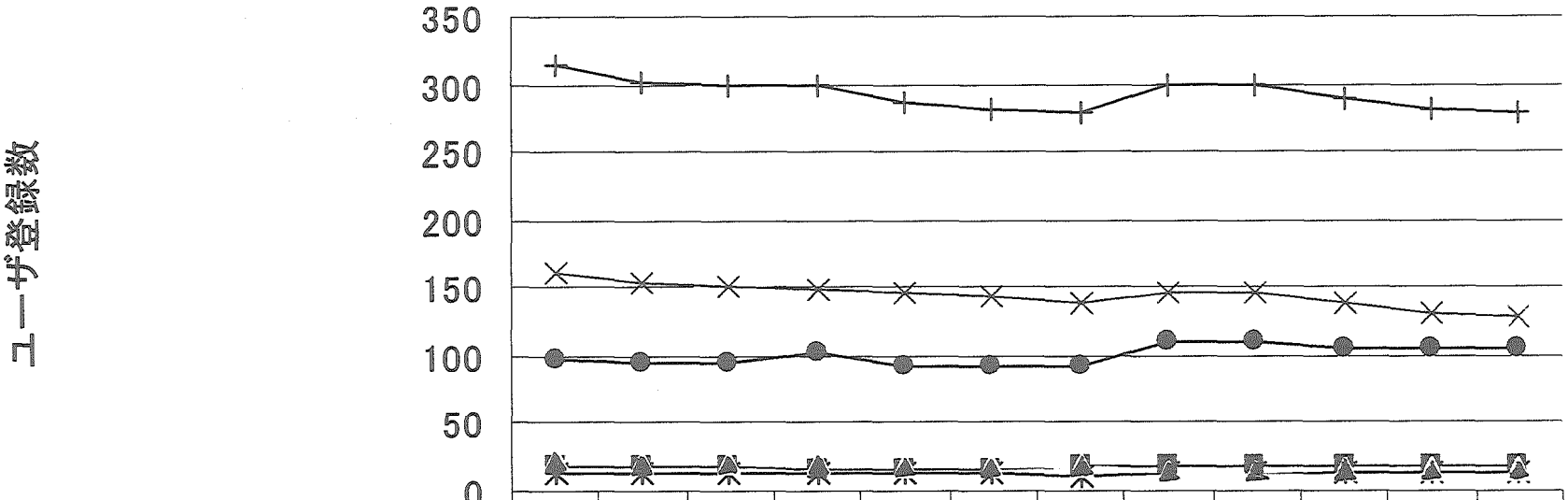
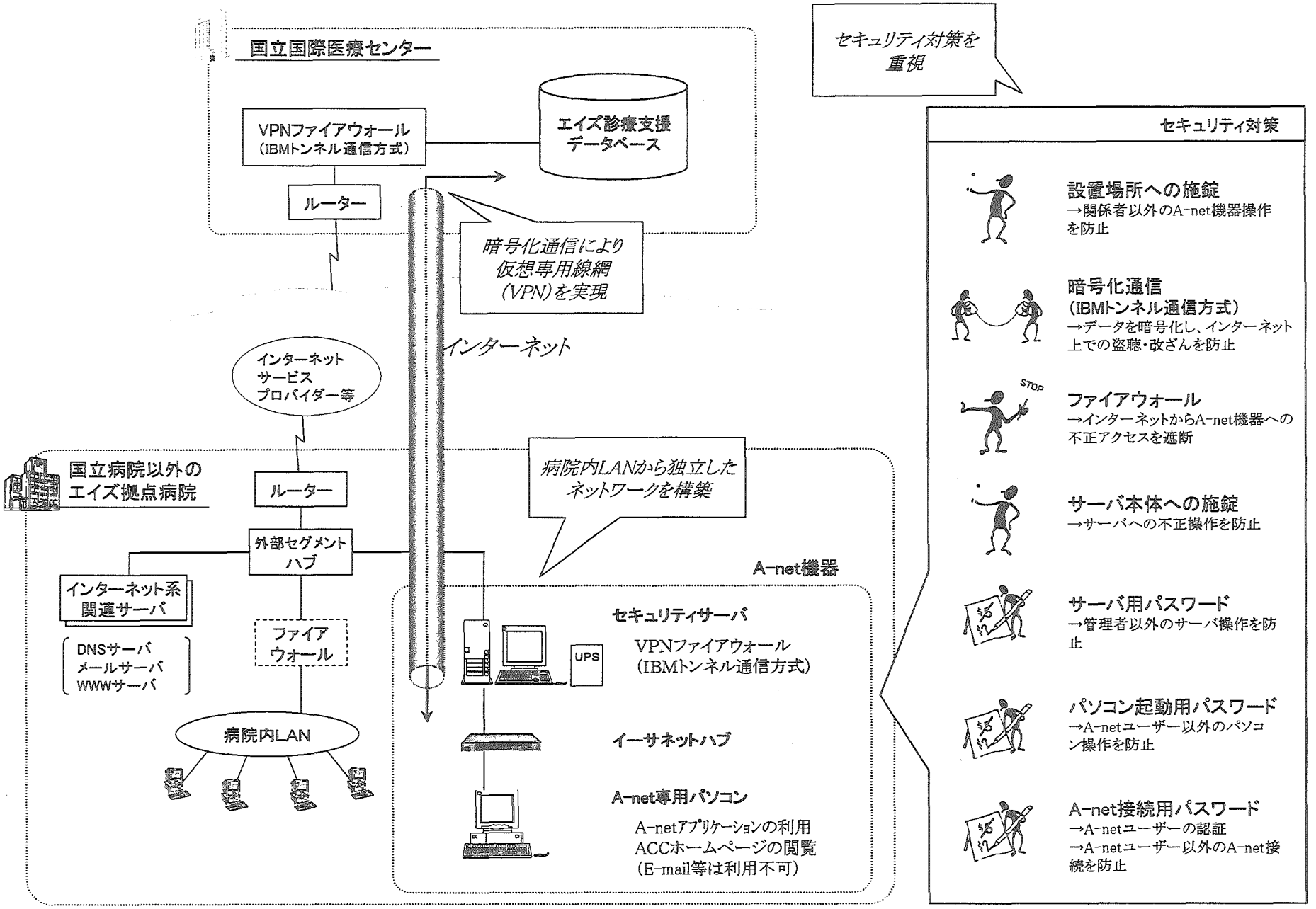
施設別参加ユーザ数



	1	2	3	4	5	6	7	8	9	10	11	12
国立国際医療センター	14	14	14	13	12	12	11	14	14	14	14	14
機構4ブロック	19	17	17	15	16	16	17	17	17	17	17	17
非機構ブロック	22	21	21	20	19	19	19	13	13	15	15	15
機構拠点	160	154	152	147	145	142	139	146	145	137	130	129
非機構拠点	98	95	95	103	93	93	93	109	110	106	104	104
合計	313	301	299	298	285	282	279	299	299	289	280	279

