20103104 7A

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２２年度　総括・分担研究報告書

研究代表者　大山　永昭

平成２３（２０１１）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。今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 との連携方法について検討を行う。

B．研究方法

平成２２年度の研究では、まず保健医療の各分野における利用シーンの整理をおこない、それに基づき医療機関内で利用される端末の抽出、及び、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要件を整理する。そして、その結果に基づき、オンデマンド VPN 技術を拡張して、医療機関からの外部情報を参照するシステムの実現方法を検討する。

C．研究結果

(1) 医療機関からの外部情報参照の必要性と課題の抽出

（ア） 医療機関等の外部情報参照状況

① 病院・診療所の場合

ある病院では、院内のネットワークを大きく２階層に分けており、１階層は、研究系ネットワークとして電子メールやWWWなどのアプリケーション、業務システムを利用し、別の階層は、診療系ネットワークとして、電子カルテや画像管理システム（PACS）、臨床データベース（AMIDAS）、スケジュール管理システム、電子照射録システム、部門システムなどの診療に必要なシステムが接続されている。研究系のネットワークと診療系ネットワークをProxyで接続するネットワーク構成とした場合、ウイルス感染事故が数件起きてしまったが、診療系のネットワークと研究系ネットワークとの物理的な接続を遮断したネットワーク構成の場合は大きな問題は発生しなかった。しかし、後者のネットワーク構成では、一般のメールやWebでの検索等のサービスが診療系では利用できず、利便性は犠牲になっている。

また、ある3つの大学病院の利用状況を調査した結果では、インターネット接続を行うネットワーク構成やセキュリティ対策は、3つの大学で大きく異なっており、すべての診療端末をインターネット接続している病院もあれば、まったくインターネット接続を行っていない病院もあった。すべての病院端末をインターネット接続している病院では、これまでのところインターネット接続によるアクシデント・インシデントは起こっておらず、現状の対策で特に不安を感じていないとのことだった。また、インターネット接続を行って取得する情報としては、医薬品の副作用情報やEBMはそれほど重要度ではなく、むしろ患者の社会的背景の把握が重要な情報であるとの実態が明らかになった。

②産業保健情報を管理する機関等の場合

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り、1．企業内の事務職管理、2．健診センターなどの健康診断の委託先、3．企業内診療所の3つに分けられる。企業内の事務職管理の場合や健診センターの医療機関で管理した情報に関してインターネット接続を行う場合、通常の病院のように業務用のシステムを利用しているため、外部のインターネットとの接続が一部に限られることが多い。一方、企業内診療所では、管理されている情報に対してインターネット接続するケースも考えられるが、セキュリティは診療所が自ら担保しなければならず、ほとんどの場合、そのスキルは不十分である。

③薬情報を利用する機関等の場合

現在薬務に関するインターネット接続を利用する場面としては、医薬品医療機器総合機構により提供されている添付文書情報の取得や、医療用の注射薬情報を表記したバーコードに関連する製品情報の取得などがあり、今後定期的なアクセスがなされるものと思われる。また、将来的には電子処方せんや電子版お薬手帳システムの構築が検討されており、これらが実際に利用されるようになると、病院情報システムからインターネットに直接接続する場合の安全性が大きく求められることになる。お薬手帳を電子的に管理する仕組みが実現された場合、お薬手帳に記録する医療用医薬品のみならず、一般用医薬品、サプリメントも含まれることになるが、医療用医薬品に関しては標準医薬品コード（ＨＯＴコード）が存在することから記録上特に問題は生じないが、ＯＴＣ，サプリメントについては標準コードがないことから、これらをどのように構築するかが喫緊の課題である。

（イ） 現状の対策と課題

厚生労働省が策定している「医療情報システムの安全管理に関するガイドライン」では、ネットワークを介して、外部と医療情報をやりとりする場合は、ネットワーク事業者・システム事業者と医療機関との間で責任分界点を明確にすることが必要とされているが、インターネット接続については、実態上、責任分界が困難であるため、ほとんどの医療機関において院内ＬＡＮの外部接続は実施されていない（図1）。

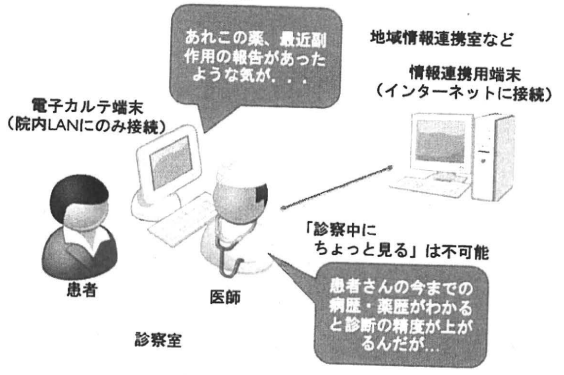

図 1　現在の外部情報参照の状況

また、1本の物理回線上で複数の論理回線（例えば病診連携用回線とインターネット接続用回線など）を利用する場合、外部への接続出口であるルータや院内LANに接続された端末などに対する悪意ある者の設定変更、不正動作などにより、医療機関の情報が他の医療機関などに流れてしまう回り込みや、意図しない外部医療機関への誤った情報伝送などの恐れがあると考えられている（図2）。このため、現時点でこのような利用をおこなうためには、利用目的に応じて、複数の物理回線を整備する必要があり、医療機関に対して割高な費用負担が生じる可能性がある。

