② 不正なエンティティ（機器及び人）による進入
③ 成りすまし
●LAN 上の脅威
④ 許可されていない機器からのアクセス
⑤ 機器の成りすまし
⑥ 許可されていない接続先（機器）への接続
⑦ 不正な利用者の利用

OD-VPN を前提とした対策は、以下を考えることができる。カッコ内は、対応する脅威を示す。前提として、ルータには、それぞれの機関を認証するための鍵と証明書が格納されているものとする。
A) 医療機関に設置されたルータ間の相互認証(②、③)
B) OD-VPN 提供者によるルータ間認証のための鍵配送（②、③、⑥）
C) IKE＋IPSec（ESP トンネルモード）による保護（①）
D)登録された機器以外でのルータ利用の OD-VPN 接続禁止（②、④、⑤、⑥）
E)正当な機器（ルータ）の OD-VPN 提供者への登録（②、④）

OSI のネットワークモデルでのネットワーク層よりも上位のアプリケーション層、つまり接続サービスあるいは特定のアプリケーションで提供する機能での対策は以下を考えることができる。
F)利用者認証（⑦）
G)セキュリティ属性を付加したアクセス制御(⑦)
H)データレベルでの暗号化（⑦）

４．２　分散ＤＢモデル
基本的には、２地点間の安全性が確保されれば十分である。利用者が医療従事者に限定されるので、OD-VPN 利用者の認証が必須となる。

４．３　集中ＤＢモデル
基本的には、２地点間の安全性が確保されれば十分である。利用者が医療従事者に限定されるので、利用者の認証が必須となる。

４．４　分散モデル
基本的には、２地点間の安全性が確保されれば十分である。

４．５　Ｎ対Ｍモデル
基本的には、２地点間の安全性が確保されれば十分である。利用者ではなく、サービスの認証による代替の可能性がある。

４．６　中継モデル
中継モデルの場合には、基本的な構成に加えて、接続を中継する機関が介在する。そのため、機関 A と機関 B の間のネットワークレベルの接続は切れてしまうため、広義の接続サービスでの安全性を確保する必要がある。

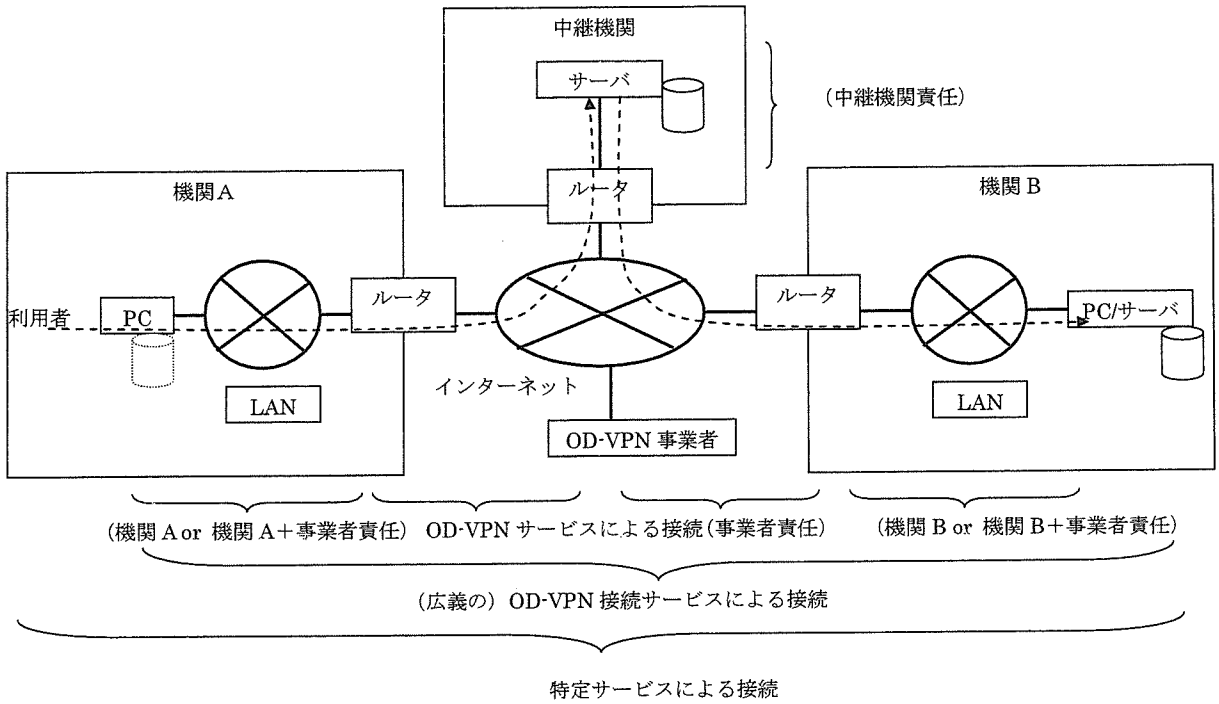

図７　OD-VPN を利用した中継モデルの構成

基本的な構成の脅威に加えて、中継期間内での脅威と対策を検討する必要がある。
●中継機関の脅威
⑧ 許可されていない機器からのアクセス
⑨ 機器の成りすまし
⑩ 許可されていない接続先（機器）への接続
⑪ 不正な利用者の利用
⑫ 悪意を持った操作者による盗聴・改ざん・すり替え

これらの脅威に対しては、
A) 医療機関及び中継機関に設置されたルータ間の相互認証(②、③、⑧、⑨、⑩)
B) OD-VPN 提供者によるルータ間認証のための鍵配送(②、③、⑥、⑧、⑨、⑩)
C) IKE＋IPSec（ESP トンネルモード）による保護（①)
D)登録された機器以外でのルータ利用の OD-VPN 接続禁止(②、③、④、⑤、⑥、⑧、⑨、⑩)
E)正当な機器（ルータ）の OD-VPN 提供者への登録(②、④、⑧、⑨、⑩)
F)利用者認証（⑦)
H)データレベルでの暗号化（⑦、⑫)
となり、通信系路上のデータをアプリケーション（サービス）レベルで暗号化する必要がある。

４．７　OD-VPN サービスと他の接続サービスとの比較

専用線、ISDN、IP-VPN などを利用した場合には、OD-VP`N サービスで提供する２点間の接

続部分がそれぞれのサービスに置き換わった関係となる。

1）専用線

通信事業者によって、2 点間の通信の安全性と接続性、帯域（接続スピード）、接続ルートが保障された常時接続の接続方法である。最近では、2 点間の通信だけでなく、複数の地点を結ぶサービスや、障害を回避するために二重に回線を用意するサービス等も展開されている。これらの 2 点あるいは複数地点を結ぶ回線は、他の回線と論理的に分離し独立した回線で結ぶ通信であることは確かであるが、完全に物理的に独立した回線であるのか否かは必ずしも明確ではない。例えば、大容量の光伝送などは、1 本のファイバーの中に、周波数帯を分離したり時間を分割するなどの方法によって多くのチャネルを設けて大容量化を実現している。この場合には、物理的には 1 本のケーブルであるが、論理的には複数のチャネルの通信を実現することが可能となっている。

