が推進されることが明確になり、安全管理GLに具体的な記載が求められるようになった。旧版の安全管理GLは医療情報の専門化とシステムを提供するベンダーおよび利用者の立場を代表するものが作業班を形成して作成したが、今回の改訂にあたってはこれらのメンバーとともに、回線提供者やネットワークサービス提供者も参加し、また通信サービスを所轄する総務省からもオブザーバが参加した。現在作業班として望みうる参加者はすべて参加していると考えることができる。

改定は主に旧版の6.9章を全面改定する形で行われている。ただし災害対策等が追加され、章番号は6.10に変更されている。

安全管理GLはA：制度的な要求事項、B：解説、C：最低限のガイドライン、D：推奨されるガイドラインという構成をとっているが、6章全体の制度的な要求事項は個人情報保護法および関連ガイドラインであり、6.10章に特別に加わった要求事項はない。したがってこの章もAはなく、Bの解説から始まっている。Bは3つのパートに分かれており、B-1は総説、B-2は具体的な要求事項、B-3は採用する通信サービス別に考慮すべき点を述べている。総説からしだいに詳細な解説に移行していると言ってよい。B-1は主に責任分界点について述べられているが、6章全体の中で、この章でだけ、一つの医療機関等で完結しない事象を取り扱うことを考えると当然と言える。責任分界点には2つあり、一つは情報の管理責任の分界点、もう一つは安全管理の責任分界点である。

情報の管理責任は情報の主権者である患者等にとって開示・訂正・利用の停止を必用に応じて求めることができる対象がどの事業者であるのかを明確にすることと言い換えることができる。個人情報保護法には他の事業者に情報を提供する場合を「委託」と「第三者提供」に分けている。委託の場合、管理責任は提供元事業者にあり、提供先事業者が個人情報保護に関する適切な対処をおこなうように監督する責務は提供元事業者にある。つまり患者等に対する窓口は提供元事業者だけである。その一方で委託に際してはあらかじめ明らかにされた利用目的の範囲であれば通知や同意の必要はない。これに対して第三者提供は個人情報保護法等で例外として記載されている場合を除いて、患者等への通知と同意が必要である。その一方で管理責任は提供先事業者に移動する。つまり提供元事業者が提供先事業者を監督する責務はない。

安全管理の責任分界点は前記の管理責任の分界点とはレイヤが異なる。患者等から見れば安全管理責任も情報の管理責任の一部であり、違いはない。しかし責任を負う側の観点で考えれば、要求されるのは所謂「善良なる管理者の注意義務」であり、この義務を果たすために通信にかかわるプレーヤの役割分担を明確にする必要がある。たとえばベストエフォートの接続サービスだけ提供する通信事業者と両端の事業者だけが存在する場合、相手の確認や経路上の守秘は両端の事業者の双方またはいずれかの責任であり、通信事業者にはこの責務はない。これに対して両端の事業者に設置された通信機器の認証と経路の暗号化を提供する通信事業者の場合、両端の事業者は通信事業者と正しく契約することで分担すべき役割を減らすことが可能になる。

B-2は一般的な要求事項の解説であり、B-3で専用線、ISDN、IP-VPN、インターネットなどに分けて詳細に得失および留意点を解説している。しかしその一方でどのような通信種別を選択する場合でも提供元事業者内で充分な情報セキュリティを確保することを求めている。これには2つの意味があり、一つは通信経路でいかに安全性を確保しても、起点・終点の事業者内でいい加減な情報の安全管理を行えば全体としての安全性を確保できないという、いわば当たり前の事実の指摘である。もう一つは通信経路に流す前に情報自体に一定の安全対策を求めている。通常は暗号化に相当する対策である。