ここで、以前我々が研究開発した、ICカード技術を利用するセキュアチップをルータに搭載し、安全にネットワーク管理・通信をおこなう仕組みであるオンデマンドVPN（任

意多地点間でオンデマンドに暗号通信路を構築する技術、OD-VPN、VPNは暗号通信路）が医療分野における標準技術として利用され始めている。OD-VPNは、セキュアチップに対してVPNで利用する認証鍵、設定情報をネットワーク事業者が直接設定するため、医療機関等を含めた他の者が絶対にVPNの設定を変更できない仕組みである。このため、ネットワーク経路上の責任分界点を技術的に分離・担保することが可能であり、現時点では、医療分野における唯一の標準技術となっている。しかし、現状のOD-VPNは、物理回線、論理回線を一体的に扱う技術であるため、医療機関内からのインターネット接続をOD-VPNを利用して実現するためには、複数の論理回線を安全に管理できる新たな技術的仕組みが必要となる。

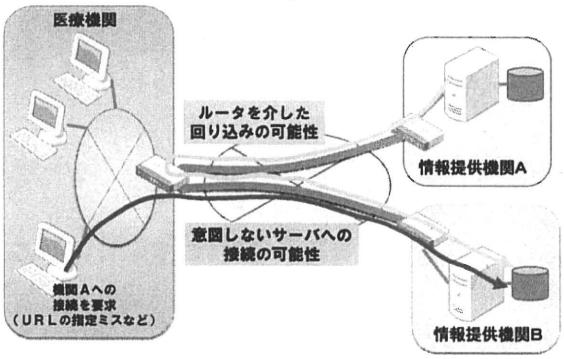

図 2　複数の論理回線を利用する場合の課題

(2) システム要件の整理

前節の実際の医療現場における利用シーンの検討を基に、病院内の情報をインターネット経由で外部利用する際の要件整理を行い、病院端末からのインターネット接続と病診連携を同時に実現するため技術的実現案の検討をおこなった。

ここで想定する利用シーンとしては、基本的な医療関連情報の閲覧（医薬品等安全性関連情報の参照などの病院外の HP などで公開されている情報を医師が参照）をおこなう場合、入院患者などが病室から上記公開情報などを参照する場合を検討し、外部情報を参照可能とする情報端末の種類を整理した。そして、安全性の問題が生じなければ、病院情報システムに接続されたすべての端末より外部サーバへのデータ入力およびデータ閲覧・出力をおこなうことができることが望ましいとし、医師等が診療時に電子カルテなどを利用する端末、病院事務室などにおかれたレセプト用端末、病院内で利用されているモバイル系端末を検討の対象とすることとした。さらに、研究分担者の意見から、医師などが個人的所有するノート PC の利用や、訪問介護などの際に病院外で利用されるモバイル端末についても考慮すべきとの意見があり、これらも検討対象に含めることとした。

以上の前提を踏まえ、本研究では、医療機関などがインターネット上で公開される情報にアクセスする際の経路及びコンテンツ管理をおこなう外部接続管理機関を導入したOD－VPNを利用することとし、このOD－VPNを利用した新たなシステム構成として、図3に示すシステムを提案した。また、このシステムに必要となる要件を以下の通り整理した。

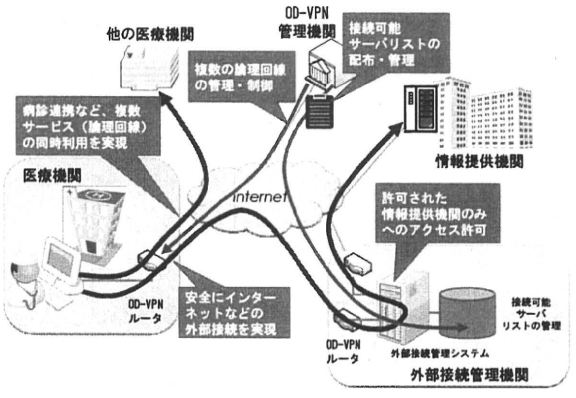

図 3　提案システムの全体像

医療機関内に対しては、OD-VPNの要件に加えて以下の要件が必要となる。

- 医療機関等の院内LANに接続される

端末の正当性を確保すること
- 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
- 正当な機器（登録機器）からのみ外部接続を許可すること
- モバイル機器利用時には、外部モバイル機器は院内LANにのみVPN（OD-VPNなど）を利用して接続されること
- 外部モバイル機器が院内LANにVPN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

また、新たに導入した外部接続管理機関についての要件は以下の通りとなる。
- 複数の医療機関からのパケットを分離し処理すること
- 許可されたWebサイト（ページ）にのみ接続を許可すること
- 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
- 証跡管理をおこなうこと

さらに、これら満足するために必要となる技術方法を検討し、以下の通り整理した。

院内ＬＡＮで利用する端末の正当性確保については、まず、院内機器の正当性確保の方法として、
- 機器に組み込まれているチップ等を利用した認証の実施（例えば、vPro搭載PCを院内LAN接続端末として利用、CPUやチップセットの中に特定のコードを埋め込み）
- PCの個別認識をハードウェアで保証することで、ソフトウェアによる欺瞞の可能性排除
- 外部からの通信による問い合わせに対応可能

を実施し、機器、ルータ間の通信の安全性確保には、
- 機器とルータ間の通信にはIPAHを利用

を、登録外機器のネットワーク接続禁止については、
- 不正PC接続検知防止システムの導入（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）
- 無線LAN利用機器の安全性確保（IEEE 802.1x（EAP-TLS,PEAP)の利用）