月

システム概要（国立病院以外）



VPNを使用している施設の現状稼動状況

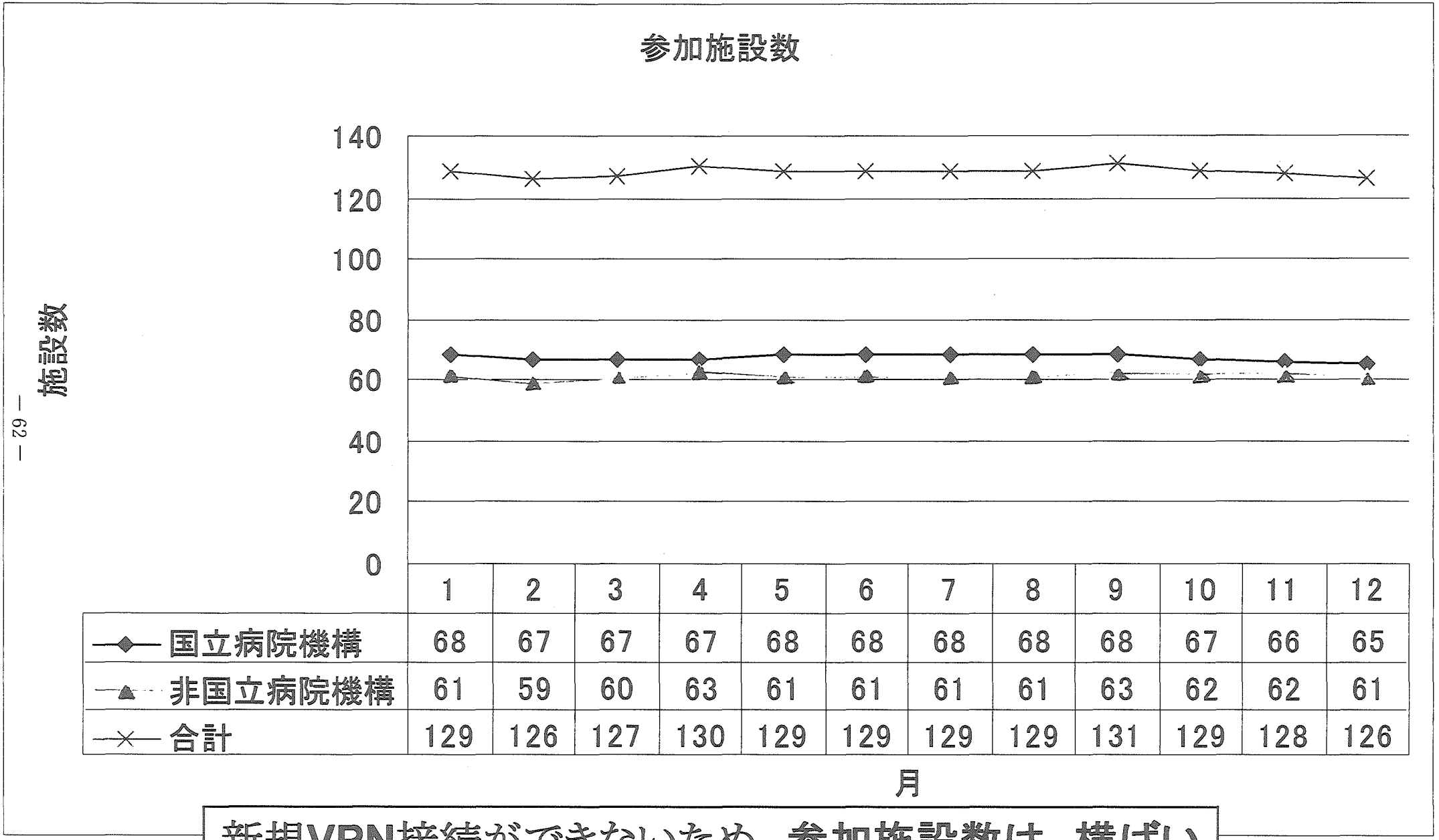
H17年度11月末施設数

導入年度	施設数	ユーザーのいる施設数
Ｈ１０年度	55	37
Ｈ１１年度	19	15
Ｈ１２年度	6	4
Ｈ１３年度	5	3
Ｈ１４年度	3	3
合計	88	62

H17年度11月末ユーザー数

	登録数	休止数
ACC	14	
国立４ブロック	17	
国立拠点	130	2
非国立拠点	104	
非国立ブロック	15	
合計	280	2

参加施設数

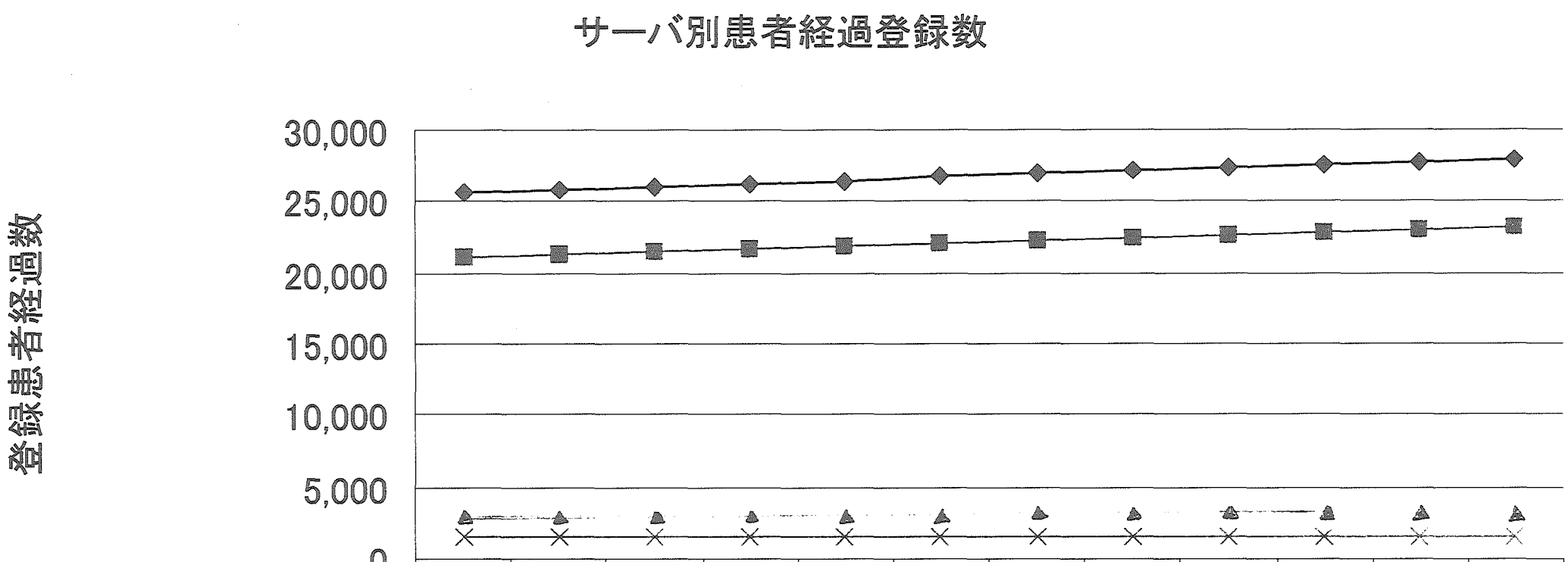


	1	2	3	4	5	6	7	8	9	10	11	12
国立病院機構	68	67	67	67	68	68	68	68	68	67	66	65
非国立病院機構	61	59	60	63	61	61	61	61	63	62	62	61
合計	129	126	127	130	129	129	129	129	131	129	128	126

