表 5.5.1 対策案の比較

		セキュリティ	利便性	運用	コスト
インターネット回線	現行 VPN	△現在の水準に合わない	×専用端末が必要であり新拠点の追加ができない	△独自技術のため専門の技術者が必要となる	○運用できる人が限られため運用コストが高い。
	新 VPN（独自技術）	◎独自に開発をおこなうため強固である	○独自の技術のため互換性がない	△独自技術のため専門の技術者が必要となる	△開発、運用に多額の費用がかかる。
	新 VPN（汎用技術）	○現在の水準をみたしている	◎汎用性があり、接続形態に自由度がある	○一般的な技術のため運用の標準化が可能	◎一般的な技術のため運用の標準化が可能
専用線（IP-VPN 網等）		◎閉域網のためセキュリティーレベルは高い	△専用線を利用するため提供出来るエリアが限られる	○一般的な技術のため運用の標準化が可能	△拠点全てに専用線を引き込む必要があるため高コスト

対策案の比較検討の結果、汎用技術を実装した新 VPN である SSL-VPN を最優先で検討することが望まれる。

SSL はオンラインバンキングや電子商取引でも使用されており実績がある。PC に通常搭載されているブラウザには、SSL-VPN のクライアント機能があり新たにソフトウェアを導入する必要が無い。

SSL-VPN は A-net のセンター側で VPN(暗号化)装置を設置すれば、拠点側で VPN 装置を設置する必要がなく保守運用性やコスト面でも優れている。

5.5.2. エンドポイントセキュリティ

本項では、A-net のネットワークの終端(エンドポイント=End Point)に接続されるものとして、エンドポイントデバイスのセキュリティ対策についてまとめる。この対策を実装するには、あらかじめ「PC 端末利用手順」や「PC サーバ利用手順」等のエンドポイントデバイスに関連するセキュリティポリシを策定しセキュリティに対する要件を定義する必要がある。

(1) 想定される脅威

A-net のネットワークのエンドポイントに配置されネットワークプロトコルを介して接続される PC 端末、PC サーバには、機密性、完全性を要する重要なデータがおかれ、システムの内側から外側に向かって見ると、システム管理者にとっては最前線の防御点である。

また、反対にエンドポイントからシステムの内側を見ると、USB などのポートに接続されたデバイスを経由した情報漏洩、および悪意のあるソフトウェアの侵入という脅威がエンドポイントから発生することを想定する必要がある。悪意のあるソフトウェアは一般的なアンチウィルスソフトを利用することによってあるていどリスクを回避できるが、アンチウィルスの定義ファイルが更新されていない時期に発生する、ゼロディアタックには対処できない。

加えて、正当な利用者が使っている、正当な端末であるかという認証や、その端末がセキュリティポリシを順守しているかどうかという認証も必要な場合がある。ある程度セキュリティの確保された場所で病院関係者だけが操作していることが保証されている場合は、比較的安全であると言えるが、将来的に患者様が自宅から自分自身で操作する場合には、このような認証方法も検討すべきである。

(2) 対策

a) ゼロディアタックへの対策は、エンドポイントへの悪意のある動作やセキュリティポリシ関連の動作(悪意は無くとも状況により危険性がある動作)を判断し抑止するためのソフトウェアを使用することにより対策できる。ふるまいによる危険な動作を抑止するソフトウェアはアンチウィルスソフトウェアと同時に動作して最大の効果を発揮する。

これらのふるまい関連の危険な動作は次のようなものを想定している。

表 5.5.2 エンドポイントへの脅威と分類

脅威の分類	脅威
悪意のある動作	➢ オペレーティングシステムに対する不正な改ざん ➢ 意図しないファイルの削除、新規ファイルの作成 ➢ 意図しないプログラムのインストール ➢ バックドアを仕掛けるプログラムのインストール ➢ バッファオーバーフロー攻撃 ➢ DoS アタック ➢ メールソフト管理下のファイル(アドレス帳)への不自然、不合理なアクセス ➢ ネットワークリソースへの不自然、不合理なアクセス(ポートスキャン、DoS 攻撃など) ➢ P2P 関連(Winny など)のファイル交換ソフトウェアのインストール