を実施することで対処可能であることを明らかにした。

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許可については、
- 機器利用時の利用者認証を必須とする
- 利用者認証方法はID, Passwordの利用も可能だが、ICカード利用を奨励（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）
- 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OD-VPNルータに対して実施。但し、認証サーバ等を導入する場合にはそれと連携をおこなう
- 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
- 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

により実施可能である。

また、外部接続管理機関の要件を満たす技術的実現方法として、
- 医療機関との間はOD-VPN で接続
- 複数の医療機関からのパケットを分離し処理
- 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の、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
- ホワイトリスト方式による Web フィルタリングを実施
- ホワイトリスト対象サイトの管理
- 接続ログの保存

を提案した。

D．結論

本研究では、OD-VPNを利用することで、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 の利用が始まっており、今後様々なサービスへの応用が期待されているが、現在のところ、医療機関内部のネットワーク管理を含めた総合的なネットワーク制御のための仕組みは確立しておらず、医師が医療機関内部から外部機関で提供される医療情報を自由に参照することは不可能である。本研究では、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、単なる医療情報の参照だけでなく、医療情報連携などにも適用可能であり、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

1．学会発表

- 鈴木裕之，喜多紘一，李中淳，平良奈緒子，小尾高史，山口雅浩，谷内田益義，山本寛繁，瓜生和久，横山隆裕，大山永昭，猪口正孝，土屋文人：公的な個人情報アカウントを利用した健康情報管理システムに関する実証実験，LOIS 研究会，Vol. 110，No. 281，pp. 15-21（2010）．
- 平良奈緒子，李中淳，鈴木裕之，喜多紘一，土屋文人，小尾高史，横山隆裕，大山永昭：薬歴情報管理の在り方に関する研究，LOIS 研究会，Vol. 110，No. 281，pp. 23-29（2010）．
- Joong-Sun Lee, Hiroyuki Suzuki, Naoko Taira, Kouichi Kita, Takashi Obi, Masuyoshi Yachida, Takahiro Yokoyma, Hiroshige Yamamoto, Kazuhisa Uryu, Masahiro Yamaguchi, Nagaaki Ohyama: The Development of a prototype e-P.O.Box and its application to personal health information management system, HEALTHINF 2011, 177 (2011).

2．解説記事等

- 小尾高史，大山永昭：医療従事者が知っておきべき医療情報受託ガイドラインのポイント，アイティービジョン，No. 23，pp. 66-68（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している。本年度は、医療で独自なHPKI認証局等「認定された特殊サービス局」利用のユースケースを取り上げた。その中でも、医療機関内の端末で診療情報提供書を作成、あるいは患者が他の医療機関から持参した診療情報提供書を医療機関内で参照する場合のシーケンスを調査した。PC端末で診療情報提供書を作成・検証するためのシーケンスを調査する為に、汎用の「医療情報ＨＰＫＩ署名付パッケージ作成・参照プログラムプログラム」を設計、そのプロトタイプを作成して検討を行った。

電子的に診療情報提供書を作成する場合は、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。この場合、署名者自身のＨＰＫＩ証明書の有効性は予め確認してあれば、毎回確認の必要はないが、タイムスタンプとしてリクエストの発行およびレスポンス受診をインターネット経由で行わなくてはならないので、結局PC端末とインターネット接続は必要となる。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の方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必要ないが、本文への署名用の証明書は診療情報提供書を発行した医師は多数にわたり、同じ医師から同じ日に何人も紹介される事は少ないので。毎回、確認の必要がある。従って、診療情報提供書の有効性検証の場合もインターネットに接続する必要がある。

ただし、「認定された特殊サービス局」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のサービス提供者が「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には医療機関はインターネット接続を行う必要がない。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る。

また、こうした検討は国際標準であるRFCC3161やHL7 CDA R2等に基づいて行なった。

A. 研究目的

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「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。

診療の安全性向上を目的として、医療機関外部にある最新のEBM 情報などを医療機関内に設置された情報端末を利用して参照することが強く望まれ，その際、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。

全体の研究では、これを実現する為に、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い、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ことをテーマとしている。

分担研究としては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。

B．研究方法

1．概要

医療機関がりインターネットを経由して提供されるサービスを利用する場合の場面として、医療機関等の検索、医薬品の副作用調査等医療機関が選択して加入する「一般情報提供サービス」とｅ文書法に基づく署名やタイムスタンプにおいて特定の限られた認証局やタイムスタンプ局等の「認定された特殊サービス局」とのトランズアクションのやり取りがある。

ＩＨＥ－ＸＤＳ（医療情報連携基盤）は地域医療連携を行う為の統合プロファイルであり、ＩＨＥではインターネット接続を前提としている。これは病院間の情報のやり取りなので、オンデマンドVPNの相互接続性が確保されればオンデマンドVPN網で利用されインターネットに直接接続されないことが「厚生労働省の安全管理のガイドライン」に従えば望ましいことになるので今回は考察対象からは除外する。

Webサービスによる「一般情報提供サービス」はREST(Representational State Transfer)あるいはSOAP(Simple Object Access Protocol)等を用いてそれぞれのサービスに沿ってシーケンスが組み立てられ、扱う情報に対するセキュリティレベルは高いものを要求されるが、シーケンス上は医療に特化した特長はなく、一般的なトランズアクションの交換になる。

