平成 23 年 4 月 26 日

平成２２年度内部監査（平成２０年度内部監査「情報システム管理状況」のフォローアップ）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 22 年度内部監査（平成２０年度内部監査「情報システム管理状況」のフォローアップ）について、以下のとおり報告します。

１．監査概要

ＰＭＤＡの業務の遂行にあたり、独立行政法人医薬品医療機器総合機構情報システム管理利用規程（以下「管理規程」という。）の遵守状況を把握するため、「平成２０年度内部監査（情報システム管理状況）報告書の検討事項のフォローアップ」を行った。

監査実施期間及び監査対象等は、以下のとおりである。

○監 査 期 間 ：平成２２年１２月１５日（水）～平成２３年1月２６日（水）
○監査実施者：監査室長、監査室員
○監 査 対 象 ：「平成２０年度内部監査（情報システム管理状況）報告書」の検討事項（以下「検討事項」という。）

※）検討事項一覧

（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ものもある。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」については情報化統括推進室（以下「ＩＴ室」という。）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は思われるが、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か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ＩＤ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ＩＤ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ＩＤ、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ＩＤ、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ＩＤ、パスワードが抹消されないで使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、ＩＴ室に登録する必要がある。

２．監査の方法

ヒアリングシートにより、検討事項に対する対応状況の確認（必要に応じヒアリング、実地調査の実施）

３．監査結果

検討事項に対して、以下の事項については概ね対応が図られているものと認められる。

（１）検討事項（１）②、⑥、⑦について

②の検討事項であるサーバ室への入退室管理等につき定めなければならない「必要な手順」については、独立行政法人医薬品医療機器総合機構入退室管理規程に基づいた手順書が作成されていることを手順書の徴収により確認した。

また、情報システムを追加、変更する場合に「予め定められた手順」を作成すること、⑥の検討事項である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」を作成すること及び⑦の検討事項である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把握することについて、現在それぞれにおいて定型的な様式等を構築中であり、今後、業務システムオーナー等の管理者へ提示される予定であることをヒアリングにより確認した。

（２）検討事項（１）⑤について

仕様書の保管状況について、各情報システム管理者において適切に管理されていることを実地調査により確認した。

（３）検討事項（１）⑧について

平成２２年５月２８日に「平成２２年度第１回情報システム運営委員会」が開催され、情報セキュリティの改善案について検討が行われたことを議事録の徴収等により確認した。

（４）検討事項（２）①について

一部のシステムにおいては、異動となった職員のユーザーＩＤ、パスワードが抹消されていない状況となっているものの、当該業務システム管理者においてユーザーＩＤ・パスワードは、一元的に管理されていることを実地調査により確認した。

（５）検討事項（２）②について

オープンソースを導入しているシステムのＩＴ室への登録状況は、ヒアリングシートによる回答結果又はヒアリングにより、前回の監査時において未登録であったシステムや新設のシステムにおいても、ＩＴ室に登録済であることを確認した。

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対応を図られたい。

（６）検討事項（１）①について

前回の監査に引き続き、市販ソフトを使用した計算シートだけのＰＭＤＡのシステムでないものが実地調査により見受けられた。

今後とも、管理規程において管理されるべき「情報システム」について定期的な確認に努められたい。

（７）検討事項（１）③について

情報システムを構成する機器で外部（データセンター等）に設置する場合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、情報システム管理者に「申請書」や「作業届」を提出することになっているが、システム導入やシステム改修等にかかる決裁で本申請に代え対応していることをヒアリングにより確認した。

決裁では本申請に代えることが出来ないといった場合においては、これらの提出を行わせているところであるが、管理規程の適切な運用のためにも「申請書」や「作業届」の提出について徹底されたい。

（８）検討事項（１）④について

アクセス記録を録ることについては、システム導入時から全てのアクセス記録を録っているものや今後、システム改修等によりアクセス記録を録ることを検討中であるものなどがある一方、前回の監査に引き続き、アクセス記録を録ることはシステム上可能であるが、アクセス記録を録っていないものなど、ヒアリングシートによる回答結果及びヒアリングにより、各システムに応じて対応が様々であった。

現在、アクセス記録を録っているシステムについて、アクセス記録の保管期間・範囲については、その記録の保管期間・範囲が十分なものか、またアクセス記録を録っていないものについてもその妥当性について、各業務システムオーナーは、必要に応じ情報セキュリティを統括するＩＴ室を交え再度検証するなどの対応を図られたい。

（９）検討事項（２）①について

前回の監査に引き続き、一部のシステムにおいて、ユーザーＩＤ・パスワードを共有している状況が実地調査の結果により見受けられた。

管理規程の適正な運用のためにも、ユーザーＩＤ・パスワードをシステム利用者間で共有せず個々に付与されるよう対応を図られたい。