一般口演 | セキュリティとプライバシー保護
一般口演20
情報セキュリティ・プライバシー
2021年11月21日(日) 15:10 ～ 16:10 G会場 (2号館3階232+233)

[4-G-3-02] 情報セキュリティ自己点検とオンラインシステム監査について

*江苅 孝[1]、日野 和彦[2]、和田 悠久[3]、曽根 洋平[4]、杉村 剛[5]、松浦 正[6]、中山 徳江[7]、福田 秀樹[8]、藤岡 和美[8] （1. 埼玉医療生活協同組合 羽生総合病院, 2. 医療法人徳洲会 新庄徳洲会病院, 3. 医療法人沖縄徳洲会 湘南鎌倉総合病院, 4. 医療法人沖縄徳洲会 高砂西部病院, 5. 医療法人沖縄徳洲会 神戸徳洲会病院, 6. 医療法人沖縄徳洲会 宇和島徳洲会病院, 7. 医療法人沖縄徳洲会 榛原総合病院, 8. 徳洲会インフォメーションシステム株式会社）
*Takashi Ekari[1], Kazuhiko Hino[2], Yukyu Wada[3], Yohei Sone[4], Takeshi Sugimura[5], Tadashi Matsumura[6], Norie Nakayama[7], Hideki Fukuda[8], Kazumi Fujioka[8] （1. 埼玉医療生活協同組合 羽生総合病院, 2. 医療法人徳洲会 新庄徳洲会病院, 3. 医療法人沖縄徳洲会 湘南鎌倉総合病院, 4. 医療法人沖縄徳洲会 高砂西部病院, 5. 医療法人沖縄徳洲会 神戸徳洲会病院, 6. 医療法人沖縄徳洲会 宇和島徳洲会病院, 7. 医療法人沖縄徳洲会 榛原総合病院, 8. 徳洲会インフォメーションシステム株式会社）

キーワード：Information Security Self-check, Online system audit, Information System Operations Management Stipulation

背景・目的：

徳洲会グループ（以下グループ）では、グループ65病院約140名の SEで構成する情報システム管理部会（以下SE部会）内に設置した法令順守部門とグループの IT部門である徳洲会インフォメーションシステム株式会社、さらに外部機関（一般社団法人医療 ISAC）の協力も得て、2019年４月よりグループ病院に対するシステム監査を開始した。これはグループ共通の『情報システム運用管理規程 第５版』に基づき、各病院で医療情報システムの運用及び患者情報の取り扱いが適切に行われているか、事前提出文書と現地訪問により監査を行い病院が一定のセキュリティを確保できるよう支援する目的で行われるものである。しかし監査は１ヵ月に１～２病院の実施が限度であり、全病院の監査完了までに２～３年を要することから、各病院でセキュリティに関する自己点検を行うこととした。

方法：

自己点検はシステム監査用の『情報セキュリティチェックシート（計79項目）』を用いて各病院で実施した。この結果に基づき監査を継続する予定だったが、新型コロナウイルスの影響を考慮して一旦中断、監査員が現地を訪問しない監査方法を検討し、2021年１月に Zoomによる初のオンライン監査を実施した。

結果・考察：

SE部会法令順守部門で各病院の自己点検結果を集約・分析した結果、各病院のセキュリティレベルに予想以上の差があることや多くの病院に共通する弱点等も判明し、グループのセキュリティ対策の課題を明らかにすることができた。またオンライン監査は綿密な事前準備と受審病院の協力もあり、訪問監査と遜色ない内容で監査を行えたと考える。
今後はこの結果に基づき、急ぎ対策が必要な病院に優先して監査あるいは個別の支援を行う、多くの病院に共通する改善が必要な事項は SE部会の会議等で積極的にアナウンスする等、各病院とグループ全体のセキュリティレベル向上の支援を継続していきたい。

情報セキュリティ自己点検とオンラインシステム監査について

江苅孝[*1]、日野和彦[*2]、和田悠久[*3]、曽根洋平[*4]、杉村剛[*5]、松浦正[*6]、中山徳江[*7]、福田秀樹[*8]、藤岡和美[*8]
*1 羽生総合病院、*2 新庄徳洲会病院、*3 湘南鎌倉総合病院、*4 高砂西部病院、
*5 神戸徳洲会病院、*6 宇和島徳洲会病院、*7 榛原総合病院、
*8 徳洲会インフォメーションシステム株式会社

Information Security Self -Check and Online System Audit

Takashi Ekari[*1], Kazuhiko Hino[*2], Yukyu Wada[*3], Yohei Sone[*4], Takeshi Sugimura[*5],
Tadashi Matsuura[*6], Norie Nakayama[*7], Hideki Fukuda[*8], Kazumi Fujioka[*8]
*1 Hanyu General Hospital, *2 Shinjo Tokushukai Hospital, *3 Shonan Kamakura General Hospital,
*4 Takasago Seibu Hospital, *5 Kobe Tokushukai Hospital, *6 Uwajima Tokushukai Hospital,
*7 Haibara General Hospital, *8 Tokushukai Information System Inc.