月

新規VPN接続ができないため、参加施設数は、横ばい

患者経過登録数



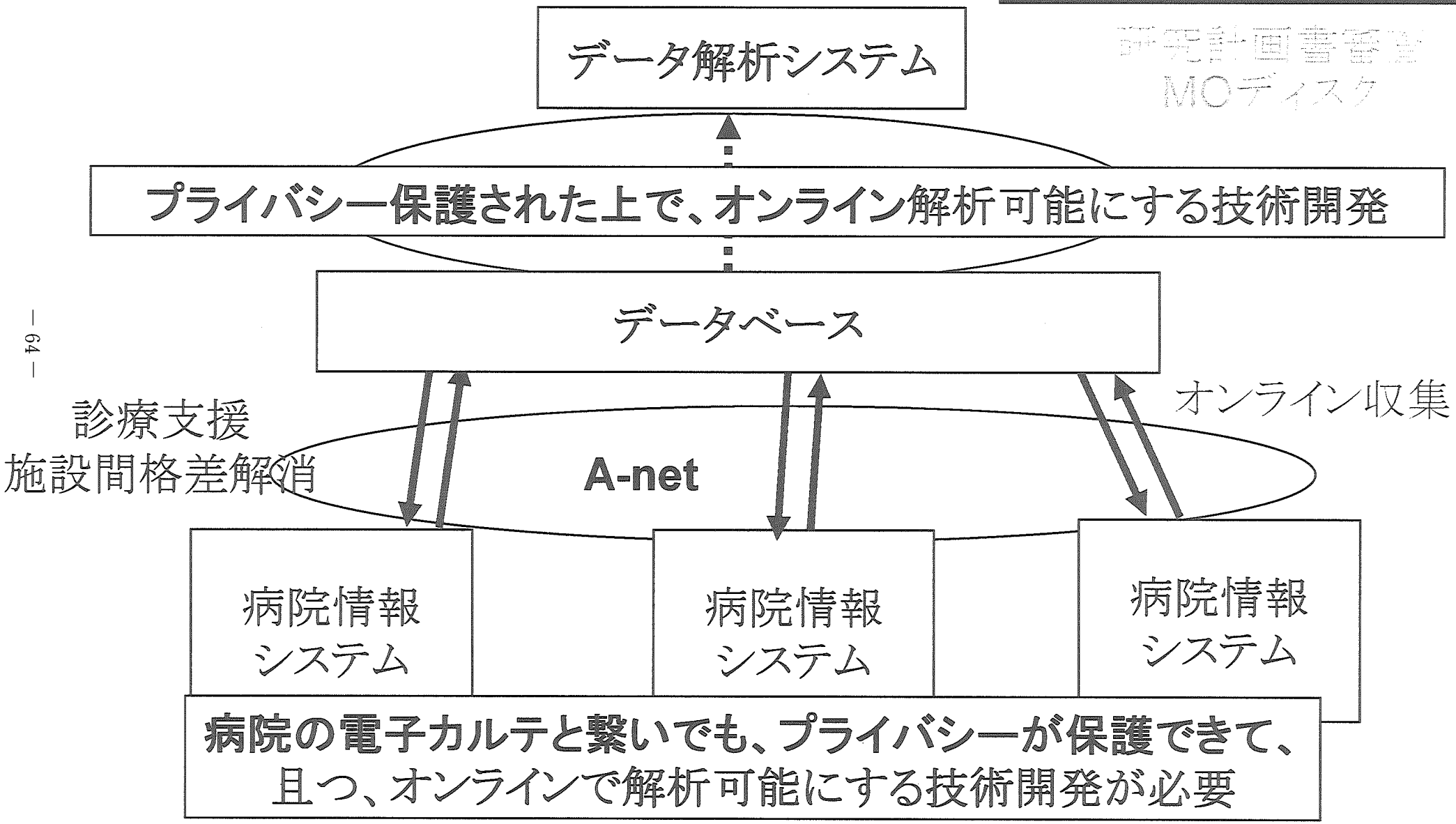
	1	2	3	4	5	6	7	8	9	10	11	12
国立国際医療センター	21,066	21,246	21,446	21,635	21,851	22,086	22,253	22,444	22,610	22,787	22,956	23,166
ブロック拠点病院	3,020	3,045	3,068	3,088	3,109	3,131	3,150	3,171	3,188	3,206	3,225	3,234
全国拠点病院	1,455	1,461	1,466	1,472	1,481	1,486	1,491	1,497	1,497	1,501	1,501	1,502
合計	25,541	25,752	25,980	26,195	26,441	26,703	26,894	27,112	27,295	27,494	27,682	27,902

患者経過登録数は、順調に増加しており、約28,000データが蓄積している

A-netにおけるデータの二次利用

解析へのハードルが高い

研究計画書審査
MOディスク



現状のA－net問題点

【アプリケーションサーバー】
　H／W保守廃止の可能性（既に一部保守廃止のH／Wもあり）
　S／Wサポート廃止

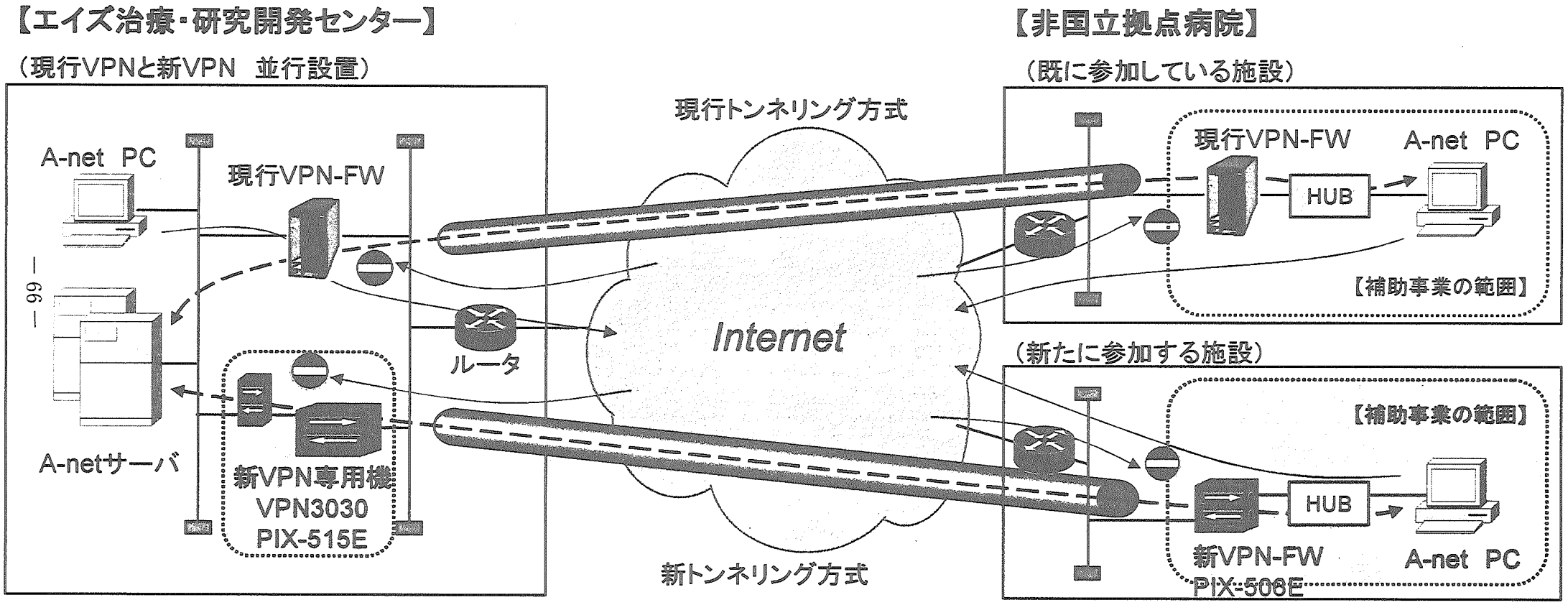
【VPN関連】
　H15年度より新規参加施設募集を休止。現行に至る。
　H／W保守廃止の可能性
　S／Wサポート廃止

