200634054A

厚生労働科学研究費補助金

医療安全・医療技術評価総合研究事業

安全な保健医療情報流通を促進する保健医療認証基盤整備の技術的方策に関する研究

平成１８年度　総括研究報告書

主任研究者　大山　永昭

平成１９（２００７）年　４月

別紙２

目　　次

厚生労働科学研究費補助金（医療安全・医療技術評価総合研究事業）
総括研究報告書

安全な保健医療情報流通を促進する保健医療認証基盤整備の技術的方策に関する研究

主任研究者　　大山　永昭　　東京工業大学像情報工学研究施設　教授

研究要旨：　今後の医療の高度化やそれに伴う機能分化の促進が想定される状況下で、患者主体の診療が実施されるためには、関連する施設等の間で、電子カルテや医療情報の伝送を安全かつ動的に行っていくためのネットワーク基盤が必要である。本研究では、多機能 IC チップを利用し、オープンなネットワーク上で、誰もが安全・手軽に情報サービスを利用可能なネットワーク基盤を医療分野に適用する方法を提案した。さらに、オンデマンド VPN がネットワーク上を流通する医療情報の保護に有効であることを実験的に明らかにし、実用化に向けた課題を明らかにした。

分担研究者　喜多　紘一　東京工業大学像情報工学研究施設 特任教授
土屋　文人　東京医科歯科大学歯学部付属病院 薬剤部長
八幡　勝也　（財）九州ﾋｭｰﾏﾝﾒﾃﾞｨｱ創造ｾﾝﾀｰ 専任主席研究員
高橋　紘士　立教大学ｺﾐｭﾆﾃｨ福祉学部 教授
秋山　昌範　国立国際医療ｾﾝﾀｰ情報ｼｽﾃﾑ部 部長
石垣　武男　名古屋大学大学院医学研究科　教授
山本　隆一　東京大学大学院情報学環　助教授
梅田　徳男　北里大学医療衛生学部　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。我々は、これまでに保健医療福祉分野の情報化において必須となる電子的な認証、特に医師･看護婦等の資格認証の必要性を示し、電子認証の実施方法や問題点の調査・検討を行ってきており、本研究では、これら研究成果を踏まえ、もう１つの重要な課題である通信回線上や医療機関内部における個人情報・医療情報等の安全性を確保する技術について研究開発を進めるとともに、保健医療分野における情報の安全な流通を保証するネットワーク基盤を構築・運用する方策について検討する。さらに、保健医療福祉分野でのネットワーク基盤整備を進めるとともに、それを活用した様々な保健医療福祉サービスの充実が求められていることから、ネットワーク基盤を利用した安全性、利便性、経済性などに優れた医療サービスの実施方法を取りまとめ、さらに保健医療福祉サービスの今後の新たな展開の可能性等を示す。

B．研究方法

工学者及び医師らの研究分担者からなる研

究班として、保健、医療、福祉の各分野における情報化推進にあたっている専門家を中心として組織し、委員会を開催して各分野における電子化の状況や情報保護に対する取り組みを調査し、安全に医療情報を取り扱うための課題の抽出と実現方法の検討を行った。さらに、安全なネットワーク基盤構築に関する検討を行っている諸機関･グループとの情報交換･連携を行い、今後、医療分野における共通ネットワーク基盤にするための方策を検討した。

C．研究結果

(1) 医療情報管理のための認証基盤における技術的要件

現在、多くの医療施設において電子カルテシステム等の電子医療情報システムの導入が進められている。それらの多くは個々の医療施設内での閉じたネットワークにおける利用に留まっており、インターネットのようなオープンなネットワークを経由した情報交換はほとんど行われていない。その理由としては、現状のシステムはベンダー毎に仕様が異なり相互運用に困難性があることに加え、データの安全性を確保するセキュリティの問題が大きい。ここでは、オープンネットワークを経由して医療施設間で安全に情報を交換するための技術的要件を整理する。

（ア） 医療情報交換に必要な電子的な認証

医療施設間で情報をやり取りする際の最も重要な課題として、情報交換を行う主体（利用者や機器）の正当性の確認が挙げられる。主体の正当性を確認する方法としては、主体が医療施設に属していることを認証し、また情報によっては医療従事者であることを電子的に認証する必要がある。さらに患者の個人情報となる医療情報については、患者の同意の認証も必要になるケースもある。上記について、（イ）～（エ）にそれぞれの具体的な対策について述べる。

（イ） オンデマンドVPNを利用した施設認証

医療施設の認証方法としては、オンデマンドVPNの利用が有効である。医療施設内のネットワークに接続された機器をオンデマンドVPN経由でのみアクセスを可能とすることにより、オンデマンドVPNが設置された医療施設間のみの情報交換が可能になる。また、オンデマンドVPNは、VPN構築のための複雑な設定が不要なため、大学病院のような大規模な医療施設から診療所のような小規模な医療施設まで容易に設置可能であり、高いスケーラビリティを実現できる。

（ウ） HPKIによる資格認証

医師や看護師等の資格を有する者のみがアクセスできる情報の場合には、アクセス者の資格を認証する必要がある。現在（財）医療情報システム開発センター（MEDIS-DC）や日本医師会によって、医療用の認証基盤（ヘルスケアPKI：HPKI）の運用が進められており、資格認証を行うインフラは整備されつつあり、その実用化が期待される。

（エ） 患者の同意

患者の同意が必要な情報へのアクセスについては、患者のICカードで電子署名することにより同意を得る手法が有効である。

(2) オンデマンド VPN を利用した医療情報交換の実施例

オンデマンドVPNを利用した医療情報の実験システムが、加古川市（検査・検診オンラインシステム）と秋田大学病院（遠隔医療診断システム）で稼動している。

（ア） 加古川地域保健医療情報システム

本システムは、疾病の早期発見・早期治療、健診の受診率向上を目的とし、各医療機関における個人の健康に関する情報の共有機能やネットワークを介した病診連携機能を提供している。

総合保健センタでは、診療所や小規模病院から検査依頼された検体を検査し、その結果を報告書（紙ベース）にて依頼元の医療機関に報告する。また、オンラインにて、検査結果を加古川地域保健医療情報センタ（以下情報センタと略記）に送付し、管理を委託された情報センタは、検査健診データベースに情報を登録・保存する。

一方、中核病院では、独自で検体の検査を実施し、検査結果を院内の地域医療データベースに登録・保存すると共に、情報センタにオンラインにて送付し、情報センタが検査健診データベースに登録・保存する。

診療所や小規模病院では、総合保健センタより、患者や受診者の検査報告書を紙ベースで受け取ると共に、情報センタの検査健診データベースに登録された医療情報を、オンラインにて検索・参照することができる。

オープンなネットワークに接続されているため、2点間の通信はオンデマンドVPNを利用して接続されている。またそれ以外にも以下の対策を施している。

- 検査情報などの情報資産を保管するサーバの安全な場所での管理・運用とアクセス制限
- 公開情報のDMZへの配置と、通信の限定
- 外部からDMZ以外へのアクセス禁止
- サービス利用者の認証・限定
- 接続先拠点との合意
- 接続先・接続元のアドレスによるアクセス制限
- 不正な中継禁止
- HTTP、メールアクセスの制限
- ウィルスチェック

これらの対策をオンデマンドVPNと組み合わせることによって、安全なシステム運用を確保している。

（イ） 秋田大学付属病院での遠隔診断

秋田大学付属病院を中心とした遠隔診断の取り組みでは、遠隔画像読影ネットワーク及び医療画像読影依頼・レポート（ASP）システムが構築されている。本システムは、地域の小規模病院や診療所で撮影されたCTやMRIの画像の読影を、専門医のいる大規模・中核病院や大学病院に依頼し、専門医が読影を行って、その結果をレポートとして返送することで、専門医不足の解消や地域医療の向上を図ろうとするものである。

