#	ご質問	回答
1	10/31に何があるのか最後まで分かりませんでした	つるぎ町立半田病院は2021年10月31日に、と大阪急性期・総合医療センターは、2022年10月31日にそれぞれのインシデントが発生しております。
2	ITに関係する部署でセキュリティを維持するためポリシーの策定やその啓蒙などを行っています。一般企業からすると常識、または最低限のレベルのポリシーだと思いますが、各事業所や部署からは「情シスが駄目駄目言う」「情シスがIT技術による業務効率化を邪魔している」「情シスは起きるか起きないかわからないインシデントの対策を頑なに守らせようとする」「業務効率化のためにはもっとポリシーを緩めるべき」と言われます。言う職員の中には上の役職の者も含まれ、徐々にポリシーを緩めなければならない風潮になってしまっていますが、このような状況で効果的な啓蒙の仕方や説得方法はありますでしょうか。 また、この講義資料を内部共有用に頂くことは可能でしょうか。	ダメとする理由を例えば既存のログを元に、組織に起きている現状を可視化して、より具体的に示すことが必要だと思います。また、万が一緩める傾向になるとすれば、組織としてどのようなリスクを受容したことになるのか、リスクをきちんと示すことが大切です。もしそれでインシデントが起きるようであれば、リスクを受容した側の責任となるでしょう。
3	インシデント発生時の連絡体制において、連絡する順番を具体的にご教示いただければ幸いです。	状況により異なりますが、まずは既存のベンダーに連絡し、現状と（契約内の）インシデント対応支援を依頼。その後、警察や所管官庁（厚生労働省）等にご連絡いただくのが良いでしょう。
4	クラウドの電子カルテ等を利用するにあたって、HIS系ネットワークの構成をどのようにするのが良いのでしょうか？	詳細は既存の環境や構成、利用方法によっても異なりますが、総務省「クラウドサービスの利用・提供における適切な設定のためのガイドライン」などを参照し、クラウドをご利用ください。
5	こちらは1回の申し込みで、前回数参加可能でしょうか？	はい、その通りです。
6	ゴミ箱理論（仮）にいたく共感いたしました。ぜひ掘り下げて、ごみを捨てる上層部にどう対処していくか、理論体系の構築を進めていただければ幸いです。	ありがとうございます。
7	ご説明あった資料の提供はあるのでしょうか。	当該サイトに公開予定です。
8	サーバ管理とクラウド運用ではセキュリティ対策上、どちらが運用しやすいのでしょうか。	オンプレミス環境という意味かと思いますが、いずれも運用のしやすさとしにくさがあります。クラウドはインフラ部分は事業者側の更新ですが、事業者のタイミングで更新されるため、利用者は更新に伴い設定の直しなどを行う必要があります。セキュアに利用するという意味で、既存のインフラに脆弱性が多い環境であればクラウド環境の方が安全でしょう。
9	サイバーセキュリティでは閉域網か否かがよく議論されますが、電子カルテなど普段は外部と接続していなくても、リモートメンテナンス用などで外部との接続ポイントが1か所でもあれば、それは閉域網ではないという解釈でよろしいでしょうか？	はい、その通りです。
10	システム・セキュリティを管理するという点において、ベースとなる考え方やガイドラインなどの一定の指針は理解できましたが、システムの調達等を行う際の調達仕様としてどのような記載を盛り込むべきか、具体的な記載事例などがあれば参考としたいのでご提示いただけないでしょうか。	参考までにIPAが公開している「情報システム・モデル取引・契約書（第二版）」https://www.ipa.go.jp/digital/model/model20201222.htmlのセキュリティプロセスをはじめとした文書等をご参照ください。
11	スライドの資料がほしい。	公開させていただきます。
12	スライドの中の従業員数に対する情報システム部門の平均人数の情報出典元について教えて下さい。院内で説明する際に必要な情報となると思うので	全国情シス実態調査2022（https://www.iij.ad.jp/svcsol/survey/all-it/2022/）をご参照ください。
13	ダウンロード式の病院で流せるコンテンツが欲しい	アーカイブ配信をご参照ください。
14	ベンダーとの契約時に盛り込んでおいたほうが良い事、特にしっかり確認しておくべきポイントはありますか？	インシデント発生時の対応条項や対応範囲の明確化、普段の脆弱性対応などの運用方針やルールをより明確にしておくとよいでしょう。
15	リモート接続の各メーカに対し、脆弱性対応等のセキュリティ強化、責任範囲、罰則等を記載した運用契約書を締結したいが、参考になるような契約案等があればお教え頂けないでしょうか。	現在、契約については検討をしておりますが、IPAが公開している「情報システム・モデル取引・契約書（第二版）」https://www.ipa.go.jp/digital/model/model20201222.htmlのセキュリティプロセスをはじめとした文書等をご参照ください。
16	ログの重要性が説明されていましたが、忙しいひとり情シス向けに「～せめてココだけは見よう～ 時短でできるログチェック」みたいな話をしてもらえるとありがたいです。	セキュリティ製品のログ設定状況とログはみましょう。侵入経路となるネットワークのログ、またADなどがあればADサーバのログなどを確認しましょう。
17	医療機関のシステム担当者の人数の実情がわかりましたらご教授をよろしくお願い致します。又、適正人数の計算方法などで参考になる情報がございましたら併せてよろしくお願い致します。	そのような情報を把握しておりません。
17	職員を対象とした情報セキュリティに関する訓練は、どのうようなものを行えばよろしいでしょうか。（100床未満の病院です）	集合型の対面またはオンライン研修、本事業で行っている初学者向けのコンテンツを用いて研修を行うことも1つでしょう。
18	診療所でシステムエンジニアのような知識が全くないがセキュリティについて任されました。講師の方の話も用語がわからないためついていけない部分がありました。この研修は参加すべきではないのでしょうか？	いいえ、本研修で継続的に学習頂ければと思います。
20	第2回からのお願いになりますが、通信システムに関する専門用語などは注釈を入れながら進めて頂けますと助かります。	できる限り対応してまいります。
21	電子カルテが感染する根本的な原因が何か知りたいです。	大阪急性期・総合医療センターの例でいえば、FW・ルーティング・権限・パスワード・セキュリティ対策ソフトの無効化など様々な要因があります。根本的に電子カルテそのもの構造が古い場合も考えられます。
22	病院側のVPNルータでいくら脆弱性を修正していても、そこに接続するベンダーのVPNルータに脆弱性があれば侵入はされる可能性はあるのでしょうか？ VPN情報を開示しないベンダーが多いので、侵入される可能性があるのであれば注意喚起を行いたいです。	VPNに限らずベンダーがサイバー攻撃を受ける可能性は否定できず、セキュリティ全般の管理や対応状況を確認する必要があります。特に病院とベンダーの接続方法を重点的に確認してください。