ポリシー関連の動作 （悪意がない場合でも危険性がある。）	➢ ウェブブラウザなどからファイルをダウンロードさせるかどうか。 ➢ ダウンロードしたファイルを実行させるかどうか。 ➢ メールの添付ファイルを開封させるかどうか。添付ファイルの危険性を考慮する。 ➢ 着脱可能な記憶装置を使用許可とするか。着脱可能な記憶装置（USB メモリなど）経由での悪意のあるファイルの侵入や情報漏洩。読み出しと書き込みの許可、不許可の区別。 ➢ PC に内蔵されている、記憶装置を使うか。読み出しと書き込みの許可、不許可の区別。 ➢ メッセンジャーソフトを使用する際、プログラムをダウンロードさせるか。 ➢ 新規にプログラムをインストールさせるか。 ➢ 既にインストールされている、特定のアプリケーションを利用させるか。

b) ユーザ認証、端末認証に関しては、802.1x のような現在、標準的で実績のある認証方式の採用を検討する。

[802.1x 概要]

- LAN および MAN 向けに標準化された IEEE Standard （標準化終了：2001 年 10 月）
- Port-Based Network Access Control
  - ✓ ネットワークの入口（Switch Port, Wireless AP）でのユーザ認証とアクセス制御手段を提供
- LAN 環境でのユーザ識別によるセキュリティ確保を目的
  - ✓ 認証されていないクライアントからの通信を（認証要求を除いて）すべて遮断し、認証されたユーザにのみ通信を許可する
- 認証は RFC の EAP を使用 - （EAP – Extensible Authentication Protocol）
  - ✓ 802.1x は認証時の通信経路の暗号化を行わないため、別途 RFC に定義された EAP と言う技術を用いて通信経路の暗号化をおこなう。
  - ✓ 認証システムには RADIUS を使用 （RADIUS 側が EAP タイプを認識する必要がある）
- 802.1x 認証を標準でサポートする OS の登場
  - ✓ WindowsXP で採用

c) 802.1x 認証での「端末認証」と「ユーザ認証」による認証方式は、端末のセキュリティポリシ（「PC 端末利用基準」など）への準拠度合いは判断できない。

A-net のネットワークへ接続を試みようとする PC 端末に実装されているセキュリティ対策（アンチウィルスソフトウェアのインストールの有無や定義ファイルの更新の日付など）をセキュリティポリシに照らし合わせて検査し、その結果をもって、A-net のネットワークに接続させるか、させないかを判断する方が、802.1x 認証よりもセキュリティ強度が高くなる。

このセキュリティポリシへの準拠度合いの検査を、802.1x でおこなう「端末認証」と「ユーザ認証」に対して「状態認証」と定義する。

IT ベンダの何社かは、これに相当する機能を提供する製品を販売している。費用対効果を考えて実装の可否を検討することが望ましい。

5.5.3. アプリケーション指向のネットワーク

A-net のシステムに保存されているデータは、治療目的に限定すると個人情報と診療情報の連結は必須である。しかし研究目的に限って考えると、個人が特定できる個人情報ではなく、研究に必要な範囲にかぎり匿名情報で十分な場合があると考えられる。たとえば、名前や生年月日や住所を特定せずに、名前の変わりに識別番号を振って次のようなデータ構造を仮定する。

番号	性別	年齢範囲	居住地域	感染歴	発症歴	その他(個人を特定できない属性情報)
00001	男性	20-25	関東	4 年	2 年	

このような情報であれば、これまでA-netに登録することに対して同意が得られなかった患者様にも理解されやすくなるかもしれない。あるいは、もっと縮小された情報でも十分に目的を達することができる場合もあることも想定できる。

注) 個人情報の匿名的な取り扱いについては、データの内容が機密性の高いものだけに事前に、患者様との合意や法律や医療、技術関係の識者達との意見交換が必要であると考える。

このようなことを実現するには、A-netのセンターのデータベースサーバから患者様の情報を取り扱う場合は、患者様情報をネットワークに送り出す時点で匿名化された情報に変換する方法があれば良い。連携機関へは必要な情報のみ匿名化して送る、すなわち、サーバではなくネットワーク機器自身がアプリケーションを理解しデータの中身を精査し変換するようなソリューションである。
IT ベンダの何社かは、これに相当する機能を提供する製品を販売している。費用対効果を考えて実装の可否を検討することが望ましい。