上記のシステムでは、遠隔診断システムのネットワークサービスとして、オンライン・インターネットVPNサービスが利用されている。また、情報の暗号化やファイルへのパスワードの付与を行うと共に、オンラインサービス提供者、回線業者、医療機関などの関係者、関係機関等が、その責任範囲を明確にし、役割を果たして行くことにより、十分な安全性を確保できている。

現在、秋田大学付属病院と大森市民病院間で実施されているが、H19年度には、専門医のいる５病院とも連携を行えるよう、拡張される予定である。

(3) オンデマンド VPN を実運用する上での課題

（１）でも述べたように、医療情報を安全に交換するためには、オンデマンドVPNによる接続が極めて有効である。しかしオンデマンドVPNを実運用することを考えた場合、技術的な課題もいくつか残っている。ここではオンデマンドVPNを実運用する際の技術的課題とその解決策について検討する。

（ア） 暗号手法の危殆化に対する対策

現在、様々なシステムで用いられている暗号の強度が近い将来危殆化するという予測がなされており、その場合に使用している暗号を安全性の高いものに更新する必要性が議論されている。しかし現在利用されている殆どのシステムでは、使用している暗号方式の更新を想定して構築されておらず、オンデマンドVPNにおいても、その対策について検討することが必要になると考えられる。ここではオンデマンドVPNの暗号方式を移行する方法について議論する。

オンデマンドVPNに用いられているICチップ内の暗号機能を更新するためには、拡張用ライブラリの追加やあらかじめ移行用の暗号ライブラリを予備として備えておく等の機能がIC チップに必要となる。しかし、製造コストの面からこういった機能を有していないチップを搭載した機器が流通することも考えられる。

そこで、更新可能なチップと不可能なチップ混在した場合でも対応可能な暗号機能移行スケジュールを検討した結果、図１のような方式が妥当であると考えられる。このスケジュールは、情報処理推進機構による「暗号の危殆化に関する調査報告書」に基づいた暗号の危殆化レベルに合わせて、レベルごとに

サービス提供者及びICチップ内蔵機器がどのような対策をすべきかを示しており、レベル３で暗号の移行が勧告されると想定している。サービス提供者は、レベル３の移行期において更新可能なICチップを搭載した機器とそうでない機器の両方にサービスを提供可能な体制を整えておく必要があり、また暗号機能を更新した場合にも、暗号や認証の信頼関係を維持してサービスを継続的に提供できるような仕組みが必要になる。

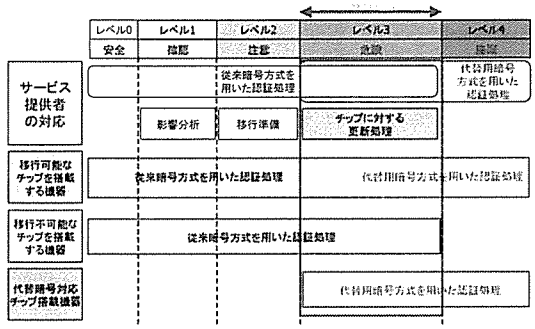

図１．移行スケジュールの例

（イ） 通信主体の秘匿

医療情報交換におけるVPN接続では、希少な病気を取り扱う病院との通信など通信相手の匿名性が要求されるシーンがいくつか考えられる。現状のオンデマンドVPNは、一般的なVPNと同様に通信主体の匿名性を有しないため、通信そのものの秘匿（どこからどこへ通信しているかを秘匿する）を必要とする用途に用いることができない。ここでは、現状のオンデマンドVPNに対し、通信主体の匿名性を確保する技術について述べる。

一般的に通信主体を秘匿する方法としては、通信主体間の間に第三者を中継ノードとして用いることで間接的な通信を行い、特定を防ぐ方法がとられることが多い。しかし、中継ノードを置くだけでは、通信パケットの盗み見によるトラフィック解析の脅威には対応できない。よって通信主体の特定を困難にするためには、中継ノードを多数用意し、その中から使用する中継ノードをランダムに選択する中継方法が有効である。また、中継ノードを利用して通信パケットのあて先を秘匿できた場合でも、選ばれた中継ノード前後でパケットを見張られた場合、パケットの関連付けによって通信主体が特定される危険性がある。これを防ぐ為には、通信を行う２者と中継ノード間で異なる鍵で暗号化されたセッションを構築し、さらにセッションごとにパケット長をランダムに変えるなどの対策が必要になる。また、中継ノードを用いたシステムでは、中継ノードに対してパケット内容の機密性を守る為に、中継ノード前後のセッションの中を更に暗号化されたパケットを通し、二重のVPNを構築することにより中継ノードにおいても平文が見えないようにする必要がある。

以上の要件に基づき、匿名通信可能なオンデマンドVPN接続システムの一例を図２に示す。このシステムでは、匿名通信を管理する機関（匿名通信管理局）を設置し、匿名通信拠点登録情報の管理、中継ノード群の管理、セキュアルータへの匿名通信のネットワーク構築指示という３つの機能をオンラインで実行させる。これにより、煩雑な設定をユーザは意識することなく自動的にＶＰＮ接続を構築可能である。図２のシステムの接続処理の流れを以下に記す。

① 地点Aのセキュアルータ A２が匿名通信管理局に地点Bとの匿名通信開設要求（A２の署名付与）
② 匿名通信管理局において、A２の署名検証。地点Aと地点Bが匿名通信サービスを受けられるかを照合。中継ノードとしてCを選択
③ 匿名通信管理局がセキュアルータA１、B１、B２、Cと相互認証
④ 匿名通信管理局とVPN管理局で相互認証
⑤ 匿名通信管理局からVPN管理局にA１、A２、B１、B２、C匿名通信用SPD、ルーティングテーブル構成情報、パケット長ランダム化要請配信要求
⑥ VPN管理局がセキュアルータA１、A２、B１、B２、Cと相互認証
⑦ VPN管理局がセキュアルータA１、A２、B１、B２、Cに構成情報を配信
⑧ 匿名通信管理局からセキュアルータA１、B１にCのアドレスとオンデマンドVPN開設要求を送信
⑨ A１―C間でのオンデマンドVPN設立（A１－C間でのトンネル成立）

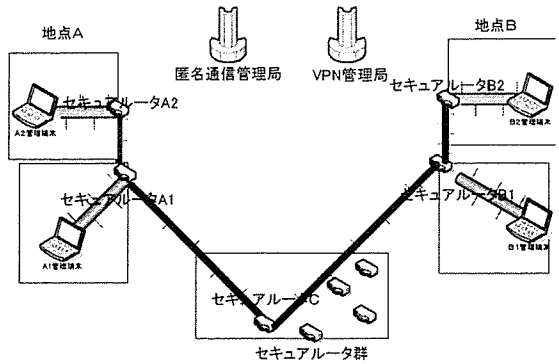

図２．匿名通信可能なオンデマンド VPN システムの実現例

⑩ C－B１間でのオンデマンドVPN設立（C－B１間でのトンネル成立）
⑪ A１、B１から匿名管理局にVPN開設完了通知
⑫ 匿名通信管理局からセキュアルータA２、B２にオンデマンドVPN開設要求
⑬ A２－B２間でオンデマンドVPN設立（A１－C間、C－B１間のトンネルを通す）

