平成 11 年度

包括外部監査の結果報告書

【情報システムへの投資とその成果】

川崎市包括外部監査人

平成12年3月23日

川崎市長　　**高　橋　　清　様**

包括外部監査人　　**森　谷　伊三男**

包括外部監査の結果に関する報告の提出について

地方自治法第252条の37第5項の規定により、平成11年度の包括外部監査の結果に関する報告を次のとおり提出します。

目　　次

情報システムへの投資とその成果

包括外部監査の結果報告書

包括外部監査の結果報告書に添えて提出する意見

総　務　局

健康福祉局

包括外部監査の結果報告書

第１　外部監査の概要

１．外部監査の種類

地方自治法第 252 条の 37 第 1 項及び第 2 項に基づく包括外部監査

２．選定した特定の事件（テーマ）

情報システムへの投資とその成果

３．監査対象期間

平成 8 年度から平成 10 年度までの執行分

４．特定の事件（テーマ）を選定した理由

川崎市では、情報のシステム化が進んでおり、それとともに賃借料、需用費等の支出が増加している。このため、情報システムにかかる予算の執行等に関する事務が関係諸法令に照らして、合規に執行されているか否かを検討することが必要であると判断したためである。

あわせて地方自治法第 2 条第 13 項（住民福祉の増進、最少の経費で最大の効果を挙げること）及び第 14 項（組織及び運営の合理化、適正化）の規定の観点から、情報システムの投資とその成果を検討することにしたものである。

５．外部監査の方法

（1）監査要点

①　情報システム投資予算の執行の合規性

・契約手続の合規性（随意契約の妥当性を含む）

・検収手続の合規性

・追加コストの有無

・運用委託の合規性

・運用状況の妥当性

・コンピュータ処理能力の妥当性（使用状況の妥当性を含む）

・金額の妥当性

② 情報システムの運営管理全般の合規性

・情報セキュリティの合規性

・システム取得・開発・保守の合規性

・コンピュータ運用管理の合規性

③ 情報システムの費用村効果に関する計画と実績の比較検討

④ 西暦 2000 年問題への対応の検討

(2) 主な監査手続

① 監査対象とした局（総務局、健康福祉局、建設局、港湾局、水道局）の委託料、使用料からサンプル（46 件）を抽出し、契約手続、支払手続の合規性を検討した。

② 総務局所管の大型コンピューター運用に関する案件及び健康福祉局の総合医療情報システム開発案件を対象として、次の手続を実施した。

・システムの効果の実現度を検討するため、費用対効果に関する計画と実績を比較検討した。

・情報セキュリティについて担当者から聴取するとともに、関連書類を査閲した。主要な作業については実施状況を確認した。

・コンピュータに係るシステムの開発、保守、運用体制の手続とその状況について担当者から聴取するとともに、各種基準や管理マニュアル等の関連書類を査閲した。主要な作業については実施状況を確認した。

・コンピュータの設置状況を視察した。

③ 健康福祉局の井田病院・医事会計システムを対象として、次の手続を実施した。

・情報セキュリティについて担当者から聴取するとともに、関連書類を閲覧した。

・コンピュータの設置状況を視察した。

④ 西暦 2000 年間題の対応状況について、体制、対応計画、完了状況、危機管理計画等を確認した。

6．外部監査の実施期間

平成 11 年 7 月 26 日から平成 12 年 2 月 10 日まで

第 2　外部監査の結果

1．総務局所管の大型汎用コンピュータ

(1) 指定データ届出の更新

「川崎市電子計算組織による処理に係るデータの保護管理に関する規程」（以下データ保護管理規程という）第 6 条第 2 項によると、特別な保護管理を必要とするデータである「指定データ」は、「データ保護統括管理者（同規定第 3 条の規定により総務局長）に通知しなければならない」とされている。しかし、総務局所管の大型汎用コンピュータに関連する指定データについては、最終届出日が平成 5 年 11 月 15 日で、それ以降の届出がされていない。

