ポスター
# ポスター2
# 情報セキュリティ・プライバシー
2017年11月21日(火) 14:15 〜 15:15 L会場（ポスター会場2） (12F ホワイエ)

[2-L-1-PP2-5] 「当院における病院情報システムに対するセキュリティ対策の報告 〜内部監査継続等で改善されたこと、今後の課題〜」

嶋田 育子, 横岡 由姫, 横濱 則也, 奥田 保男 （国立研究開発法人量子科学技術研究開発機構 放射線医学総合研究所 臨床研究クラスタ 病院医療情報室）

［背景］放射線医学総合研究所病院（以下、当院）では、平成18年から継続的に医療情報システムに対するセキュリティ対策として PDCAサイクルを立案し実施している。主な内容は①医療情報セキュリティ講習会、②セルフチェック、③内部監査であり、医療情報を取り扱う職員を対象にセキュリティに対する意識の向上を図っている。
［方法］本研究では②セルフチェックと③内部監査について、職員の意識の変化など継続的に実施した結果を評価し、その効果について検証する。なお、セルフチェックは、医療情報システムを取り扱う全職員を対象に、個人情報、パスワード、 USBメモリなどの取り扱いについてアンケート形式で実施している。また、内部監査は、対象とする部門を18に分け、3年を1サイクルとし年に5〜6部門を対象に実施し、監査項目は当院で定める医療情報セキュリティ手順書に基づき選定している。
［結果］2012年度と2016年度に実施したセルフチェックの回答を比較すると、全6項目の質問事項について「実施している」と回答した割合が1項目を除き10ポイント以上向上した。内部監査について一例を示すが、2013年度実施時、診療情報を含むファイルを保管している棚や居室の施錠に不備があった。しかし、内部監査を繰り返し行うことで施錠の徹底などを図ることができた。このように、監査対象部門において前回の指摘事項は概ね改善された。これらの結果からこのような対策を定期的に実施することにより職員の意識改革に一定の効果が得られることがわかった。
［考察］パスワードの変更に関しては、自発的に変更するのは困難、短期間で変更すると忘れてしまい業務に影響が出る、など定期的な変更への否定的な意見があった。当院では静脈認証も一部実施しているが、今後は運用的な視点と経済的な視点を含め、他の手法なども考慮しセキュリティ対策について検討を進める必要があると考える。

当院における病院情報システムに対するセキュリティ対策の報告
～内部監査継続等で改善されたこと、今後の課題～

嶋田 育子[*1] 、横岡 由姫[*1] 、横濱 則也[*1] 、奥田 保男[*1]
[*1] 国立研究開発法人量子科学技術研究開発機構 放射線医学総合研究所 臨床研究クラスタ病院医療情報室

Report on security measures for hospital information system at our hospital
- Improvement by continuous internal audit etc., future tasks -

Shimada Ikuko[*1] ,Yokooka Yuki[*1] ,Yokohama Noriya[*1] ,Okuda Yasuo[*1]
[*1]National Institutes for Quantum and Radiological Science and Technology National Institute of Radiological Sciences Clinical Research Cluster Hospital Medical Informatics Section

Since 2006, the National Institute of Radiological Sciences Hospital (hereinafter, “our hospital”) has been continuously implementing PDCA cycle as a security measure for medical information systems to improve security consciousness for the employee who handles medical information by following ways:(1) medical information security workshops, (2) self-check, (3) internal audit. In this research, we evaluate the results of (2) self-check and (3) internal audit and verify the effect. Self-checking is carried out for all employees handling with medical information systems in a questionnaire form regarding handling of personal information, passwords, USB memory. As for internal audits, we divide the target division into 18 and carry out 5 or 6 divisions every 3 years. Audit items are selected according to medical information security procedure stipulated by our hospital. Comparing the answers of self-checks conducted in FY 2012 and FY 2016, the percentage of respondents who answered "Implemented" for all six question items increased by 10 points or more except for one item. As example of internal audit in 2013, there was “locking error”: the shelf or the room where medical information was filed. However, by performing internal audits repeatedly, the defaults pointed out in last audit were improved. From this result, we found regular audit attains some progress in re-forming consciousness of employees. Regarding change of password, there were negative opinions on regular change because of the difficulties for the voluntarily change and forgetting by frequent change in a short period. Although our hospital partly uses vein authentication, it is necessary to consider other methods as security measures from operational and economic viewpoint for the future.