専用線の場合、安全性に関しては事業者が責任を持つので、DSU を結ぶ 2 点間の間での第三者による盗聴・改ざん・すり替えなどの危険性は無い。しかし、悪意を持った通信事業者の内部操作者による盗聴・改ざん・すり替えなどの危険性は残る。固定した地点間を結ぶ方法としては、最も安全性の高い接続サービスであるといえる。但し、他の地点との接続ができないという柔軟性に欠けることと、一般的には他の接続方法と比較してコストがかかるといわれている。

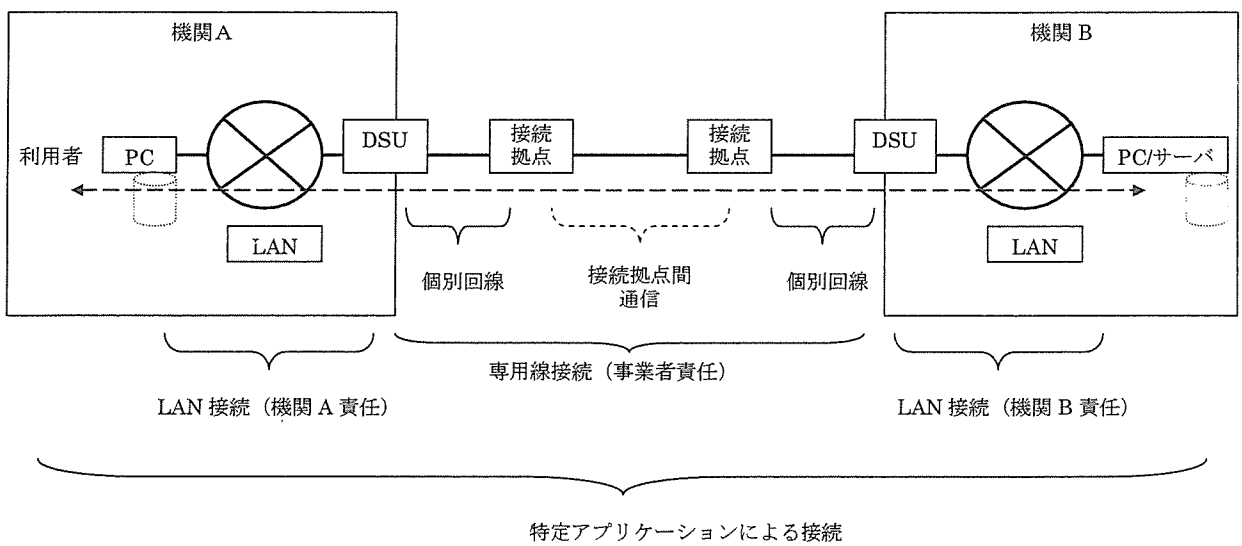

図８　専用線を利用した接続構成

専用線を利用した場合、以下の脅威が想定される。

●専用線上の脅威

⑬ 悪意を持った関係者による盗聴・改ざん・すり替え

これに対する対応としては、

G)データレベルでの暗号化（⑬）

で対策とすることができる。

2）ISDN

任意の２地点を、接続要求に応じてディジタル公衆回線網を利用して接続する方法で、2 点間の通信を通信事業者が保障する接続方法となる。第三者による盗聴・改ざん・すり替えなどの危険性は無いが、悪意を持った通信事業者の内部操作者による盗聴・改ざん・すり替えなどの危険性は残る。正しい相手を指定したときの接続性、帯域（一般には狭い）は事業者によって保証されている。そのため、脅威・対策に関しては、専用線と同じになる。但し、利用者の誤使用による誤った接続先との接続などには注意する必要がある。

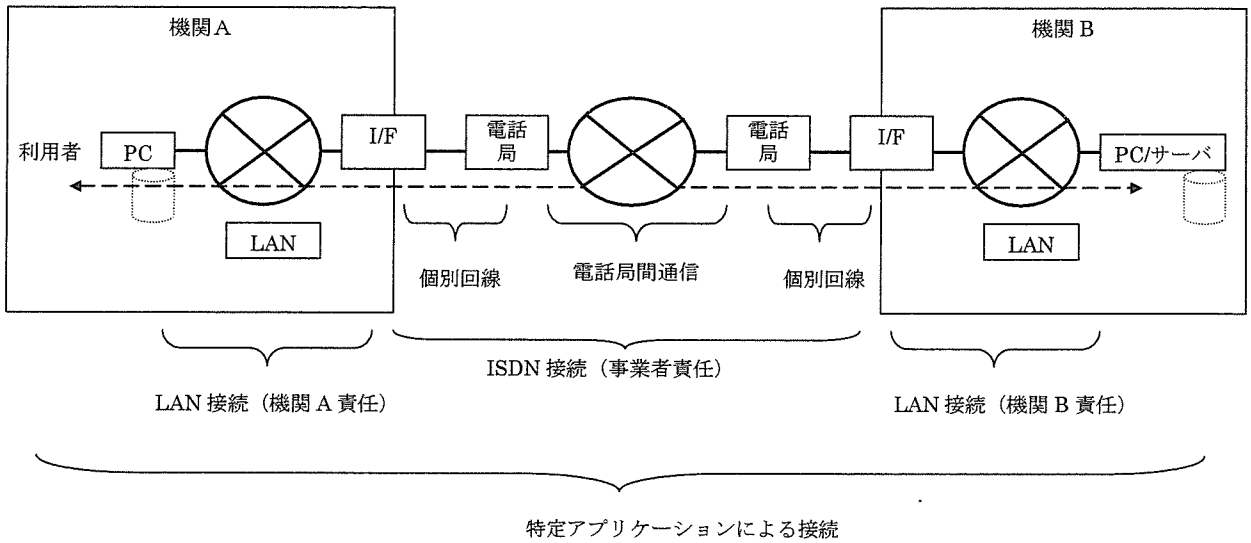

図９　ISDN を利用した接続構成

3）IP-VPN

通信事業者が提供する通信網、あるいはインターネットを利用した IP 通信網の上に、複数の拠点間の通信だけが可能なクローズド名ネットワークを構築する方法である。常時接続の可能な接続方法であり、オープンなネットワーク上に接続する拠点を認証するため鍵情報を共有することとなる。インターネット等オープンなネットワークを利用するので、基本的な脅威・対策は、OD-VPN と同じとなる。一般には通信コストは下がるが、帯域などが保障された接続ではない。また、インターネットの接続は、インターネットサービスの提供者が責任を持つが、鍵の管理などは、設置者あるいは事業提供者が責任を持って設定・管理するのが一般的である。