CはB-1、B-2、B-3から当然帰結する指針ばかりであり、6.10章にはDはない。

D．考　察

安全管理GLの改定に関しては、B-1の責任分界点の記述に関して考察を加える。ここで記載されている委託と第三者提供の区別は個人情報保護法に一定の理解があれば当たり前のことであるが、保健医療福祉分野ではともすれば曖昧なままで情報提供が行われることもないとはいえない。たとえば遠隔画像診断を例に考えると、画像診断自体は検体検査と同様に委託業務と考えるのが自然である。しかし、もし、診断に用いた画像情報を後日の参照画像とするために、あるいは症例研究のために診断機関側で保存した場合は単純な委託とは言えない可能性がある。保存期間が限定されており、保存中期間中は提供元医療機関が監督を行っていれば委託であるが、そのような契約でない場合は第三者提供と考えざるとえない。

現実に病理検査や遺伝子検査などにも同様の場合が存在し、しかも現状では委託と第三者提供の区別がかならずしも明確でない場合もあると思われる。オンライン化した場合に限らないのではあるが、あらためて

注意喚起が必要で、その意味で安全管理 GL の記載は重要と思われる。ただ、結果の項で述べたように、レイヤの異なる安全管理に関する責任分界点と連続して述べられており、ややわかりにくい印象があり、将来の改善点と考えられる。

E. 結　論

医療情報システムの安全管理に関するガイドラインの改定について調査と考察おこなった。妥当かつ必要な改定であるが、やや表現がわかりにくい点があった。

F. 健康危険情報

特になし。

G. 研究発表

論文発表

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。

次期 A-net の運用形態の理論的検討

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 は、従来専用の VPN 網を用いて、運用が行われてきた。この方式は、各医療機関毎に VPN 機器とファイアウォールを含めたネットワーク接続形態の変更が必要であり、膨大な費用を要していた。本研究では、次期 A-net システムの運用形態についての検討すべき論点とその解決策の検討を行った。その結果、SSL-HTTP にクライアント認証もしくは生体認証を組みあわせた形によるシステムの運用が現実的で、セキュリティ面でも必要に足ると思われた。

A．研究目的

HIV 診療支援ネットワーク（A-Net）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。このため、ファイアウォールを含めたネットワーク接続形態の変更と VPN 機器の導入が必要であり、非常に導入経費が高価である他、維持費用もかさんでいた。

本研究の目的は、A-net リプレースに向けて、今後の安全で効率的な A-net の運用形態について理論的な検討を行うことにある。

B．研究方法

従来からの A-net の現行システムの状況と問題点を前提にした上で、A-net 次期システムの構想についてのセキュリティ維持・向上の視点から理論的に検討を行った。

C．結果

ネットワーク上のデータの安全確保のための視点として、(1)通信内容の機密性の確保、(2)通信相手の認証、(3)通内内容の改ざん防止が要件として挙げられる。以下のこの３点からの A-net の現状と今後の運用形態の検討結果を示す。

(1)通信内容の機密性の確保

従来、VPN を活用して機密性の確保を行ってきた。A-net 運用開始当時と比較して、SSL-HTTP 対応のブラウザーが普及が進んでおり、その 99%以上は 128 ビット以上の暗号に既に対応している。今後は、SSL-HTTP による保護で必要に足ると思われる。

(2)通信相手の認証

VPN では、ID、パスワードによる認証の他、お互いサーバと医療機関との間で VPN 機器による相互に認証が行われている。SSL-HTTP を利用した場合でも、ID、パスワードによる認証は行われるが、SSL-HTTP では、サーバ側認証にのみでクライアント側の電子認証は行われていない。この点は、現行レベルのセキュリティよりも低下してしまうと考えられる。これを防ぐ方策として、サーバ側が、WWW ブラウザ用のクライアント公開鍵証明書によって、クライアント側ブラウザーもしくは個人を認証する方法が考えられる。また適当な生態認証の方法を組み合わせる方法も考えられる。

(3)通信内容の改ざん防止

現行の SSL-HTTP でも現行の VPN レベルの改ざん防止対策はとられていると考えられる。

D．考察

時間の経過による技術の進展により、セキュリティ保護技術は進化・発展を続けており、A-netもこれに合わせた進化・発展が必要である。特にSSL-HTTP対応ブラウザーの普及、SSLによる暗号の鍵長の延長によりSSL-HTTPによるソフトウエアベースでの安全な通信が可能となってきている。

