#	ご質問	回答
セキュリティの重要性理解と経営者の意識		
1	管理者から職員への落とし方に悩む	定期的にメールや内部ポスター、勉強会などで発信することが必要ですが、効果的なのはセキュリティ機器で検出（防御・検知）できている情報を組織内に共有することです。組織内で健全に監視や確認が行われていると思わせることによって職員の意識を徐々に高めることができるでしょう。
2	スタンドアロンPCを何台も準備しておくことは難しい。大阪ではすぐに調達したとお聞きしました。どうやって調達したかお聞きしたい。最低限のデータはバックアップを取っていますが、もっといい方法があれば教えてください。	ベンダーなどに相談し、調達することができました。今後、広域的な枠組みで端末を準備しておくことも必要でしょう。バックアップはデータに限らず、使う端末やソフトウェア、設定情報など様々なバックアップが必要です。バックアップ環境をローカルに持つのではなく、クラウドを活用し環境を含むバックアップを確保しておくことも1つの手段でしょう。
3	相談できる人がどれだけいるのか冒頭で話されていましたが、それを受けての説明がわからなかったです。病院の経営者として、相談できる人を、とくに売り上げ目当てのベンダーさんでない人を、たぶん信頼できる数人になるんじゃないかと思うのですが、どうやって見つけて味方につけていく手段があるのでしょうか？	日頃から周囲で信頼できる人を探すとともに、セキュリティに関する検知情報や相談がありましたら、MISTサイトの「インシデントかも？」などからお問い合わせをください。内容のご相談など行わせていただきます。
セキュリティの基本と考え方		
1	SOCを外注したらいくらかかるか？とあったが、厚労省のガイドラインでもSOCの記載はないと思われる。その一方、ゼロトラストの考え方では内部に侵入された場合の対策も必要である。実際どんなツールがあるのか。	セキュリティオペレーションを自組織で行うか、外部で行うかの違いであり、セキュリティ運用としての必要性はガイドラインにもある通りです。具体的なツールを記載するのは難しいですが、既存の環境を活用すれば新しいセキュリティ製品を買わなくてもゼロトラストは実現できる可能性はあります。
2	説明責任の観点からログの管理が大切であることはわかりましたが、どのようなログをどのように管理すればよいかが判らないので教えて頂けますと幸いです。	こちらのログに関する資料をご確認ください。（https://www.jpcert.or.jp/research/APT-loganalysis_Presen_20151117.pdf）
経営者の心がけと対策		
1	経営者として、優先度の高い事項は、何か？1.特定（情報の棚卸し）、2.評価、3.対応、という理解で良いでしょうか？	まずはインシデントが起きない環境であるか、特に外部との接続点を「特定」していくことが必要でしょう。システム、機器、ネットワーク、データなど様々な情報資産を特定し、評価、対応と進めていくのがリスクベースアプローチの基本的な進め方です。
2	組織全体を巻き込んでインシデント時対応の練習をしたいが、そこに興味を向かせるためにはどのようなやり方効果的でしょうか。	大阪急性期総合医療センターの報告書の概要版を確認させたり、経営会議の場等でBCP見直しや訓練をする等が考えられます。
ITガバナンス確率に向けて		
1	情報資産の把握、棚卸しと有りましたが、どの程度の粒度、細かさで把握すべきでしょうか？病院における具体例や手順を示して頂きたいです。	医療機関におけるサイバーセキュリティ対策チェックリストマニュアル https://www.mhlw.go.jp/content/10808000/001105752.pdf 2（1）以降を是非ご確認ください。
経営者のセキュリティ意識と知識		
1	＜経営者用チェックリスト＞ 経営者用チェックリストの詳細内容を知りたい。時間が短くチェックできなかった。	医療機関のサイバーセキュリティ対策チェックリストをご確認ください。 https://www.mhlw.go.jp/content/10808000/000845417.pdf
2	＜経営者用チェックリスト＞ 医療機関のサイバーセキュリティ対策チェックリストは医療情報システムの安全管理に関するガイドライン5.2版でのチェックリストに見えたのですが、6.0版のチェックリストに加えこちらも活用するというご趣旨でよろしいですか？	現時点では、公開されている版をご覧ください。