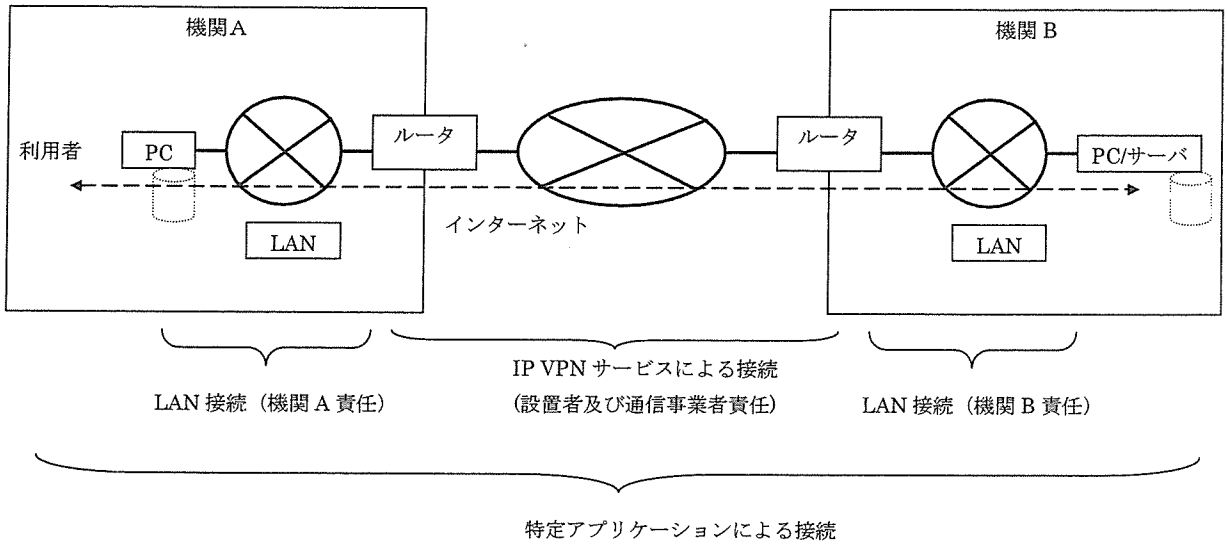

図 11　IP-VPN 接続を利用した接続構成

4）参考：NGN

将来の通信網といわれているＮＧＮは、音声や情報をディジタル回線によって結ぶ一定の品質と安全性を保証した IPv6 回線網である。基本的には ISDN と同じ構成となり、脅威、対策も同じとなる。2 点間の接続だけでなく、サービスレベルでの接続も想定されているので、将来はより安全性の高いサービスが提供される可能性もある。

６．考察

６．１　オンデマンド VPN の有効性評価

医療分野で想定される典型的と考えられるユースケースに基づいたモデル検討の結果、様々な接続形態の基本は２点間の通信であり、その安全性確保が重要な一項目であると。その理由は、医療施設間を結んだ情報流通の中で、主体となるべき医療機関の責任範囲が及ばない部分であり、医療機関の運用等で脅威に対抗する対処が打てないからである。

２点間の接続形態としては、例示した、OD-VPN、専用線、ISDN、IP-VPN、等様々な可能性があるが、機能的には等価な２点間の接続方式と考えられる。但し、安全性を確保するための技術的対策、責任を持つ主体が異なるので、利用者は、コスト・安全性の程度などを考慮し選択する必要がある。機能、責任の範囲の違いを次の表に示す。

	OD-VPN	専用線	ISDN	IP-VPN
成りすまし防止	OD-VPN 事業者が提供する認証基盤によって２点間の認証を行うことによって対策する。	通信事業者が負い、特定の２点間の通信だけを成立させるので、脅威とならない。	通信事業者が負い、特定の２点間の通信だけを成立させるので、脅威とならない。（番号違いなど、利用者の誤使用	設置期間の管理者、あるいはサービス提供者が設定した認証鍵による認証によって対策する。

			による誤った接続を防ぐ対策は必要)	
盗聴防止	IPSec＋IKE によって保護。暗号の安全性に依存する。 通信上は、事業関係者も第三者も同等に対策される。	第三者の盗聴はない。悪意を持った事業関係者に対する盗聴には、流通する情報の暗号化などの対策で対応可能。	第三者の盗聴はない。悪意を持った関係者に対する盗聴には、流通する情報の暗号化などの対策で対応可能。	IPSec＋IKE によって保護。暗号の安全性に依存する。 通信上は、事業関係者も第三者も同等に対策される。
改ざん防止	IPSec+IKE	通信事業者が保証する	通信事業者が保証する	IPSec+IKE
責任	2 点間を結ぶ通信の安全性は、通信事業者（2点間の接続性）と、OD-VPN 事業者（通信の安全性）が負う	通信事業者が負う	通信事業者が負う	通信事業者（2点間の接続性）と設置者（通信の安全性）が負う
その他	サービスの提供を受ける任意2地点間の接続が可能。 オープンなネットワークを利用するので、帯域（スピード）は保証されない。	固定の2地点（多地点）の接続のみ可能 安全性、帯域、接続先は事業者が保証	サービスの提供を受ける任意2地点間の接続が可能。 安全性、帯域（広くはない）、接続先は事業者が保証	固定の多地点の接続可能 オープンなネットワーク上にクローズなネットワークを構築するので、帯域などは保証されない。

6．2　中継モデルの評価

中継機関が介在する場合には、医療機関の責任の範囲外となる中継点での情報の保護が重要な課題となる。そのためには、ネットワークレベルでなく、上位のアプリケーションレベルで流通する情報を暗号化し、中継機関の関係者に対しても情報の機密性を保障する必要がある。

7．結論

これまで、医療関連施設間をネットワークを介して医療情報を流通させるためには、個人情報の保護のために専用線等を利用し、あらかじめ固定された拠点間での限定的な通信だけを許可する運用がされることが多い。しかしながら、今後は多数の関連施設を必要に応じて結ぶこと

で情報の流通を促し、医療情報を積極的に活用した高度な医療提供や、それに伴う機能分化や連携を実現することが必要となる。その際には、医療情報の流通を安全かつダイナミックに実現するための技術の利用が必要となる。安全性の観点からの評価により、オープンなネットワークを利用してダイナミックに 2 点間の通信を実現する OD-VPN であっても、機能的には専用線と同じ機能を提供可能であり、個人のプライバシーに関わる情報も安全に流通させることが可能である。但し、医療機関の管理が及ばない通信事業者、中継事業者などが間に入る場合には、アプリケーションレベルで暗号化や電子署名を付加するなどによって、流通する情報の機密性、完全性を保護する必要がある。