ここでは、医療で独自な「認定された特殊サービス局」とのシーケンスを取り上げる。その中でも、院内の端末で診療情報提供書を作成、あるいは患者が他の医療機関から持参した診療情報提供書を医療機関内で利用するシーケンスをとりあげる。

その為に、PC端末で診療情報提供書を作成・検証するために、汎用の「医療情報HPKI署名付パッケージ作成・参照プログラムプログラム」を設計、そのプロトタイプを作成してシーケンスの検討を行った。

2．　「医療情報 HPKI 署名付パッケージ作成・参照プログラム」の設計

2．1　プログラムの概要

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。その際、真正性の保証の為に電子署名およびタイムスタンプを付与することが要求される。本プログラムは医師あるいは患者がＰＣ上で収集した情報を医療情報（既に電子署名およびタイムスタンプを付与された情報を含む）をパッケージ化して、電子署名およびタイムスタンプを付与して提供・参照することを目的とする。

本プログラムは医用画像、心電図波形、検体検査結果等の電子化された各種医療情報を患者や医療機関等に提供するためのデータパッケージを生成するソフトウェアである。医療情報の提供の際には提供情報の概要を記述した提供情報本文を作成し、外部参照ファイルの属性情報（種別、URI、ファイル名等）を添付書類として記述し、外部参照ファイルとリンクする。各種医療情報また、提供する医療情報の真正性を保証するために提供情報本文に対して HPKI 証明書による電子署名とタイムスタンプの付与を行う。提供情報本文は HL7 CDA R2 規格に準拠する形式とし、そのフォーマットは日本 HL7 協会から公開されている「診療情報提供書規格」[1]に従う。また、本アプリケーションでの提供情報本文に対する電子署名・タイムスタンプの付与は同じく日本 HL7 協会から公開されている「CDA 文書電子署名規格」[2]に沿う方式とする。上記に合わせて以下の機能を備えるものとする。

1）別途パッケージ化され署名・タイムスタンプ処理を施されたデータも外部参照ファイルとしてパッケージ化することができること。

2）パッケージ作成とともにパッケージを参照し、本文と外部参照ファイルを参照するとともに、電子署名やタイムスタンプの確認を行えること。

3）既にパッケージ化されたファイルに署名およびタ

イムスタンプを付与すること。

4）既に署名やタイムスタンプアが表示されたパッケージを表示し、署名およびタイムスタンプを検証できること。

2．2　基本動作

（1）パッケージ本文の生成

パッケージに必要なCDA文書作成の為のヘッダー項目およびボディ部の診療情報項目を選択し、添付書類として医療情報パッケージを含めた外部ファイルを選択する。

（2）電子署名およびタイムスタンプ付与

電子署名およびタイムスタンプ付与の有無を選択する。

（3）データパッケージの生成

（1）および（2）で入力した情報に従って、パッケージの作成および署名およびタイムスタンプの付与を行う。（2）にて、署名あるいはタイムスタンプが選択されていない場合は、それらが付与されないパッケージが保存される。

（4）パッケージデータの確認表示

上記作成後、パッケージデータが正常に作成され、署名およびタイムスタンプが付与されたかを確認する為に作成されたパッケージの内容と署名およびタイムスタンプを検証する表示を行う。

（5）既作成パッケージの表示

パッケージ作成機能とは独立して既に作成されたパッケージを選択し、内容を表示し、電子署名あるいはタイムスタンプの有無を確認し、検証する。

（6）既作成パッケージへの署名およびタイムスタンプの付与

パッケージ作成機能とは独立して既に作成されたパッケージを選択し、電子署名およびタイムスタンプを付与する。付与後は正しく付与されたか検証する為に（4）と同様に表示する。

2．3　機能仕様

（1）パッケージのタイトルは想定される文書名をプログラム内に予め登録し、それを選択するものとする。その場合「その他」の文書名も登録する。選択する為のテーブルは編集可能とする。

（2）提供情報記述項目、検査グループ名称、添付ファイル種別は入力時、ドロップダウンメニューにて選択可能とし、メニューリストはファイル化し、各項目が削除、追加修正等編集可能とする。

（3）パッケージの表示はCDA本文のXML文章に対してスタイルシートを使用して表示する。スタイルシートと文書との対応は対応テーブルを予めプログラム内に登録する。テーブルは編集可能とする。

（4）パッケージのファイル生成および保存形式はZIPファイル形式とする。

（5）データパッケージを添付書類とする場合は所定のZIPファイルを選択する。

（6）本文からデータパッケージをリンクするにはZIPファイルを解凍し、本文のパッケージのOTHERディレクトリ―の下にサブディレクトリを作成しそれをルートとするファイル構造を保持して展開する。本文からはこの展開された構造で添付するパッケージの中のCDA文書本文をリンクする。

（7）パッケージ構造は日本HL7協会から公開されている「可搬電子診療文書媒体規格」[3]による。

C．研究結果

1．「「医療情報HPKI署名付パッケージ作成・参照プログラム」プロトタイプの作成

1．1　データパッケージ構成

1．1．1　本文ファイルと外部参照ファイルの構成

提供される医療情報の概要と署名が記述される本文ファイルと本文ファイルと共に提供される各種医療データ（外部参照ファイル及びデータパッケージ）は本文ファイルに外部参照ファイルのリンク情報（パス情報）を記述することにより、その関係性を保持した。本文ファイルにリンクされる外部参照ファイルは複数個指定することができ、各々のリンク情報（本文ファイルに対する相対パス）が属性情報（ファイル名、フ

