送られてくるので同じものを毎回確認する必要がない。確認の頻度を用途によって下げるか、安全な手段で別途確認していれば、医療機関内の個々のＰＣは確認の必要がないので、インターネットと接続する必要はない。

４．「電子署名認証局」と「タイムスタンプ局」とのインターネット接続の必然性

こうした「特殊サービス局」は数が限られるので、サービスとしてオンデマンドVPN接続を行うか、オンデマンドVPNのサービスプロバイダーがサービスとしてプロキシ経由で「特殊サービス局」へ接続するサービスを提供することが技術的には考えられる。

この場合、医療機関はインターネット接続を行う必要がなく、オンデマンドVPNを利用する環境でも目的を達成することが出来る。

また、医療機関内に署名あるいはタイムスタンプ用の代理サーバをおく場合は個々のPC端末を直接インターネット接続する必要はなくなり、代理サーバと「認定された特殊サービス局」の間をインターネット接続もしくはオンデマンドVPN等のセキュアーな専用回線に相当する接続を行えばよい。

Ｅ．結論

本年度は多階層構造を持った報告書への署名およびタイムスタンプの例として「じん肺健康診断結果証明書」を取り上げて検討した。記名押印に替わって、電子署名およびタイムスタンプを行う場合は、署名者自身のＨＰＫＩ証明書の有効性は予め確認できていても、タイムスタンプとしてリクエストおよびレスポンスをインターネット経由で送受しなくてはならない。その為に結局インターネット等外部との接続は必要となる。

また、電子署名およびタイムスタンプの検証について考えると、タイムスタンプはタイムスタンプサービス局のタイムスタンプ署名用の証明書が確認されていれば毎回確認の必要がない。また、署名文書を確認する場合、署名用の証明書は依頼施設が同一であることが多く、医師も一連の健診機関では同じになることが多いので毎回確認する必要がなく、確認済みフラグなどの証明書のステイタスを示すイエローブックを置いて利用するようにすれば外部と接続する回数を減らすことが出来る。

また、こうした「特殊サービス局」がオンデマンドVPN接続経由でサービスを提供するか、オンデマンドVPNのサービスプロバイダーが「認定された特殊サービス局」との中継サービスを行う場合、医療機関はインターネット接続を行う必要がない。

本年度は「じん肺健康診断結果証明書」に注目して検討をおこなったが、証明書のフォーマットがまだ確定していないので、ＣＤＡフォーマットを部分報告書に分割されるものと仮定して、それを作成することを念頭にシーケンスの検討を行った。今後、この検討を踏まえ、「じん肺健康診断結果証明書」の標準規格作成に生かすとともに、実運用の為のシステム提案や、「HPKI署名付き医療情報パッケージ作成・参照プログラム」の改良に生かしていく予定である。

Ｆ．参考文献

[1] HL7J-CDA-005 診療情報提供書規格;
http://www.hl7.jp/intro/std/HL7J-CDA-005.pdf;
2007年9月

[2] HL7J-CDA-002 CDA 文書電子署名規格;
http://www.hl7.jp/intro/std/HL7J-CDA-002.pdf;
2006年5月

[3] HL7J-CDA-004 可搬電子診療文書媒体規格;
http://www.hl7.jp/intro/std/HL7J-CDA-004.pdf;
2006年4月

[4] RFC3161 X.509 インターネット PKI タイムスタンププロトコル (TSP)
http://www.ipa.go.jp/security/rfc/RFC3161JA.html
; 2001年 8月

厚生労働科学研究費補助金（地域医療基盤開発研究事業）
病院情報システム端末からの安全なインターネット直接接続に関する研究
分担研究報告書

薬務関連に関わる情報管理及び提供方法の実施方策の調査・検討

研究分担者　土　屋　文　人（国際医療福祉大学）

研究要旨

院外処方率が全国平均で６０％超えた現在、患者の薬歴をどのように記録すべきかについては、その記録先が医療機関、薬局という異なった施設、システムで行われるため大きな課題となる。また、処方情報については、医療費抑制策の一環として後発品使用推進が２年毎に出されるが、その都度、方針が変更されるため、システム対応がネコの目のように変更せざるを得ないのが実情である。

しかしながら、どのような制度であれ、患者の薬歴をどのように電子的に記録するかは、制度に左右されることなく、原点に戻って検討すべきであることから、処方情報、調剤情報を記録するためのコードについて検討を行った。