5.5.4. ネットワーク境界部のセキュリティソリューション

A-net のセンターでは現在、ネットワーク境界部のセキュリティソリューションとして、ファイアウォールと VPN のみを利用しているが、現在のネットワークセキュリティの脅威から考えてファイアウォールだけでなく侵入検知装置や進入防御装置の導入の検討が必要になるかも知れない。

その場合、何台もネットワーク境界部のセキュリティソリューション製品を購入すると、導入コストも運用コストも非常に高いものとなる。

現在ではこれらの機能を複合化した製品があるので、セキュリティ要件を精査した上で、このような製品を A-net のセンターへの導入を検討することが望ましい。

以上

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

報　告　書

改訂履歴

改訂年月日	版番号	改訂理由・内容
2008 年 3 月 20 日	1.0	初版発行

目　次

1 はじめに

(1) 背景

『HIV 診療支援ネットワークシステム（以下、「A-net」とする)』は、患者さんのプライバシー保護を図りながら、患者さんの診療情報の一部をエイズ治療・研究開発センター（以下、「ACC」とする）のホストコンピュータに入力し、エイズ治療・研究開発センターとエイズ治療ブロック拠点病院、拠点病院をネットワークで結ぶことにより、患者さんが受診される病院相互で診療情報を共有し、HIV 診療を円滑にし、かつ患者さんの地元で質の高い診療を可能にすることを目的としています。[HIV 診療支援ネットワークシステム（A-net）の説明文書より引用]

しかしながら、A-net は平成 10 年に試験運用を開始したシステムであり、システムを構成するハードウェアやソフトウェアの老朽化に加え、サポート期限の切れたハードウェアやソフトウェアも散見されるようになってきている。このような状況下で、万が一大規模なトラブルが発生した場合には、システムの復旧や継続運用が不可能な状況に陥る可能性も考えられ、大きな問題を抱えている。

また、当時は最新のセキュリティ対策を講じていたものが、年月の経過とともに近年のセキュリティ管理手法とは乖離したものとなりつつあり、更には現在一般的に用いられる汎用技術ではなく、あまり使われなくなった独自技術を採用していることが、今後のシステム改修や継続運用にあたっては大きな障害となっている。

更に、患者の個人情報の取扱いやプライバシー保護をめぐり、強固なセキュリティの確保に努めたため、利便性という観点からみると満足のいくものではなく、蓄積されたデータ量とその内容からシステムそのものの利用価値も高いとはいえず、アクセス数も伸び悩んでいる状況である。

よって、現在の A-net に代わる次期 A-net の開発に向けて、現状の課題の整理を行うとともに、医師及び患者からも積極的に利用されるシステムの構築を目指して、その解決策や目指すべき方向について検討することとする。

(2) 基本的な考え方

情報システムは、人々の利便性や作業効率を高め、我々の生活の一助となるべき活躍を担うものである。よって、A-net についても、HIV の治療や研究開発に努める医師や患者にとって利便性や研究効率を高め、その成果によって治療負担の軽減や治癒率の向上、更には今後の治療や予防活動全般における研究に役立つことを期待されている。

患者のプライバシー保護は最重要課題ではあるが、高度なセキュリティ対策を施し見栄えの良いシステムを構築したとしても、それが利用されなければ研究への活用度が低くなる。

本研究においては、昨年度実施した、A-net セキュリティ監査の結果を基に記された「A-net セキュリティ監査報告書」で指摘された A-net の現状の問題点や次期 A-net の方向性の助言意見を踏まえ、次期 A-net のシステム開発において重点的に検討が必要と思われる「利便性の向上」、「セキュリティの確保」、「運用管理の向上」について、詳細に検討することとする。

また、A-net 自体の利便性の向上、利用価値の向上について検討するため、机上での検討に加えて、サンプル的な電子カルテシステムとして、株式会社ノーバメディコ製「MyProdoc」を用いた検証環境を構築し、現在の課題に対する対応策について検討する。