ファイル種別、ハッシュ値等）と共に記述した。本文ファイル及び外部参照ファイルおよびデータパッケージは、以降に記述されるディレクトリ構成を保持した状態で全てのファイルが一つの圧縮ファイルとして生成した。

１．１．２　データパッケージの階層構造

本文ファイルは別のデータパッケージに含まれる本文ファイルの外部参照ファイルとしてリンクされる場合がある。この場合、リンクされる本文のデータパッケージ中のディレクトリ及びファイル（外部参照ファイル）はその構造を保持した状態でリンク元のデータパッケージ中のOTHERディレクトリ以下のサブディレクトリ（リンク先データパッケージのルートディレクトリ）以下に生成した。

１．２　機能仕様

１．２．１　本文ファイルの生成

本アプリケーションで本文ファイルを生成する際、本文ファイルに含まれる属性情報（患者情報、提供元医療施設、提供先医療施設、傷病名など）はGUI（Graphical User Interface）からユーザーによって入力された情報に基づいて生成した。本文ファイルは入力された属性情報と添付される外部参照ファイルの属性情報（ファイル名、相対パス、ハッシュ値など）を元に、HL7 CDA規格に準拠したXMLファイルとして生成した。本文ファイルは本アプリケーションが動作する端末上のハードディスクに生成した。ファイルの命名規則は以下の通りとした。

診療情報提供書20101225102340.XML

本文タイトル文字列　パッケージ生成日時（YYYYMMDDhhmmss）　固定拡張子

１．２．２　本文ファイルの表示

本文ファイルの表示は本アプリケーションのGUIを介して行った。表示可能な本文ファイルはHL7 CDA規格に準拠したXML形式のみとし、外部参照ファイルの表示は本アプリケーションでは行わない（外部参照データの表示は対応する別のアプリケーションで行う）。本文ファイルに電子署名が付与されている場合は電子署名の属性情報（署名者、署名日付、有効性など）の表示も合わせて行い、本文ファイルの真正性について確認する機能を提供した。表示する本文ファイルの選択は本文ファイルが含まれるデータパッケージファイルまたは本文ファイルをユーザーがGUIで指定することにより行った。本文ファイルの表示にはスタイルシートを用いた。

１．２．３　外部参照ファイルの選択

本文ファイルにリンクされる外部参照ファイル（医用画像、心電図波形、検体検査結果等の電子ファイル）およびデータパッケージは本アプリケーションのGUIからローカル上のハードディスクに保存されたファイル（データパッケージのZIPファイルを含む）を指定することにより選択した。外部参照ファイルは複数選択可能とし、選択後のファイルはGUI上に表示した。一度選択されたファイルの中から任意のファイルを指定して選択を解除することも可能とした。選択された外部参照ファイルに対するリンク情報は本文ファイル生成時に自動で生成され、本文ファイルに記述した。外部参照ファイルにデータパッケージが選択された場合、選択されたデータパッケージを解凍した後、パッケージに含まれる本文ファイルに対してリンク付けを行った。

１．２．４　データパッケージの生成

本アプリケーションで生成される本文ファイルとそれに添付される外部参照ファイルは単一のデータパッケージとして生成した。データパッケージはローカル上のハードディスクにファイルとして生成した。データパッケージファイルを生成する場所はユーザーが本アプリケーションのGUIを介して任意の場所を選択できた。パッケージ化の処理はZIPアルゴリズムを使用し、「２．２．データパッケージのディレクトリ構成」及び「２．３．データパッケージの階層構造」に記述されているディレクトリ及びファイル構成を保持した状態で圧縮処理を行った。

また、外部参照ファイルとしてデータパッケージ（ZIPファイル）の本文がリンク付けされている場合、

リンクされているデータパッケージを解凍し、リンク元のパッケージと共に一つの圧縮ファイルとして生成した。データパッケージファイルの命名規則は以下の通りとした。

診療情報提供書20101225102340.ZIP

本文タイトル文字列　パッケージ生成日時(YYYYMMDDhhmmss)　拡張子

1．2．5　データパッケージの解凍（アンパッケージ）

本アプリケーションで生成されたデータパッケージは、任意のデータパッケージをユーザーが選択して本アプリケーションで解凍（アンパッケージ）する事ができた。アンパッケージ後はデータパッケージに含まれる本文ファイルと外部参照ファイルをハードディスク上の任意の場所に個別に保存した。(アンパッケージ後の本文ファイルの表示については「1．2．2　本文ファイルの表示」を参照)

1．2．6　電子署名付与

電子署名に用いられる署名アルゴリズム、署名形式、署名対象となるファイルフォーマット等は以下の通りとした。電子署名の対象となるものは「診療情報提供書規格」に準拠したHL7 CDA形式のXMLファイルのみとした。

パッケージ生成時および既にパッケージ化された署名なし本文ファイルあるいは単独の本文ファイルに署名を付与した。

1）署名アルゴリズム：RSA-1024ビット/SHA1
2）署名付与方式：XML-Signature and Syntax準拠、Enveloping形式
3）署名対象フォーマット：HL7 CDA R2

1．2．7　電子署名検証

本文ファイルに付与された電子署名の検証は本アプリケーションで行った。電子署名の検証の処理は署名対象ファイルの改竄の有無、署名付与に使用された証明書の妥当性、及び添付された外部参照ファイルの改竄のチェックを行った。