＜経緯＞
　H12年度をもって現行使用しているIBMトンネリング方式のVPN　S／Wの販売を停止。
　H13年度～H14年度についてはIBM内での例外処理により特別にライセンスを供給
　この2年間の間に、新しい仕組みへの移行について厚生労働省疾病対策課にて、検討。しかしながら、未だ移行という決定がなされていない。

新規に参加施設を増やせない

国立病院機構以外では使えなくなる

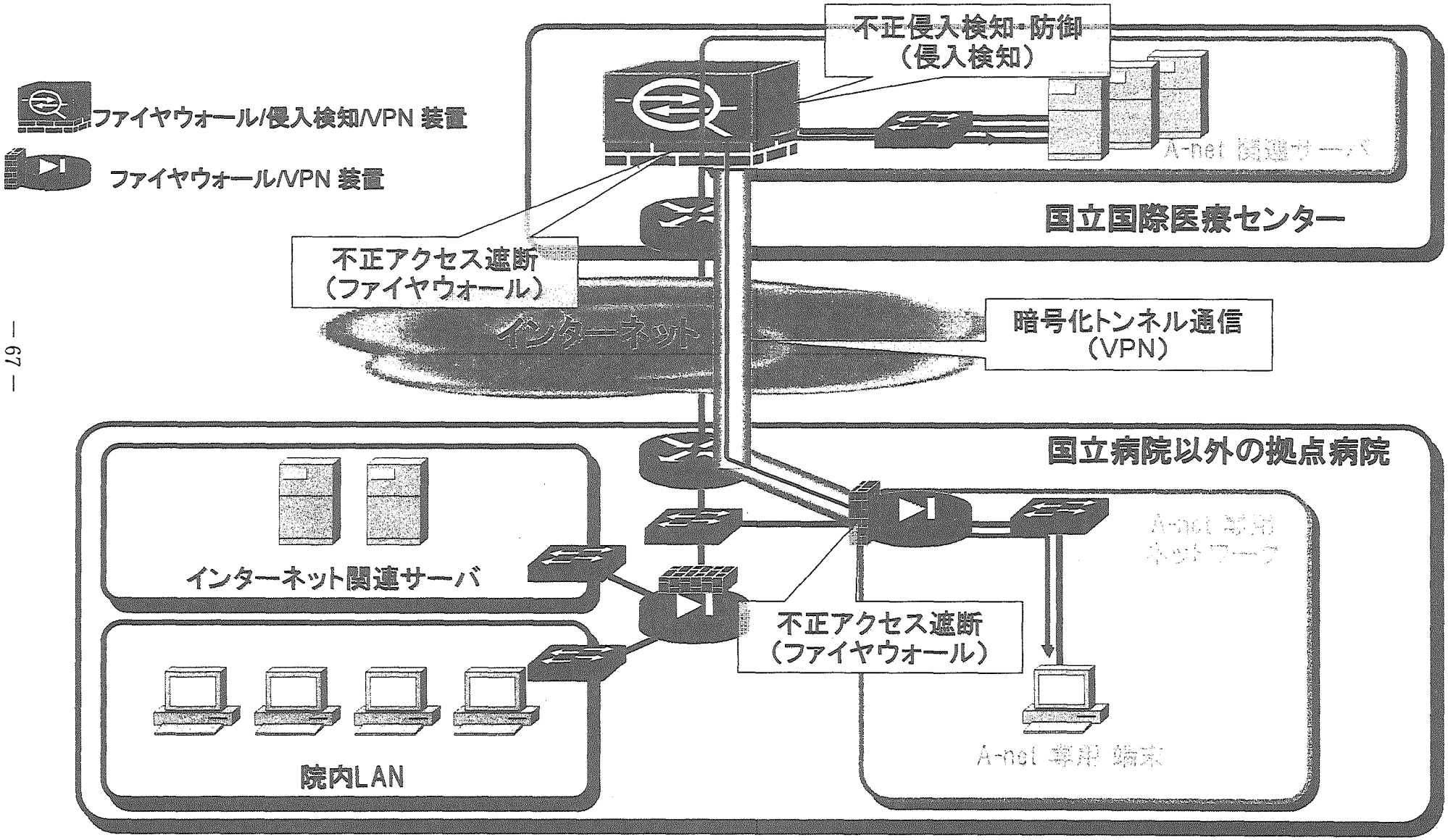
A－net　新VPN接続構成（案）



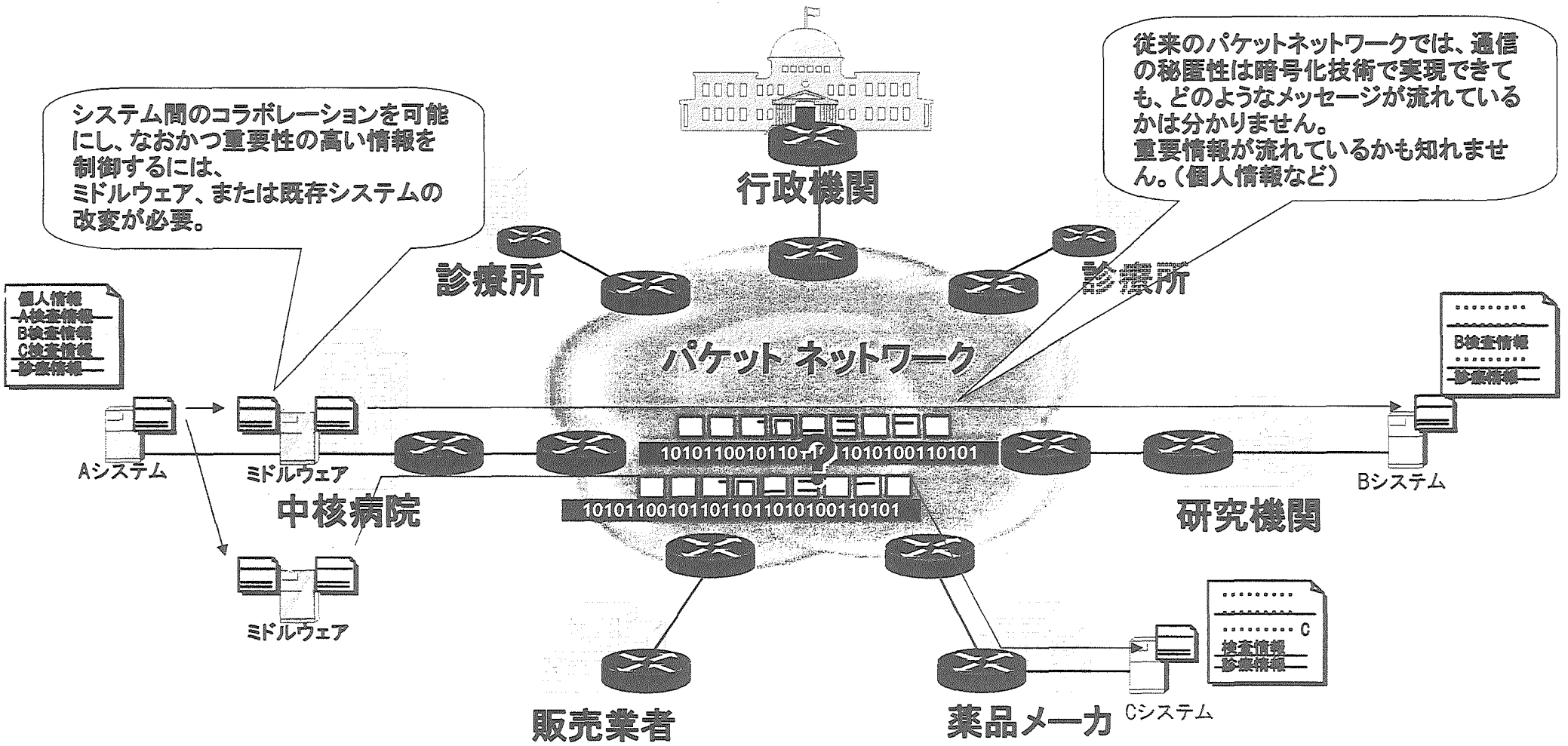
新規に参加施設を追加可能

国立病院機構以外でも徐々に更新可能

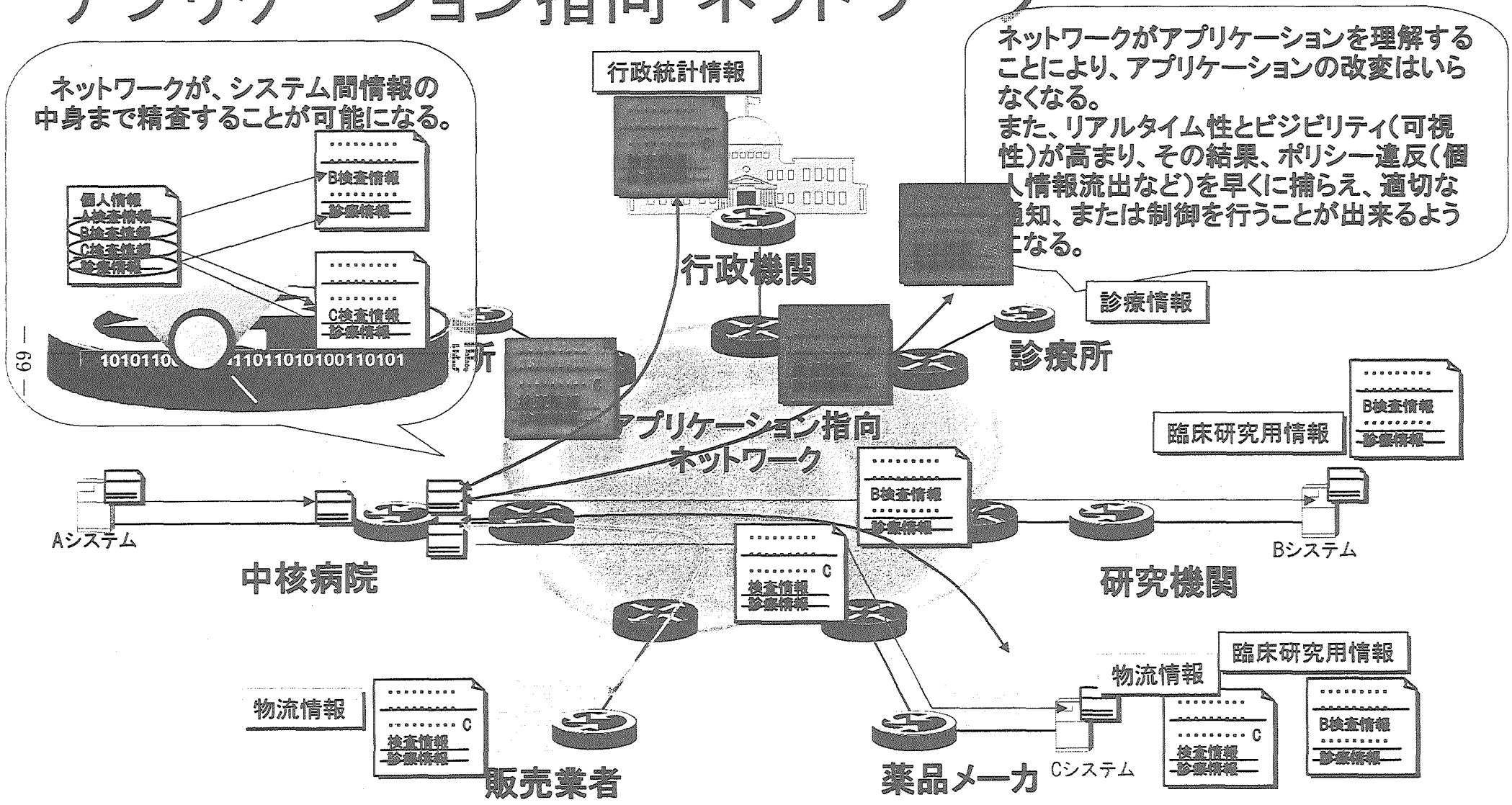
A-net リプレース 検討案



従来型 データネットワーク



ネットワークがアプリケーション言語を話す
アプリケーション指向 ネットワーク



目的指向型ネットワーク:研究用・診療用・行政用を同一インフラで実現

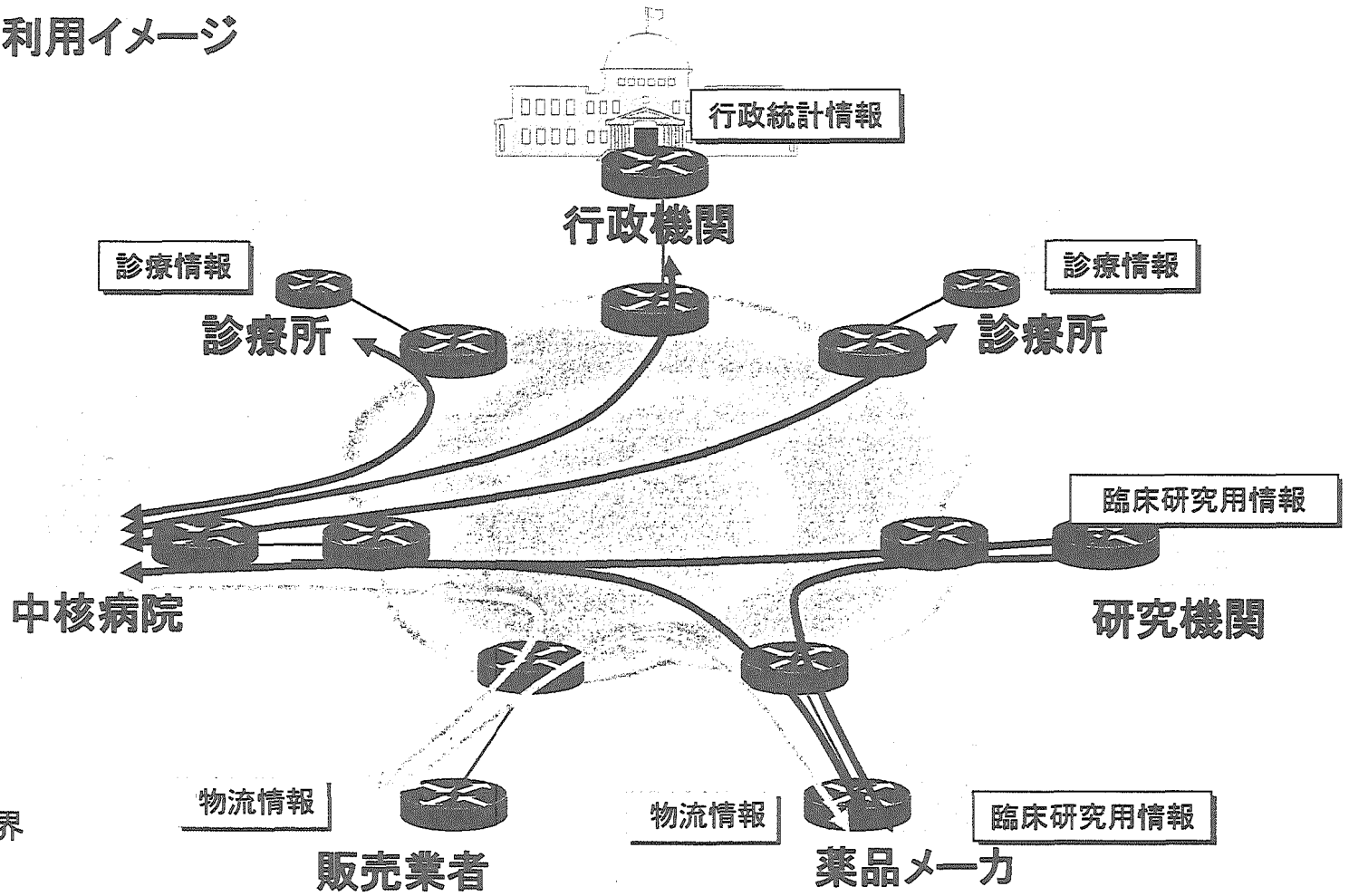
診療支援ネットワークの将来像

医療情報の相互利用イメージ

医療情報の相互利用

各機関システムの
コラボレーション

従来型ネットワークの限界



単一入力多目的利用：プライバシーの保護と利便性の両立

情報通信技術的検討