現行のA-netは、VPN機器を用いて独自のVPN網を構築して運用が行われている。このため、個別医療機関毎にファイアウォールを含めたネットワーク接続形態の変更作業が必要であり、専用VPN機器の導入・設定等も含めて、すべてA-netの費用でまかなわれなければない構造になっており、非常に高価なシステムになっている。専用ハードウエア機器の使用により、保守・更新経費も将来に継続してわたってかかってくる。

今後は、SSL-HTTPを活用したソフトウエアベースのセキュリティ保護技術を活用することによって、導入・運用経費の大幅な削減が重要であると思われる。クライアント側認証のセキュリティ低下を補うためには、クライアント認証もしくは生体認証等の対策が必要であるが、そのの具体的な内容については、今後更に検討が必要である。

E．結論

早急に新システムへの移行が望ましい。

F．健康危険情報

なし

G．研究発表

1) 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 36:159-165, 2006
2) Sano Y, Adachi M, Kiuchi T, Miyamoto T. Effects of nebulized sodium cromoglycate on adult patients with severe refractory asthma. Respiratory Medicine 100:420-433, 2006
3) Matsuba H, Kiuchi T, Tsutani K, Uchida E, Ohashi Y: The Japanese perspective on registries and a review of clinical trial process in Japan. Clinical Trial Registries - Practical Guide for Sponsors and Researchers of Medicinal Products, Birkhäuser Verlag, 83-106, 2006
4) Kawai S, Hashimoto H, Kondo H, Murayama T, Kiuchi T, Abe T: Comparison of Tacrolimus and Mizoribine in a Randomized Double-Blind Controlled Study in Patients with Rheumatoid Arthritis. Journal of Rheumatology 33(11):2153-2161
5) 木内貴弘、中島範宏、吉田謙一.異状死症例データベースの構築と運用、病理と臨床 24(7):753-756, 2006
6) 吉田謙一、木内貴弘．ビクトリア州法医学研究所における事故予防と医療関連死調査の取り組み．判例タイムズ 1209、54-59, 2006
7) 木内貴弘、青木則明. UMINとヘルスリテラシー、体の科学 September(250):68-71、2006
古川裕之、石川洋一、大津洋、小出大介、木内貴弘．臨床試験データの電子的伝達の標準化に関するアメリカ合衆国視察訪問 —米国視察報告より．月刊薬事 48(11):1769-1778, 2006
8) 木内貴弘. 臨床試験登録の現状と今後．日本臨床血液学会雑誌 47(7):564-570, 2006
9) 木内貴弘.情報システムの活用とセキュリティ．臨床試験の進め方、南江堂 118-121, 2006

H．知的財産権の登録・出願状況

なし

国立国際医療センター 殿

A-net セキュリティ監査報告書

Version 1.0

2007 年 3 月 28 日

目次

1. はじめに

1.1. 本書について

本書は、「HIV 診療支援ネットワークシステム(A-net)」(以下、A-net と略)の現状に対するセキュリティ監査報告と最新の情報セキュリティ標準やネットワークコンピュータ技術を踏まえた、「HIV 診療支援ネットワークシステム(A-net)」の将来的な"あるべき"姿について記述したものである。

本書の目的を次に示す。

① A-net に対するセキュリティ監査をおこない、不適合事項を明確にし改善への助言をおこなう。
② セキュリティ監査の結果を踏まえて、最新の標準や技術を踏まえた次期 A-net のあるべき姿をセキュリティ面から論じたものである。

2. 導入区分

A-net のセキュリティ監査をおこなう上で、A-net のシステムとしての概念を理解する事が必要である。ネットワークは、点であるデバイスをシステムの概念に従い、点から線へと有機的に結びつかせ、システム利用から得られる効果を最大にするための支援をおこなう。

セキュリティ技術やセキュリティ管理は A-net 上を流れる医療情報を含む個人情報を外部の脅威から保護し、正当な権限を持つものが安心して利用するための支援をおこなうものである。