その結果、厚労省標準医薬品コードであるHOTコードは調剤記録の正確性を担保するという点では十分な機能を果たしているが、正確な薬歴記録を作成するには必ずしも十分でないことが示された。そのためには成分を基本としたコードを新たに作成することが必要と思われる。

Ａ．研究目的

処方情報の電子化については香川、沖縄、石川というようにある程度地域を限定した形で実証実験が行われている。これらは限られた医療機関、薬局を対象として行われていることから、ここで明らかになった課題は克服することが求められることは当然であるが、電子処方せんを実効あらしめるための基盤整備としては個人認証やデータセンター等の課題以外に、基本的な基盤整備として医薬品のコードや用法に関する整備を確保する必要がある。

平成 23 年に発生した東日本大震災においては、被災地においてお薬手帳の重要性が認識され、またどこでもMY病院構想においてもお薬手帳の電子化に関する検討が先行して行われている。お薬手帳に記載される情報は基本的には調剤情報である。調剤情報としては調剤された「物」が特定されていること、服用（使用）する量に関する情報、用法、投与日数（総量）が記載されることが項目としては必要であるが、その情報の粒度は、現行のお薬手帳においては統一されていない。そのため、記載された量が１回量のものもあれば１日量のものもあるのが現状であり、また、計量調剤を行った散剤ではその重量が記載されているものもあるため、服用する際に１包を服用すべきところに、その重量である２ｇが数字のみ記載されていたため、患者が２包服用してしまうというような事故も発生している。このように、情報システムにおいて、

記載すべき情報の粒度が一致していないことは大きな問題となる。

また、医薬品のコードについては現在標準コードであるHOTコードが存在するにも拘わらず。実際にはYJコードが使用されているケースが大部分である。これらは医薬品コードに関する理解不足も根底にはあるが、調剤情報と処方情報を区別せずに扱ってきたことにも原因がある。しかも、中医協において、突如として「一般名処方」が提案され、一般名を含む形で処方をした場合には院外処方せん料を高く設定することが実施されたが、一般名表記方法の定義が明確ではなく、かつ公表されたマスタが極めて一部の薬品のみであったため、現場に無用の混乱を招いている。また、医療基盤ネットワーク検討会において電子処方せんに関する新たなレポートが出されたことから、今後電子処方せんのための基盤整備が今まで以上に進展すると思われる。

そこで本研究においては、真の薬歴を記録するために必要となる医薬品コードや用法に関して、再検討を行うこととする。

B．研究方法

現時点において厚労省標準として認定されているHOTコードおよびYJコードを対象に患者薬歴として長く記録を残すための要件および課題を明らかにする。

C．研究結果

(1)HOTコードは調剤情報を正確に記録することができるように、HOT9で調剤された医薬品が特定され(併売品も区別可能)、HOT11で調剤された包装形態(10錠シート、21錠シート等)をも記録可能となるよう設定されたコードである。これに対してYJコードはもともと薬価基準に収載された医薬品について統一収載の形で収載されている場合にこれらを製造会社が区別できるようにしたコードである。それゆえ製造承認が基本になっているため、併売品については区別ができない仕組みになっている。

医薬品を処方する際に、併売品の区別をする必要性はないため、処方時に使用するコードとしては、HOTコードでなくYJコードで実質的不自由はない。しかしながら、HOTコードはHOT9において末尾2桁を「00」にすることにより、当該医薬品名称を一般名で表記できるような構造になっており、その点では今回の診療報酬改訂において実施された一般名処方に対しては完全対応可能な機能を内在している。厚労省保険局が発表した一般名マスタはごく一部の医薬品しか対象としていないのみならず、内容の正確性についても保証されておらず、急遽決定された制度へのとりあえずの対症療法的コードと言わざるをえない。

HOTコードに比してYJコードはその構成内容に薬効、投与経路、成分等構成要素に意味付けを行っているが、YJコードが作成されてから四半世紀近く経つことから、ある項目については桁を使い切ってしまっており、今後は意味付けが却って問題になってしまうことは明白である。

一方、調剤情報を正確に記録するという観点からは、HOTは併売品を区別でき、かつ包装形態まで記録することができることから、これらが全く区別できないYJコードは、調剤記録をするコードとしては不適と言わざるを得ないにも拘わらず、保険薬局のシステムはレセプトシステムであり、レ

セプトの作成、調剤録の記録等が目的であるため、その情報の粒度はレセプト請求の粒度で十分という考えが定着していることから、問題はないものとして処理されてきたものである。