(4) 社会保障サービス全般への展開

医療情報交換のためのネットワーク基盤は、その他の公的なサービスに対しても同様の認証基盤が利用可能であり、ネットワーク基盤の普及を考えた場合、多くのサービスが利用できたほうが普及しやすいと考えられる。このように社会保障サービス全般に対して利用可能な認証基盤を構築するためには、一枚のICカードで様々なサービスを利用できるような仕組みや、様々なサービスで利用する個人情報をひとつのアプリケーションで管理できるような仕組みが必要になる。

このような要求に対しては、国民が自身の情報を一括管理するための電子私書箱の設置（図３）が有効である。電子私書箱には、本人を確認するための公的なICカードでログインし、情報の管理は個人が主体となって行う。この電子私書箱により、様々な情報が一元的に管理できるようになる。

D．考察

近年、様々な診療情報を医療施設や患者等の間でネットワークを介して電子的に交換・共有する試みが行われているが、個人情報保護のために専用回線等を通じ、あらかじめ固定された施設間における限定的な運用がなされていることが多い。しかしながら、

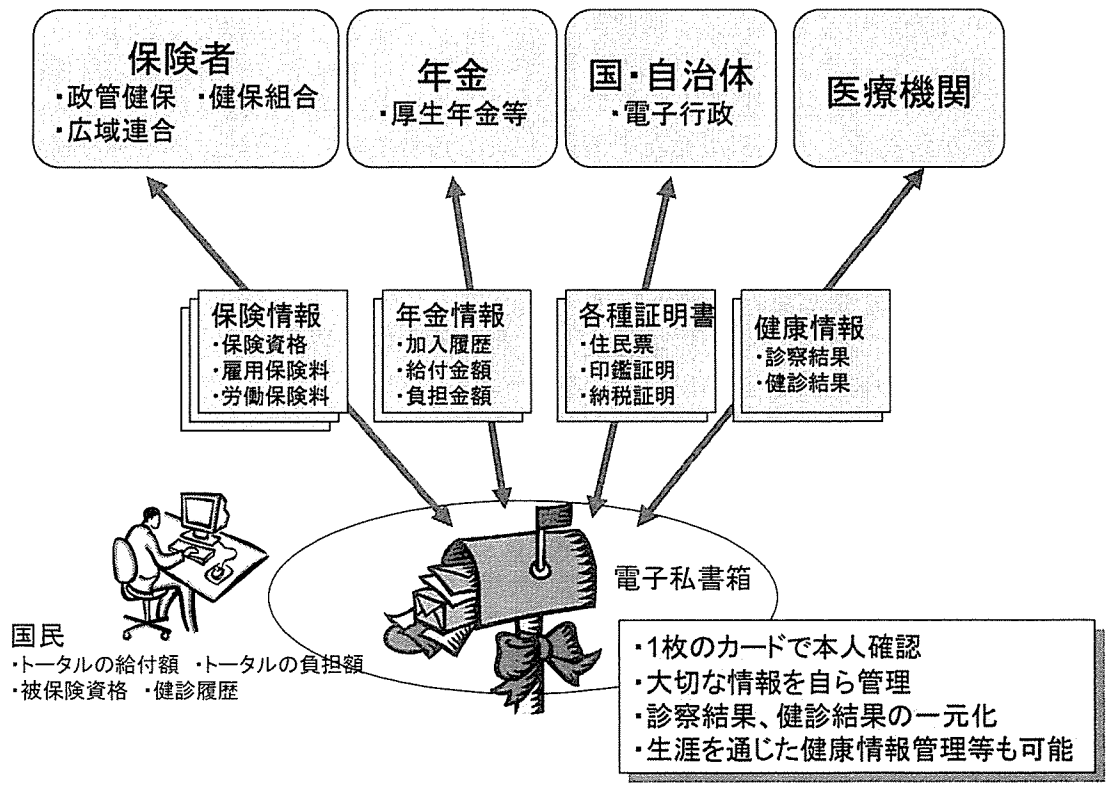

図３．様々な公的サービスの情報を一元的に管理する電子私書箱の概念

今後、更なる医療の高度化やそれに伴う機能分化の促進が想定され、このような状況下で患者主体の診療が実施されるためには、関連する施設等の間で、医療情報の伝送を安全かつダイナミックに行っていくためのネットワーク基盤が必要である。

また、医療情報の伝送を行う際には、電子署名法やe-文書法等などの新たな制度への対応や情報セキュリティの確保及び個人情報保護の実現を必須要件とし、医療施設におけるセキュリティ対策、ネットワーク上の安全な情報伝達、情報の真正性保証等を実現する保健・医療・福祉分野における共通的な技術的基盤を構築すべきである。ここで、オンデマンドVPNは、利用者や利用環境をネットワーク経由で迅速に確認し、複数の情報機器で動的にセキュアなネットワークを構築することができることから、医療分野における共通的なネットワーク基盤の候補として有効である。また、オンデマンドVPNを利用した機器等の認証機構とこれらを利用する医師等の認証機構を用いることで、医療施設に設置された情報機器を用いた医療従事者であることを保障した上で医療情報へのアクセスコントロールを実現できるため、保健医療福祉分野においては、オンデマンドVPNを利用したネットワーク化を促進することにより、医療にかかわる多くの機関が相互に情報交換可能な環境下で電子カルテに代表される医療情報の電子化を進めることが可能になり、個人情報保護を実現しつつ必要な情報の授受を実現する基盤が構築可能となると考えられる。例えば、患者が他の医療施設へ紹介される際の負担軽減や、医師が患者の診断・治療に関するアドバイスを他施設の専門医から得られる、他の医療機関を受診する際に過去の情報を参照して適切な治療に役立てるなど、患者や医療従事者に対する明確なメリットがもたらされるため、共通基盤の早期構築を進めることが望ましい。

さらに、今後はネットワーク基盤の整備とともに、それを活用した様々な保健医療福祉サービスの充実が求められており、ネットワーク基盤を利用した安全性、利便性、経済性などに優れた医療サービスの具体的検討が必要である。また、保険、年金等の他の公的なサービスを一元的に利用可能な仕組みについても検討を行っていく。

E．結論

本研究では、保健医療福祉分野の電子認証を実施する方策を検討し、実現に向けた課題を明らかにした。住基カードの配布、公的個人認証サービスの開始など、実施に向けた環境は整いつつある。近年、電子カルテによる医療機関連携の運用も進んでいることから、PKIに基づく個人および資格認証の仕組みを早急に確立することが望まれる。

本研究で得られた成果は、安全なネットワーク基盤を利用した保健医療福祉サービスの研究開発に活用される予定となっている。具体的には、保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアムや現在オンデマンドVPN技術の研究開発を行っている研究グループとの間で成果を共有することで、これら研究グループが進めている医療機関相互における情報連携の実証実験や医療サービスの検討等への反映や、オンデマンドVPNを構成する技術仕様へフィードバックすることを予定している。

さらに、ネットワーク基盤の整備だけでなく、それを活用した様々なサービスの拡充が求められており、今後、本研究で得られた成果を活用して、新たな保健医療福祉サービスに関する研究開発が行われることを期待する。

F．健康危険情報

該当なし

G．研究発表

1．論文発表

- 大山永昭：医療機関における個人情報保護とセキュリティシステム；日本病院会雑誌，53(10)，118-136(2006)

2．学会発表

- 小尾高史，鈴木裕之，谷内田益義，山口雅浩，大山永昭：多機能 IC チップを利用した任意多地点間 VPN のための鍵交換

手法；ワイヤレス・テクノロジーパーク 2006 講演予稿集，20-21(2006)
- 押田知己，谷内田益義，鈴木裕之，小尾高史，山口雅浩，大山永昭：多機能 IC チップを利用したネットワークサービスにおける暗号技術の更新とサービスの継続利用の実現；電子情報通信学会 2007 年総合大会講演予稿集，225(2007)
- 浦野雄平，小尾高史，大山永昭，谷内田益義，鈴木裕之：多機能 IC チップを利用した任意多地点間 VPN における通信主体情報の秘匿；電子情報通信学会 2007 年総合大会講演予稿集，230(2007)