Keywords: hospital information system, audit,

1. 背景

平成28年4月の診療報酬改定で「電子的診療情報評価料」が新設された。「電子的診療情報評価料」の算定要件には、「厚生労働省「医療情報システムの安全管理に関するガイドライン」を遵守し、安全な通信環境を確保すること」と明記されている。安全な通信環境を確保するためには、運用状況を定期的に確認し、問題があれば適宜改善する必要がある。

2. 目的

放射線医学総合研究所病院（以下、当院）では、平成18年から医療情報セキュリティに対する意識の向上を図ることを目的としてPDCAサイクルを立案し実施している（図1）。主な実施内容は、①医療情報セキュリティ講習会 ②セルフチェック ③内部監査であり、対象は医療情報システム（電子カルテ、PACS等）を使用するユーザー（診療系アカウント保有者）および部署である。

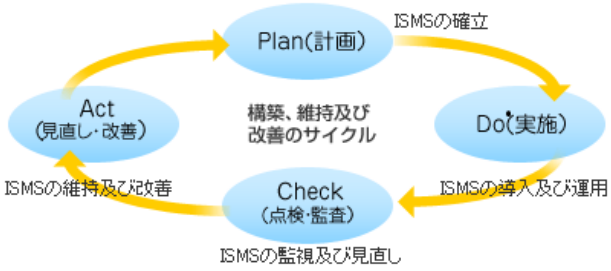

図 1 情報セキュリティマネジメントシステム(ISMS)における PDCA サイクル

3. 方法

1年間のスケジュールを図2に示す。ここで毎年4月に3日間開催する①医療情報セキュリティ講習会は、当院が定める医療情報セキュリティ実施手順書に基づき実際するものであり、医療情報についての基礎知識について講習する。対象者は診療系アカウントを保有する全ユーザーである。なお、7月末時点で当該講習を未受講のユーザーは、アカウントが抹消される。

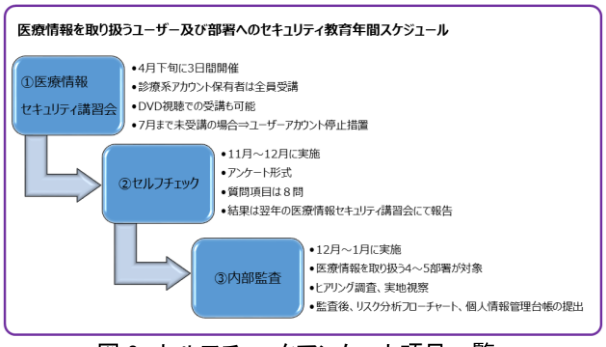

図 2 セルフチェックアンケート項目一覧

②セルフチェックも同様に医療情報システムを取り扱う診療系アカウントを保有する全ユーザーを対象に、個人情報の取り扱いやパスワードの変更頻度、USBメモリの取り扱いについてアンケート形式で実施する。アンケートの集計結果は翌年の医療情報セキュリティ講習会にて報告する（図3）。