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）
分担研究年度終了報告書

安全な保健医療情報流通に向けたネットワークのセキュリティ評価の技術的方策に関する研究

分担研究者　　近藤　克幸　秋田大学医学部附属病院

研究要旨

本研究は、個人情報・医療情報の安全な流通を担保するセキュアネットワーク基盤の安全性を検証することを目的として、利用形態を念頭に、通信のモデル化とそのシステム要件の明確化を図ると共に、実際のシステムにてこれらの妥当性、効果・有効性を検証する事を目的としている．そこで，本分担研究中では，ユースケースに基づいたネットワークのモデル化を行うべく，医療分野におけるユースケースの抽出と明確化を図った．具体的には，実地医療で行いうる医療連携を想定し，情報の蓄積と言う観点から４パターンに分類し，それぞれのパターンに相当する具体的なユースケースを想定した．そして，その想定に基づき，ネットワークのモデルを１対１の施設連携と，地域内で複数の施設が連携した場合について考えた．また，具体的なシステム構築では外部ネットワークと施設内 LAN（診療系システム）の接点が発生するケースも多いと思われ，考察した．外部ネットワークとの境界となるルータ，あるいは直接に外部との通信を行う連携用サーバ群，さらに，一般の施設内診療系端末の，それぞれの階層について，セキュリティ水準を考慮しつつ，専用ルータの設置や専用回線の敷設の範囲を明確にし，技術的保護の水準を決定し，責任分界点を明確化し，階層毎に適切な運用ポリシーの策定と遵守が必要と考えられる．

A. 研究目的

本研究は、個人情報・医療情報の安全な流通を担保するセキュアネットワーク基盤の安全性を検証することを目的として、利用形態を念頭に、通信のモデル化とそのシステム要件の明確化を図ると共に、実際のシステムにてこれらの妥当性、効果・有効性を検証する事を目的としている．そこで，本分担研究中では，ユースケースに基づいたネットワークのモデル化を行うべく，医療分野におけるユースケースの抽出と明確化を図る事を目的とした．

B. 研究方法

実地医療において，遠隔地の医療機関間で行いうる医療連携を想定し，まず１医療機関対１医療機関の連携を情報の蓄積と言う観点から４パターンに分類し，各分類につき，ユースケースを抽出した．４パターンとは，①情報の発信側施設にデータが蓄積するタイプ，②情報の受信側施設にデータが蓄積するタイプ，③共用データセンターを利用するタイプ，④情報の蓄積を伴わないタイプ，の３つである．

次いで，これらに各医療機関内 LAN との関

連を加えて考察し，最終的には遠隔医療連携が地域的拡がりを見せ，複数の医療機関が関与する場合にこれらを当てはめる事で，全体としてのネットワーク構成を考察した．

（倫理面への配慮）

本研究は実際の患者への適用を行うものではなく，あくまでもユースケースを想定してモデル化とセキュリティ要件を検討するもので，倫理面への特別な配慮は必要なかった．

C．結果

1．情報の発信側施設にデータが蓄積するタイプ

1－①．遠隔画像診断

代表的なものに，遠隔病理診断や遠隔放射線画像診断が挙げられる．遠隔病理診断としては，最近普及しつつあるデジタル顕微鏡を利用した遠隔病理システム（バーチャルスライドシステムを含む）が代表的である．このようなシステムでは，病理画像のキャプチャーデバイスたる顕微鏡と画像サーバが一体化，またはセット化されている事が多い．また，遠隔放射線診断の場合も発信側施設にPACSを設置し，受診（診断）側施設が外部からネットワークを介して画像を参照するケースはあり得る．

これらの場合は，発信側施設でデータの蓄積が行われる事になる．

アクタ：発信側施設，受信側施設

概要：発信側施設で取得した病理画像や放射線画像を受信側施設が参照し，読影の上で所見を返送する．

前提条件：遠隔病理診断では，発信側施設はデジタル顕微鏡と画像管理用のDBおよび画像公開用サーバを，遠隔放射線診断では，発信側施設はPACSを保有する．いずれの場合も受信側施設はビューア（Webクライアントの場合も含む）があり，双方はネットワークで接続される．

イベントフロー：

(1)発信側施設は画像をデジタルデータ化し，患者情報を付加してDBに格納の上，受信側施設に読影依頼する．

(2)受信側施設は発信側施設のDBにアクセスし，画像を参照し，読影の上で所見を入力する．（紙媒体での返送もあり得る）

(3)発信側施設は所見を参照する．

（ネットワークのモデル）

発信側施設がDBを保有し，受信側施設は当該DBに外部からアクセスして情報を参照する事となる．

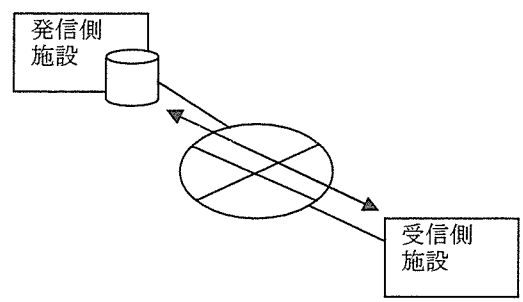

図1　発信側DB，1対1

なお，受信側施設は必ずしも大規模ではないが，専門医を有する施設となることから，複数の発信側施設と連携を行う事は十分想定される．従って，地域単位でネットワークを考えた場合は，下図のような構成になろう．

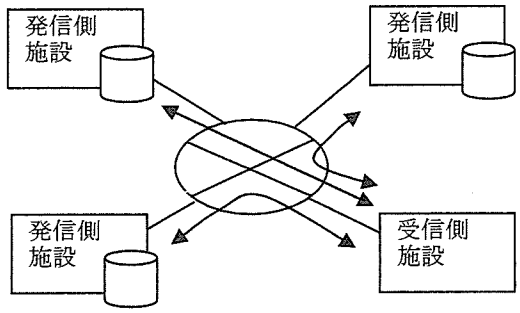

図２　発信側 DB，多対１

このように，複数医療機関が接続する場合は，特に受信側施設においては複数の相手先と双方向性の通信が行われる事となり，複数の経路に対する安全性を確保する必要がある．特に Web ベースの診断用クライアントの場合など，複数の発信側施設に対して１台のクライアント機器が共用される事もあり得る．そのため，受信側施設が接続先を任意にコントロールでき，かつそれぞれの通信路の安全性が確保できるような方策が望ましい．

なお，これらのケースでは，外部の受信側施設から発信側施設内の患者 DB へのアクセスが必要となる．その場合，発信側施設では通常の診療で発生した画像データを格納している DB を連携用に共用し，受信側施設に開放する運用も十分想定され，患者情報の管理面での懸念が残る．すなわち，読影を依頼していない患者情報が不用意に参照されないよう，運用ポリシーの遵守と監査，あるいはシステム自体の権限制御機能などの配慮が必要となる．ただし，本問題は本研究の主たるテーマとやや趣を異にするため，詳細は省略する．