検証後は本アプリケーションのGUIに署名の署名検証結果、付与に使われた証明書属性情報、及び署名検証に失敗した際の理由の表示も行った。

1）署名検証方式：XML-Signature and Syntax準拠、Enveloping形式
2）証明書の検証：HPKIへの適合性/証明書チェインチェック/CRL（失効）確認
3）外部参照ファイル検証：各外部参照ファイルに対するハッシュ値の確認

1．2．8　タイムスタンプ付与

タイムスタンプの付与は本アプリケーションで電子署名が付与されると同時に実行した。タイムスタンプの付与の対象となるのは電子署名付与の対象となった電子ファイルのみであり、外部参照ファイルに対して、直接タイムスタンプの付与は行わず、パッケージ化してそのCDA文書本文に署名と同時にタイムスタンプを付与した。TSAからのタイムスタンプトークンの取得はRFC3161[4]に準拠したプロトコルを用いて行った。取得したタイムスタンプトークンはXAdES-T（XML Advanced Electronic Signatures）形式で対象文書に記述した。

1）タイムスタンププロトコル：RFC3161
2）ハッシュアルゴリズム：SHA-512

1．2．9　タイムスタンプ検証

タイムスタンプの検証は本アプリケーションで付与したタイムスタンプに対して行った。タイムスタンプ付与の対象となった電子ファイルの改竄の有無、TSA証明書の検証を行いタイムスタンプ時刻及び検証結果の表示を行った。

タイムスタンプの検証は下記の項目について行った。

1）フォーマット検証:RFC3161に基づく構文検証(TSTの検証)
2）署名検証：タイムスタンプの署名を検証
3）TSA証明書検証：タイムスタンプの中に含まれるTSA証明書の検証
4）対象文書検証：タイムスタンプ付与の対象となった文書の改竄の検証

1．3　本文ファイルフォーマット

提供情報本文のファイルフォーマットは「診療情報提供書規格」に準拠した（HL7 CDA R2形式）。

2．プロトタイプ動作画面

2．1　提供書作成プログラム

作成画面を図1に示す。

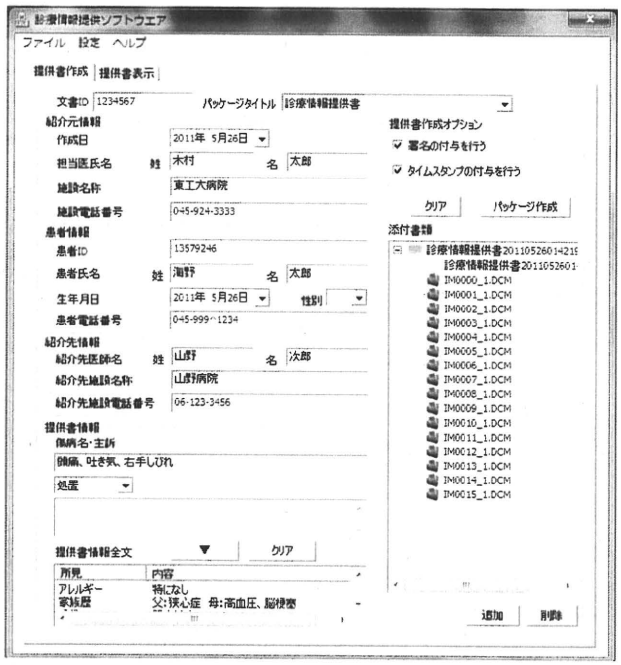

図1　提供書作成画面

右側の添付書類に記述されたDICOMファイル名群は複数枚のマルチスライスのCT画像の外部参照ファイルとして記述された。右上の「パッケージ作成」のボタンをクリックすると電子署名およびタイムスタンプが付与される。

添付ファイルとしてMFER波形形式、HL7 V2.5形式、Word、EXCEL、XML,PDF形式でも扱うことが出来る。又、こうしたファイルにXML形式の電子署名とタイムスタンプをほどこすことが出来る。

2．2　提供書表示プログラム

表示画面を図2に示す。左側の欄が通常の診療情報提供書と同様な画面が表示されている。最下段は添付ファイルの一覧が示され、これはフィルムを紹介先へ持参する時の封筒のような役割をしている。左側にもDICOMファイルの記述があるが、こちらはデータパッケージのような添付ファイルを持った提供書を付属の添付ファイルとして扱う時に階層構造を表示することが出来る。

右上の「署名検証」ボタンをクリックするすることにより検証結果を表示することが出来る。

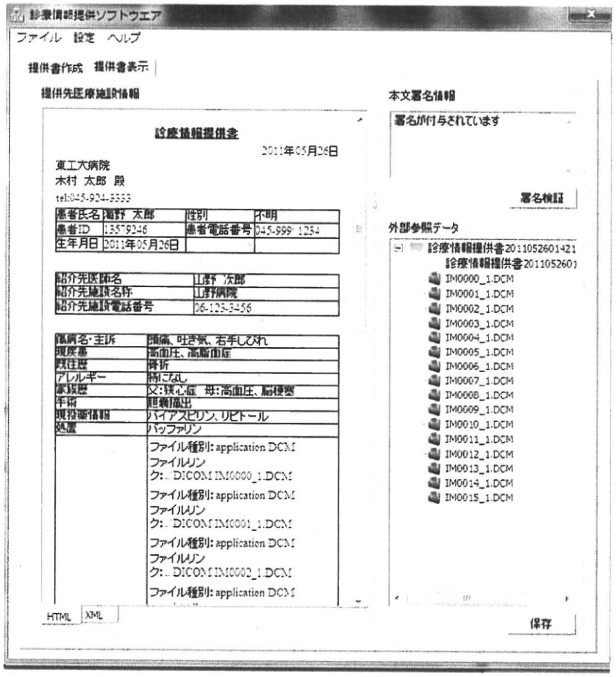

図2　提供書表示画面

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日本医師会あるいはMEDIS-DCが管理する認証局の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確認できていれば、署名時は失効確認を省略できるのでインターネットとの接続は必要がなくなる。