A-net運用開始時点では、インターネットを介してセキュリティを保った状態で施設同士をつなぐ技術である仮想専用線網の研究報告も医療分野においては、ほとんど行われていなかったが、現在ではさらに安全な技術が開発されており、A-netにおけるセキュリティ技術水準は過去のものになり、最新技術による更新が必要。

「個人情報の保護に関する法律」を踏まえ、プライバシー保護に役立つ最新のセキュリティ技術と臨床現場で利用可能な利便性を両立するための、目的指向型ネットワーク：研究用・診療用・行政用を同一インフラで実現可能性の検討。

A-netのシステム運用管理体制は、個人情報保護のポリシーにほぼ準拠していると考えられたが、パスワード認証だけでは不十分であり、指紋認証などの生体認証との組み合わせが必要。

今後の課題

一方、A-netのデータ項目は1998年に決められており、HAART(ハート)療法等に適応が不十分であり、早急に対応する必要がある。

疾病管理のシステムにおいて、個人情報保護法を踏まえた今後のエイズ対策に必要な臨床疫学研究を可能にする疾病データベースの設計を行う必要があると考えられた。

以上を踏まえ、来年度以降で具体的システムの提案と実証実験を行いたい。

厚生労働科学研究費補助金（HIV診療支援ネットワークを活用した診療連携の利活用に関する研究）

分担研究報告書

A-netにおける国立大学病院VPNとの連携運用の検討

分担研究者　木内 貴弘 東京大学医学部附属病院大学病院医療情報ネットワーク研究センター教授