手続実施の煩雑さ等により届出がなされていないことも考えられるために、実態を調査し、理由を分析した上で、現状に合った適切な処置を取ることが望まれる。

(2) 委託契約書におけるセキュリティ関連条項の記載

総務局所管のコンピュータに係わる平成 8、9、10 年度の電子計算組織による処理の外部委託に関する契約書 48 件中の半数強については、データ保護管理規程の第 21 条第 1 項第 3 号から第 8 号に掲げるセキュリティ関連条項の中で必要と考えられる事項が明記されていなかった。

これらの事項は委託時のデータの保護の観点から重要であり、同規定第 21 条にしたがって契約更改時等には不足している事項の追加が必要と考える。

なお、データ保護管理規程の第 21 条は以下のとおりである。

「電子計算組織による処理を外部に委託する場合において契約書を作成するときは、別に定めるもののほか次の各号に掲げる事項を契約書に明記しなければならない。

① 秘密保持に関する条項
② 再委託の禁止または制限に関する条項
③ 指示目的外の利用及び第三者への提供の禁止に関する条項
④ データの複写及び複製の禁止に関する条項
⑤ 事故発生時における報告義務に関する条項
⑥ データファイルの帰属権に関する条項
⑦ データの授受及び搬送に関する条項
⑧ データの保管及び廃棄に関する条項

2　前項に規定する契約書の作成を省略するときは、前項各号に掲げる事項を明記した覚書を取り交わさなければならない。」

(3) 機密保護に関する誓約書の管理

データ保護管理規程第 23 条（要員の派遣）においては電算業務を外部委託する際、責任者及び本人の双方から誓約書を提出させるとしている。しかし、受託業者によっては誓約書を会社が一括してまとめて代表取締役から徴求しており、業者の使用者個人から徴求していないケースがある（㈱エヌアイディ　平成 8 年 4 月 1 日、平成 9 年 4 月 1 日、平成 10 年 4 月 1 日分）。

また、運用保守支援委託契約（平成 9 年 4 月 1 日）により、外部受託業者がコンピュータ室に入退重しているが、作業時間が少ないという理由によって誓約書を徴求していない。

同規程第 23 条にしたがい、受託業者のみならず、業者の使用者個人からも機密保護に関する誓約書を徴求することが必要である。また、規程の趣旨に鑑み、常駐かどうかにかかわりなく使用可能な（アクセスしうる）データの重要性により、誓約書を徴求することが望まれる。

なお、誓約書については、管理簿を作成していないため、誓約書徴求の網羅性を上位者が管理することが困難となっている。今後は、管理簿を作成し、誓約書の徴求管理を行うことが望まれる。

2．健康福祉局所管の総合医療情報システム

(1) 委託契約書におけるセキュリティ関連条項の記載

電子計算組織における処理を外部に委託する場合、委託契約書にセキュリティ関連事項が記載されていなかった旨、「1．総務局所管の大型汎用コンピュータ（2）」で指摘した。健康福祉局所管の総合医療情報システムにおいても、医療事務センターにおける要員派遣の委託契約書には秘密の保持関連事項しか記載されておらず、データの外部への持ち出しを禁止する事項等は記載されていなかった。また、日本アイ・ビー・エム㈱との委託契約書にも秘密の保持関連事項が記載されているのみである。

電子計算組織における処理を外部に委託する場合は、データ保護管理規程の第 21 条（契約書の記載事項）にしたがい、同規程の諸事項を契約書に含めることが必要である。

(2) 記録媒体の耐火金庫での保管

健康福祉局所管の総合医療情報システムにおける患者に関するマスターファイル等の重要なデータがバックアップされている磁気テープは、耐火金庫に保管することが規定されているが、川崎病院は磁気テープ保管用の耐火金庫を所有していないため、現状、磁気テープはコンピュータ室内の耐火仕様でないロッカーに施錠保管されている。

バックアップデータの保管は規定どおり耐火金津に保管すべきである。更にコンピュータ室や建物（川崎病院）における大規模な災害発生時の対策として、バックアップデータは遠隔地に保管することが望まれる。