厚生労働科学研究費補助金（医療安全・医療技術評価総合研究事業）
分担研究報告書
認証業務等提供事業者、医療機関における運用方法の検討
分担研究者　喜多紘一
東京工業大学　像情報工学研究施設　特任教授

研究要旨　保健医療分野における認証基盤のモデルを利用した、具体的なサービスへの応用の検討を行った。ヘルス情報共有のための４つの基盤のうちの、個人健康管理情報の蓄積・利用の基盤として、個人健康情報参照システムで健診情報を個人宛に配布し、ワインポイントサービスを行う電子私書箱構想を取り上げた。それを実現する為のネットワークとしてHPKI連携オンデマンドVPNが有効と考えられ評価した。評価方法としては厚生省から出されている「医療情報システム安全ガイドライン」の「外部と個人情報を含む医療情報を交換する場合の安全管理」の項目の最低限のガイドラインを用いた。その結果、オンデマンドVPNはインタネットを用いたオープンなネットワークで接続する場合に、オンラインサービス提供事業者が脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供する場合として、医療機関等の自己責任範囲が少なくなるメリットがある。また、HPKIと連携することにより医療機関と包括的に接続できる方式を実現することができる。

A．研究目的

分担研究として「認証業務等提供事業者、医療機関における運用方法の検討」を行う。本研究では、医療に関する施設の間で電子化された診療情報を交換又は共有する場合などに、安全な医療情報の流通を推進する際に必要となる、「保健医療福祉分野に適した公開鍵基盤の構築」及び、医療機関内外において個人情報・医療情報等の安全性を確保するために必要となる「様々な権限管理に対して公開鍵基盤を活用するための技術的方策」を明らかにすることを目的とする。平成18年度は、保健医療分野における認証基盤のモデルを確立した上で、具体的なサービスへの応用の検討を行う。

１．　ヘルス情報共有のための４つの基盤

ヘルス情報共有の基盤は図１で示すように４つの観点がある。第一は脳卒中のように地域連携クリニカルパスによって専門医を順次転院する場合に情報を移転していき、専門医が連携をとる為に適したデータベースである。急性期の緊急措置と専門的な治療、回復期のリハビリを経て家庭にもどり、かかりつけ医によるフォローアップとの連携をとるのにそれぞれのパスで便利なデータベースが構築される必要がある。第二はかかりつけ医が患者個人の全体像を把握し、自分の手に余るときは適当な医師へ紹介し、日常の健康状態のフォローアップを行うのに適したものである。第三は行政や研究などの蓄積されたデータの処理に用いられるデータベースで匿名化したり、統計を取りやすくするための工夫が必要である。最後の４番目は個人が情報を自己管理しやすく、個人ごとにまとまって生涯にわたり健康情報を保管できるデータベースである。これらが別々のデータベースになり、インプット時点から分かれるのか、同一データベースで出力や内部の管理スキームが異なるかはこれからの諸般の動きによるが、４つの利用方法があることには変わりがない。前の三つのデータベースはこれまでパイロット事業がいくつか行われてきた。第４番目の個人データの管理に関するシステムの構築についてはCD-Rデータを提供するシステムの検討が開始されているが、そのデータを個人がどのように管理するか、あるいはCD-R以外にデータの提供を受けるべきシステムについての検討がなされていない。

２．個人健康情報参照システムの電子私書箱構想

この為の一つのソリューションとして図２の電子私書箱を用いた個人健康情報情報参照システムが考えられる。

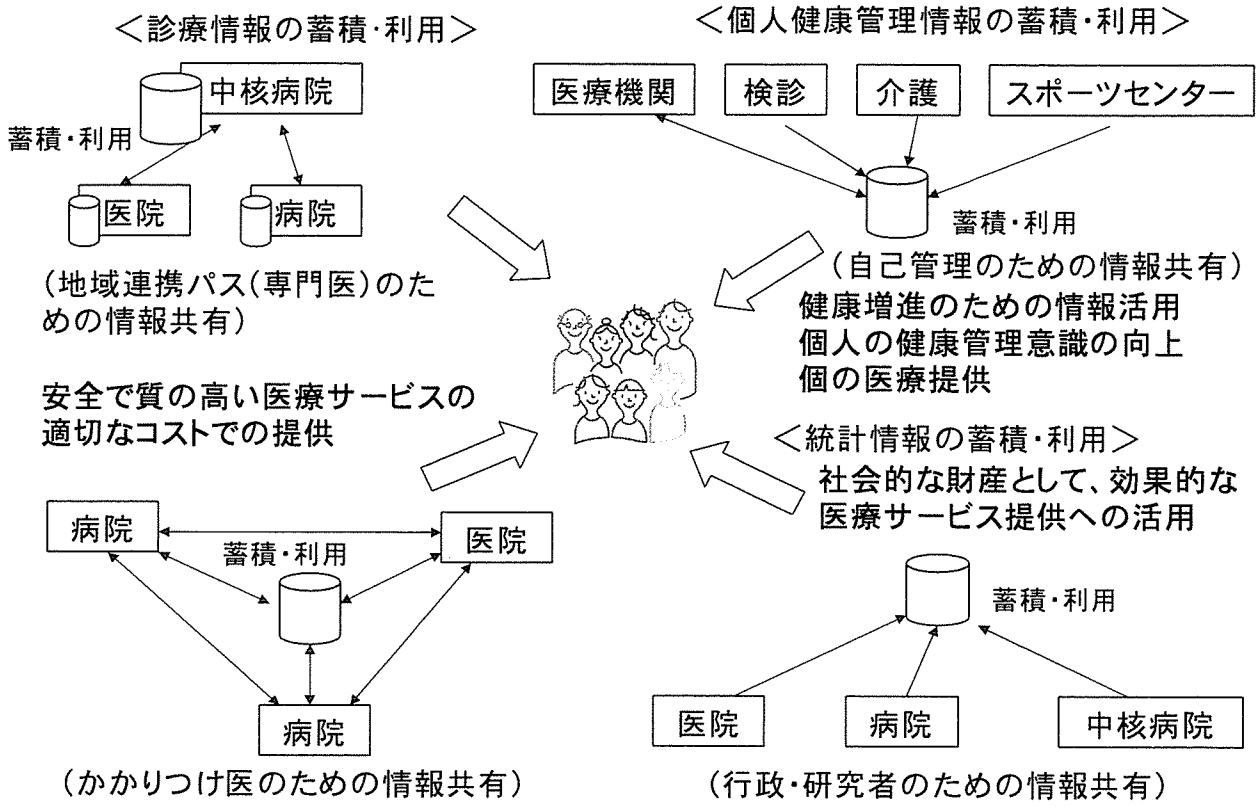

図1　ヘルス情報共有の為の4つの基盤

この考え方は2007年4月5日のIT戦略本部で決定されたIT新改革戦略の「政策パッケージ」[1],[2]や（社）日本経済団体連合会から出されている「社会保障制度のＩＣＴ化促進に関する提言－社会保障ＩＣＴ化の基本イメージについて－」[3]の中にまとめられている。

「政策パッケージ」の本文を抜粋すると以下である。「社会保障に関する国民個々の情報は、医療機関や保険者等、機関毎に個別管理されており、これらは自らの情報であるにも関わらず、本人が必要に応じて自由にアクセスし、利活用できる状態にはない。そこで、これらの情報を国民が自らのものとして簡単に収集管理可能な仕組み「電子私書箱（仮称）（電子情報アカウント）」を検討し、2010年頃のサービス開始を目指す。この電子私書箱が生活をサポートする重要なツールとして利活用される社会の実現を目指す。」となっている。実現の為の方策としては以下である。