しかしながら、電子処方せんが実用化されるようになれば、処方情報と調剤情報の内容面においての突合（調剤エラーがないか否か）が患者レベルでも容易に確認できることが求められることになる。その意味ではHOTコード、YJコードのいずれも、薬歴として記録するという目的からみれば、機能として不十分ということになる。それは薬歴の意味を考えれば、先発品から後発品に切り替えられても、成分からみれば、同一であることから、薬歴記録用に、調剤情報を医薬品の成分を基本にして記録するコードを別に定める必要があるのではないかと考えられる。

D．考察

薬歴を正確に記録するという観点から成分を基本とした形態のコードを作成しようとした場合の現時点における問題点を明確にするため、HOTコードの過去10年間の経緯を含め検討を行った。その結果、剤形をどのように記録するのかが最大の課題であることが判明した。剤形は製薬会社がさまざまな工夫をしており、今後さらに増加することが考えられること、および例えばドライシロップのように、薬価基準上の剤形としてはシロップ剤になってしまうが、外形からの剤形は散剤（顆粒剤）になっている等、目的によってその区分が異なる等の問題もある。これらをどのように解決すべきかについてさらなる検討が必要と思われる。

また薬歴記録用のコードを作成するとした場合、その基本を「成分＋投与経路＋剤形」という形でまずまとめ、処方情報はこのレベルで記録をし、その後に調剤情報を付記することがよいのではないかと思われる。

E．結論

一般名処方をはじめ、処方情報を巡る環境変化はこの十年間極めて大きい。従来のこの制度に対症療法的に対応が行われてきたが、これらはその場としては必要であるが、原点に戻って、患者に出された薬剤の正確な把握即ち正確な薬歴の記録の観点から処方情報、調剤情報を考慮すると、成分を基本とする薬歴記録用のコードの作成が必要不可欠であるとの結論に達した。今後はこの結論を具現化するための実証を行いたい。

F．研究発表

なし

1．論文発表

なし

2．学会発表

なし

G．知的所有権の取得状況

1．特許取得

なし

2．実用新案登録

なし

3．その他

なし

厚生労働科学研究費補助金（地域医療基盤開発研究事業）
病院情報システム端末からの安全なインターネット直接接続に関する研究
分担研究報告書

産業保健医療に関わる情報管理及び提供方法の実施方策の調査・検討

研究分担者　八幡勝也　産業医科大学産業生態科学研究所作業病態学　非常勤講師

研究要旨
産業保健分野における、インターネット接続は、多くの場合には所属企業の管理下に置かれる。

A．研究目的

医療機関でのインターネットの利用について産業保健における情報管理について検討する。

産業保健の場合には、企業によりその組織運営が大きく異なり、情報管理の考え方を検討する必要がある。

B．研究方法

産業保健の組織形態による情報管理を検討する。本分担では、一般の医療機関ではなく、企業内診療所および業務委託について検討する。

C．研究結果および考察

産業保健の管理形態の種類（表）

産業保健情報の管理形態は、企業での産業保健体制により大きく異なる。

1．企業内担当事務職の取り扱い
2．企業内医療者による取り扱い

1．企業内担当事務職の取り扱い

企業内の事務管理職が管理する場合には、企業全体の情報管理体制の一環となる。

よって、健康情報も企業におけるインハウス情報として、労務情報や人事情報と同じ扱いとして管理される。いずれも従業員の個人情報で企業の業務として担当部署により利用される。

健診情報の多くは、健診センターなど医療機関に業務委託して、その結果を納品させる。その際には一般の企業間取引での個人情報保護に準じた取り扱いを行う。

従業員に健康異常が発生した場合には、主に労務担当者が担当となり、労務管理の中で処理される。長期にわたるな場合やメンタルヘルスなどの労務担当者の手に余る場合に、契約した産業医に相談がある。その際には、外部の主治医などの関与がある場合には、従業員本人の許可の元で、産業医から相談することがあるが、電話もしくは手紙に寄ることが多く、インターネットはほとんど使われない。

2．企業内医療者による取り扱い

企業内にで医療者が担当する場合には、大きく企業内診療所として診療を行う場合と安全衛生部門として医療者が診療以外の安全衛生業務を担当する場合である。

企業内診療所というのは、そもそも安全衛生法施行に伴う「昭和47年9月18日発基第91号」の見地からすると、通常あり得ないと考えられる。