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。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、インターネットと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．「認定された特殊サービス局」とインターネット接続の必然性

「認定された特殊サービス局」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「認定された特殊サービス局」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。

５．診療情報書作成の動作について

「医療情報ＨＰＫＩ署名付パッケージ作成・参照プログラムプログラム」の表示は提供書表示画面の左下の「XML」のボタンをクリックすることにより、提供書のCDA文書フォーマットによるXML記述を表示することが出来る。署名およびタイムススタンプのフォーマットが正しく記述されているか、項目コードの値やOIDを確認できて便利である。

提供書の情報はレベル２による自由記述なので、所見項目を適当に選択すすると必要な情報を書き込むことが出来る。また、報告書のパッケージタイトルを選択することにより、診療情報提供書ばかりではなく、検体検査報告書とか画像診断レポートとか、画像１枚に対してもXML署名が行える。

こうしたタイトルや所見項目はドロップメニューで選択することが出来るが、メニューにない場合は設定により、CSVのテーブルに項目を追加することにより、増やすことが出来、応用範囲の広いものとなった。

これにより、「公的アカウント構想による電子生涯個人健康手帳」のようなシステムのプロトタイプを作成する場合に、個人へ提供し管理するデータを作成出来、応用範囲を広げることが出来た。

Ｅ．結論

診療情報提供書を作成する場合に、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、自身のＨＰＫＩ証明書の有効性が確認できていても、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受け取らなくてはいけないので、結局インターネット接続は必要となる。

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は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必要ないが、本文への署名用の証明書は診療情報提供書を発行した医師は多数にわたり、同じ医師から同じ日に何人も紹介される事は少ないので。毎回、確認の必要がある。従って、診療情報提供書確認の場合もインターネットに接続する必要がある。

ただし、「認定された特殊サービス局」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は医療機関はインターネット接続を行う必要がない。

また、シーケンス調査の為に作成した、「医療情報HPKI署名付パッケージ作成・参照プログラムプログラム」は、報告書のパッケージタイトルを選択することにより、診療情報提供書ばかりではなく、検体検査報告書とか画像診断レポートとか、画像１枚に対してもXML署名およびチャイムスタンプの付与および検証が行える。

さらに、全体の研究の目的であるインターネットに安全に接続する場合に必要な措置のテストを行う場合の一つのユースケースとしてこのプロトタイプを使用できる。

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）
総合研究報告書

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

患者が服用・使用している医薬品の記録を一元化することが重要であることから、電子版お薬手帳を想定して、ＯＴＣ薬についてコード化を検討した。ＯＴＣの現状を考慮すると、医療用医薬品における標準コードであるＨＯＴコードをそのまま適用することはできないものの、ＪＡＮコードとの対応、再使用の禁止等ＨＯＴコードの基本を受け継ぎつつ、新たなコードを作成することが必要であるとの希有論になった。

Ａ．研究目的

現状において病院情報システムからインターネット接続により利活用の頻度が高い情報としては、医薬品医療機器総合機構により提供されている、添付文書情報をはじめとした各種情報がある。また、平成20年9月出荷分から医療用医薬品の注射薬に医療安全の目的でバーコードが印刷されるようになったことから、このバーコードに関連する製品情報を管理している医療情報システム開発センターに対しても今後定期的なアクセスがなされるものと思われる。

また、現段階では法的に認められていないものの、将来的には電子処方せんが利用されるようになることは想像に難くない。また、内閣府では電子版お薬手帳システムの構築を検討しており、これらが実際に利用されるようになると、病院情報システムからインターネットに直接接続する場合の安全性が大きく求められることになる。

このように現時点においては実現していないものの、近い将来実用化すると思われる薬務関連に関わる情報に対して、病院情報システム端末から安全なインターネット直接接続を考えた場合、克服すべき課題を有すると思われる情報にはどのようなものがあり、またそれらの情報の提供方法、利用方法等を含めこれらの情報提供および実施方策に関する調査検討を行うこととする。

Ｂ．研究方法

本年度においては、内閣府による電子版お薬手帳システムの構築が検討されていることから、本研究においては、電子版お薬手帳を実用化しようとした場合の情報管理等において、どのような課題があるかについて検討を行うこととした。

お薬手帳とは、患者が服用・使用している医薬品について患者個人毎に記録を行うとともに、患者自身が服用・使用している際に発生したイベントを記録して、医師や薬剤師に対して服用中に起きた事象について次回診察時等に伝え忘れることのないようにすることで、医師等がこの情報を参考にして処方の変更や量の調節を行う参考にすることを想定しているものである。