ア　利便性の向上

使いやすいシステム、使う価値があるシステムの開発を目指して、具体的な利便性向上策の検討を行う。

イ　セキュリティの確保

A-net の最重要課題であるセキュリティの確保について、様々な面から対策内容の検討を行う。

ウ　運用管理の向上

A-net のシステム全体の運用管理方針や効率的な管理のための各種手法の検討を行う。

(3)　現状の問題点

ア　技術上の問題点

昨年度実施した、A-net セキュリティ監査の結果、明らかになった技術上の問題点を【表 1-1】に記す。

【表 1-1　技術上の問題】

項　目	現在の問題点
アプリケーションサーバ	・ ハードウェアのサポート停止予定。 （一部のハードウェアは既に停止。） ・ ソフトウェアのサポートの停止。
VPN 機器	・ 平成 12 年度で現 IBM のトンネリング方式の VPN ソフトウェアの販売が終了となり、平成 13 年度と平成 14

	年度は、IBM の例外処理によりライセンスを供給されたが平成 15 年度以降は、新規参加施設募集を休止し現在に至る。 ・ ハードウェアのサポート停止予定。 ・ ソフトウェアのサポートの停止。
クライアント側の Web ブラウザ	・ Netscape Communicator4.75 という平成 12 年（2000 年）に公開された Web ブラウザが必要であり、Internet Exploler 6 が業界標準の現在では操作や新規参加の障壁となっている。
セキュリティ標準への準拠	・ 当初のコンセプトは先進であったが、開発から 10 年が経ち、現在のセキュリティ技術標準、セキュリティ管理標準から遅れ始めている。
技術の古さ	・ 物理的な機器と基本ソフトウェアがともに今の水準からすると古く、新しいコンセプトを受け入れ開発できる余地が無い。
性能問題	・ 上記に関わる問題でもあるが、ハードウェア機器のパフォーマンスが現在の水準からすると良くない。

イ　運用上の問題点

昨年度実施した、A-net セキュリティ監査の結果、明らかになった運用上の問題点を【表 1-2】に記す。

【表 1-2　運用上の問題】

現在の問題点
限定された施設でしか、自動取り込みができない。
自動取り込みができない施設では、入力に手間がかかる。 その手間が嫌がられて使われないという悪循環に陥っている。
端末買い上げによって、技術の進歩やセキュリティ標準の変化に容易に対応できない。
登録には患者の同意が必要であり、全数登録が難しい。
入力項目、内容の妥当性。
アクセスできる環境が限られる。

(4)　問題点の解決に向けて

現状の問題点を踏まえて、具体的な解決案についてそれぞれのカテゴリ毎に検討する。

ア　利便性の向上

- 場所を選ばず、どこからでも同じような環境で利用できる方法の検討
- 標準の Web ブラウザでアクセスが可能なシステムの検討
- 情報の連携による利便性向上策の検討
- 患者の個人情報など、システムとして管理するべき必要がある情報の精査

イ　セキュリティの確保

- 様々なセキュリティ対策について、効率的な適用についての検討
- 最新かつ汎用的な VPN 方式の検討

ウ　運用管理の向上

- 今後の運用として、ハードウェアなどのサポート切れによる影響が少ない運用形態の検討
- 標準技術、汎用技術を採用し、今後永続的に利用できるシステムの検討
- 職員の負担が少ないながらも、システムの現状が把握できる運用管理形態の検討

2 利便性の向上

(1) 市場動向

現在一般に普及している電子カルテシステムは、特定の端末からサーバへアクセスする「クライアント・サーバ型システム」か、端末内部に情報を保持する「スタンドアロン型システム」が大勢を占めている。また、これらは独自の院内ネットワークにのみ接続されており、他の医療機関との情報連携やデータ交換などは積極的に行われているとはいえない。

頻繁に新制度の発足や制度変更が行われる医療分野においては、これらの電子カルテシステム自体も最新の医療事情に対応するためには、頻繁に開発や改修を実施し、これを継続的に繰り返す必要があった。そのため、これらの開発や改修に合わせて、サーバだけでなく、利用する端末に対しても必要なソフトウェアの導入や設定変更などの作業が発生する場合もあり、運用負荷が高くなっている。

しかし、現在の情報システムの世界では、各端末に標準で導入されている Web ブラウザを用いてサーバにアクセスする「Web 型システム」が一般的になってきている。我々の身近なところでも、航空機や新幹線のオンライン予約システム、銀行や証券会社のオンラインバンキングやオンライントレードなどが例としてあげられる。

Web 型システムでは、サーバで集中管理を行うため、端末の新規導入やシステムの仕様変更のために、複雑な再構築や設定などの展開作業を必要としない。

また、様々なセキュリティ技術と併用することによって、インターネットに接続された世界中のどの端末からでも、セキュリティに配慮しながら、システムへのアクセスが実現している。