「電子私書箱サービスのあり方（サービス主体者、将来像等）及び実施方法（安全に情報交換するための仕組み、データ形式、ガイドライン等）について、2007年度に内閣官房で産学官からなる検討会を立上げ、１年を目処に検討を行う。その結果を踏まえ、関連する制度整備等を行う。

さらに、電子私書箱の社会保障以外の分野（電子申請・民間サービス等）への利用拡大について検討を行う。」となっている。

例えば図２にこれを個人健康情報参照システムへ応用した例で説明する。現在、健診システムシステムの結果報告は現在紙で配布されているのが通常であるが、これを、オンラインで電子私書箱と呼ばれるサーバに送付する。このデータは親展扱いで、受診者の鍵で暗号化されている。受診者はこれを医師に見せたいものあるいは保管したいものを暗号化してビューボックスに保管する。保管したものを整理したり、関連する届出、処理や健康相談する場合にはコンセルジュに依頼をすることにより実行することができる。

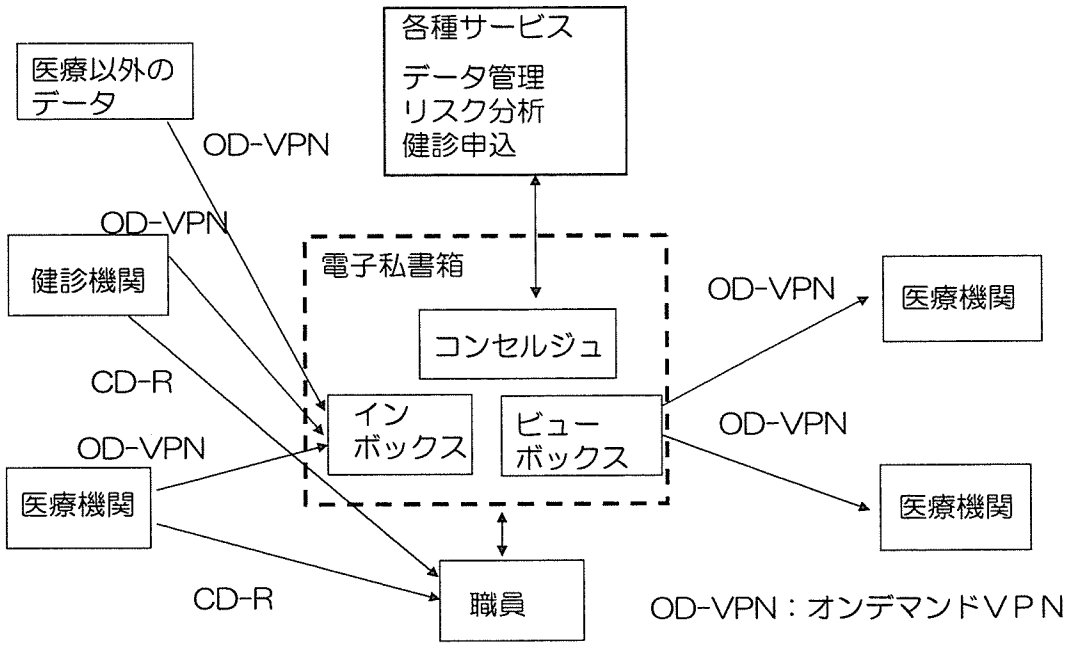

図2　個人健康情報参照システムの電子私書箱構想による実現

3．HPKI連携オンデマンドVPN

こうしたシステムを実現する場合のネットワークは電子私書箱からみると接続相手は固定ではなく、データを送り込んでくる施設および、データを見せる場合は複数となり、接続先を切り替える必要がある。また、アプリケーションソフトウエアをセキュアチャネル形成のために変更しないことが望まれる。

現状の医療分野のセキュアネットワークでは専用線、ＩＳＤＮもしくはＩＰ－ＶＰＮが用いられることが多い。インタネット上で安価に使用するために、インタネットＶＰＮが使用され始めている。

しかし、通常使用されているインタネットVPN仕様では1対1(Fixed VPN)の固定接続であり、パラメータもマニュアルで設定されて相手を切り替えるには手間がかかり、また、マニュアルなので瞬時に切り替えることはできない。

医療機関同士の通信ではN対Nで相手を自由に切換えられるＶＰＮが要求される。この要求を満たすものとしてオンデマンドＶＰＮが開発されてきている。通常のオンデマンドＶＰＮは、接続先をあらかじめ通話を許可した相手を相互に登録しておくか、都度、相手先を申請して相手側も同時に接続申請をした場合に接続を許可される方式となっている。緊急時に新しい接続を行うことは接続条件の成立に手間がかかり、間に合わない。

接続先の施設からあらかじめ「医療機関であれば接続を許可する」旨のポリシが登録されている場合には、接続先から新規接続申請者に対して、それぞれ接続したい旨の申請が個々になされていなくても、接続申請時に「医機関であること」がオンラインで確認できれば、医療機関との接続を許可すれば医療機関と包括的に接続できる方式を実現することができる。接続許可時、医療機関の管理責任者名および医療機関名の真正性が保証され、成りすましを防ぐことができる。

その上、こうした包括的なポリシを実現するネットワークは健診情報システム、遠隔医療システム、医療地域連携システム等の医療サービス提供者の施設が予め登録

できない場合に有効である。サービス提供者をあらかじめ登録する必要がないので、サービス提供者を自由に選択することができ患者の囲い込みを防ぎ、医療機関であることは確認されるので信頼できる医療ドメインを形成することができる。

そこで、本研究は接続先が医療機関であることが確認でき、且つN対Nで接続可能とし、さらに医療機関等の包括属性であれば接続するなどのポリシに従って接続を許可するＶＰＮを構築することを目的とする。[4]

B．研究方法

本研究ではN対Nで接続可能とするオンデマンドＶＰＮ方式にＨＰＫＩによる医療機関の認証を利用する方式を検討する。

オンデマンド VPN はセキュアチップによる 2 階層 PKI を利用してオンラインで接続相手先を容易に切り替える事ができる。オンデマンド VPN 方式の医療応用は HEASNT(保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム)を中心に普及活動が行われている。また、HPKI は厚生省が証明書ポリシ[5]を作成し、普及を進めている。

C. 研究結果

１．オンデマンドＶＰＮの特徴

１） IPSec による通信チャネルにより、成りすまし、改ざん、盗聴を防止（機器認証可能・機器所有者認証）

２） IP 層でセキュリティを保証するのでアプリケーションソフトウエアの変更が不要

３） 必要に応じてどの医療機関とも接続できるメッシュ型通信（１対１ではなくN対N通信）

４） 患者の来院に応じて接続できるオンデマンド通信（繋ぎっぱなしではなく、要求に応じた接続）

５） 複数地点で連携した遠隔診療を実現するマルチセッション通信（１本の回線で複数相手接続）

６） ＶＰＮの IPSec 接続に必要なパラメータや鍵交換が２階層ＰＫＩによりオンラインで設定可能

７） 接続ポリシがＶＰＮプロバイダーの定めた一律のポリシだけではなく、個々の加入者のポリシも加味可能。

２． ２階層ＰＫＩチップを用いたルータ

VPN 用パラメータをサービス提供者からダウンロードする為には、図 3 に示すセキュアチップ(多機能 IC チップあるいは e-Key チップともいう）を機器に組み込む。