③内部監査は、病院情報システムを取り扱う18部門を対象に、3年を1サイクルとし1年に5～6部門の監査を実施する。

監査項目は当院で定める「医療情報セキュリティ実施手順書」に基づくものであり、特にセキュリティ事故に直結する可能性の高い4項目を選定している。内訳は「記録媒体の管理・処分」「利用者アカウント」についてそれぞれ2項目である。「記録媒体の管理・処分」は、医療情報が記録されている紙媒体の保管場所について、主に施錠状況についての確認と、医療情報室から貸し出しを行っている使用許可済みのUSBメモリを使用している事を確認した上で、それらの使用状況の確認を行う。「利用者アカウント」は、医療情報システムにおいてID・パスワードによるログインが必要な部門システムの確認と、パスワードの定期的な変更がなされているかを確認する。いずれも該当部署の個人情報セキュリティ管理者へのヒアリング、および実地調査を行う。結果は「実施している」「一部実施」「実施していない」「対象がない」の4段階評価を行い、監査人意見および改善事項と共に該当部署へ報告する。

本研究では、②セルフチェックと③内部監査について、職員の意識の変化などを分析した結果を時系列に評価し、その効果について検証する。

セルフチェック　アンケート項目

項目	内　容
①	個人情報が記録されている書類や外部記録媒体、ノートパソコン等は放置せず、未使用時、退勤時、部屋が無人になる時には施錠保管している
②	個人情報が記録されている書類や外部記録媒体の廃棄はシュレッダー等、決められた方法で実施している
③	電子カルテ、Viewer端末上でUSBメモリ等の外部記憶媒体に個人情報を記憶する場合には、医療情報室が配布するUSBメモリを使用しパスワードによる保護もしくは暗号化処理を行う
④	個人情報を院外へ持ち出す場合は、事前に責任者に承認を得る等の所定の手続きを行ったうえで持ち出している
⑤	パスワードの変更を3ヶ月毎に実施している
⑥	個人情報の漏えいなどの情報セキュリティ事件・事故時を発見した場合の対応手順について理解している。 <事件・事故を発見した際には、当該事案の内容等を直ちに情報セキュリティ担当者と管理者に報告し、指示を仰ぐ>

図 3　セルフチェックアンケート項目一覧

4.　結果

2012年度と2016年度に実施したセルフチェックの回答を比較すると、全6項目ある質問事項について「実施している」と回答した割合が1項目を除き10ポイント以上向上した。とくに顕著に「実施している」との回答が増加した項目は、個人情報を院外へ持ち出す際の手続きについての問いであった（図4）。医療情報セキュリティ講習会でも、昨今起こった個人情報データの流出、紛失事故について具体的に紹介し、注意喚起を行っており、ユーザーの関心度も上がってきたためと推測できる。その他の項目に関しても、概ね向上している事が確認できる。

つぎに、内部監査について一例を示すが、2013年度監査を実施した部署において、診療情報を含むファイルを保管している棚や、居室の施錠に不備があり、この点について改善を要求したが、内部監査での指摘により、それらの施錠の徹底などをはかることができた。

このように、監査対象部門において前回の指摘事項は概ね改善されており、定期的な監査によって職員のセキュリティに対する意識向上が見られた。これらの結果からこのような対策を定期的に実施することにより職員の意識改革に一定の効果が得られることがわかった。また、監査の対象部門より「個人情報取り扱い台帳」および「リスク分析フローチャート」を提出してもらっている。「個人情報取り扱い台帳」は、各部門で取り扱っている個人情報が記載されている書類について洗い出しを行い、それについて「保有個人情報の基本的内容」「取得・入力」など10の大項目、全38の詳細項目について記入してもらうものである。「リスク分析フローチャート」は、電子カルテおよび連携する部門システムにおいての通常行う業務フローを図式化し、想定されるリスクと、それに対する安全対策を記述するものである。これらは、前回監査時から比較して、変更となった箇所を適宜修正、更新する事は勿論だが、定期的に見直すことにより、リスクの再認識としても有効である（図5）。