１－②．患者公開型電子カルテシステム

発信側施設である医療機関が保有する電子カルテシステムの情報を，患者自身にネットワーク経由で公開するタイプのシステムである．

アクタ：発信側施設，患者

概要：発信側施設で入力済みの電子カルテシステムを患者に公開する．

前提条件：発信側施設は電子カルテ（DB）を保有する．患者側はネットワーク経由で自己の情報を参照する手段を有す．双方はネットワークで接続されるが，患者自宅等からのアクセスが多いため，インターネットを利用する．

イベントフロー：

(1)発信側施設は患者情報をデジタルデータとして電子カルテ DB に格納する．

(2)患者はインターネット経由で発信側施設の電子カルテサーバにアクセスする．

(3) 患者は自己が受診した時の，自己のデータを参照する（Web 型クライアントが利用される事が多い）

（ネットワークのモデル）

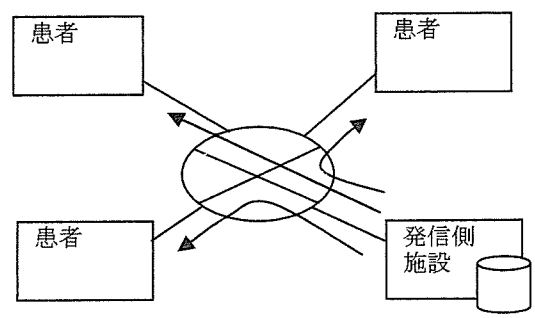

図３　患者公開型電子カルテ

この場合，受信側に相当する患者は多数になる事が多い．また，医療機関のように存在場所の特定が必ずしも固定的ではない．

そのため，情報を参照する患者を特定するための手段を十分考慮する必要がある．

２．受信側施設にデータが蓄積するタイプ

２－①．遠隔画像診断

遠隔病理診断については，１項で挙げた画像管理 DB と一体となったデジタル顕微鏡を利用する形態の他に，デジタルカメラを利用して顕微鏡画像をデジタル化し，受信側施設に画像データを送信し，受信側施設で DB に格納する方法もある．

遠隔放射線診断についても同様に，発信側施設でデジタル化された画像データを受診側施設に送信して PACS に格納したり，あるいは，発信側施設から受信側施設の DICOM サーバに直接 DICOM 通信で書き込む方法などがある．

これらはいずれも，受信側施設にデータが蓄積する形態の遠隔画像診断である．

アクタ：発信側施設，受信側施設

概要：発信側施設で作成した画像データを受信側施設の DB に格納し，受信側施設で読影の上で所見を返送する．

前提条件：発信側施設は画像のデジタル化の手段を有し，受診側施設は画像データを格納する DB を保有する．双方はネットワークで接続される．

イベントフロー：

(1)発信側施設は画像をデジタルデータとし，患者情報を付加して受診側施設に送信する．

(2)受信側施設は受診した画像データを DB に格納する．

(3)受信側施設の専門医が画像を参照し，読影の上で所見を入力する．（紙媒体での返送もあり得る）

(4)発信側施設は所見を参照する．（受信側施設がレポート管理サーバを保有し，発信側施設が同サーバを参照する場合，所見参照のユースケースは１項に準ずる）

（ネットワークのモデル）

受信側施設が DB を保有し，発信側施設は当該 DB に外部からアクセスして情報を参照する事となる．

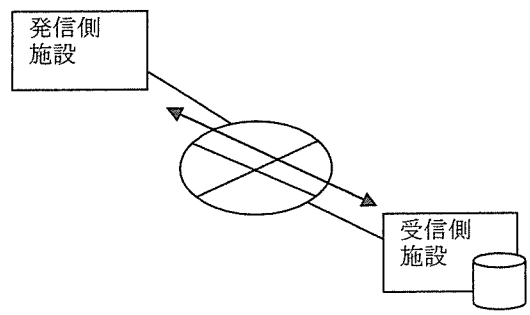

図４　受信側 DB，１対１

一般には受信側施設の規模が大きく，外部連携用のサーバを保有し，複数の発信側施設と連携を行う事が多いと思われる．従って，地域単位でネットワークを考えた場合は，下図のような構成になろう．

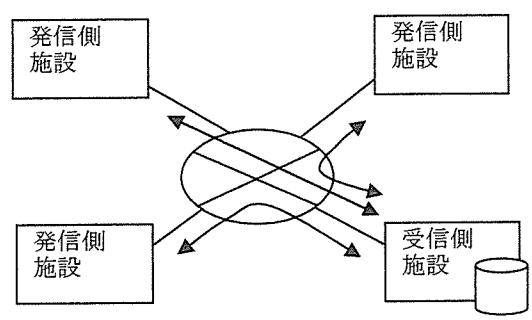

図５　受信側 DB，多対１

このような場合は，受信側施設は常時複

数施設からの接続を可能としておき，発信側施設が任意に接続をコントロールできる事が望ましい．あるいは，送信側施設が読影依頼時に他の手段で連絡を行い，両者の合意のもとに接続できる方法を考慮するべきであろう．１項と同様に，接続確立時における通信路の安全性確保が必須であることは言うまでもない．

２－②．患者紹介関連システム

情報の発信側施設が，例えば患者紹介時の各種情報（病歴，投薬歴，検査データ，画像データなど）を送信し，受信側施設が被紹介施設として DB にそれらの情報を格納する形態である．この場合は，２－①項の遠隔画像診断とほぼ同様の形態となる．

アクタ：発信側施設，受信側施設
概要：発信側施設で作成した患者データを受信側施設の DB に格納し，受信側施設では情報を参照し，患者受信時に診察する．
前提条件：発信側施設は各種情報を入力する．受診側施設は患者データを格納する DB を保有する．双方はネットワークで接続される．
イベントフロー：

(1)発信側施設は紹介に必要な情報を入力し，受診側施設に送信する．（送信せずに，受信側施設が用意した Web 型情報入力用サーバに発信側施設がアクセスして入力する形態も多い）
(2)受信側施設は受診した患者データを DB に格納する．
(3)患者受診時または受診前に，受信側施設の医師が情報を参照し，診察する．

（ネットワークのモデル）

この場合，ネットワークのモデルは２－②項と同様なので図は省略する．ただし，地域内で複数の医療機関がこのようなモデルに該当する場合は，やや複雑になる．すなわち，発信側施設は唯一の施設に対して紹介するわけではなく，患者の病態やきょうじゅう地域に応じて複数の受信側施設に対して紹介する可能性がある．また，時として受信側施設が発信側施設になる事もあろう．従って，その場合のモデルは下図のような構成になろう．

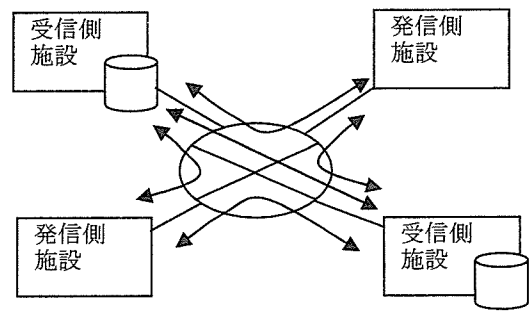

図６　受信側 DB，多対多

３．共用データセンターを利用するタイプ

３－①．共用データセンター型システム

地域の複数医療機関が共用するデータセンターを利用する場合である．情報の発信側施設は，複数医療機関を受診する患者や，他施設への患者紹介時に，各種情報（病歴，投薬歴，検査データ，画像データなど）をデータセンターに送信し，受信側施設が被紹介施設としてデータセンターの情報を参照するタイプである．

