「ISMSの動向と医療分野への適用」

第34回日本医療情報学連合大会　ワークショップ 6

「ISMS の動向と医療分野への適用」

2014年11月7日 幕張メッセ

より

ISMSの動向と医療分野への適用

ワークショップのプログラム

（発表者の所属・肩書はワークショップ開催時点）

1. 医療機関経営者の立場からの医療情報セキュリテイマネジメント

   ① 安藤裕［（独）放射線医学総合研究所重粒子医科学センター病院 病院長］
   ○ 放射線治療専門病院における ISMS 構築とIHEの導入

   ② 熊本一朗［鹿児島大学医学部附属病院 病院長］
   ○ 大学病院における医療データのマネジメント

2. Andreas Gehrmann［Managing Director SRMS & Associates Pte. Ltd.］
   ○ Healthcare information security in the cloud
   ○ Security standards and risk assessment

3. 森口修逸［株式会社エム・ピー・オー 代表取締役］：
   ○ 高度医療研究機関の役割と新 ISMS によるマネジメントシステム

4. 高取敏夫［JIPDEC 情報マネジメント推進センター センター長］
   ○ 日本のＩＳＭＳ認証取得の現状と情報の高度利用

5. ラウンドテーブル　司会：鈴木淳夫（千葉大学非常勤講師)
   ○ 高度医療研究機関とＩＳＭＳの実践　参加者：講演者全員

ISMSの動向と医療分野への適用

参加者:向って左から（所属・肩書はワークショップ開催時点）

- **熊本一朗**［鹿児島大学医学部附属病院 病院長］
- **安藤裕**［（独）放射線医学総合研究所重粒子医科学センター病院 病院長］
- **Andreas Gehrmann**［Managing Director SRMS & Associates Pte. Ltd.］
- **高取敏夫**［JIPDEC 情報マネジメント推進センター センター長］
- **森口修逸**［株式会社エム・ピー・オー 代表取締役］

ISMSの動向と医療分野への適用

ワークショップ　高度医療研究機関とＩＳＭＳの実践　発言要旨（文責：鈴木）

１．高度医療研究機関における情報セキュリテイマネジメントの課題

鈴木】ISMSの目的は「組織のリスクマネジメントにより利　害関係者に信頼を与えることを意図している」にも関わらず、現実としてISMS導入による関係者の「評価疲れ」増大を懸念する意見もある。この折り合いをどうつけたらよいか？

熊本】病院に対する様々な評価要求が増えている中、ISMS導入は職員への負荷がさらに増えるので評価疲れと表現した。ただし、ISMSの主旨を理解した上で現状で可能な範囲で情報セキュリティ活動を行っている。

安藤】当院は2007年以降ISMSの手法を取り入れたセキュリティマネジメントを実施しており、職員の間にも活動が定着していると思う。色々と手間のかかるところもあるが、きちんと行っていると言えることはもしも何か問題が起きても弁解にはなる。

高取】これまでISMSについて色々な業界を見てきたが、総じて言えることは無駄な苦労が多いことである。詳細なリスクアセスメントを作って動かしても本当に効果があるか分からない。リスクマネジメントの本質を理解した上で各病院及び組織に合ったリスクマネジメントを行うべきである。

ISMSの動向と医療分野への適用

ワークショップ　高度医療研究機関とＩＳＭＳの実践　発言要旨（文責：鈴木）

２．リスク分析の対応と情報資産（個人情報・匿名化情報・メタ情報　等）

鈴木】これまで情報保護と言えば個人情報保護だけに関心が集まる傾向があった。個人情報は重要であるが医療情報の一部でしかない。情報全体を含めた管理をどうするか

熊本】情報管理者あるいは院長としてこれまで個人情報流失に注意してきたが情報資産を管理し利用する立場から、例えば臨床研究においては倫理審査委員会を通す、DWH(Data WareHouse)の使い方についても無制限ではなく内容により倫理審査委員会を通すなど、情報資産のリスク分析を行っているつもりである。しかし、先ほどのISMSに関す議論を聞いていると内部監査だけでなく外部からの監査を受けることにより自分たちの気付かなかった「抜け」や考え方の甘い部分を指摘されることがあるかもしれない。そのような点から今後チェック体制をより厳しくするべきだとも思う。

安藤】当病院は研究所としての性格から研究のための情報資産は重要な位置づけになっている。普通の研究者が研究する場合は院内のIRB（倫理審査委員会）を通し、さらにゲノム関連研究の場合は連結可能匿名化を行うことになっているが、１年に１度外部監査を行い、管理体制を始め匿名化や情報の扱いがきちんと行なわれているかどうかチェックする体制を整えている。

ISMSの動向と医療分野への適用

ワークショップ　高度医療研究機関とＩＳＭＳの実践　発言要旨（文責：鈴木）

３．マルチベンダシステムの情報セキュリテイマネジメント（責任分界点の明確化）

鈴木】病院情報システム全体を見ると例えば電子カルテはA社であってもネットワークで繋がれたPACSはB社、心電システムはC社..などほとんどの病院ではマルチベンダシステムである。情報セキュリティマネジメントから見た対応はどうか？

熊本】一番危ないところだと認識していて病院のネットワークにつなぐシステムはちゃんとした契約を結ぶこと、特に外から侵入の可能性のあるリモート保守の契約などもきちんと見ておかないといけない。その上でネットワーク全体については医療情報部が厳しく監視しており、契約はもちろん異常がないかの検知、監査を含めて管理し、インフラである病院情報システムが止まらないように気を使っている。