１階層目の PKI は機器製造時にセキュアチップに組み込まれる。機器を所有した機関は、そのサービス提供者

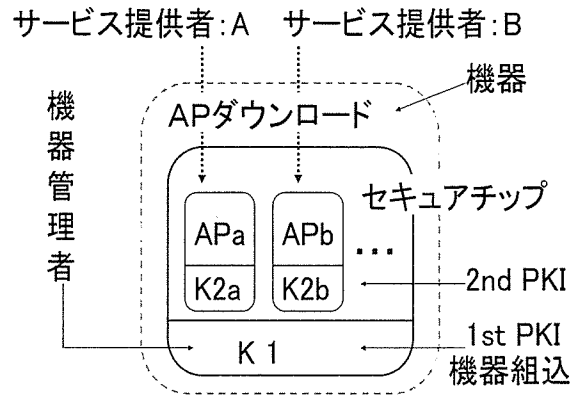

図3 セキュアチップ(e-Keyチップ)

に１階層 PKI を用いて所有者情報を登録するとともに必要なアプリケーションをダウンロードする。セキュアチップのアプリケーションはサービス提供者ごとに独立してダウンロードできる。オンデマンド VPN の場合は機器がルータとなり、オンデマンド VPN は一つのアプリケーションとなる。

３．HPKI（保健医療福祉分野 PKI）

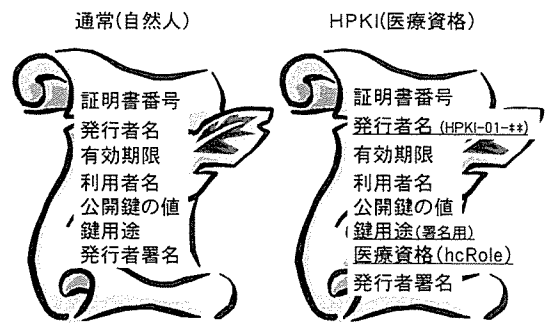

図4 HPKI(保健医療福祉分野PKI)

医療分野では記名押印にかわる電子署名としてHPKI の構築が厚生労働省を中心に進められている。図４に示すように公開鍵証明書内に医療関連の国家資格あるいは施設管理責任者情報を格納できるので、通常の PKI 証明書の

ような自然人の確認だけではなく国家資格保有者や施設管理責任者を確認することができる

4．　機器所有者登録

機器所有者登録は電話で言えば電話番号を入手することに当たる。ルータを所有した場合にはＰＣ購入時にユーザ登録をするように、１階層目のPKI（機器証明書）を用いてサービス提供者に対して所有者登録を行う。この際、所有者が医療機関の場合はその旨接続ポリシ登録として該当項目に記入するとともに、登録文書にHPKIで署名を行う。これによりサービス提供者は医療機関であることを確認することができる。この際、サービス提供者は機器管理者のルータ使用許可を得た後、２階層目の公開鍵証明書（接続証明書）等必要なアプリケーションをダウンロードさせる。

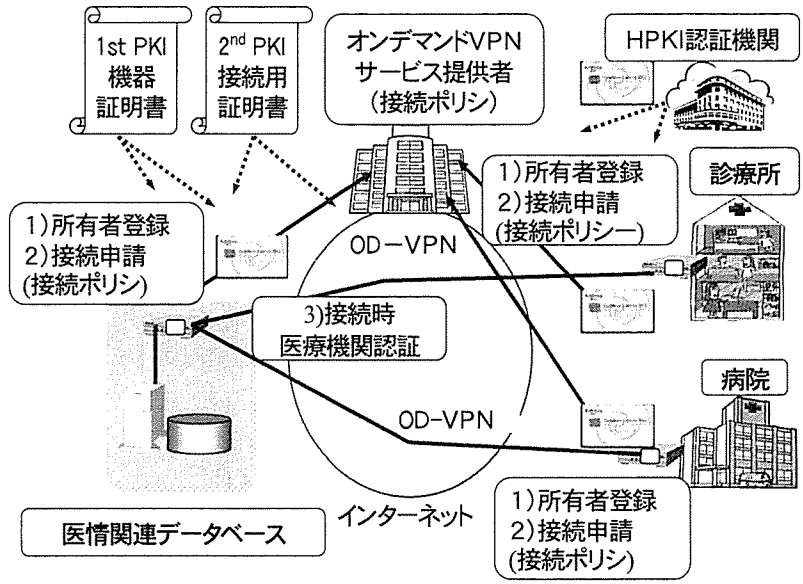

図5　HPKI連携オンデマンドVPN

5．接続許可申請

接続許可申請は電話の場合の相手の電話番号入手、あるいは相手への自分の電話番号の連絡にあたる。これは直接、接続相手先を相互に指定する方式と、医療機関なら接続を許可するというような包括的に接続先ポリシを設定する方式がある。後者の場合は個々の相手の接続情報を入手する必要がない。前者の場合は相手も自分のルータの接続許可申請をするまで設定条件のダウンロードを行えないが、後者の場合は相手側から医療機関であれば接続を許可する旨のポリシが出ていれば、直接こちらを指定した許可申請がなくても接続パラメータをダウンロードし、相手へはその旨を通知すれば良い。

6．通信の接続

通信を行うには通信目的に合った「ポリシ」と対応する「接続相手」を確認して接続する。例えば医療地域連携で「医療機関であること」を接続条件にする場合は、接続許可申請時のポリシ申請に従いHPKIによる医療機関としての所有者登録の出ているルータのみに接続可能とするように制御する。

以上の全体像をまとめると図５のようになる。

D．考察

１．医療情報システム安全ガイドラインの考え方

厚生労働省より発行された「医療情報システム安全管理ガイドラインン」の第２版がパブリックコメント段階が終了し、発行されようとしている。[6]

第２版では６章に「災害等の非常時の対応」の項が新たに追加され、６．１０項の「外部と個人情報を含む医療情報を交換する場合の安全管理」が充実された。6.10では「考え方」として、以下の項目に分けて説明されている。

B 考え方

B-1．責任分界点の明確化

B-2．医療機関等における留意事項

①「盗聴」の危険性に対する対応

②「改ざん」の危険性への対応

③「なりすまし」の危険性への対応

B-3．選択すべきネットワークのセキュリティの考え方

Ⅰ．クローズドなネットワークで接続する場合

①専用線で接続されている場合

②公衆網で接続されている場合

③閉域IP通信網で接続されている場合

Ⅱ．オープンなネットワークで接続されている場合

B-1の責任分解点の明確化では、個人情報保護法上、委託と第三者提供の２種類があることを述べている。また、「オンラインで情報を提供する場合、情報主体である患者と情報が乖離する。患者と乖離している間は情報を取り扱う事業者のどれかが責任を負う必要があり、どの事業者が責任を負っているかが明確で誤解のないものでなければならない。」とも述べている。可用性や機密性の責任、リモートログインの責任なども述べられている。

B-2では医療機関等における留意事項として、情報を送信しようとする場合、「盗聴」、「改ざん」、「成りすまし」に対して、その情報を適切に保護する責任が発生することを述べている。

B-3では医療機関が選択するネットワークの観点で回線事業者がネットワークとして「セキュリティを担保する場合」と「担保しない場合」の２つに分けて考えている。

1）回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保する場合：
回線事業者とオンラインサービス提供事業者が提供するネットワークサービスの内、これらの事業者がネットワーク上のセキュリティを担保した形で提供するネットワーク接続形態であり、多くは後述するクローズドなネットワーク接続である。また、現在はオープンなネットワーク接続であっても、Internet-VPNサービスのような通信経路が暗号化されたネットワークとして通信事業者が提供するサービスも存在する。