更には、一つのシステムで更新した情報が他のシステムにまで連携して反映されるなど、情報連携によって飛躍的に利便性が向上し、システムの利用範囲が拡大している。

これらの現状を踏まえて、より使い勝手が良く、医師の負荷を軽減するようなシステム、患者にも積極的に利用してもらえるようなシステムの方向性を検討する。

(2) 対策

ア　インターネット経由での利用

現在のシステムでは、アクセスできる環境が限られる（ACC や拠点病院などの限られた場所でしか利用ができない）という制約がある。セキュリティを考慮すると、A-net 稼働当時としては的を射た方法であったと推測されるが、インターネットや様々なセキュリティ技術が普及した現在においては、利用者にとって不便なシステムになっていると言わざるを得ない。

これらを解消するために、インターネット経由で、どこからでもどのパソコンからでも利用が出来るような環境作りが必要であるといえる。これにより、場所と時間を選ばずにシステムにアクセスできるため、利便性そのものは飛躍的に高まると期待できる。

しかしながら、インターネットは全世界とつながる公の場である。患者の情報など秘匿性の高いものを取り扱う本システムにおいては、様々な脅威に対する充分なセキュリティ対策を施す必要がある。必要と考えられるセキュリティ対策については、別項にて検討する。

イ　汎用パソコンでの利用

現在のシステムでは、専用のソフトウェア（Netscape Communicator）がインストールされた端末でしか利用できないなどの問題点がある。また、現在ではあまり利用されていないため、操作性の問題が指摘され、またA-netの開発や改修に対する障害の一因にもなっている。

しかし、現在では、一般的なWindows OSに代表されるパソコンが各家庭に普及してきており、街中にはインターネットカフェをはじめとして手軽にインターネットを利用できる環境が整備されてきている。

このような状況下で、特定の端末からの利用に限定することは、セキュリティ対策としては有効に機能するものの、それらのソフトウェアの配布などに係る手間と費用が発生し、効率的ではなく、また利便性を損なっている。

よって、一般家庭に広く普及しているパソコンから簡単に利用できるシステム、利用料が発生せず、かつ長期的なサポートが受けられるソフトウェアで利用できるシステムなどを開発する必要がある。

現在では、オンライン予約やインターネットバンキングをはじめとする様々なシステムにおいて、Windows OS標準のWebブラウザ（Internet Explorer）などの利用を想定したシステムが数多く開発・提供されており、次期システムにおいては一般に広く普及しているWebブラウザなどの利用を想定したシステム開発を検討するべきである。

ウ　リアルタイム処理

ホストを利用した旧来のシステムなどは、日中時間帯において利用者に対してサービスを提供し、夜間に『バッチ処理（又は、「一括処理」とも言う）』を実施して、更新されたデータの集計や反映及びデータ転送などを行うシステムが主流であった。

しかし、最近では利用者が入力した時点で直ちに情報が反映され（「リアルタイム処理」と言う）、また必要な複数のサーバ等に対してそのデータが転送されるような仕組みが一般的である。

次期システムにおいては、リアルタイム処理を前提として、常に最新の情報に触れることができるようなシステムを検討する必要がある。

また、リアルタイム処理を検討する上では、データ容量が大きくなる動画や画像データの取扱いについても慎重に検討し、必要最低限のサーバにのみ保持する仕組み作りや、必要時にのみ取り出すような仕組みを検討する必要がある。