At Tokushukai Group, The Information System Administrative Committee (SE Committee) is formed by 65 group hospitals and 140 SEs. Legal Compliance department in the committee, Tokushukai Information Systems Company Ltd., as an IT department of the group, and with the cooperation of external agencies, they have conducted system audit based on the “Information System Operational Management Regulation, 5th Edition”. However, the audit work was limited to 1 or 2 hospitals per month so that the completion of the entire hospitals audit has taken 2 to 3 years. Therefore, Security Self-check using the common check-sheet has been conducted at each hospital in 2020. As the result, it has revealed the issues and concerns, such as a huge difference on security level among the hospitals and existence of the common weak points. Based on this result, the system audit is planned, but in considering the COVID-19 pandemic circumstances, first online auditing is conducted in January 2021. We have perceived that the online auditing bears comparison with door-to-door auditing.

Keywords: Information Security Self-check, Online system audit, Information System Operations Management Stipulation.

1. 緒論

徳洲会グループでは、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」（以下「厚労省ガイドライン」という）と、会計監査で求められる IT 内部統制の必要要件にもとづくグループ病院統一の「情報システム運用管理規程」（以下「運用管理規程」という）を作成し、電子カルテを導入した 65 病院に設置している。

運用管理規程は病院にあれば良いというものではない。電子カルテをはじめとする医療情報システムの利用やシステムで管理される医療情報の取扱い等に際し、ここに記されたルールを守り、適切な運用をすることで厚労省ガイドラインを遵守し、医療情報・病院・職員を守ることができる。徳洲会グループでは、運用管理規程に基づく運用が各病院で適切に行われているかを確認するため、関連文書や病院での職員インタビュー、現場確認によるシステム監査を 2019 年より実施している。しかし、対象となる全病院の監査には数年を要することや、新型コロナウイルス感染症の影響により現地訪問によるシステム監査が困難な状況となり、監査で使用するチェックシートを用いた「情報セキュリティ自己点検」を各病院で行い、またグループ初となるオンラインでのシステム監査を 2021 年 1 月に実施した。

2. 目的

これらの取り組みは、徳洲会グループ各病院の情報セキュリティレベルを向上させ、医療情報の漏洩等の事故を未然に防止するため、各病院で医療情報システムの運用および医療情報の取り扱いが適切に行われるよう支援することを目的としている。

3. 方法

3.1 体制

運用管理規程の管理・改訂、システム監査、情報セキュリティ自己点検などは、徳洲会グループの「情報システム管理部会」（以下「SE 部会」という）の内部に設置された法令順守部門と徳洲会インフォメーションシステム株式会社（以下「TIS」という）が主体となり、一般社団法人医療 ISAC（以下「医療 ISAC」という）の協力も得て実施している。

SE 部会は、徳洲会グループ 65 病院に在籍する院内システムエンジニア（以下「院内 SE」という）約 140 名で構成する病院横断的な組織で、医療機関の IT に関する情報提供・共有、教育・研修、災害・障害対策やセキュリティ対策などに取り組んでいる。TIS は一般社団法人徳洲会の 100%出資の関連会社で、徳洲会大阪本部内に置かれていた情報システム部が 2009 年 10 月に独立した組織であり、徳洲会グループ全体の IT 化を推進する役割を担う。また医療 ISAC は 2013 年に設立された一般社団法人メディカル IT セキュリティフォーラムが 2019 年に米国を拠点とするグローバルな医療系サイバーセキュリティ連携団体 Health Information Sharing and Analysis Center との事業提携により改組した団体で、医療分野における情報セキュリティの重要性の啓発と問題解決のためのソリューション提供を行っている。

3.2 情報セキュリティ自己点検の概要

情報セキュリティ自己点検は、システム監査で使用する「情報セキュリティチェックシート」にもとづき各病院が自院のセキュリティ状況を把握する目的で行う。チェックシートは組織体制、規程やマニュアル等文書類の整備、パスワードやアンチ