このようなネットワークの場合、通信経路上におけるセキュリティに対して医療機関等は最終的な結果責任を負うにせよ、管理責任の大部分をこれらの事業者に委託できる。もちろん自らの医療機関等においては、善良なる管理者として注意義務を払い、組織的・物理的・技術的・人的安全管理等の規程に則り自医療機関等のシステムの安全管理を確認しなくてはならない。

2）回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保しない場合：

例えば、インタネットを用いて医療機関等同士が同意の上、ネットワーク接続機器を導入して双方を接続する方式が考えられる。この場合、ネットワーク上のセキュリティに対して回線事業者とオンラインサービス提供事業者は責任を負わない。そのため、上述の安全管理に加え、導入されたネットワーク接続機器の適切な管理、通信経路の適切な暗号化等の対策を施さなくてはならず、ネットワークに対する正確な知識のない者が安易にネットワークを構築し、医療情報等を脅威にさらさないように万全の対策を実施する必要がある。
今回のガイドラインの改訂では「外部と個人情報を含む医療情報を交換する場合の安全管理」において使用できるネットワークとして、セキュリティ担保の観点から以下の５通りに分類してガイドラインを示したのでわかりやすくなっている。

1）クローズドなネットワークで接続する場合
① 専用線で接続されている場合，
② 公衆網で接続されている場合，
③ 閉域IP通信網で接続されている場合、
2）オープンなネットワークで接続する場合
① 回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供する場合
② 医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合

つまり今まで明確ではなかった、オープンなネットワークで接続される場合、即ちインタネット接続の使用に対してB-3で一定の考え方を示したことは有意義である。以下に詳細に引用する。

「B-3の冒頭で述べたように、オープンなネットワークで接続する場合であっても、回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供することもある。医療機関等がこのようなサービスを利用する場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できる。そのため、契約等で管理責任の分界点を明確にした上で利用することも可能である。

一方で、医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合は、管理責任のほとんどは医療機関等に委ねられるため、

医療機関等の自己責任において導入する必要がある。また、技術的な安全性について自らの責任において担保しなくてはならないことを意味し、その点に留意する必要がある。」

オンデマンドVPNは前者の「回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供」に当たる。

2．患者等に診療情報等を提供する場合

診療情報等の開示が進む中、ネットワークを介して患者（または家族等）に診療情報等を提供する、もしくは医療機関内の診療情報等を閲覧する可能性も出てきた。その為にガイドラインでは、その際の考え方について触れている。以下にガイドラインを少し整理しなおすと以下のようになる。

患者等に情報を提供する場合には、以下の注意が必要である。

1）ネットワークのセキュリティ対策

2）医療機関等内部の情報システムのセキュリティ対策

3）情報の主体者となる患者等へ危険性や提供目的の納得できる説明

4）非ITに係わる各種の法的根拠等も含めた幅広い対策を立てること

5）それぞれの責任を明確にした上で実施すること。

その理由としては

1）情報を閲覧する患者等のセキュリティ知識と環境に大きな差がある。

2）一旦情報を提供すれば、その責任の所在は医療機関等ではなく、患者等にも発生する。

3）医療機関等が患者等の納得が行くまで十分に危険性を説明し、その提供の目的を明確にする責任があり、説明が不足している中で万が一情報漏洩等の事故が起きた場合は、その責任を逃れることはできない。

4）オープンネットワークを介する場合、盗聴等の危険性は極めて高く、かつ、その危険を回避する術を患者等に付託することも難しい。

オープンネットワーク接続であるため利活用と安全面両者を考慮したセキュリティ対策が必須である。

5）患者等に情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けしておく必要がある。

6）そのため、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いる必要がある。

3．最低限のガイドライン

以上の考え方に基づき最低限のガイドラインが示ささされている。

1）ネットワーク経路でのメッセージ挿入、ウイルス混入などの改ざんを防止する対策をとること。
施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策をとること。
セッション乗っ取り、IPアドレス詐称などのなりすましを防止する対策をとること。
上記を満たす対策として、例えばIPSecとIKEを利用することによりセキュアな通信路を確保することがあげられる。

2）データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用規程により、採用する認証手段を決めること。認証手段としてはPKIによる認証、Kerberosのような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワードなどの容易に解読されない方法を用いるのが望ましい。

3）施設内において、正規利用者への成りすまし、許可機器への成りすましを防ぐ対策をとること。これに関しては、医療情報の安全管理に関するガイドライン「6.5技術的安全対策」で包括的に述べているので、それを参照すること。

4）ルータなどのネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶVPNの間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408で規定されるセキュリティターゲットもしくは

それに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。

5）送信元と相手先の当事者間で当該情報そのものに対する暗号化などのセキュリティ対策を実施すること。たとえば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化などの対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。

6）医療機関間の情報通信には、当該医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社など多くの組織が関連する。
そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。

・診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に係わる操作を開始する動作の決定
・送信元の医療機関等がネットワークに接続できない場合の対処
・送信先の医療機関等がネットワークに接続できなかった場合の対処
・ネットワークの経路途中が不通または著しい遅延の場合の対処
・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処
・伝送情報の暗号化に不具合があった場合の対処
・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処
・障害が起こった場合に障害部位を切り分ける責任
・送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対処

また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。

・通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。
・患者等に対する説明責任の明確化。
・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。
・交換した医療情報等に対する結果責任の明確化。
個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。

7）リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること。
また、メンテナンス自体は「6.8章　情報システムの改造と保守」を参照すること。

8）回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。
また上記1および4を満たしていることを確認すること。

4．ＨＰＫＩ連携オンデマンド VPN のガイドラインによる評価
1）ネットワーク経路での改ざん防止・盗聴防止・成りすまし防止：
IPSec, IKE による VPN の使用。一般のインタネットとコンテンツとは遮断しているので要求を満足している。
2）データ送信元と送信先での相手の確認
ルータ間でオンデマンド VPN サービス提供者が相手先を確認し、保証しているので要求を満足している。
3）施設内での正規利用者への成りすまし防止
ルータに接続される端末の技術的安全対策によるので、オンデマンド VPN の対象範囲外であるが、オプションとしてルータで本人確認機能も追加可能であり、これを利用する方法もある。施設内の運用規定による。
4）安全が確認できる機器の使用、および施設内のルータ経由接続の遮断
オンデマンド VPN 機器は各社の適合性を公開することにしているので要求を満たしている。また、ルータで経由接続できないことを条件にしているので要求を満たしている。

5）送信元と相手先の当事者間で当該情報そのものに対する暗号化などのセキュリティ対策を実施すること。
オンデマンド VPN は暗号化されているので要求を満たしている。さらに個人健康管理情報参照システムではＳＳＬを用いるのでクライアント・サーバ間も暗号化されている。
6）関連組織の責任分解点・責任の所在を契約書で明確にすること。
オンデマンド VPN ではルータの設定を含め、オンデマンド VPN サービス提供者にあるので、明確になりやすいので要求を満たすことが比較的容易いに実現できる。
7）リモートメンテナンス適切な管理
ルータ自体のリモートメンテナンスは各社仕様によるが、オンデマンド VPN をリモートメンテナンスのネットワークとして利用するとアクセスポイントの設定やアクセス権限管理がやりやすくなる。
8）業者に対する脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないかの確認。
オンデマンド VPN サービスは脅威分析や回線の可用性への考え方は明確なので確認が容易である。

以上を総合すると「オープンなネットワークで接続されている場合」にオンデマンドVPNは安全ガイドラインを満足しやすいネットワークといえる。

5．その他のオンデマンドVPNへの要求事項

HPKI認証局による国家資格付および管理責任者の公開鍵証明書の内容が相手側に伝わり、有効な公開鍵証明書であることが検証できる必要がある。

このためにVPNサービス提供者はそのような検証手段とGUIを提供する必要がある。また、期待しているポリシーによるVPNサービスかどうかはVPN提供者およびVPNモードの確認を行う必要がある。