セキュリティ監査をおこなうためには、システム概要の把握し、そこで利用されているセキュリティ技術やセキュリティ管理を把握することが必須である。

本章では、A-net のシステムを理解するためのシステム概要を記載する。

2.1. A-net の概要

A-net の概要および目的は、Web サイトに公開されている情報により下記に引用する。

1999 年 12 月 1 日

HIV 診療支援ネットワークシステム総括管理者（厚生省国立病院部政策医療課長）

1. システムの目的

「このシステムは、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。

あわせて、患者さんの氏名・住所・電話番号を除く診療情報を集積し、HIV医療に関する質の高い研究に活用することも目的としています。」

「HIV診療支援ネットワークシステム（A－net）について」

http://www1.mhlw.go.jp/topics/a-net/tp0114-1_12.html

（平成 11 年 11 月 8 日 最終更新）より。

すなわち、ネットワークに接続されたコンピュータシステムを利用することによる医療連携と HIV 医療に関する質の高い研究に活用することを目的としている。

3. 概要区分

3.1. セキュリティ標準

A-netのセキュリティ監査をおこなうにあたり、セキュリティ監査のベースラインとなるセキュリティ標準として日本規格協会発行の、JIS Q 27001:2006 (情報セキュリティマネジメントシステム-要求事項) を採用した。

JIS Q 27001:2006は、ISO/IEC 27001:2005の日本語版であり、日本情報処理開発協会(JIPDEC)の情報セキュリティマネジメントシステム(ISMS認証基準 Ver. 2.0: Information Security Management System Ver. 2.0) の改訂版でもある。

JIS Q 27001:2006を採用した理由を次に記す。

[理由]

- 現時点での国際的なセキュリティ標準であり、企業や団体における適切な情報セキュリティ管理体制、管理策や認証基準として社会的な認知度が高い。
- 情報セキュリティマネジメントの観点で、網羅性があり、漏れが少ない。
- 平成19年3月1日時点で、厚生労働省より意見を求められている、「医療情報システムの安全管理に関するガイドライン(第2版)」でも、JIS Q 27001:2006で言うところのISMS的な考え方が取り込まれており、整合性がある。

また、昨今の情報セキュリティに関連するインシデント(事件、事故)を鑑みて、コンプライアンスとして次の法律、ガイドラインを参考にし、JIS Q 27001:2006 の不足部分を担保する。

[参考とする法律、ガイドライン]

- 「プライバシーマーク制度」
- 「個人情報保護に関する法律」(通称「個人情報保護法」)
- 「不正アクセス行為の禁止等に関する法律」(通称「不正アクセス禁止法」)
- 「電子署名及び認証業務に関する法律」
- 「The Health Insurance Portability and Accountability Act of 1996」健康保険のポータビリティとアカウンタビリティに関する法律 (通称「HIPPA」)

加えて医療分野における情報システムのガイドラインということで、厚生労働省より公開されている次の情報も参考にする。

[厚生労働分野の参考とするガイドライン]

- 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン(平成16年12月24日通達)(平成17年8月5日修正)
- 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」に関するQ&A(事例集)

（平成 17 年 8 月 5 日）

・ 「医療情報システムの安全管理に関するガイドライン 第 2 版（案）」

これは正式版ではなく、本セキュリティ監査時で「意見募集中案件」であったが前版に比べて、より現状の情報技術に対応しているので、こちらを参考にする。

3.2. セキュリティ監査の範囲

JIS Q 27001:2006(情報セキュリティマネジメントシステム-要求事項)の付属書Aに記載されている情報セキュリティの管理策は次の11分野に分類される。A-5, A-6などとあるのは、付属書Aの管理番号である。

① セキュリティ基本方針 (A5)

② 組織のセキュリティ (A6)

③ 資産の分類および管理 (A7)

④ 人的セキュリティ (A8)

⑤ 物理的および環境的セキュリティ (A9)

⑥ 通信および運用管理 (A10)

⑦ アクセス制御 (A11)

⑧ 情報システムの取得、開発および保守 (A12)

⑨ 情報セキュリティインシデント管理 (A13)

⑩ 事業継続管理 (A14)

⑪ 順守 (A15)