ウイルスソフトなど技術的対策、データ抜き出し等のルール、端末やサーバ運用の状況、BCP 対策、セキュリティに関する院内周知等、計 81 項目で構成され、それぞれの項目を○(充足)・△(一部充足)・×(未充足)・NA(該当なし)で評価し、△と×の項目にはその理由を記載する。各病院で実施された結果を法令順守部門で集約、分析し報告書にまとめ、2020 年 10 月に開催された SE 部会全国会議で報告した。

3.3 経過

2019 年 12 月～2020 年 1 月:各病院に情報セキュリティチェックシートを配布し、病院は約 1 か月をかけて自己点検を実施、結果をチェックシートに記入して法令順守部門へ提出した。

2020 年 2 月～4 月:提出されたチェックシートを法令順守部門で採点し(各項目に付けられた○は 5 点、△は 3 点、×および NA は 0 点)、結果のグラフ化を行い、分析・評価を行った。

2020 年 5 月:新型コロナウイルス感染症拡大防止のため、予定されていた訪問によるシステム監査が出来ないことから、法令順守部門でこれに代わるセキュリティに関する取り組みを検討した。その結果チェックシートのうちの重要項目(厚労省ガイドラインと会計監査の IT 内部統制、いずれの要件にも含まれる 16 項目)について、各病院が前回の自己点検で△・×を付けたものに対し改善を行い、○と評価できるようにグループ病院での事例や改善策を収集し提供することとした。

2020 年 6 月～7 月:院内 SE からの意見にもとづき、チェックシートの項目を一部見直し、前述の事例・改善策を追記した「情報セキュリティ重要項目チェックシート(16 項目)」を作成した。

2020 年 8 月～9 月:「情報セキュリティ重要項目チェックシート」を配布、各病院では改善に取り組んだ上で重要項目の自己点検を行い、結果をチェックシートに記入して提出した。

2020 年 10 月～11 月:提出されたチェックシートを法令順守部門で集約・採点・分析し、報告書にまとめた。

3.4 情報セキュリティ自己点検の結果

情報セキュリティ自己点検の結果は法令順守部門により次のような形で報告書とした。

① 概要:経緯・目的・実施期間・点検方法など
② 病院ランキング:合計点による病院のベスト 20・ワースト 20
③ 項目ランキング:項目のベスト 20・ワースト 20
④ 各項目の○・△・×・NA の病院数(円グラフ)とコメント
⑤ 総評と今後の取り組み

③のワーストランキング上位の項目を以下に示す。

・ やむを得ず個人所有のパソコン・タブレット等を院内 LAN に接続する場合、また院内業務に利用する場合は申請・承認の手続きのもとに行われている。(図 1)

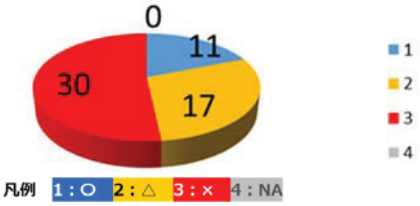

図 1 個人所有のパソコン等の院内 LAN への接続

・ アプリケーション ID のログイン試行回数は5回以下に設定されている。(図 2)

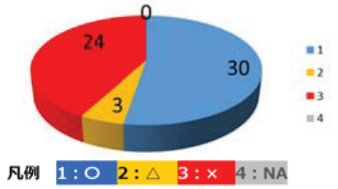

図 2 アプリケーション ID の試行回数

・ 不要なアプリケーション ID の残存有無が定期的に確認されている。(図 3)

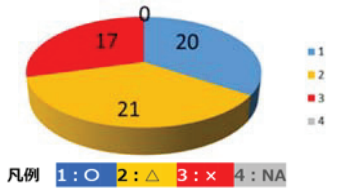

図 3 不要なアプリケーション ID の残存有無確認

・ 共用の ID はルールに基づき運用している。(図 4)

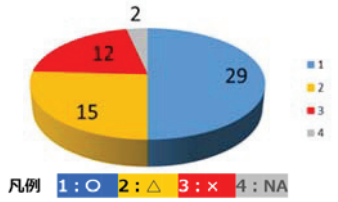

図 4 共用 ID の運用

また、ベストランキング上位の項目を次に示す。

・ ウイルス対策ソフトは適正なライセンス数を購入している。(図 5)

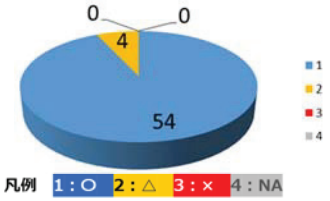

図 5 ウイルス対策ソフトのライセンス数

・ 個人情報保護に関する包括同意掲示が患者に見える場所に張り出されている。(図 6)