エ　臨床情報の自動収集

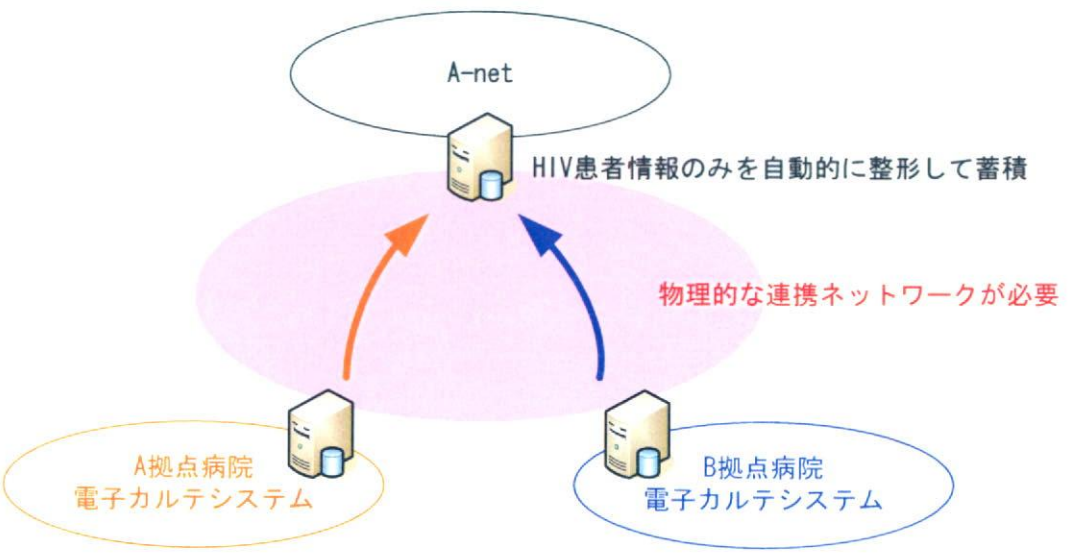
現在の A-net では、患者が来院（又は、受診）した際の診療情報や臨床情報などは、主に ACC や各拠点病院など（以下、「各拠点病院」とする）の独自の電子カルテシステムなどを用いて管理されている。それらの情報の中から、HIV 患者の必要情報だけを抽出し A-net に反映させる仕組みが充分に講じられておらず、医師による手入力が必要となっている。

このように A-net へのデータ入力の手間がかかるため、データ蓄積が円滑に進まず利用する価値が低くなり、よって手間を惜しんでデータ入力を行わなくなるという悪循環に陥っている。

次期システムにおいては、電子カルテシステムなどから該当する患者の診療情報や臨床情報などを自動的に抽出し、A-net 側のデータベースに反映する仕組みが欠かせない。

現在、データフォーマットに関する標準仕様が定められていないため、複数の電子カルテシステム間において、データ互換性の問題が発生する。これらのデータフォーマットの標準化や、どのメーカ製の電子カルテシステムを利用していても、A-net に情報を反映できる仕組みを検討する必要がある。

更に、各拠点病院独自の電子カルテシステムは、セキュリティの観点からも閉ざされた院内ネットワークにのみ接続されており、他の医療機関やインターネットへの接続を行っていないケースが多く、自動でのデータ連携には課題がある。そこで、各拠点病院間を閉域に接続する新ネットワークの構築や、そのネットワークと各拠点病院独自の電子カルテシステムとの接続についても検討する必要がある。しかしながら、これには各拠点病院内のセキュリティポリシーやネットワーク構成の変更を伴う場合もあるため、各拠点病院を巻き込み、早急に検討する必要がある。



【図 2-1　A-net と電子カルテシステムとの情報連携イメージ】

オ　管理する情報

現在は、個人情報保護法や各種ガイドラインなどによると、臨床研究への活用が目的であったとしても、原則として患者の同意の上で個人情報を管理する必要がある。この臨床研究における患者に対するインフォームド・コンセント（臨床研究の意義、目的、実施方法、個人情報保護の方法などの説明や同意の確認などの行為）が不十分であったりするため、提供される情報が少なく、利用者が低迷する要因ともなっている。

個人を特定できない情報の利用にあたっては、個人情報保護法の適用を受けないが、生年月日や性別、血液型などを組み合わせると個人を特定される場合も考えられるため、同法の適用除外に該当する可能性は極めて低いと言える。

そこで、臨床目的に限り、患者を容易に特定可能な個人情報（例えば、氏名、住所、電話番号など）を用いない場合に限っては、個人情報保護法の適用除外とするなど、関連機関との調整を行い、一定のルールに従って柔軟に利用できるように検討するべきである。

また、患者団体の代表者と研究責任者が代表で同意文書を交わすなど、今までの概念だけに囚われずに代替的な対応策を検討することが重要である。

更に別の手段としては、各拠点病院での初診時に、カルテ作成に係る個人情報の提供を依頼する際に、これらの個人情報について臨床目的にも利用することを明記（利用目的や、その範囲、苦情申出先などを周知）し、予め同意を得ておく方法などを広く模索する必要がある。