それ故お薬手帳に記録される対象としては、医療用医薬品のみならず、一般用医薬品、サプリメントも含まれることになる。医療用医薬品に関しては標準医薬品コード（ＨＯＴコード）が存在することから記録上特に問題は生じないが、ＯＴＣ，サプリメントについては標準コードがないことから、これらをどのように構築するかが喫緊の課題である。サプリメントについては、あまりに対象が広すぎ、また通常の流通ではなく、インターネットを介して個別に行われることも少なくないことから、本年度の研究対象からは外し、ＯＴＣ医薬品について検討を行うこととした。

Ｃ．研究結果

ＯＴＣが医療用医薬品と大きく異なるのは、ＯＴＣの多くが配合剤となっていることである。そのため、ＨＯＴコードのように成分を基本としたコード体系にはなじまないことが確認された。また、配合剤の各成分の量が変化することもあるため、コード化を行うに際して、医療用医薬品と同様の分類を行うことが困難であった。

また、ＯＴＣの名称は共通のブランドをもちながら末尾部分で含まれる成分の違いを示している場合が多いことから、この面においてもＨＯＴコードと同一の体系には合致しないことが判明した。

現時点ではＯＴＣの分類は医薬品の含有する成分を、副作用、相互作用、使用方法の難しさ等の項目を評価して、以下のような３つのグループに分類されている。

第１類医薬品：ＯＴＣ医薬品としての使用経験が少ないものや副作用、相互作用などの項目で安全性上、特に注意を要するもの。

第２類医薬品： 副作用、相互作用などの項目で安全性上、注意を要するもの。またこの中で、特に注意を要するものを指定第２類医薬品とする。

第３類医薬品： 副作用、相互作用などの項目で安全性上、多少注意を要するもの。

また、販売をすることができる資格としては、薬剤師あるいは登録販売者（第二類、第三類のみ販売可）と定められている。

一方、ＯＴＣにおける重篤な副作用の多くは第一類および指定第二類であるが第三類であっても発生はしていることから、ＯＴＣの一部のみを電子手帳の記載対象とすることは好ましくない。

さらに、現行においては、当該医薬品が含有する成分を基本に分類が行われてきたが、今後は製剤そのものを対象に分類を行うことが計画され、漢方薬を手始めとして現在作業中である。

以上の状況に鑑みると、ＨＯＴコードのような構造・体系が確立しているコードを短期間で付与することは困難であると思われることから、とりあえず当面の間は、ＯＴＣが有するＪＡＮコードに単純に対応するコードをとりあえず作成することでお薬手帳への対応を可能とすることが確実な方法と思われる。ただし、医療用医薬品においてはＨＯＴ９で製品と対応していることから、ＯＴＣにおいても同様に９桁を基本として、それに包装形態、包装数量を考慮して１３桁とし、ＪＡＮコードと１対１の対応とすることが適切であるとの結論に達した。

Ｄ．考察

ＯＴＣを医療用医薬品と同一の構造、体

系でコード化することは現時点では困難が伴うことから、ＨＯＴコードと同一の桁数にした上で付番を行うことが適切であるとの結論を得たことから、次年度はこの結果を具現化するため作業を行う予定である。これにより、企業をキーとして作成されているＪＡＮコードに比して、「物」を中心としたＨＯＴ類似のコード体系に近い形でコード化が行われることになる。しかしながら、作成される予定のコードはＨＯＴコード同様に、再使用は行わないとの原則は堅持することにより、電子版お薬手帳に記録を行うことが可能になるとともに、将来ＯＴＣに対して、より系統だったコードを付与する場合に、多いに役立つものと考える。

Ｅ．結論

ＯＴＣ薬に医療用医薬品の標準コードであるＨＯＴコードをそのまま流用することには困難が伴うことが確認された。しかしながら、電子版お薬手帳を実効性あらしめるためには、ＨＯＴコードに準じたコードを作成することが求められていることから、当分の間、ＨＯＴコードの構造、体系に類似したコードを作成することで対応を図ることが重要であると思われる。

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（地域医療基盤開発推進研究事業）

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

企業における保健活動は産業医の契約形態によって異なる。よって、情報管理も企業と産業医の契約関係に分けて検討する必要がある。

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、雇用及び契約形態が複数あり、それにより情報管理の考え方を検討する必要がある。

B．研究方法

産業保健の雇用形態および契約形態を整理し、それによる情報管理を検討する。」

C．研究結果および考察

産業保健の管理形態の種類（表1）

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。大きくは、1．企業内の事務職管理、2．健診センターなどの健康診断の委託先、3．企業内診療所の3つである。

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。

健診センターなどの健診受託機関に委託している場合には、健診センターの医療機関としての医療情報管理の対象と成る。

企業内診療所の場合には、企業内の一部門の場合と独立している場合に分かれる。一部門の場合には、企業内の情報管理の対象となるが、独立している場合には、医療機関としての管理の体制が求められる。

インターネットとの関わりで検討すると、企業内の部門として活動する際には、外部との情報交換が大きく制限される可能性が高い。

医療機関であれば、通常の病院のように業務用のシステムしかなく、外部のインターネットとの接続が一部に限られることが多い。

企業内診療所であれば、インターネットの接続のセキュリティは、診療所自身で担保しなければならない。しかし、ほとんどの場合、そのスキルが不十分である。

E．結論

産業保健分野における、インターネット接続は、各企業の体制によって異なる。それぞれの実情に合わせて検討しなければならない。

F．健康危険情報

特になし

参考文献

なし