上記の11分野の中の「情報セキュリティ基本方針」そのものや「組織のセキュリティ」や人の雇用等に関係する「人的セキュリティ」は本セキュリティ監査の範囲外とし、他の分野のネットワーク セキュリティとシステム セキュリティに関連する項目に重点をおいた。すなわち、

- 資産の分類および管理 (A7)
- 物理的および環境的セキュリティ (A9)
- 通信および運用管理 (A10)
- アクセス制御 (A11)
- 情報システムの取得、開発および保守 (A12)
- 情報セキュリティインシデント管理 (A13)
- 事業継続管理 (A14)
- 順守 (A15)

について監査をおこなった。

3.3. 対象システムのセキュリティ標準への準拠状況

A-net試験運用開始時が平成10年(1998年)であったせいか、公開されている資料を閲覧する限り、現在の社会的認知度の高い標準に準拠したセキュリティ技術やセキュリティ管理手法を適用しているわけではないようである。

ただし、厚生省保健医療局国立病院部政策医療課様より、web にて公開されている情報である、「HIV診療支援ネットワークシステム(A－net)について」(http://www1.mhlw.go.jp/topics/a-net/tp0114-1_12.html) を読む限り、「個人情報の保護」、「コンピュータウィルス対策」、「システムの無停止運用」、「大規模災害時の対策」など、情報セキュリティの3要素である、機密性、可用性、完全性に加えて真正性、責任追跡性、信頼性などの考え方を取り入れており当時のセキュリティに対する一般社会の意識から類推すると先進的な考え方を取り入れていると言える。

また、当該webサイトに、そのような記述があるわけではないが、通商産業省(平成10年当時)により制定されていた「情報システム安全対策基準」平成9年9月24日最終改正版の内容は反映されているようである。

3.4. 情報資産

3.4.1. 情報資産の洗い出し

セキュリティ監査をするためには、「何」を「どんな」脅威から守るにあたり、その対策（管理策）の有無を調べ、次にその対策（管理策）が存在した場合でも、その対策内容が必要十分に有効であるか、必要十分に機能しているかどうかを検討しなければならない。このためには、守られるべき情報資産を洗い出して特定する必要がある。

3.4.2. 情報資産区分

A-netの情報資産を大きく分類すると次のようになる。

[情報資産区分]

1. パソコン、サーバ、ネットワーク機器などの物理的な情報資産。
2. パソコン、サーバに保管されるデータやソフトウエアなどの電子的（光学的、磁気的なものも含む）な情報資産。ネットワークに流れるデータも含む。
3. 紙や媒体などに含まれる情報資産。
4. 人的情報資産

本セキュリティ監査では、1.の「物理的な資産」、2.「電子的な情報資産」と3.の「媒体などに含まれる情報資産」も2.の「電子的な情報資産」と便宜上同じ範疇で考える。

3.4.3. A-netが取り扱う物理的な情報資産

A-net のサーバルームに置かれている物理的な情報資産は次のようなものがある。

情報資産の内容	各種サーバ類
	各種クライアント類
	ネットワーク機器
	媒体そのもの
	ケーブル類
	電源関係（2 重化電源、無停電電源装置など）

3.4.4. A-netが取り扱う電子的な情報資産

サーバ内、クライアント内、ネットワーク上に関わらず、次のような電子的な情報資産がある。

情報資産の内容	操作者の情報
	患者情報（氏名、生年月日、保険種類、住所、投薬情報、副作用情報、アレルギー情報など患者個人に付随する情報）
	コンピュータ基本ソフトウェア
	アプリケーションソフトウェア

3.5. 脅威と脆弱性

3.5.1. 脅威の分析

A-net の情報資産に対する脅威(リスク)は、完全性、機密性、可用性の観点で次のものを想定する。

表 3.5.1 脅威の分析

人為的脅威 意図的、計画的脅威	偶発的脅威	環境的脅威
不正侵入	送信エラー(送信先間違い)	地震
ウィルス、ワーム、スパイウェアなど	悪意のあるソフトウェア	火災
悪意のあるソフトウェア	ソフトウェアエラー(バグなど)	ちり、ほこり
成りすまし	要員不足	湿気
盗難	要員のスキル不足	ハードウェアの物理的な故障
ソフトウェアエラー(意図的なバグ)	湿気	ハードウェアのサポートがなくなる
操作ミス	停電	ソフトウェアのサポートがなくなる
湿気	火災	
火災		