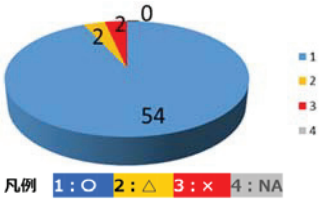

図 6 個人情報保護に関する包括同意掲示

・端末からデータを抜き出せないよう設定している。(図 7)

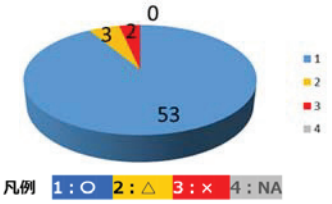

図 7　端末からデータを抜き出せない設定

・ID による操作履歴はログとして取得されている。(図 8)

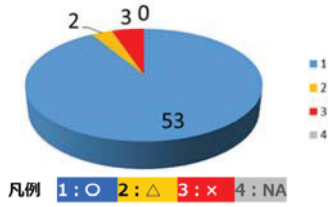

図 8　ID による操作履歴ログの取得

3.5 重要項目自己点検時の配布資料

「情報セキュリティ重要項目自己点検(16 項目)」チェックシート配布時に、病院事例や改善策をチェックシートに記載するとともに、参考として実際に使われている帳票やマニュアル等も各病院へ提供した。内容は次のとおり。

- 役務任命簿(記入例)
- ID・権限登録・変更・削除申請書(記入例)
- ID・権限の登録・変更・削除に関する申請／承認フロー
- ID・権限棚卸結果報告書(記入例)
- 入退室記録管理表(記入例)
- サーバルーム点検簿
- データ登録者検索操作説明書
- イベントビューア起動マニュアル
- アカウントの適正な利用について(院内周知資料)
- パスワード設定ルールについて(院内周知資料)

3.6 重要項目自己点検の結果

「情報セキュリティ重要項目自己点検(16 項目)」の結果は法令順守部門により前回の「情報セキュリティ自己点検」の結果と同様の形式で報告書とした。この中で④ 各項目の○・△・×・NA の病院数(円グラフ)とコメント については、前回の結果との比較を行いその内容を記載した。

前回の結果から○と評価した病院数が大きく増えた、つまり改善が進んだ項目を次に示す(矢印の左側の数字が前回、右側が今回の全体に占める○を付けた病院の割合)。

- 不要なアプリケーション ID の残存有無が定期的に確認されている ： ○ 34% → 60%
- サーバ OS 上の不要な ID の残存有無が定期的に確認されている ： ○ 31% → 68%
- 運用管理者・情報システム管理者・情報セキュリティ管理者等の役務者が任命されている ： ○ 56%→ 80%
- 自身の ID を他の職員が利用するなどの不適切な運用をしていない ： ○ 59% → 88%

逆に改善進捗が思わしくない項目を次に示す。

- アプリケーション ID のパスワードは英数混在文字が求められている: ○ 62% → 75%
- サーバは第三者に触れられないようラックに設置して施錠している: ○ 69% → 82%
- アプリケーション ID のパスワードは最低 2 ヵ月に 1 度変更している ： ○ 88% → 89%
- サーバ OS のセキュリティイベントログ(少なくともログイン/ログアウトログ、ログイン失敗ログ)が取得されている: ○ 78% → 89%

3.7 オンラインシステム監査の準備と実施

「情報セキュリティ自己点検(81 項目)」を実施した際(2019 年 12 月～2020 年 1 月頃)は、その結果にもとづき監査対象病院を選定し、システム監査を継続する予定であった。しかし、新型コロナウイルス感染症の影響を考慮して一旦中断、監査員が現地を訪問しない監査が可能かを法令順守部門で検討し、2021 年 1 月に Web 会議によるグループ初のオンラインシステム監査を行った。オンライン監査実施を決定してから、約 4 か月で次のとおり準備を行った。

2020 年 10 月:法令順守部門メンバーが在籍する新庄徳洲会病院を対象病院とし、試行的に実施を行うこととした。

2020 年 11 月～12 月:法令順守部門で監査方法の検討を行い、監査を効率的に実施することを目的に、従来は訪問して現場を確認していた項目の中でも事前の文書監査が可能と判断したものについては、現場の写真や画面のハードコピーの事前提出を求め、これにより監査当日の限られた時間の中で、またオンラインという環境でも訪問監査に近い監査を行うこととした。その結果、これまでは全 81 項目中 37 項目について事前文書監査を行っていたが、これを 57 項目へと大幅に増やすこととなった。