医療機関の運用としてはこうした確認を行う必要がある。又、提案したVPNはセキュアなチャンネルを作るだけなので、患者の同意の確認や、アクセスポリシーに基づいたエマージェンシー時、主治医団、一般医療スタッフおよび事務関係者によるアクセス管理の区別はそれぞれの医療機関で別途行う必要がある。

データを共有する場合のRepositoryとしてのデータベース、そこの登録内容を管理するRegistryやID管理は別途必要である。こうしたエンティティの管理はそのドメインでの共通、もしくは個人による管理があり、暗号化やアクセス方法等、そのシステム設計はこれからの課題である。

こうしたエンティティに対する公開鍵証明書の発行は実在性や責任の所在を示す為に必要である。

E．結論

1．オンデマンド VPN の「医療情報システム安全管理ガイドライン」への適合性

オンデマンド VPN はインタネット上で「回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供」するネットワークに当たる。

オンデマンド VPN はインタネット上で使用可能で「医療情報システム安全管理ガイドライン」にそって評価すると医療機関側の責任が比較的少なく、それに適合させることのできるネットワークである。

2．HPKI 連携によるオンデマンド VPN

HPKI と連携することにより医療機関と包括的に接続できる方式を実現することができる。

3．HPKI 連携によるオンデマンド VPN の手順のまとめ

オンデマンド VPN 機器所有者はオンデマンド VPN サービス提供者へルータの機器所有者登録を行う。この時、オンデマンド VPN サービス提供者はルータのセキュアチップ機能を利用し１階層目の PKI によりルータがオンデマンド VPN として正当なものかどうかの機器認証を行うとともに利用者としての正当性を認証する。

接続を行うときは接続先の認証パラメータをオンデマンド VPN サービス提供者へ接続許可申請を行う。接続ポリシに合わせてオンデマンド VPN サービス提供者はルータの２階層目の接続用のパラメータをオンラインでダウンロードし、設定ささせる。
このとき、機器所有者登録時に HPKI で管理された証明書を使用して署名を行った登録申請書を提出することにより VPN サービス提供者は接続許可申請者が医療機関を認証することができる。接続先が、それにより接続を許可

するポリシであれば、それに従ってオンデマンドVPNサービス提供者が接続パラメータをダウンロードすることにより医療ドメインを形成することができる。

通信を開始する場合は接続許可された接続先を選択するすることにより通信を開始することができる。接続先のHPKIの証明書に記述された、hcRoleやＤＮ等を接続元で参照可能にすることで先が医療機関であることを接続元でも検証することができる。

通信相手を変える場合は、すでに許可された接続先を選択するか、まだ許可されていない場合は新たに許可申請を行い、許可後選択すればよい。そのときのパラメータはオンラインでダウンロードすれば良いのでＮ：ＮのＶＰＮ接続がリアルタイムで可能となる。申請書には接続可能な相手先を個別指定又は属性による包括指定を行う。接続相手の公開鍵証明書等のパラメータはあらかじめ接続相手から入手するか、Directory から入手する

４．オンデアデマンドVPNサービス提供の機能

１）機器証明書とルータ開設申請書と結びけたものにより、そのルータノードをユニークにする為の管理体制。(機器を購入した場合の機器登録と同様の機能)

２）VPNサービスセンターの機能として機器所有者登録、接続許可申請、通信開始要求、接続拒否機能、強制切断要求および接続監視機能が必要である。

３）多機能ICチップが安全なチップであることを認定する機関あるいはルータのメーカが自己責任で認定する必要がある。

４）ルータメーカは１階層目の機器証明書を入手して秘密鍵とともにルータに組み込む。この時の認証局は製造メーカとVPNサービスセンターがその正当性を検証できる必要がある。

機器証明書は多機能ICチップのセキュアルータや機器等への用途を証明するもので、その認証局はメーカとの間で、私有鍵の発生と公開鍵の認証局への送付手段を取り決める。

５）セキュアネットワーク以外にRepository、Registry、ID管理およびDirectoryが必要である。これらのエンティティの安全管理に対してもセキュアネットワークは有効で、そのための秘密鍵と公開鍵証明書が必要となる。

Ｆ．参考文献

[1] IT新改革戦略 政策パッケージ, IT戦略本部, 2007,)
http://www.kantei.go.jp/jp/singi/it2/dai40/40siryou7.pdf
[2] “IT新戦略 政策パッケージの概要について”, IT戦略本部, 2007
http://www.kantei.go.jp/jp/singi/it2/dai40/40siryou6.pdf
[3] “社会保障制度のＩＣＴ化促進に関する提言ー社会保障ＩＣＴ化の基本イメージについてー”, (社) 日本経済団体連合会, 2007
[4] 喜多 紘一, セキュアネットワークとして医療ドメインを形成するオンデマンドＶＰＮについての研究, 第26回医療情報学連合大会, P3-3, 2006
[5] “保健医療福祉分野PKI認証局　証明書ポリシ V1.1”, 厚生労働省, 2006
http://www.mhlw.go.jp/shingi/2006/03/dl/s0330-8a.pdf
[6] “医療情報システム安全管理ガイドラインン　第２版”, 厚生労働省, (2007)

平成１８年度　厚生科学研究報告書

薬務関連における個人情報管理の実施方策の調査・検討

分担研究者　土屋　文人（東京医科歯科大学歯学部附属病院薬剤部）

（研究要旨）　薬務関連における個人情報管理について、医療安全の面からも問題とされている入院患者の持参薬及び平成18年度の診療報酬改訂によって後発医薬品使用推進策として実施された処方せんにおける後発医薬品への変更に関する問題の２つを対象に調査・検討を行った。その結果、両者とも現行の病院情報システムでは容易に扱うことができず、患者個人に使用された医薬品に関する情報管理に大きな問題が存在することが確認された。また、今後の対応としては病院情報システムの構造改善と標準医薬品コードの機能増強が重要であることが示唆された。

A　研究目的

処方せんの電子化に関する問題をはじめ、患者が使用している医薬品等に関する情報については様々な問題が存在している。しかしながら医療安全の観点から、これらの情報の電子化が進展しないことは大きな障害となる。平成19年4月実施の改正医療法では、医薬品の安全管理の体制として、医療機関と薬局等の情報共有の重要性が指摘されている。そこで本研究においては、①入院時に患者が持参する医薬品、あるいは退院時に患者に持参させる医薬品（以下持参薬という）の情報管理に関する諸問題、②平成 18 年度の診療報酬改訂によって後発医薬品使用推進策として実施された処方せんにおける後発医薬品への変更に関する情報管理上の問題、の 2 点についてその実情を調査すると共に、医療安全の観点から患者の薬歴情報管理のあり方について検討を行う。

B　研究方法

（1）　持参薬に関する情報管理に関する諸問題

持参薬に関しては以前から存在していたが、その使用が限られていたため、大きな問題とはならずに経緯してきたが、DPC の導入により、大学病院等においても持参薬を使用する事例が増加したこと、及びら平成 17 年に発生したリウマトレックスに関連した医療事故により大きな問題として認識されることとなった。これらは基本的には医療機関間、あるいは医療機関と薬局間の情報伝達が正確に行われていないこと及び、現行の病院情報システムが想定していなかったことも相俟って問題となっている。そこで本研究においては患者にしようされる医薬品の情報管理の観点から、持参薬に関する問題の背景及び現状を調査する。

（2）後発医薬品に関する情報管理に関する諸問題

平成18年度の診療報酬改訂により、後発