

平成 22 年 3 月 31 日

平成 20 年度内部監査（情報システム管理状況）報告書

独立行政法人医薬品医療機器総合機構
理事長 近藤 達也 殿

監査室長 天 城 勝 仁

独立行政法人医薬品医療機器総合機構内部監査規程第 8 条の規定に基づき、独立行政法人医薬品医療機器総合機構（以下「PMDA」という。）の平成 20 年度内部監査（情報システム管理状況）について、以下のとおり報告します。

記

1. 監査概要

平成 20 年度内部監査計画に従って、PMDA が保有・管理する情報システムについて、PMDA 情報システム管理利用規程（以下「管理規程」という。）に基づき適正な管理がなされているかにつき、監査を実施した。

監査実施期間、監査対象・内容などは以下のとおり。

○監査実施期間：平成 20 年 10 月～11 月 [※]

○監査対象：PMDA が保有・管理する情報システム

○監査実施者：監査室長及び監査室員 2 名

※）平成 21 年度も状況の確認のためのヒアリングを実施。

2. 監査の方法

PMDA が保有・管理する情報システムについて、当該システムの管理者に、その管理状況についてヒアリングを実施した。ヒアリングの実施にあたっては、管理規程の各規定に基づき「システム管理規程監査ヒアリング事項」を作成し、本チェックシートの各項目について確認を行った。

また、各情報システムの機器類について、実査を行い保管状況の確認を行った。

※）監査対象システムは、34 システムである。

3. 監査結果

今回の監査は、PMDA に導入されている情報システムの管理状況について

確認を行ったところであるが、管理規程に基づき、概ね適正に管理されているものと認められる。

なお、より一層の情報システム管理の正確性、効率性、安全性の確保のために以下の点につき検討されたい。

4. 検討事項

1) 各情報システムに共通する事項及びシステムの管理体制について

① 管理規程の適応を受ける「情報システム」は、「PMDAに導入されたシステム」であり（第1条）、「ハードウェア、ソフトウェア、ネットワーク、記録媒体で構成されるものであって、これら全体で業務処理を行うもの」である（第2条第1号）ところ、平成21年11月現在、本規程の適応を受けるとして登録されているシステムは、稼働中、開発中を含めて41のシステムがある。しかしながら、これらの情報システムの中には、PMDAのシステムでないものや、市販ソフトを使用した計算シートだけのももある。また、逆に「情報システム」として管理されるべきシステムが登録されていないものもある。本規程において管理されるべき「情報システム」について、管理規程の規定に照らして確認し、再度整理すべきである。

② 管理規程においては、サーバ室への入退室管理等につき「必要な手順」を定めること（第13条第6項）や、また、情報システムを追加、変更する場合は「予め定められた手順」に従い実施すること（第36条）など、情報システムの利用管理に当たって、運用基準を定めることが規定されているが、これらが実施細則や運用指針として明文化されているものはほとんど見受けられない。

このような「手順」についてはIT室において整備し、各システムにおいて、必要に応じ整備することが必要である。

③ 管理規程においては、情報システムを構成する機器で外部に設置する場合（第18条第1項）や業務システムの仕様変更等に伴う設定変更などの作業を行う場合（第27条第2項）などは、それぞれ管理規程により規定された様式を用いて「申請書」や「作業届」を提出することとなっているが、設置許可等にかかる決裁で本申請に代えている場合が多く見受けられる。

許可申請にかかる決裁（稟議書）は、起案者の手元には残るが、許可権限者（システム総括管理者／IT室）には保管されないことから、許可申請にかかる決裁の際に、同時に規定された「申請書」等の提出も求めるべきである。

- ④ 管理規程においては、各情報システムについて、アクセス記録を残すことが規定されている（第26条第1項）が、一部のシステムでは、アクセス記録を録ることはシステム上可能であるが、これを録っていないものもある。

システムの性格や機能により、アクセス記録やその保存が必要ないものもあると思われるが、各システムでセキュリティの観点からアクセス記録・保管の是非を検討し、必要と判断されれば保管すべきである。

また、アクセス記録が保管されているシステムについても、どの程度の期間と範囲で記録が残されているかを、システム管理者は把握しておき、その保存期間・範囲についても、検討する必要がある。

- ⑤ 各情報システムにかかる導入時や改修時の仕様書については、各管理者の執務室で保管しているものもあるが、導入や改修における契約原議への添付で替えられているものもある。

契約に係る原議については、当該文書の保存期間の満了とともに廃棄されることから、これら仕様書については、各情報システム管理者において、適正に保管・管理を行うべきである。

- ⑥ 管理規程においては、情報システムの管理記録の保存（第27条第1項）や情報システムを開発、改修等する場合におけるセキュリティ対策として遵守する事項（第37条）、情報システムの開発、運用または保守等を外部の者に委託する場合にその委託契約書に記載すべき事項（第52条）等が規定されている。

これらの事項については、契約における仕様書などに記載されなければならないところ、仕様書には記載が無く口頭などで伝えられている場合が多いが、これらの事項については、業務仕様書に記載され、明文として業務受託業者に伝えられる必要がある。

なお、IT室においては、これらの「受託者が遵守すべき事項」を反映した統一的な「基本仕様書」の様式を準備中であり、今後は、各情報システムの開発、改修などにおいてはこれら様式を活用することが望まれる。

- ⑦ 管理規程においては、情報システムにかかるサーバやクライアントなどシステム機器を廃棄するにあたっては、そこに保管されていたデータが復元不可能なたちでの廃棄が規定されている（第53条）。

これまでのシステム機器等の廃棄にあたっては、廃棄前にデータの消去を行ったり、データの消去を廃棄業者に依頼してきている。

今後は、システム機器の廃棄にあたり、どの程度のデータ消去の仕様となっているかは把握しておく必要がある。

- ⑧ 管理規程においては、情報システム運営委員会の設置（第 8 条）と定期的な開催（第 10 条）が規定されているところであるが、近年は、同会議が開催されていない。

上記のとおり、情報システムの管理・運営については、種々検討すべき事項があることから、常に問題点などを検討していく場として、同委員会の開催は必要と考えられる。

2) 個別の情報システムについて

- ① 管理規程においては、情報システムの管理にあたっては、ユーザー I D 及びパスワード等による利用者認証機能を設けることとなっている（第 22 条第 1 項）が、一部のシステムについては、ユーザー I D 及びパスワードが使用者間において共有されていたり、一つのユーザー I D、パスワードしか付与されていないシステムもある。

セキュリティの観点から、ユーザー I D、パスワードはユーザー個々に付与されるようシステムの整備を検討すべきである。

また、異動となった職員のユーザー I D、パスワードが抹消されないで利用できる状況となっているシステムもあるので、当該業務関係者以外の者が当該システムを使用できる状況を放置しない環境とすることが必要である。

- ② システムの中には、PMDAにおいてシステムを構築しているものもある。これらのシステムについては、システム稼働のためネット上のオープンソースを導入しているものもある。

管理規程においては、ソフトウェアの調達にあたっては、当該製品が情報セキュリティを確保する上で、支障がないかシステム総括管理者の確認を受けることとなっているところ（第 35 条第 2 項）、システム構築の必要に応じ、オープンソースの導入を行うことはやむを得ないと思われるが、導入したソフトについては、I T室に登録する必要がある。