研究要旨　A-netリプレースに向けて、A-netと国立大学病院側の接続方法の検討を行った。A-netは、現在独自のVPNを用いて運用がなされている。国立大学病院では、国立大学病院VPNが稼動しており、A-netも国立大学病院VPNと連携して運用する方がコスト的に有利であると考えられた。ただし、A-netのセキュリティのレベルを維持するために、国立大学病院VPN側にA-net専用Webプロキシーの設置等によるセキュリティ向上対策が必要である。また各国立大学病院で国立大学病院VPNへの接続の際してセキュリティ上の問題点がある場合も考えられるため、A-netによる個別対応が必要な場合も想定された。

A．研究目的

HIV診療支援ネットワーク（A-Net）は、国立病院（HOSPnetを活用）以外には、独自の専用VPNネットワークを利用して運用を行ってきた。国立大学病院では、平成１２年度より、全国立大学病院を結ぶ、国立大学病院VPNの運用を行っている。本研究の目的は、A-netリプレースに向けて、国立大学病院側の接続方法を検討することにある。

B．研究方法

国立大学病院VPNの現状分析を行い、研究班会議におけるA-netの問題点とその改善点の検討を踏まえつつ、A-netと国立大学病院VPNの連携の方法と問題点等について技術的な側面から検討を行った。

C．結果

国立大学病院VPNは、４２の国立大学病院が接続されているが、VPN機器接続の形態が各大学のネットワーク構成の制約によって異なっており、大学によっては、大学病院内部以外の大学内からのアクセスも可能となっている例が見られた。現行で、国立大学病院VPNは、国立大学病院の事務系の情報提供・データ収集に活用されており、患者情報を含む個人情報のやりとりは行われていない。

