#	ご質問	回答
その他		
1	今回は大規模病院を想定した部分も多かったが、対策費用も人材も確保しづらい診療所レベルでの研修者向けセキュリティ対策研修予定はありますか？	システム・セキュリティ管理者向けの研修はできる限り汎用的な対策に焦点を当てています。当該研修の受講をお願いします。
2	本日はありがとうございました。システムベンダーからは、普段リモートメンテナンスをしてもらっていますが、セキュリティ上は、あまりよくないのでしょうか。	リモートメンテナンスの実施方法を確認してください。（どこでも誰でもメンテナンスできるような状況にないか、接続先のセキュリティ対策は適切に行われているかなど）
3	バックアップが重要なのは理解できますが、何日分位の差分バックアップがとれていれば良いのでしょうか？	各機関のデータ量や費用面でも対応可能な日数が異なると思われるため、何日分が適切かとは言い難く、できる限り長い期間バックアップを取得して頂く必要があります。
4	医療情報システムのアップデートは動作しなくなるリスクがあるため，導入・更新時でないと，病院にとってはかえってリスクとなることが想定される．しかし，厚労省の予定している立入検査の令和6年度中の確認事項には，セキュリティーパッチ（最新ファームウェアや更新プログラム）を適用していることが求められており，実現不可能ではないかと考えている．このあたり，経営者側として，取るべき対策や考えておくべきことがあればご教授いただきたい.	セキュリティーパッチ（最新ファームウェアや更新プログラム）を適用に向けた調整や確認など、病院としての方針を各ベンダーに適切に伝えるとともに現場調整の推進をお願いします。
5	いわゆる総合病院なのだが、リハビリや歯科口腔外科の部門システム会社のセキュリティというかシステム構築能力からそもそも水準に達していないと判断せざるを得ず、では代わりの会社はといっても似たり寄ったりで、これでセキュリティ対策と言われても身動きができない。経営者としての行動指針をぜひ。	セキュリティの専門家に確認を行ったり、対応が行えている他院等との連携を行い、セキュリティの対応推進をお願いします。また、「医療情報システムの安全管理に関するガイドライン」をはじめとした各種ガイドラインを確認していない場合もあるため、熟読及び対応推進をお願いします。
資料		
1	本日使用した資料はどこかで入手できますか？	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。
2	今回の研修で用いた資料は提供いただけないでしょうか	
3	研修資料の掲載は有りますか？	
4	当日の資料について、後日ダウンロードできるというお話があったかと思いますが、いつ頃・どのように入手できるようになりますか？	
5	CISOの下に位置する立場で、経営層ではありません。今回の研修内容などを踏まえて、病院全体を動かしてくれるように働きかけたいと思います。資料とあるものを前もって印刷していたが、使えませんでした。今回の研修内容の資料はどこにあるのでしょうか？	