これらは現行法令やガイドラインだけでは対応できないケースも想定されることから、関連省庁を巻き込んだ対策が不可欠である。

一方、患者本人に対するデータ提供については、患者本人の過去の受信履歴や検査結果が一目で確認できることや、それらの詳細なデータの提供が求められる。また、同じような症状を持つ他の患者の状況を集約された統計データや臨床情報などとして、分析して分かりやすく加工したデータの提供が望まれる。

医師に対するデータ提供においても、通常の医療機関による外来・入院患者に対して管理する情報とは異なる情報の管理が必要である。膨大な不要な情報に埋もれて、目的の情報が即座に取り出せないのでは、本来の目的を達しているとはいえないため、A-net の本来の目的に立ち返り、必要最低限でかつ有益な情報を管理し利用できるように、そのデータの管理範囲をもう一度確認し、見直す必要がある。

今後のシステム開発においては、厳重に管理するべき必要がある情報の種類や、その重要度、利用範囲、開示区分なども合わせて検討する必要がある。

(3)　まとめ

A-net の利便性を向上させるため、このようにいくつかの施策が考えられるが、現状の A-net の環境と比較するとセキュリティレベルを落とさざるを得ない事項、他の拠点病院を巻き込んで検討する必要のある事項、また、関係省庁などを含めて慎重に検討する必要がある事項などに分類される。

システム開発や改修などが伴う技術的な対策については、現行の A-net のシステム改修が困難なことから、次期 A-net の開発までの実現は期待できないが、他の調整事項についてはいち早く検討を進めることが必要である。

これらの諸施策の実施によって、利便性の向上、利用価値の向上が図られ、A-net そのものの存在意義が高まることを期待する。

3 セキュリティの向上

(1) 市場動向

近年、情報セキュリティへの意識の高まりを受けて、多くの民間企業や中央省庁、及び各種団体において、情報資産を保護するためのセキュリティ対策が実施されている。

特にインターネットなどの外部ネットワークとの接続点においては、強固なファイアウォールを設け、不正アクセス、DoS 攻撃（又はサービス妨害）及びクラッキングなどの外部からの脅威に対する対策を積極的に講じている。

一方で、近年では自宅などから持ち込んだ私有パソコンによるウイルスの蔓延や、Winny に代表される P2P ソフトによる情報漏洩など、内部の要因による事故や事件が全体の 7 割以上を占めると言われるようになってきた。

これらに対処するために、内部ネットワークで利用者や使用する端末の認証を行うことで許可された利用者や端末に対してのみ、ネットワークやシステムの利用を許可するといった認証システムが注目を集めており、利用者の認証によるネットワークアクセス権限の制御や、端末へのパッチの適用状況などの環境をチェックし、一定のセキュリティレベルに達した端末のみを内部システムにアクセスできるようにする検疫システムなどの技術が、多くのメーカから提供されている。

また、技術的に強固なセキュリティ対策を施したとしても、それを利用する利用者の意識が低ければ、セキュリティ事故を完全に防止することはできない。よって、利用者に対する教育や注意喚起にはじまり、最低限順守するべき ID やパスワードの管理などの対策事項を明確にし、順守させる必要がある。

このような、インターネットなどの外部からの通信に対する外部セキュリティ対策、院内やサーバ設置箇所などイントラネット内部通信に対する内部セキュリティ対策、利用者に対する教育などを含む人的なセキュリティ対策などの要素を組み合わせて、多層的にセキュリティ対策を実施することで、大きなセキュリティ事故を防止する必要がある。

本項では、これらの外部からの脅威に対する対策方法、認証などの内部アクセス制御の技術、及び包括的なセキュリティ対策の主な実現方式や課題点、適用条件の検討を行う。

(2) セキュリティ対策の整理

A-net におけるセキュリティ対策について、まず、昨年度の A-net セキュリティ監査でも評価基準に用いた ISMS（Informatin Security Management Systems）の認証基準である「JIS Q 27001」の各項目に基づいて、主に誰が、どの装置がその対策の対象となるのかを【表 3-1】で整理する。

各項目は、「JIS Q 27001」の附属書 A「管理目的及び管理策」に準じる。

なお、対象となる○や△が記載のない項目については、各拠点病院を統括する組織管理