3.5.2. 脆弱性の分析

A-net の情報資産に対する脆弱性を検討した。ここで検討した「脆弱性」の定義は、脅威の発生を起因する可能性のある情報資産固有の弱点を想定している。

脆弱性自体は、それだけでは障害とはならないが、脅威を顕在化させ、損害や障害を発生させてしまう可能性がある。

表 3.5.2 脆弱性の分析

脆弱性の分類	脆弱性の例	脅威の例
物理的、環境的	入退室設備の不備	盗難
	電源設備の不備	停電、誤作動
	災害を受けやすい環境（例：地盤、川や海に近いなど）	洪水、地震、台風
ハードウェア	極端な温度、湿度	故障、誤作動
	記憶メディアの不良	故障、情報漏洩
	老朽化	故障、代替部品の入手
ソフトウェア	不完全な仕様	ソフトウェアバグ、誤作動
	アクセス制御が不完全	成りすまし、改ざん、情報漏洩
	パスワードの不備	不正アクセス、改ざん、情報漏洩
	監査証跡（ログ）が取れない	不正アクセス
	バックアップの不備	障害発生時の復旧不能
	ドキュメントの不備	操作ミス
	サポート期間の終了した基本ソフトウェアやアプリケーションソフトウェア	放置されたセキュリティホール、最新の標準との不整合による不具合
通信	保護されていない通信経路	盗聴、情報漏洩
	ケーブル接続、配線の不備	通信傍受、通信不能
	暗号化されていない通信	盗聴、情報漏洩

3.6. 情報資産の評価

洗い出した「情報資産」について、情報資産の価値を評価する場合は、次のような手順になる。

表 3.6.1 情報資産の評価

機密性(Confidentiality)区分	個人情報
	関係者外秘情報（部門外秘情報）
	システム関係の情報
	公開情報
完全性(Integrity)区分	データの誤りや情報の落ちがどのレベルまで許されるか
可用性(Availability)区分	どのくらいシステムが使えなくても耐えられるか

機密性、完全性、可用性の分野で、上記の表の観点でポイント化するが、A-netという重要な「個人情報」を扱う場所での「情報資産」の保護という観点で、公開情報を除き、すべての個人に付随する「情報資産」は最重要「資産」分類として守られるべきものとしてセキュリティ監査をおこなった。

3.7. セキュリティ監査の実施方法

本セキュリティ監査の実施方法であるが、A-netそのものが非常にセキュアなシステムのため、実システムを対象にしたポートスキャンやペネトレーション攻撃をおこなうことによる脆弱性検査をおこなうことができなかった。

また同じ理由でA-netそのものの、詳細なシステム仕様書、設計書、プログラムのソースコードを閲覧することによる精査もできなかった。加えてA-netの実環境におけるサーバやネットワーク機器などの設定情報を閲覧することによる調査ができたわけでもない。

このような背景から、本セキュリティ監査の入力情報は主に次にあげるものである。

表 3.7.1 セキュリティ監査の入力情報

文書関係	HIV診療支援ネットワークシステム(A－net)について 厚生省保健医療局国立病院部政策医療課より、web にて公開 http://www1.mhlw.go.jp/topics/a-net/tp0114-1_12.html (平成 11 年 11 月 8 日 最終更新)
	平成 18 年度 HIV 診療支援ネットワークシステム保守運用業務仕様書 (IBM 様より受理)
	A-net 構成概要図 (IBM様より受理)
	A-net 2006部会用資料 (国立国際医療センターエイズ治療研究開発センター様より受理)
聞き取り調査	医療関係者、A-netシステム開発ベンダ担当者への聞き取り
操作関係	A-netの保守(試験)系システムへの操作見学と実操作