第３　利害関係

包括外部監査の対象とした事件につき、私と川崎市との間には地方自治法第 252 条の 29 の規定により記載すべき利害関係はない。

以　上

包括外部監査の結果報告書に添えて提出する意見

平成12年3月23日付けの包括外部監査の結果報告書に関連し、以下のとおり意見を申し述べる。なお、意見を述べるにあたっての基本的視点は、財務事務及び経営管理であり、行政政策の理念に深く立ち入ったうえでの観点ではないことを念のため申し添えておく。

総 務 局

1．情報システムに係るリース契約

（1）リース契約相手先の決定について

随意契約に基づく、電子計算組織等のリース契約の相手先毎年間契約額は以下のとおりである。

（単位：千円）

件　　名	契　約　者	平成8年度	平成9年度	平成10年度
電子計算組織賃借料				
	富士通㈱川崎	1,525,378	1,847,200	1,786,140
	日本ＩＢＭ㈱	1,630	1,630	140,315
	昭和リース	339,212	298,877	106,437
	計	340,842	300,507	246,752
庁内ＬＡＮ等賃借料				
	富士通㈱川崎	14,275	27,332	52,025
	昭和リース	27,175	27,703	25,428
	計	41,450	55,035	77,453
ＴＤＭ賃借料				
	富士通㈱川崎	27,204	29,549	26,397

平成 10 年度にＩＢＭ機器のリース契約を昭和リースから日本ＩＢＭに変更しているが、このように大幅のシフトでありながら、随意契約で行われているため、契約先の選定にあたって契約相手先毎の経済性等の検討がどのように行われたかが明らかでない。

また、平成10年度では次期システムの選定が行われ、コンピュータの機種ＩＢＭ９１２１－３２０をＩＢＭ２００３－１０４に変更しているが、機種の選定過程については種々の説明がなされているものの、リース契約の相手先選定の過程は明らかではない。

契約先の変更について担当部局である総務局は、「システム障害時の保守体制強化の観点及び経済性を含め、内部で検討を行い、昭和リースとも協議の上、妥当と判断したものであり、決裁権者の決裁により最終的な意思決定を行っていることから問題ないと認識している。」と説明している。しかし、従来の契約金額の枠内ということで、電子計算組織運営委員会での審議書類においても、経済性についての検討結果について説明がないまま契約が変更されている。情報システム投資の意思決定に際しては、機種の選定と同様にリース契約の相手先毎の条件について検討を行い、手続の透明性を高めるため、選定の理由、経済性、経緯等を文書に残し明らかにすべきである。

(2) 電子計算機のリース契約について

「1. 情報システムに係るリース契約（1）リース契約相手先の決定について」において随意契約に基づく電子計算組織のリース契約の相手先毎の年間契約額を示した。

これらの契約は、形式上単年度の随意契約であるが、実質的には数ヵ年（概ね 5 年）の継続使用を前提とした契約であり、またリース料の算定もそうした前提に基づいて行われている。

数ヵ年にわたる継続使用（数年の債務が発生する）を前提としながら、毎年度、単年度契約を随意契約で締結する方法は適当とはいえず、あらかじめ債務負担行為を設定した上で契約を締結すべきである。

数ヵ年の継続使用を前提とした全てのリース契約について債務負担行為を設定した上で契約を締結することは、その膨大な件数から実務上の対応は難かしいと思われる。しかしながら、市の財政において数ヵ年に及ぶ実質的債務負担行為の実態が、まったく明らかにならないことも健全な財政運営の観点からは問題である。

したがって、例えば金額ベースで毎年の支出額が一定規模を超えるリース契約については、複数年の使用を前提とした競争入札を行い、債務負担行為を設定したうえで契約を締結するといった手続を行うことを検討する必要がある。

2．情報システム導入の成果

（1）インターネット・イントラネットシステム

各システム所管局長は、システムを開発または変更する場合、「川崎市電子計算組織の運営に関する規則」第 11 条に基づいて、当該システムの内容、費用対効果、開発や運用の体制、データ保護等について記載した業務調書を作成しなければならないことになっている。