A-netで、国立大学病院VPNを活用する方法としては、まず単純にA-netセンターと国立大学病院VPNのハブである大学病院医療情報ネットワークセンターを相互接続する必要がある。これで国立大学病院内部のすべて端末からA-netが活用可能となるが、A-netではアクセスできる端末を厳密に制限する必要がある。このための方法として、大学病院医療情報ネットワークセンターにおいて、フィルターリング、専用Webプロキシーの導入する。専用Webプロキシーによって、IPレベル、IDとパスワードによる個人レベルの認証が可能な他、公開鍵証明書をA-net端末に導入することによって、厳密な端末の認証も可能である。

D．考察

A-netは、独自のVPNを用いて運用が行われている。このため、VPN機器の導入・設定、維持管理がすべてA-netの費用でまかなわれなければない。これに対して、国立大学病院VPNを活用する場合には、A-netサーバと大学病院医療情報ネットワークセンターの間をVPNで接続すれば運用可能であり、セキュリティ向上のための専用プロキシー等の導入コストを加えてもコスト的には非常に有利といえる。しかしながら、各大学の国立大学病院VPNへの接続形態には、セキュリティ上問題があるケースも見られるため、このような場合にはA-net独自のVPNによる個別対応を検討する必要があると考えられる。

Kosuge T, Kiuchi T, Mukai K, Kakizoe T for the Japanese Study Group of Adjuvant Therapy for Pancreatic Cancer (JSAP). A multicenter randomized controlled trial to evaluate the effect of adjuvant cisplatin and 5-fluorouracil therapy after curative resection in cases of pancreatic cancer. Japanese Journal of Clinical Oncology 2006 (http://jjco.oxfordjournals.org/にて公表中。印刷物は未刊。)

吉田謙一、木内貴弘. ビクトリア法医学研究所における医療関連事故予防への取り組み. 日本医事新報 4228:57-62, 2005

木内貴弘. インターネットで変わる臨床研究. 医療白書、日本医療企画、417-421、2005

乙津浩二、池永裕輝、村井伸昭、大塚健一、吉田元、門川英男、松葉尚子、木内 貴弘：大学病院医療情報ネットワーク OASIS システムの現状と今後. 第２５回医療情報学連合大会論文集 (CD-ROM)、2005

大塚健一、門川英男、村井伸昭、吉田元、松葉尚子、木内貴弘: 次期 UMIN 電子メールサービスの概要. 第２５回医療情報学連合大会論文集 (CD-ROM)、2005

村井伸昭、苅尾七臣、高山京子、下澤達雄、安東克之、門川英男、大塚健一、鎌田智子、乙津浩二、松葉尚子、木内貴弘: UMIN 学術雑誌論文投稿・査読管理システムの開発. 第２５回医療情報学連合大会論文集 (CD-ROM)、2005

松葉尚子、津谷喜一郎、大橋靖雄、内田英二、木内貴弘: 大学病院医療情報ネットワーク臨床試験登録システム (UMIN-CTR)の開発と今後. 第２５回医療情報学連合大会論文集 (CD-ROM)、2005

電子カルテの安全性確保に関する調査研究

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　電子カルテをはじめとする医療のIT化は単に医療機関の事務の合理化のために行われるのではなく、国民の医療の向上に役立つものであるべきである。IT化によって大きく国民の医療の向上に寄与する電子化診療情報の用途の一部として、医療機関間の情報交換である診療情報提供書と利用者である患者への情報提供が挙げられる。A-netはこの先進的な試みといえる。もちろん安全性確保が前提であり、A-netはこれに取り組み実績をあげてきた。しかし、A-net上の情報を活用する際に、同意等の問題を解決したとしても、A-netを離れたからの情報の安全管理にも配慮が必要になる。本研究ではネットワークから抽出した情報を利用する際に現時点でもっとも容易に実現できる可搬媒体で利用の安全管理を研究するために、医療機関間の診療情報提供書や患者への情報提供を実現するにあたっての安全確保の手段として、暗号化および電子署名の標準的な適応方法を確立した。

A．研究目的

高度情報通信社会の急速な進展、個人情報保護への関心の高まり、データ保護に関するＥＵ指令やHIPAA法に関連した米国規則など、諸外国のプライバシー保護、セキュリティの規制の変化等から、我が国においても保健医療分野での個人情報保護のあり方に関して、国際動向や現在のセキュリティ技術水準を踏まえた一定の方向性を示すことが緊急かつ重大な課題となっている。その一方で、高度な経済効率を達成しているわが国の医療において、経済的に破綻をきたさずさらなる医療の質の向上にはIT技術の導入は避けられない。医療情報システム全般に対しての安全指針は平成15年3月に厚生労働省が安全管理に関するガイドラインを示したところであるが、この指針はあくまでも医療機関内での医療情報の安全管理を中心に記載されたものであり、施設間の情報交換や患者等の利用者への情報提供に関しては部分的に触れられているにすぎない。本研究の目的はA-net上に蓄積された情報を二次利用する際に可搬媒体を利用することを想定し、その安全管理のモデルとするために、電子化診療情報提供書と患者への情報提供書をとりあげ、その安全管理の手段として電子署名と暗号化の手法の標準を示すことにある。

B．研究方法

電子カルテには様々な情報が格納されるが、その中には記載する医師等が自らの考えを整理するための事項や、病院内での事務処理のための事項、さらには電子カルテシステム自体の運用のための情報も含まれる。本研究が対象としている提供書はこれらの情報を含まない、患者に関する情報のみからなる。紙ベースの場合は記載量の制限から、取捨選別が必要であったが、電子情報では記載量の制限は緩く、多くの場合取捨選抜は必要ない。また医療機関間での情報提供と患者への情報提供の間に、若干の差はあるが、主に情報の受け手の理解力や受容性を考慮したものであり、検体検査、処方履歴、画像検査などの客観的事実はほぼ同じものと考えてよい。そこで、まず可搬媒体を用いた提供書のモデルを検討した。ネットワークではなく可搬媒体をモデルを検討したのは本研究班の全体の成果として期待されるセキュアなネットワークがわが国の基盤として確立するのは本年度中には期待できず、その一方で CD-R や DVD-R などの可搬媒体は安価で書き込みに用いる機器も用意に入手可能であるためである。つぎに責任の所在を明らかにし、改ざんを防止するための電子署名のあり方について考察し、その標準を提案した。さらに可搬媒体へ格納する際の暗号化について標準を提案した。なおこれらの標準案の作成にあたっては日本 HL7 協会の SIG の活動の一部としておこなったが、経費はすべて本研究班の研究補助金を使用し、混同はない。