ここに記した情報と日本規格協会発行の、JIS Q 27001:2006 (情報セキュリティマネジメントシステム-要求事項)の附属書A(規定)管理目的及び管理策の項番に沿って可能な限りで助言型のセキュリティ監査をおこなった。

3.8. セキュリティ監査

JIS Q 27001:2006(情報セキュリティマネジメントシステム-要求事項)の付属書 A に従ってセキュリティ監査をおこなった。A-7, A-8 などとあるのは、付属書 A の管理番号である。管理策の全文は著作権法の関係で記載していない。

それぞれの項目について実施状況を下記の区分でコメント記入した。

レベル	判断基準
0	該当しない。範囲外。
1	整備していない。
2	整備している。
3	運用している。
4	継続的に改善している。

3.8.1. 資産の管理

A.7 資産の管理		
A.7.1 資産に対する責任 目的:組織の資産を適切に保護し, 維持するため。		
番号	管理項目	実施状況
A.7.1.1	資産目録	4 A-net のハードウェア資産、ソフトウェア資産は台帳等により目録が作られ管理されている。(保守運用業務仕様書に記載。)
A.7.1.2	資産の管理責任者	4 管理責任者は指定されている。(保守運用業務仕様書に記載。)
A.7.1.3	資産利用の許容範囲	4 A-net のハードウェア資産、ソフトウェア資産およびそれらに含まれる電子的な情報資産は利用範囲について明確に文書化され実施されている。
A.7.2 資産の分類 目的:情報の適切なレベルでの保護を確実にするため。		
番号	管理項目	実施状況
A.7.2.1	分類の指針	4 分類されている。(保守運用業務仕様書に記載。)
A.7.2.2	情報のラベル付け及び取扱い	4 A-net の目的に従い、ハードウェア資産、ソフトウェア資産、電子的な情報資産は型番、シリアル番号などにより分類され管理されている。(保守運用業務仕様書に記載。)

3.8.2. 物理的及び環境的セキュリティ

A.9 物理的及び環境的セキュリティ		
A.9.1 セキュリティを保つべき領域 目的：組織の施設及び情報に対する認可されていない物理的アクセス，損傷及び妨害を防止するため。		
番号	管理項目	実施状況
A.9.1.1	物理的セキュリティ境界	4　サーバ類、ネットワーク機器のある区画（以下、センターと略）は、物理的に保護されている。（保守運用業務仕様書に記載。）
A.9.1.2	物理的入退管理策	4　適切な入退室管理が行われている。（保守運用業務仕様書に記載。）
A.9.1.3	オフィス，部屋及び施設のセキュリティ	1　明確な記述が見当たらない。
A.9.1.4	外部及び環境の脅威からの保護	4 センターに関しては、火災、地震対策など環境の脅威からの保護策はある。（聞き取り調査による。）
A.9.1.5	セキュリティを保つべき領域での作業	4　機密管理についての内部教育や機密文書の取り扱い規定などにより担保されていると考える。（保守運用業務仕様書に記載。）
A.9.1.6	一般の人の立寄り場所及び受渡場所	4　センターは物理的に隔離されており、入退室管理策も策定されており問題ないと考える。（保守運用業務仕様書の記載内容より判断。）
A.9.2 装置のセキュリティ 目的：資産の損失，損傷，盗難又は劣化，及び組織の活動に対する妨害を防止するため。		
番号	管理項目	実施状況
A.9.2.1	装置の設置及び保護	4 保護されている。（聞き取り調査による。）
A.9.2.2	サポートユーティリティ	4 保護されている。（聞き取り調査による。）
A.9.2.3	ケーブル配線のセキュリティ	4 保護されている。（聞き取り調査による。）
A.9.2.4	装置の保守	1 可用性、完全性を維持するための文書化された手順はあるが、一部、老朽化してベンダの保守期限が切れたものがあり、必要十分とは言えない。
A.9.2.5	構外にある装置のセキュリティ	1 リモート接続による管理策については、装置そのもののセキュリティ対策については、ウィルス対策等しか見当たらず、覗き見（ショルダーハッキング）対策やクリアスクリーン ポリシなどに関する記述が不足しており不十分