当案件の業務調書においては、インターネットシステム及びイントラネットシステム（インターネット関連技術を利用した内部用ネットワーク）が扱われている。

当業務調書において、その定性効果は記載されているが、定量効果については、当該システム運用以前に稼働していた、当該システムと同様の機能のインターネットシステム（いわゆるホームページによる情報受発信）との比較を行い、機能そのものの変更はないため、ゼロとされている。

したがって定性効果と費用から投資判断を行う必要があるが、業務調書に投資を是とする客観的な根拠が十分には記述されていない。当該案件が了承されたことに関して、その根拠が容易にかつ客観的に理解できるような資料を整備しておくことが望まれる。

当業務調書において提案されていたイントラネットを利用した議会議事録検索システムは当監査時点において、まだ構築されていない。

当案件に含まれている川崎市庁内用の電子メールは、利用の前提となるパソコンの庁内普及率が各課に 1 台以下なので、本格的な利用の段階に至っていない。中期計画によると、平成 15 年時点でもパソコン導入台数は約 2，500 台で、市の事務を担当しパソコンを使用する予定の職貞数約 8，000 人に村し、3 人に 1 台程度の普及度である。

以上の点を考えると、当面あるいは少なくとも当監査時点では、イントラネットの効果については、十分に実現されているとは言い難い。今後、利用環境の整備が望まれる。

（2）情報システムの事後評価制度

大規模オンラインシステムの省力化効果（定数削減効果）については、「オンライン要員適正配置検討委員会」、財政的な視点では財政局財政課、組織人員編成の視点では総務局行政システム推進室が、それぞれ関連所管局と共に一定の評価機能を果たしている。

しかし、情報システムの費用対効果について、システム稼働後の評価、いわゆるシステムの事後評価を網羅的に行うための制度的なルールは存在せず、この観点での事後評価は実施

されていないといえる。

「川崎市電子計算組織の運営に関する規則」第 14 条によると、「総務局長は、必要と認めるときは、所管局長に対し電子計算組織による処理をした業務について、実施状況の報告を求めることができる。」とされている。しかし、総務局によると、この規則にしたがって報告が求められたケースは少なくとも最近では見られないとのことである。実施状況に関する報告の必要性を判断するには、電子計算組織運営委員会による審議を行った全システムについて、実施後の状況を継続的に把握するための何らかの仕組みが必要と考えられるが、そのための特別な手続等はない。

システムの開発にあたってはその可否が電子計算組織運営委員会によって審議されているが、稼働後に所期の投資効果が得られたかどうかの結果に関しては、網羅的に把握されていない。すなわち Plan（計画）－Do（実施）－See（評価、点検）の管理サイクルから見て See にあたる部分が不十分といえる。

総務局を中心として既にシステム評価制度の整備に向けた調査研究が実施され、平成 9 年度に「システム評価制度構築に係わる調査研究最終報告書」が出されているが、当監査時点においてシステム評価制度は実施されていない。また、投資の可否を判断するための客観的統一的な基準や指標、例えば目標とする投資回収期間（年数）や投資利益率（投資に対する効果の割合）等は決められていない。

今後は同報告を参考にし、事後評価を含めたシステム評価制度の早期導入が期待される。

3．情報システムのセキュリティ

(1) 外部バックアップデータの保管委託先のデータの保護

現在、総務局所管の大型汎用コンピュータのバックアップデータを記録した磁気テープの保管を外部業者に委託しており、磁気テープは県外にある当該業者の建物に保管されている。

データ保護管理規程第 20 条において、所管課長は委託先におけるデータ保護管理に関する状況について調査しなければならないことが規定されている。しかし、データ（磁気テープ）の保管状況の確認方法等に関する具体的なルールは明文化されていない。当該業者に対して委託開始時及び平成 11 年 2 月に現地調査が行われているが、それ以外には保管状況の調査は実施されていない。

バックアップデータの外部保管を業者に依頼する場合、委託先におけるデータ保護状況の

確認手続を文書化し、委託開始後も不測の事態発生時の影響を考慮して適宜保管状況の実地調査を実施することが必要である。

上記に限らず、庁舎外における、データ入力（パンチ）、処理結果の帳票出力（印刷）、磁気媒体等の廃棄など、委託先にある当市の重要なデータについては、その管理や保管状況の実地調査を適宜実施することにより、個人情報等の情報資産を適切に保護することが可能となる。