3	バックアップを取っていても、サーバー等が使用不能になると環境整備からすすめると復帰まで2ケ月はかかると言われています。他に方法はないのでしょうか？	クラウドを活用することが良いと思われます。
4	ITガバナンスの重要性は十分理解できるが、実際の医療現場ではやはり情報セキュリティ担当者が必要である。国家としてそのような人材の養成や研修システムはあるのでしょうか？	厚生労働省の事業の一環として、本研修事業が実施されています。
その他		
1	＜事例＞ 今まで個人の歯科クリニックが攻撃された事例はありますか？ ハッカーの攻撃対象はサーバーで、それを持たない零細個人クリニック、しかも診療が終わればPCの電源を必ず落としている場合、それでもハッキングされますか？	コンピュータウイルスに感染した事例は確認したことがあります。攻撃対象にできるものはなんでも攻撃を行い、サーバーもクライアントも攻撃者がサイバー攻撃に用いる1つのリソースとして活用するため攻撃基盤（ボット化）にされる場合もあります。PCの電源を落としても起動時にコンピュータウイルスが起動するように組み込まれていた場合、電源のON/OFFを繰り返しても感染している場合があります。
2	＜助成金＞ 医療療養型の病院です。 セキュリティ対策をどこまですべきかわからいのとランニングコストがかなり重くのしかかるため、電力ル導入できていません。検討中のベンダーにサイバー攻撃受けた場合の対応内容を確認したところ、「有料で復旧作業するのみ」 の回答でした。 今後、全国統一プラットフォームなどが構築された際のセキュリティはどうなるのでしょうか。 また、導入し易くなるような助成金や安価なシステムなどの予定はないのでしょうか？	厚生労働省の事業の一環として、本研修事業が実施されています。
3	＜契約＞ 今、一番不安なのが、各システムの業者が対応しているリモート環境の安全性です。 この環境は各社各様で、その安全性が当院側では分からない状況です。 これを回避するには、①当院側で、これを監視、制御できる仕組みを準備する。 ②各社と改めてセキュリティに関する契約を結び、被害時の責任を明確にすることで、各社自身もこの環境維持に注力するような体制を取る。かと考えていますが、これ以外に注意、対処すべき対策等あれば、お教え頂けますでしょうか。 また、②の件で、この各社との契約等の情報があればお教え頂ければありがたいです。	貴院のアクセスポリシー（リモートメンテナンスポリシー）を作成頂く必要があると思います。当該ポリシーにおいて、病院が指定した端末（IPアドレス）や環境（メンテンナンス室）からしか接続を認めないことや、接続端末は脆弱性がなく最新のパターンファイルや最新のふるまい検知ルール等を利用してスキャンを行った結果、感染がないと思われる端末からアクセスさせるなど、まずは方針の明確化、規程を作成することが必要でしょう。また契約については個別に契約を結ぶか、今後契約書や仕様書等に明確にしておくとよいでしょう。特に明確にするべきは例示でも何をインシデントして捉え、発生時にどのような支援をしてくれるのか明確にすることです。またサプライチェーンを鑑みればインシデント条項などを設けて、インシデント発生時には情報提供を求めることや場合によっては調査する場合があることなども明記しておくと良いでしょう。
4	＜パスワード＞ 当院のVPN内のクライアントPCの中に、ローカル管理者アカウントのログインパスワードを設定していないものがあります。ネットワーク上の不正アクセスがあった場合、ログインパスワードはウィルス感染の拡大にどのような役割を果たすのでしょうか？ログインパスワードを設定していないとどのようなリスクがありますか？	端的に言えば端末の乗っ取りを招きやすくなります。例えばバックドアに感染した場合、リモートでログインなしでその端末を使用することができます。対象端末を踏み台として特権アカウントを有する内偵するための端末に悪用されたりされるリスクもあるでしょう。またそもそも誰でもその端末を利用できる環境自体、誰でも患者情報などの情報にアクセスできる環境であり、適切な情報管理が行われていません。またいつでも情報を持ち出せるような内部不正を許しやすい環境ともいえるでしょう。
資料		
1	研修で使用されていた資料についての配布をしていただけないでしょうか？	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。
2	質問ではありませんが、研修会の資料をいただけませんでしょうか。	