アクタ：発信側施設，データセンター，受信側施設
概要：発信側施設で作成した患者データをデータセンターの DB に格納し，受信側施

設ではデータセンターにアクセスして情報を参照する．

前提条件：発信側施設は各種情報を入力する．データセンターは患者データを格納する DB を保有する．受信側施設はデータセンターの情報を参照するためのクライアントを保有する．３者はネットワークで接続される．

イベントフロー：

(1)発信側施設は紹介に必要な情報を入力し，受診側施設に送信する．（送信せずに，データセンターが用意した Web 型情報入力用サーバに発信側施設がアクセスして入力する形態も多い）

(2)データセンターは送信または入力された患者データを DB に格納する．

(3)受信側施設は，必要時にデータセンターにアクセスし，情報を参照する．

（ネットワークのモデル）

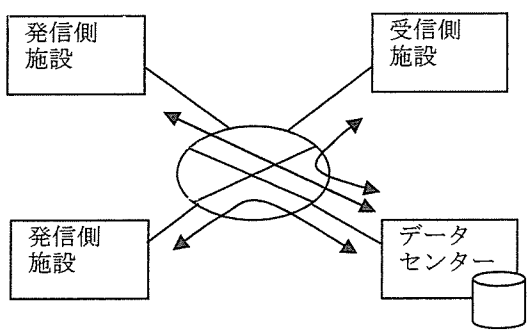

図７　データセンターDB，多対１

このような場合は，データセンターは常時複数施設からの接続を可能としておき，発信側施設が任意に接続をコントロールできる事が望ましい．接続確立時における通信路の安全性確保が必須であることは言うまでもない．

４．情報の蓄積を伴わないタイプ

４－①．遠隔手術支援システム

発信側施設における手術中の画像をリアルタイムに送信し，受信側施設の支援医師がディスプレイ上で参照し，音声や画像でアドバイス等を伝達するシステムである．

アクタ：発信側施設，受信側施設

概要：発信側施設で撮影している動画像または静止画像を送信し，受信側施設はディスプレイで参照，アドバイスを伝達する．

前提条件：発信側施設は動画像または静止画像のデジタル化の手段と送信設備を有し，受診側施設は受信設備を保有する．両者はネットワークで接続される．

イベントフロー：

(1)発信側施設は手術画像を撮影し，デジタルデータとして送信する．

(2)受信側施設は支援医師が受診した画像データを参照する．

(3)受信側施設の支援医師が画像を参照しながらマイクや画像等を利用して，アドバイスを伝える．（電話等の通信手段を利用する場合もある）

（ネットワークのモデル）

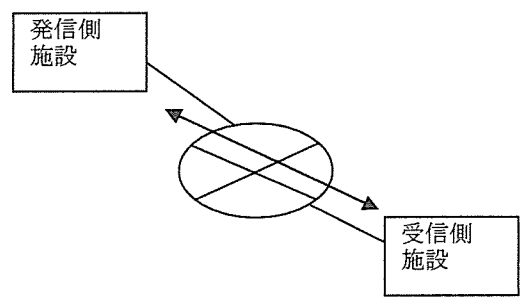

図８　手術支援システム

この場合は，一般に１対１の接続で完結する場合が多い．また，目的とする手術の終了とともに接続が不要となる．

４－②．遠隔カンファレンスシステム

発信側施設はシステムを利用して，動画像に加えてプレゼンテーション用の資料などを送信する．受信側施設はクライアントアプリケーションで情報を参照する．なお，一般にこの類のシステムは開始時受信側施設からも，情報を送信できる場合が多く，必ずしも発信側・受信側と言う分類ができない事が多い．また，発信側施設には接続可能施設情報など，若干の情報を蓄積したサーバを配置している事が多く，厳密には情報を蓄積しないタイプとは言えないが，授受する情報はリアルタイム性を有し，かつ，ＤＢに格納されるものではないため，このタイプに分類した．

（ネットワークのモデル）

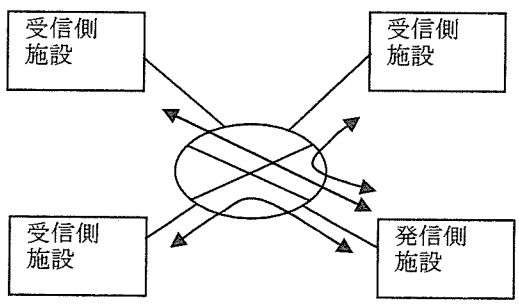

図９　カンファレンスシステム

５．施設内 LAN と外部ネットワーク

１項から３項に例示したタイプのシステムでは，各施設内 LAN 上に構築されている診療系システムに格納されているデータが，送信用のデータとして利用される事も多い．この場合，連携用の外部ネットワークと施設内 LAN による診療系ネットワークに何らかの接点が生じる．その場合は，暗号化や認証をはじめとする安全性の確保をどの範囲で行うかが問題となる．

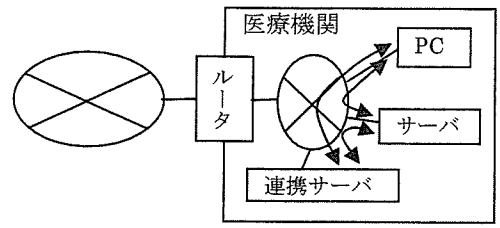

図１０　施設内 LAN と外部

すなわち，上図のうち，施設と外部の境界に相当するルータ，あるいは，施設内 LAN に接続される連携用サーバまでは言うまでもなく十分な安全性を確保する必要がある．しかし，施設内サーバと連携用サーバ，あるいは，施設内 PC と連携用サーバの間も全く同等の手段を用いる事が可能かと言う点では議論があろう．一般に施設内 LAN に接続されている診療系端末は，連携の中核になりうる施設の場合は数百台に達することが多いと思われる．この場合，全ての通信路に専用ルータや連携用専用回線の敷設を行う事は現実的には困難である．仮に可能だった場合でも，施設内 LAN の診療系システムの端末同士の接続も同時に影響を受ける可能性もあり，何らかの配慮が必要となろう．

外部施設との安全なネットワーク環境を普及させるためにはコストの問題も重要な要素である．従って，外部ネットワークとの境界となるルータ，あるいは直接に外部との通信を行う連携用サーバ群，さらに，一般の施設内診療系端末の，それぞれの階層について，セキュリティ水準を考慮しつつ，専用ルータの設置や専用回線の敷設の範囲を明確にし，技術的保護の水準を決定し，責任分界点を明確化し，階層毎に適切な運用ポリシーの策定と遵守を行う事が必

要と考えられる.