(2) バックアップされたデータを元に戻すテスト

データのバックアップはライブラリ装置（磁気テープ数百巻を収納し、自動的にデータのバックアップを行う装置）により毎日実施され、復旧を行う時には最新のファイルをプログラムが指示して元に戻す（リストアする）ことになっている。しかし、確実に元に戻せるかどうかのテストは実施されていないため、バックアップされたデータから元のデータが復旧ができるかどうかは確認できていない。過去において、民間企業でバックアップされたデータから元のデータが復旧できなかったケースも報告されている。

不測の事態が発生した場合の影響が大きい重要なデータについては、必要な機器、要員等を確保し、バックアップテープによる復旧テストを適時実施して、元のデータの復旧が確実にできることを確認することが望まれる。

(3) プログラムのテスト環境から本番環境への移行手続

総務局所管の大型汎用コンピュータにおいては、プログラムを新規に作成または変更するためにテスト環境（テストを行うためのコンピュータ内部の場所）が設けられている。新規開発または変更されたプログラムは、テスト完了後、テスト環境から本番環境（実際の運用環境）へ移行される。プログラム完成時にプログラムをテスト環境から本番環境に移行するための責任者による文書での承認手続はなく、担当者によって移行作業が実施されている。

承認された正規のプログラムのみによる処理を確保するため、新規開発または保守されたプログラムをテスト環境から本番環境に移行するための承認手続の整備が望まれる。

(4) セキュリティに関するリスク評価の観点の導入

昨今、病院や電気通信事業者等から個人情報が漏洩した事件が発生しており、また個人情報保護に関して、社会的環境や情報技術の環境も変化している。たとえば従来は、十分な安全対策が講じられたコンピュータ室に設置された総務局所管の大型汎用コンピュータを中心として電算処理が行われていたが、最近は、各部署の執務室に設置されたパソコンなどの小型コンピュータで処理されることが増えており、執務室では通常、常時施錠するなどの特別な安全対策は施されていない。さらにネットワーク化等に伴い処理内容も複雑化している。

したがって、従来想定されていなかったセキュリティ上のリスク、たとえば個人情報の漏洩や改ざん等に対する危険性が高まっていると考えられるため、どのようなリスク（危険性）がどこに存在するのかを見極め（リスク分析)、もし不測の事態が発生した場合にどの業務やシステムにどのような影響があるかを明確化（市民や業務等への影響分析）しておくことが、セキュリティ（安全）対策を講じる上で非常に有効であると考える。なお、リスクは環境の変化等に伴って変化するものであり、適時リスクの見直しが必要である。

また、セキュリティ対策はともすると優先順位が低く置かれがちなため、セキュリティ対策実施部署やセキュリティ対策実施者の所属する部署とは別の部署（組織的に独立した部署）が、定期的なセキュリティに関する監査等を実施することによって、セキュリティ対策の実効性を検証することが望まれる。

健康福祉局

1．システム化の全体構想

両病院で稼働しているシステムに医事会計システムがあるが、川崎病院及び井田病院において別々のホストコンピュータ（中心となるコンピュータのことで、両病院においてはＩＢＭのＡＳ４００が使用されている）により、同じ医事会計のパッケージシステム（既成品のソフトウェア）を使用して処理されている。しかし、病名コード等は両病院により異なる体系になっており、システムの一部変更作業（カスタマイズ作業）も別々に実施されている。

例えば医業収益に関する各科目別請求額、収入済額、未収額などの医事会計システムによる処理結果は、病院財務会計システムに手作業により再入力されている。

井田病院においては、平成 10 年 2 月に医事会計システムが導入されたが、導入直後（平成10 年 3 月）に、医事会計システムから既存の栄養管理システムに入院時食事療養費データを受け渡すことにより、栄養管理システムから新規に 6 帳票が作成できるようにシステム追加業務が委託されている。