安藤】マルチベンダーシステム全体を医療情報室が管理し、医療情報室が窓口となって各メーカーと契約し、責任分界点を決めている。各部門で調達するシステムに関しても医療情報室が入札仕様書に入れる文言のひな形を作って各部門に事前配布している。

ワークショップ　高度医療研究機関とＩＳＭＳの実践　発言要旨（文責：鈴木）

４．職員の頻繁な異動に対応したISMSの力量の維持拡大策（教育実施プラン）

鈴木】病院、特に高度研究医療機関においては職員の異動が頻繁である。ISMS教育面から見た対応はどうか？

熊本】大学病院は教育病院としての側面も持っている。医師・看護師を始め関係者に対して医療・診療面のみならず情報セキュリティに関しても教育病院である。鹿児島県で唯一の大学病院・特定機能病院として教育した人材が地域に出て行くことによって市中病院から開業医に至るまで情報セキュリティの考え方を広めることができる。

情報セキュリティは地域の医療機関全体で支える必要があり、大学病院では人が入れ替わることが大変と捉えるのではなく教育して地域に送り出すことを文化と捉えるようにポジティブに考えるべきである。

安藤】当病院では毎年4月に全職員に対する情報セキュリティ講習を行っており、未受講者はIT使用許可を取り消すこととしている。中途採用者等にはDVD教育ビデオを貸し出して対応している。

ISMSの動向と医療分野への適用

ワークショップ　高度医療研究機関とＩＳＭＳの実践　発言要旨（文責：鈴木）

５．医療分野におけるクラウド利用に関して

鈴木】今後医療に関するクラウド利用が注目されている。日本でも地域連携等で使われ始めているが、本日はゲルマン氏よりシンガポールにおける医療連携にクラウド利用の例の紹介があった。医療においては可用性と機密性のバランスが重要であるとの内容だと理解したが、さらにコメントがあればお願いしたい。

Gehrmann】医療でもっとも重要なのは事業継続計画（BCP：Business Continuity Plan、BCMS：Business Continuity Management System）である。もしも医療分野のクラウドのサービスプロバイダが事故を起こせば大変なことになる。そこで医療における事業継続(Business continuity)マネジメントが重要となるがこれは情報セキュリティマネジメントと別物ではなく一体のものとして総合的にマネジメントすべきものである。

これまでシンガポールにおいて経験した多くの事例はこれからのクラウド利用の参考になると思われる。

ワークショップ　高度医療研究機関とＩＳＭＳの実践　発言要旨（文責：鈴木）

６．地域医療連携とISMSについて

鈴木】熊本先生のご講演の中にあったように鹿児島県は南北600Kmに及ぶ広大な地域をカバーしている。この地域全体の医療を支えようとする立場から見てどうか？

熊本】このような広範囲の地域の医療を支えることはIT無しでは不可能である。例えば奄美群島で手術が必要かどうかわからない患者さんが２泊３日かけて鹿児島大学病院まで来て結局手術しなくて良いとなって帰るというのでは経済的損失が大きい。これは事前に遠隔カンファレンスを行えば判断できることである。このように広範囲をカバーするのが地域医療連携であり、ITは必需品と言える。

鈴木】放医研は患者の紹介・逆紹介が多く、他医療機関との連携が必要になる機会が多いが対応は？

安藤】当病院の場合、９５％が紹介患者である。画像データが重要なので送ってもらうようにしているが、現状はCDで送ってもらうことが多く、ネットワーク経由はほとんどない。例えばあるサーバーにパスワードを付けてUPしていただいた画像をダウンロードするということは暫定的に行っている。

将来的には紹介状と共にネットワーク経由で送受信するのが望ましいと思うが、現状では当院の電子カルテは外部ネットワークとはセキュリティ面から遮断されておりできない。今後ネットワーク経由でセキュリティの高い状態で医療情報を送受信するためのガイドライン整備を望みたい。

ISMSの動向と医療分野への適用

ワークショップ　高度医療研究機関とＩＳＭＳの実践　発言要旨（文責：鈴木）

７．医療機関における情報セキュリティについて

鈴木】医療機関に対する情報セキュリティについてコンサルタントの立場からコメントをお願いしたい。

森口】熊本先生とのお話の中で大学病院同士が相互監査しあっていることを聞いたが良い考えだと思う。内部監査は自分の部署以外を相互監査するものであるが、業務内容を全然知らない人から監査を受けるのではなく、他大学病院の同じ部門の人から監査を受けることを制度化すると目標に一歩近づくと思われる。

ワークショップ　高度医療研究機関とＩＳＭＳの実践　発言要旨（文責：鈴木）

・質疑応答

質問者】厚労省の安全管理ガイドラインには「ISMSの実践」が書かれている。本日のお二人の院長先生講演はガイドラインを守っている中でISMSを実践しているのか、ガイドラインとは独立して実践しているのかがよくわからなかった。

森口】先ず、ガイドラインの記述は「望ましい」であり、MUSTとは書かれてない。

熊本】当病院ではISMSは取得してはないがそれに準じた形の対策は行っている。ISMSの取得は職員にとってもハードルが高いので取得を目標とするのは時期尚早と考える。国立大学病院同士の相互チェックなどを通してレベルを高めた上でチャレンジしたいと考える。

質問者】ガイドラインの記述は「望ましい」であることについて了解した。参考までに今年本院に厚労省の特定共同指導が入ったが最初に聞かれたことはBCPを含めガイドラインを守っているかどうかであった。