E. 研究発表

学会発表・論文発表　未

F. 知的財産権の出願・登録状況

該当なし

ネットワーク利用形態の特徴抽出・分類・モデル化に関する調査研究

分担研究者　山本　隆一　　東京大学大学院情報学環　助教授

研究要旨　平成19年に改定された医療情報システムの安全管理に関するガイドライではネットワークを介して外部と情報を交換する場合の指針の記載が大幅に強化された。本研究班はその指針に基づいた運用を検討するものであるが、分担研究者は利用形態の特徴を抽出・分類した。

A．研究目的

2006年1月に公表されたIT新改革戦略においては医療のITによる構造改革が重要なテーマとしてとらえられ、その具体的な施策の多くは個々の医療機関がネットワークを介して外部の機関と情報を交換できることが前提となっている。これまでの医療の情報化は主に医療機関内部のIT化に関心がもたれ、外部との情報交換も限定された地域での情報連携にとどまり、網羅的・全国的なレベルの情報交換は表立って議論されることは少なかった。そのために平成15年に第1版として厚生労働省から公表された「医療情報システムの安全管理のためのガイドライン」(以下、「安全管理GL」と呼ぶ) も外部との情報交換に関しては抽象的な記載が一部に見られるだけで具体的な指針は示されていなかった。しかしIT新改革戦略や2006年6月に公表された重点計画2006では広域ネットワークを活用した情報交換が網羅的で全国的にできることを求めており、それに対応するために改定が行われた。本研究はこの改訂内容を前提として、医療機関が外部と電子化情報を交換する場合のネットワーク利用形態の特徴を分類・抽出し、モデル化することにある。

B．研究方法

大規模医療機関から小規模保険薬局にいたるいくつかの医療機関を訪問調査し、また厚生労働省ネットワーク基盤検討会の「安全管理GL」の改定の作業班に主査として参加し、作業班での議論をもとに利用形態の特徴を抽出した。

C．研究結果

1．回線種別による分類

安全管理GLでは回線種別を専用線、ISDN、IP-VPN、Internet VPNに分類し、さらにIP-VPN、Internet VPNは単一の事業者が提供する場合と複数の事業者が提供する場合に分けている。確かにこれらの分類は妥当でそれぞれ、費用や保証するものも異なる。しかし費用は別として回線が保証するものに違いはあるとしてもあくまでも回線の両端の間に限定される。ネットワークの専門知識を持たない医療機関から見れば図1のように接続されていると思われがちであるが、実際は図2のように様々な中継点が入りうる。つまり回線事業者が一定の保証を与える部分と医療機関の間に管理があいまいな領域が生じる可能性がある。

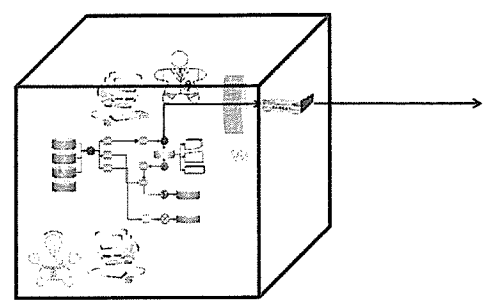

図1　VPN接続(医療機関から見た場合)

したがって安全管理 GL では送付元事業者内で暗号化のような情報自体の安全対策を講じたうえで回線に送出する、Object security の確保を求めている。つまり回線種別による分類はネットワークの利用形態の分類にとってはそれほど大きな要素とは言えない。

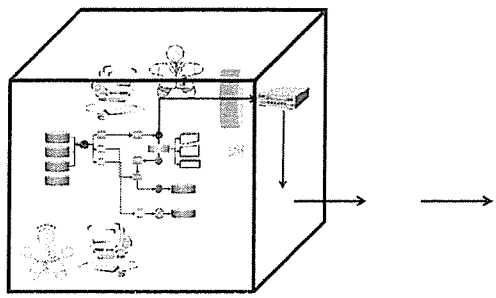

図2 実際のVPN接続

2．機器の安全性と認証の有無による分類

安全管理 GL では C の最低限のガイドラインでネットワーク機器に一定の安全性を求めている。またネットワークの機器のなりすましの回避も求めている。保健医療福祉機関内に置かれるネットワーク機器の管理責任はその機関にあるが、ネットワークサービスによっては機器認証までサービスに含むものもある。機関内に直接終端を持つ専用線ではこのような機器認証は必然的に行えることになる。またインターネット VPN でも HEASNET の提唱する仕様のようにサービスに含まれるものもある。このような機器認証がサービスとして提供されるか、ネットワークの両端で事業者同士が自分たちの責任で行う場合では運用の容易さに大きな差があり、本研究班の目的からみても重要な分類軸と言える。また実際には操作者の認証も重要な意味がある場合も多い。一般には利用者の認証はその機関の責任で行われるが、前述の HEASNET が提唱している仕様では利用者の認証も可能であり、保健医療福祉機関はさらに低負担で安全性の確保が可能になる。したがって利用者の識別・認証機能もこの分類軸の要素として含めるべきであろう。

3．利用目的とトポロジーによる分類

3－1．B to B と B to C

安全管理 GL では利用形態にかかわらない一般的な要件として Channel Security と Object Security の両立を求めている。しかし、B to B の情報交換と B to C の情報交換ではその要件が異なる。したがって利用形態のもっとも上位の分類は B to B と B to C の２つに分類することが妥当であろう。B to B の場合はネットワークを介して複数のアプリケーションが動作する可能性があるが、たとえば患者等に自身の診療情報をネットワークで開示する場合はクライアント・サーバ型の単一のアプリケーションで行われる。つまり単一のプロトコールで実装することが可能で、現実にそのようなアプリケーションを用いている現存のプロジェクトはすべてHTTPSのみを用いている。単一のプロトコールしか用いない場合はおオープンネットワークでSSLを用いるだけでもセッションを乗っ取ることはできないために、両端の認証さえ正しくできればSSL だけで十分な安全管理が可能と考えることができる。これに対して複数のプロトコールが共存する場合はオープンネットワークでSSLを用いるだけでは安全性とは言えない。

3－2．スター型ネットワーク接続

例えばレセプトオンラインのように多数の医療機関が一か所に接続する必要がある場合に、ネットワーク自体もその一か所とスター型に接続する場合である。専用線の場合は実際の回線もスター型になるが、２０万件の医療機関等が１か所のセンターと専用線で接続することは現実的ではない。実際には理論的にスター型の接続をすることになる。またこの亜型として間接的にスター型接続をする場合もありえる。いくつかの医療機関が下位センターにスター型に

