#	導入研修　大阪急性期・総合医療センター事例コース　第3回　組織編	回答
1	医療情報システムサイバー攻撃に対するBCPが整備できていて、訓練も行われていれば、全日空のシステム障害発生時、空港における紙チケットによる円滑な乗客誘導、日本航空2024年1月2日　羽田衝突事故　乗客全員避難　のように、たとえ災害が起こっても円滑な対応はできると見込まれますが、医療機関に於いて、BCPをベースにこのような円滑な対応が実現した、という実例を未だ見たことがありません。 現時点に於いて病院の実例はなくとも、自施設がいつ何時システム災害が発生し、初動対応を迫られる、その取り組み方法を世間が注意深く見ている、という事態になることはあり得るため、そのような心構えでBCP作成や訓練、内容のアップデートに取り組んでいくべきと愚考いたしますが、ご見解はいかがでしょうか。	令和6年度の診療報酬の改定においても、診療録管理体制加算の見直しが行われます。 https://www.mhlw.go.jp/content/12404000/001220531.pdf 内容としては、 1.非常時に備えたサイバーセキュリティ対策が講じられるよう、専任の医療情報システム安全管理責任者の配置及び院内研修の実施を求める医療機関の対象範囲について、現行の許可病床数が400床以上の保険医療機関から許可病床数が200以上の保険医療機関に拡大する。 2.医療情報システムのオフラインバックアップ体制の確保、「医療情報システムの安全管理に関するガイトドライン」に基づく業務継続計画(BCP)の策定及び訓練の実施についても新たに評価を行う。 となっています。
2	①基幹システムが障害起きた時、紙カルテ運用の対処としてワープロ端末の準備とご紹介がありましたが、そのワープロ端末に求められる要件があれば情報共有いただきたいです（Officeとプリンタの設定をしておけば問題ないか等）。これは病院で決めることかと思いますが、大阪の病院等の事例を踏まえて、「このソフトを入れて役に立った」「事前に同意書類のテンプレートをデスクトップ上に配置しておいた」等、具体的な情報があると準備しやすく助かります。 ②病院にセキュリティ担当者(ある程度のセキュリティの知識がある者)がいる前提でご講演いただいていることに少し違和感を感じました。システムベンダがセキュリティの専門家ではないのとおっしゃっているのと同様、病院はシステムベンダより更にセキュリティに明るい人材は乏しいです。経営者に諸々を分かってもらうためには、セキュリティの担当者が入念な調査・背景を把握した上で動かなければなりません。その業務を委託しようにも、本講演では"丸投げ"という表現をされており、病院の職員がやるしかないと思うのですが、通常の業務に忙殺され、セキュリティ業務を専任で実動できている職員がいる病院は少ないと思います。（安全管理責任者の存在はあくまでトップであり、実動は末端の職員です。かくいう私も、全体の業務の1割程度しかセキュリティの業務に割り当てられていません）そういった病院もいることを前提で、整理するポイントをアドバイスいただけると有難いです。	①Officeとプリンターの設定で結構です。さらに紙カルテ運用において、指示だし・指示受けの際の用語や様式をあらかじめ定めておくことも重要です。 ②人材不足は病院の大小に関わらず共通の課題ですが、その中でも対策が十分である病院との差は、経営者がその必要性を理解しているか否かだけだと考えています。 経営者に理解してもらう方法の一つとして、サイバーインシデントを起こしてしまった際の記者会見を想像してもらうのはどうでしょうか。 (a)何が起きたのか、(b)その影響範囲はどのくらいで、(c)いつ頃復旧するのか これらは最低限、記者から正確な回答を求められ、できなければ経営責任問題です。 ポイントはセキュリティ対策の良し悪しに限らずインシデントは起こり得るということ。 (a)(b)(c)を即座に回答できる(その材料をそろえられる)組織はインシデント発生確率は著しく低下するということです。 これらを準備するには、日頃のセキュリティ運用管理に必要な人員や適切なベンダーへの委託、有識者の支援などが必須となるため、丁寧に突き詰めていけば自動的に人材不足問題にスポットが当たると思います。丁寧に突き詰めるテーマは、P.24～28を参考にしていただければと思います。

#	導入研修　大阪急性期・総合医療センター事例コース　第3回　組織編	回答
3	ガバナンスとは、内部統制(組織の上下関係)とは違う、横(組織の外部から内部、内部から外部、例えばセキュリティコンサルタント)の関係と考えますが、大阪急性期・総合医療センターには、外部からリスクについて忠告してくれる別組織は、インシデントが発生するまでいなかったという解釈でよいのでしょうか。	基本的に、ガバナンスと内部統制は同意だと思います。このご質問のイメージの差は、内部統制が世の中で謳われた時期に、いわゆる「横」の必要性を明示化されなかっただけだと思います。御存知の通り、医療に限らずその事業を継続するうえで、外部組織との連携やインシデントの影響は管理されるべきものでしたし、セキュリティの知見がなければ相談が必要でしたが、内部統制の専門家がそれを明言してこなかったのが原因と考えます。 大阪急性期・総合医療センターは、インシデントが発生するまでこの「横」の関係はありませんでした。特にセキュリティに関しては、ベンダーが考えていてくれていると信頼していましたが、今回のインシデントを機にベンダーに対するアンケートを実施した結果、ベンダーのほとんどがセキュリティを検討していないことがわかりました。
4	サイバーセキュリティ―対策に関する予算は計画していないため、予算のかからない対策などあれば教えてほしい	予算を抑えて(キャッシュアウトしないで)対策する方法はありますが、それには人員不足やセキュリティ知識不足、ベンダーの知識不足など課題があると思います。 それらを解決するためには、サイバーセキュリティ―対策に関する予算を計画しなければなりません。まずはそこからだと思います。上記項目#2②を参考にしてください。
5	サイバーインシデント発生時のレベルごとの公的機関などへの通報基準	医療情報システムの安全管理に関するガイドライン第6.0版（経営管理編）においては、以下を示しています。 不正ソフトウェアの混入などによるサイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（平成 30年 10 月 29 日付け医政総発 1029 第 1 号・医政地発 1029 第 3 号・医政研発 1029 第 1 号厚生労働省医政局関係課長連名通知）に基づき、所管官庁への連絡等、必要な対応を行うこととなっている。
その他		
1	本日の資料掲載先として紹介されていたイーラーニングはどこから申し込めるかご教授ください。	以下のURLよりお申込みください。申込受付が3/11(月）までとなります。ご受講期間は3/29までです。 https://mhlw-training.saj.or.jp/training/#5
資料・アーカイブ		
1	第三回しか参加していないが、2回目と1回目の資料も入手したい。可能だろうか？	本事業終了時（年度末頃）に、公開予定です。 公開した際には、MISTサイト（ https://mhlw-training.saj.or.jp/ ）からお知らせいたします。