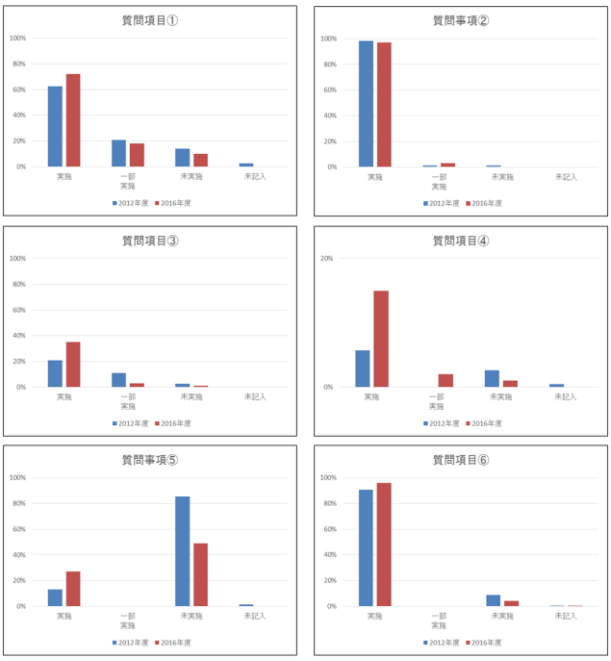

図 4　セルフチェック回答　2012年度－2016年度比較

大項目	詳細項目	大項目	詳細項目
①保有個人情報の基本的内容	それはどの様な個人情報ですか？（一括りに出来る時はグループ名）	③保管	保管責任のある部署はどこですか？
	グループ内の具体的な個人情報名は？		（定められている場合）保管期間は？
	誰の個人情報ですか？		実際の保管期間は？（又は、いつの分から保管していますか？）
	どれ位の件数の個人情報がありますか？		普段どこに保管されていますか？
	1ヶ月あたりどれ位の件数が追加されますか？		保管場所の施錠は、どのようになっていますか？
	どの様な目的で利用されますか？		その情報は、どの様な形態で保管されていますか？
	記載されている具体的な個人情報は？	④バックアップ	バックアップ作成責任のある部署はどこですか？
②取得・入力	個人情報を取得・入力する際の管理責任者は誰ですか？		バックアップの保管期間は？
	その情報の取得元は？		バックアップは普段どこに保管されていますか？
	どういう手段で取得していますか？		バックアップ保管場所の施錠は、どのようになっていますか？
	取得時はどのような形態の情報ですか？		バックアップ情報は、どの様な形態で保管されていますか？
	取得時に、行っているセキュリティ対策は何ですか？	⑤破棄／廃棄	その情報を廃棄する場合どのようにしていますか？
③移送／送信	どういう手段で移送・送信していますか？		破壊した情報の廃棄先はどこですか？
	移送・送信時の情報の形態は何ですか？	⑥第三者提供	経常的な、院外への提供先がある場合、それはどこですか？（選択式）
	移送・送信時に、行っているセキュリティ対策は何ですか？		その情報を提供する場合の媒体は何ですか？
④利用／加工	この情報を利用・加工する業務やシステムがあれば記載して下さい	⑦アクセス権	それは限られた人のみが利用・閲覧できる状態になっていますか？
	経常的に複製を作成する場合、その方法は何ですか？		アクセス権の管理責任者は誰ですか？
⑤委託	その個人情報を外部に委託する場合は、委託先はどこですか？		用いているアクセス制御の方法は何ですか？
	委託の目的は何ですか？		
	委託契約書はありますか？		

図 5　個人情報取り扱い台帳確認項目

5.　考察

セキュリティに対する意識の向上は見られるが、パスワードの変更に関しては、「自発的に変更するのは困難」「短期間で変更すると忘れてしまい業務に影響が出る」など、依然として定期的に変更することへの否定的な意見が多くみられた。

当院では、電子カルテのログイン時に静脈認証を実施しているが、その他のシステムへはID・パスワード入力での従来通りのログイン方法である。今後は運用的な視点と経済的な視点を含め、他の手法なども考慮した上で、セキュリティ対策について更なる検討を進める必要があると考える。

参考文献

1）厚生労働省. 医療情報システムの安全管理に関するガイドライン
2）IPA情報処理推進機構. 情報セキュリティマネジメントと PDCA サイクル
http://www.ipa.go.jp/security/manager/protect/pdca/index.html