接続し、下位センターが上位センターにスター型に接続するタイプで多段にもなりうる。

３－３．P2P（メッシュ）型ネットワーク接続

一般のインターネットは論理的にはメッシュ型ネットワーク接続であるが、保健医療福祉分野で患者等の個人情報を交換する場合、単純なメッシュ型ネットワーク接続はあり得ない。メッシュ型と言っても一つのトランザクションでは両端が特定されたP2P の接続である。接続アプリケーションを起動する際に明示的に相手を指定してP2P コネクションを確定するか、アプリケーション層でのルーティングをすることになる。アプリケーション層でのルーティングはプロキシサーバやゲートウエイで実現は不可能ではないが標準的な手法は確立されていない。また必要に応じて異なる P2P コネクションを安全に確立することは専用線接続では不可能で、ISDN、IP-VPN、インターネット VPN のいずれかを用いることになる。ISDN は直接接続する場合は本質的にこの機能を有する。IP-VPN で実現するためには、各保険医療福祉機関はアプリケーションごとに別の IP-VPN の契約をすることになり現実的ではない。インターネットVPN は理論的にはVPN 装置を操作すれば VPN 接続先を変更することは可能である。しかし一般の VPN 装置は相手先を固定することを前提に設計されている。ただし HEASNE の提唱する OnDemand VPN は十分な機能を有する。

３－４　組み合わせトポロジー

スター型は多段階のトポロジーがありうることは前述したが、それ以外の組み合わせもありうる。ISDN の場合、距離による料金差があり、一般に同一局番内は廉価である。したがって中継点を置き、中継点以降はブロードバンドを用いることで経済的効果を上げることが可能である。

しかし組み合わせる理由は経済的なものばかりではない。例えば送付する情報に電子署名とタイムスタンプを付与する場合、電子署名はその機関内だけでも可能であるが、タイムスタンプはタイムスタンプ付与機関（TA）に接続しなければ付与できない。アプリケーション毎に閉域内に TA を持てば送付の際にタイムスタンプを付与することは可能であるが、送付のタイムスタンプが同じタイミングで行われるとは限らない。また送付された情報の署名やタイムスタンプを検証する場合には CRL/ARL の確認が必須であるが、これも基本的には外部の CA および TA へのアクセスが必要になる。合理的な運用のためには、伝送のアプリケーションと同時に TA および CA へのアクセスが確立されているほうがよい。しかし一般の保険医療福祉機関でこのような複雑な接続を安全に確立するための技術的負荷は高いことが予想される。これを解決するためには接続サービス自体が TA/CA への接続をサービスするか、中間にゲートウエイを置いて、そこで TA/CA へのアクセスとアプリケーションによるルーティングをサポートすることが考えられる。後者の場合はトポロジーが組み合わせられることになる。

４．評価

どの分類でも安全な接続は可能である。しかし、効率は大きく異なる。専用線は外部からの干渉の除外と高速性という点では大きな利点を持つが、IT 新改革戦略で目指しているようなさまざまなアプリケーションが共存する状態では利用に限界がある。本院と分院のような固定的で大量の情報交換が必要な場合には選択肢にはなりうる。ISDN は最近のブロードバンドの低価格化を考えれば他に選択肢がある状態では利点はほとんどないが、ISDN しか選択できない地域もまだ存在する。IP-VPN は他の干渉を防ぐ意味では十分な効果があると考えられるが、複数のアプリケーションを使う

場合に費用の増加はまぬかれない。さらにIP-VPNと言ってもさまざまな形態があり、インターネット VPN と区別できない場合もある。そのような場合、接続事業者が固定的になるという点で問題がある。またIP-VPN 自体は閉域性は確保されるが暗号化は一般にされないために、接続点での盗聴に対して別の対策が必須となる。インターネットVPNは様々な仕様が存在し、その多くは廉価で利便性が高いことを優先しているために、複数のアプリケーションで使う場合には適さない。しかしHEASNET提唱規格であるOnDemand VPNはすべての要件を満たし、接続事業者を選択しない点で経済面からも可用性の面からも利点が多い。その一方でTA/CAのアクセス機能は現時点ではどの接続サービスもサポートしていないために実装に際して工夫を要する。

D．考察

接続携帯の分類とモデル化を行って評価したが、現時点ではブロードバンドが利用可能な状況ではインターネット VPN の中でHEASNET提唱のOnDemand VPNが経済面も含めるともっとも効率が高いと考えられる。しかし電子署名およびタイムスタンプを使用するためには接続に工夫が必要であることが明らかである。OnDemand VPNのような接続サービスがTA/CAへのアクセスをサービスとして提供することも解決の一つではある。しかし、将来にわたって TA/CA へのアクセスだけが必要かというとそうではない。IT新改革戦略にあるような生涯利活用可能な健康情報データベースができた場合、あらゆる保険医療福祉機関はそのデータベースに必要に応じてアクセスできることが求められるし、例えば薬品に関する緊急安全性情報や EBM データベースへのアクセスも必須であろう。さらに必要なコンテンツが増える可能性もある。このように考えると、汎用の接続サービスがこれのコンテンツへのアクセスを提供し続けることは無理がると考えられる。保健医療福祉分野専用のサービスであれば可能と思われるが、その場合コストの増大を招きかねない。その意味では結果の３－４で述べたゲートウエイの設置が合理的解決法と考えることができる。本研究班での実証実験もこのような機能を備えることも可能なモデルを含めていることは評価できる。

E．結論

平成 19 年に改定された医療情報システムの安全管理に関するガイドライではネットワークを介して外部と情報を交換する場合の指針の記載が大幅に強化された。本研究班はその指針に基づいた運用を検討するものであるが、分担研究者は利用形態の特徴を抽出・分類した。HEASNET 提唱の OnDemand VPN の経済面も含めた有効性を確認するとともに、ゲートウエイセンターの必要性を示唆した。

F．健康危険情報

特になし。

G．発表

論文

１．山本隆一、大江和彦、田中勝弥、「電子化診療情報の患者への提供の在り方に関する調査研究」、文部科学研究補助金特定領域情報爆発 IT 基盤成果報告書、2007

２．山本隆一、「医療施設における個人情報保護」、病院設備、48 巻・1 号，P.74-79，日本医療福祉設備協会，2006 年 1 月

３．山本隆一、「個人情報保護法の導入と診療現場の改革」、病院設備、48 巻・2 号，P.140，日本医療福祉設備学会，2006 年 3 月

４．山本隆一、「医療における個人情報保護」、（特別講演／５回糖尿病教育資源共有機構学術集会）、肥満と糖尿病（別冊）、5 巻・30 号，P.18-26，（株）丹水社，2006 年 7 月

５．山本隆一、「遠隔画像診断のセキュリテ

ィと個人情報保護」、Rad Fan、5巻・1号，P.18-19（株）メディカルアイ，2006年12月
6．山本隆一、「電子カルテとプライバシー保護」、日本医師会雑誌、135巻・9号，P.1954-1954，日本医師会，2006年12月

H．知的財産権の登録・出願状況

現在のところなし。