C．研究結果

（1）可搬媒体での提供書モデルの検討。

診療情報提供書や患者等への情報提供書の電子化モデルはこれまで、いくつか試作されている。代表的なものは a.）吉原らが中心となって作成し、現在 MedXML コンソーシアムが保守・管理を行っている MML3.0 に基づくもの、b.）日本医療情報学会が作成した MERIT-9 診療情報提供書 ver. 2、c.）また静岡県で木村らが提案している MERIT-9 診療情報提供書 ver. 3 がある。これらはいずれも事実上の国際標準である HL7 CDA に準拠しているという共通点がある。前2者は CDA Release 1 に準拠し、最後の MERIT-9 診療情報提供書 ver 3 は CDA Release 2 に準拠している。これらはいずれの実証実験としての実装例があり、継続的に使用され、有用であることが証明されている。そこでこれらのすべてを本研究の対象とした。これはいずれも HL7 CDA に準拠しているために共通の特徴がある。本文は XML インスタンスであり、放射線画像のような非 XML インスタンスは外部参照ファイルとして結びつけることができる。

（2）電子署名規格の作成

電子署名はわが国には電子署名法があり、法律にしたがって電子署名であれば原則として記名押印に代えることができる。また厚生労働省は 2005 年 3 月に保健医療福祉分野認証局ポリシを公表し、医師等の医療従事者の公的資格を確認可能な電子署名基盤の整備を進めている。診療情報提供書には作成者である医師等の記名押印が求められ、また患者等に提供する情報提供書も責任の所在を明確にし、改ざんのないことを保障するために電子署名を施すことが望ま

しい。一方で XML インスタンスに対する電子署名は国際的に RFC 3275 として標準案が作成されており、またタイムスタンプを含めた署名技術も W3C で XAdES として提案されている。本研究で行うことはこれらの標準の適応方法を規定し、またこれらで不十分な点があれば追加することである。

まず不十分な点があるか、であるが、RFC3275 や W3C XAdES は基本的には XML インスタンスのみを対象としている。XML インスタンス内に非 XML オブジェクトを埋め込む技術は存在するが、先にあげた診療情報提供書のモデルはいずれば本分である XML インスタンスの外側に外部参照ファイルとして置くことを認めている。さらに診療情報の提供書では放射線画像や検体検査結果などの客観情報の多くは外部ファイルとして格納される可能性が高く、電子署名の影響が外部ファイルに及ばなければならない。前述の提供書モデルはいずれも外部ファイルを URI で指定しているために、URI の指定と同時に外部ファイルのハッシュ値とその計算に用いたハッシュ関数を本文である XML インスタンス内に格納すれば、本文に電子署名を施すことによって、外部ファイルを含めて責任の所在を明確にし、改ざんを検出可能とすることができる。そこで本研究で提案する規格にはこの仕組みを追加した。また XAdES は大きな規格で、署名延長も対応可能となっているが、本研究ではタイムスタンプまで、つまり XAdES-T までの実装を必須とし、多はオプションとした。また前述した厚生労働省が公表した保健医療福祉分野認証局ポシリに準拠した証明書、すなわち ISO 17090 に準拠した HPKI による電子署名を使用可能とし、署名アルゴリズムは RSAEncryptionWithSHA として、SHA は 128 ビットの SHA-1 の脆弱性が問題になっていることから、SHA-2（256 – 512 ビット）も含めた。

（3）暗号化規格の作成

医療機関間の診療情報提供書といえども可搬媒体に格納する場合は一時的にせよ患者等が所持することになる。紙ベースの診療情報提供書でも同様で、この場合、管理責任は患者等が所持している間は患者等にある。つまり紛失して中身が他人に見られても本人の責任である。これとアナロジーを考えるなら、可搬媒体の格納された電子化診療情報も患者等が所持している間は患者等に管理責任があることになる。しかし、格納されている情報は大量で、第三者に暴露した場合の危険性について、すべての患者が十分認識していると仮定することが合理的と言い切ることは難しい。可能であれば何らかの防御策を講じておくことが望ましい。解決策として暗号化が考えられるが、暗号化には副作用もある。暗号化された情報は復号できなくなる可能性があり、診療に関わる情報の場合、復号できない、つまり可用性が損なわれることは時には重要な問題になりうる。また暗号アルゴリズムやどのファイルを暗号化するかなどの暗号化の方法は様々であるが、これらをあらかじめ合わせておかないと復号はできない。また同じアルゴリズムでも鍵の選び方で暗号強度が異なる。一般に暗号強度を上げることは鍵長が大きくなることを意味し、鍵の管理を複雑にする。

対象となる提供書は第三者に見られてもそう大きな問題にならないような内容もあ

りうるし、知られることによって本人に重大な損害を与えかねない情報が含まれる場合もある。

以上のような観点から、本研究で提案した規格は、暗号アルゴリズムを 128 ビットの最大鍵長を持つブロック暗号のうち、ISO 18033 の Part 3 に記載されているものに限定し、また鍵長を 128 ビットまでの任意の長さに設定できるようにした。具体的には鍵のパディングルールを明確にし、例えば 4 桁の数字のような短い鍵長でも利用可能とした。また媒体に格納するファイルの中に、暗号化をおこなったファイルが何かを示す情報ファイルを置くことを義務付け、このファイルを暗号化しないように規定した。

D．考察

診療情報の IT 化には目的があり、医療機関によって様々な目的で IT 化を行う。A-net ではもちろん AIDS 診療をどこでも同じ水準で受けることができることが主な目的である。しかし、診療を向上させるためには A-net 上のデータの二次利用もかかせない。ネットワーク上ですべての二次利用に対応することは困難であり、情報をネットワーク外に取り出すことも将来的には考慮されなければならない。そのような場合に備えて、可搬媒体での情報の安全管理を研究しておくことは意義深いと考えられる。

本研究で提案した電子署名と暗号化の 2 つの標準案は A-net に限らず、一般の医療機関で扱う情報において可搬媒体で患者等を介して搬送したり、患者等に提供する場合の安全管理を満たすことを目指したものである。

電子署名は方法論的には確立されて久しくまた、わが国では制度的にも整備が進んでいる。しかしまだ実際の普及という点では十分とは言えない。これはわが国においては行政手続きと密接に関係した電子署名のみが先行整備されたためで、国民から見ればもともとあまり使われない用途から整備されたためかも知れない。これに対して保健医療福祉分野の公的資格を確認できる HPKI 電子署名はかなり頻繁に生成される診断書や診療情報提供書に用いられるもので、これが整備されることによって初めての広く用いられる電子署名基盤になる可能性がある。

しかし、診療情報提供書で見てもわかるように、署名対象となる文書は単純な構造ではない。診療情報は様々な形式の情報を含む、いわゆるマルチメディア情報であり、電子署名もそのことに十分配慮したものである必要がある。本研究で提案した規格はマルチメディア外部ファイルを URI およびファイル自体のハッシュ値および計算に用いたハッシュ関数を基本情報である XML インスタンス中に埋め込むことで、形式的には単純な XML 署名でありながら、複数のファイルからなるマルチメディア情報全体に電子署名の効果である責任の所在の明確化と改ざんの検出可能性を及ぼすものである。添付の規格書でわかるように対象を HL7 CDA に準拠した文書全体とし、外部ファイルの扱いは CDA の Release 1 と Release 2 で使い分けている。Release 1 では外部ファイルの参照に拡張を許しているために、Local Markup としてハッシュ値およびハッシュ関数種別を含む XML エレメントを定義することができる。しかし