関連するシステムを別々に開発せずに、両病院を含めた情報化構想、及び全体的計画のもとにシステム開発を行うことにより、システム間のデータのやり取り（インターフェース）の合理化や重複する開発作業の削減等が可能となり、全体としてのシステム開発費や運用費の削減、処理効率の向上を図ることができる。

たとえば、両病院の医事会計システムは同一のパッケージを使用しているので、現在のように 2 台のホストコンピュータを使用せず、当システム導入前に行っていたように 2 台分の処理能力のある 1 台のホストコンピュータを使用し、通信回線で端末を結ぶ方法も考えられる。

なお、この方法を検討する場合は、各々の方法に関して、以下のようなメリット、デメリットを考慮する必要がある。

期待できる主なメリットとしては、1 台で済むホストコンピュータの使用料、保守費、運用にかかわる委託費等の費用の削減があげられる。

また、デメリットとしては、通信機器、回線、工事等の通信関連費用の増加分や、通信回線でのデータの送受信時に、端末での応答（レスポンス）時間がある程度かかることが考えられる。応答時間については、旧システム稼働時に比較して最近は高速の通信回線や通信機器が比較的安価に調達することが可能となっているので余り大きな障害にならないものと考えられる。

その他考慮すべき事項として以下の項目がある。

・ホストコンピュータの処理能力

・通信データの量、データ発生の時間的パターン

・統合化のための作業量（コード体系、両病院事務の分析調整等）

2．川崎病院総合医療情報システム

（1）定量効果算定の妥当性

システム導入に際して、定量効果の妥当性を判断するために、システム導入に伴う増収効果を算出しているが、この計算方法に一部修正が必要な部分が見受けられた。

具体的には、平成 7 年 11 月 17 日付けの業務調書（業務名：「川崎病院総合医療情報処理業務」）における「外来患者の増加による増収効果」に対応したシステム以外の費用、すなわち外来収入を得るために要した費用、例えば医師や看護婦の人件費、薬品費、医療材料費等を、「外来患者の増加による増収寄与分」から差し引く必要があるが、それが差し引かれていない。

提出された業務調書では、効果から費用を差引いた正味効果の累積額（差引累積額）が、実施 4 年度目から黒字になっているが、外来収入を得るために要した費用を控除すると実施後 5 年度目でも赤字のままである。システム導入に伴う増収効果を計算する際は、増収分に伴う費用の増加分も考慮しておく必要がある。

定量効果の算定に対する理解が必ずしも十分ではないものと見受けられるため、必要に応じて業務調書作成者のための研修等の実施が望まれる。

当監査の時点では、システムが一部しか稼働しておらず、稼働部分だけの費用及び効果が個別に（サブシステム単位に）算出されていないため、費用対効果の実績については適切に評価できないが、外来患者数及び診療単価の実績は次のとおりである。

1 日あたりの外来患者数は、平成 10 年度（実施第 2 年度）において、計画ベースでは 2,000 人であったが、実績ベースでは 1,715 人である。また外来患者の診療単価は、平成 10 年度において、計画ベースでは 10,000 円であったが、実績ベースでは 9,507 円にとどまっている。したがって「外来患者の増加による増収効果」は計画値より低減しており、差引効果（効果一費用）が計画より低減する可能性がある。

(2) 情報システムのセキュリティ

① パスワード

総合医療情報システムにおいては、業務を開始する際にパスワード（暗証番号）を入力する必要があるが、現在、パスワードがわからないと他の人の手助けがしにくいという理由で、比較的容易に類推が可能なパスワードが設定されている。これは、当該システムの全面稼働までこの設定を変更しない予定となっている。

類推が容易なパスワードを使用していると、他人になりすましてシステムを使用することが容易になり、セキュリティの観点からは好ましくない。

また、当システムのセキュリティ対策として、「データへのアクセス履歴情報の管理」（当システムの要件書の「保護措置等」(5) に記載）があげられているが、他人のユーザＩＤ（利用者を識別するための番号や文字等）を使用した場合は、当然本人としてのアクセス履歴（利用状況に関するコンピュータ上の記録）は残らないため、適正なアクセス履歴管理は行えない。