2020 年 12 月末:新庄徳洲会病院へ 2021 年 1 月にオンラインにてシステム監査を行うことを通知、合わせて事前文書監査用の資料提出を依頼した。

2021 年 1 月中旬:新庄徳洲会病院より、事前文書監査用の資料一式が提出され、監査員が文書監査を行った。

2021 年 1 月 29 日:Web 会議で新庄徳洲会病院、監査員所属病院、TIS を繋ぎ、システム監査を実施した。

2021 年 2 月上旬:法令順守部門で監査結果の検討を行って監査報告書を作成、新庄徳洲会病院へ提出した。

2021 年 3 月上旬:新庄徳洲会病院より改善報告書と関連資料が提出され、法令順守部門会議で内容に問題ないことを確認し、報告完了とした。

4. 結果と考察

「情報セキュリティ自己点検(81 項目)」は、法令順守部門で各病院の結果を集約・分析した結果、全般的に『端末やサーバ設定など直接的に SE が関わる』項目は概して成績が良く、一方『マニュアル作成や運用方法の院内周知など』の項目は思わしくない傾向が見られた。各病院のセキュリティレベルに予想以上の差があることや多くの病院に共通する弱点なども判明し、グループのセキュリティ対策の課題を明らかにすることができた。また、項目の中で実際の運用に合わないもの、基準が曖昧で病院によって判断が難しいと思われるものもあり、チェックシートのブラッシュアップの必要性も感じた。

その後各病院が改善に取り組んで行った「情報セキュリティ重要項目自己点検(16 項目)」の集計結果では、全ての項目で前回の結果より改善が見られ、他病院の事例や改善の具体策の提示に一定の効果があることが確認できた。しかし重要項目に絞ったにも関わらず、なお△や×が多い(つまり改善されていない)病院があり、法令順守部門で改善の支援を検討している。

オンラインシステム監査は、病院側には事前提出資料を増やすことにより、監査までの準備に負担をかけることとなった

が、これにより当日の確認事項が大きく減り、これまでより余裕をもった監査が実施できた(従来の監査時間:約 2 時間 40 分 → オンラインでの監査時間:約 2 時間 20 分)。また監査病院で院内 Wi-Fi とタブレット端末のカメラ機能を利用した現場職員へのインタビューがスムーズに行えたり、書画カメラを使用した書類提示で問題なく閲覧できる等、監査を受けた新庄徳洲会病院の協力もあり、訪問監査と遜色ない内容で監査を行えたと考える。しかし、院内 Wi-Fi が届きづらい場所では画像や音声の状態が悪くなったり、また監査開始時の説明や総評に参加した職員の表情や反応が Web カメラ越しでは分かりづらい等の課題も確認でき、今後の監査ではこれらを改善する工夫を考えている。

5. 結論

いわゆるコロナ禍においては、これまで考えられなかった大きな制約があらゆる分野にかかり、法令順守部門が行ってきた取り組みも例外ではなかった。しかしその中で実施した「情報セキュリティ自己点検」「同重要事項自己点検」は、システム監査を受けずとも病院内でセキュリティ上の問題を把握しそれに積極的に対応し改善を進められるという結果をもたらし、またオンラインシステム監査は、病院と監査員双方の労力・時間・コストを削減しつつ、訪問監査に近い内容と結果を得ることができ、いずれも成果があったと考える。

今年度後半はさらに新たな取り組みとして、自己点検でセキュリティ面の問題が判明した病院に対し Web 会議による個別面談と支援を行うことを計画している。こうした様々な活動により、各病院とグループ全体のさらなるセキュリティレベル向上を目指していきたい。

セキュリティレベルの向上は煩雑さ・使い勝手の悪さを伴う場合もあるが、病院が要配慮個人情報を日常的に取り扱うというその環境の特殊性からも、一般の企業等と比較してより高いセキュリティに対する意識と対策が必要である。法令順守部門の取り組みを各病院が理解し受け入れ、協力することで厚労省ガイドラインの求める『管理責任』と『説明責任』を果たすことが出来ると考えている。

6. 謝辞

今回の取り組みを行うにあたって、情報セキュリティ自己点検チェックシートの作成およびシステム監査に助言と支援を頂いた一般社団法人 医療 ISAC の皆様に深謝いたします。

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 第 5 版. 2017.
2) 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 第 5.1 版. 2021.
3) 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 第 5.1 版に関する Q&A. 2021.
4) 一般財団法人医療情報システム開発センター. 保健医療福祉分野のプライバシーマーク認定指針 第 4 版. 2018.