情報保護の観点から、パスワードの有効性を高めるために、容易に類推ができないパスワードの設定が望まれる。

② コンピュータ（サーバ）のセキュリティ管理

当該システムは、処理を中心的に行うコンピュータ（サーバ）と利用者用の複数のパソコンがネットワークを介して接続されており（いわゆるクライアントサーバシステム）、サーバの運用作業は、業者に委託されている。

サーバのセキュリティに関する管理は個人情報の保護等の観点から重要であるが、サーバの具体的な管理方法や基準について、文書化され承認されたものは確認できなかった。

社会環境やネットワーク化の進展等のシステム処理環境の変化に応じて、セキュリティ上のリスクや業務・事務への影響が変化している。セキュリティ対策はこれら環境の変化に対応して実施される必要がある。

当該システムのような場合は、サーバの保守・運用管理のためのルールの整備が必要である。サーバの管理のために必要なルールは通常以下の事項に関するものを含む。

・サーバ（システム）管理責任者の役割・権限・責任と日常作業担当者の役割・権限・責任

・サーバの保守・運用管理担当者用のユーザＩＤ承認・異動に伴う変更・廃止手続

・サーバの保守・運用管理担当者用のパスワードの設定と管理

・データの利用（アクセス)、複写の制限、廃棄等

・セキュリティに関する監視・監査

特に、サーバの保守・運用管理担当者用のユーザＩＤは、データのアクセス権限の設定・変更、ユーザの設定、ユーザの権限の設定等について、ほぼ自由に行えるという強い権限を有するため、適切な管理が必要である。また、そのパスワードは短期間（必要とされる機密の程度に応じて、例えば１か月から３か月程度以内）に変更されることが望まれる。

③　患者、病状等に関するデータの印刷

端末ごとにプリンターが設置されており、患者、症状、レントゲンフィルム等のデータをプリンターにより印刷することが可能である。当該システムを利用するためにはパスワードが必要であるが、それが比較的類推されやすい現状では、権限がない者による印刷や持ち出しの可能性がある。

なお、現状フィルムの貸出しや電子情報を学会に持ち出すこと等に関する明文規定はないが、この制定が今後予定されている。

今後、情報の持ち出し等に関するルールの明文化、類推が容易でないパスワードの使用、印刷できるプリンターの特定や時間帯の制限等の個別の対策を実施すると共に、システムのユーザ、システム要員、その他すべての職員の各々の特性を考慮したセキュリティ教育の実施が望まれる。

④　コンピュータ室への入退管理

川崎病院のコンピュータ室は、システム要員が常駐しているものの、施錠は常時されていないため部外者が入室する可能性がある。

またコンピュータ室であると推測できる表示があるため、部外者にもその所在が分かり、セキュリティの観点からはリスクを高めているといえる。

セキュリティ上問題があるためコンピュータ室である旨の表示の削除、あるいは表示内容の工夫、扉の常時施錠実施について、不測の事態発生時の影響を考慮して検討がなされることが望まれる。

3．井田病院医事会計システム

（1）バックアップテープの遠隔地保管

医事会計システムのバックアップデータは、ホストコンピュータ（ＡＳ４００）付属のカートリッジテープ装置にて作成され、曜日毎に世代保管されているが、カートリッジテープを遠隔地に保管するなどの措置がなされていない。このため、火災、地震等の広域災害によりホストコンピュータの記憶装置（磁気ディスク）とバックアップテープが同時に被災した場合、データが喪失してしまう可能性がある。

遠隔地の安全な場所に、バックアップデータを定期的に保管することが望まれる。

（2）コンピュータの設置場所

ホストコンピュータ（ＡＳ４００）は、給排水設備に近い場所に設置され、設置場所の天井にはスプリンクラーがあり、作動した場合は水を被る可能性がある。コンピュータの設置環境としては適切といえない。

コンピュータは熱や水に弱いことを考慮して適切な設置場所を確保するとともに、部屋の施錠等により業務上必要のない者が触れることができないよう、対策を講じることが望まれる。

以　上