#	ご質問	回答
1	今日の研修では、小規模の場合オフラインのNasに保存という話でしてたが、クラウド保存の電子カルテでは、バックアップの対策として注意することがあるのか？	クラウド保存の電子カルテの場合、クラウド電子カルテ事業者がバックアップを取得していると考えられます。クラウド上のバックアップは、一般的にその保存場所として、①同じデーターセンターの同一建屋の同じラック群、②同じデータセンターの同一建屋の異なるラック群、③同じデータセンターの異なる建屋のラック群、④異なるデータセンターの異なる建屋のラック群の4つが考えられます。①はラックの電源やネットワークに障害があると、失われる可能性があり、それを防ぐために異なるラック群や異なる建屋、異なるデーターセンターに分散するのが一般的です。こうした観点から、電源喪失、ネットワーク喪失の影響や、大震災でのデーターセンター(DC)の建屋崩壊などの影響についてどのような対策を取っているかをベンダーに確認するのが良いと思います。近年のDCでは免震構造を取っている場合は、例え、同一DC内であっても、異なる建屋もしくは異なるラックに分散設置であれば、完全な喪失を招くことは少ないと考えることができます。他方、免振でない場合は、異なるDCが望ましいと考えられます。
2	log情報をモニターする必要性はわかりましたが、logを監視し異常と思われる内容があれば通知するようなツールがあればご紹介ください。	ログ監視の製品は多数ありますが、SIEM（Security Information and Event Management：セキュリティ情報とイベント管理）と呼ばれる統合型のログ分析ツールから、ログ集計を目的としたものまで、様々で、価格も十数万円から数百万円まであり、一概にこれという製品をご紹介することは難しい状況です。 そこで、無償の製品ですが、Microsoft Log Parser 2.2 日本語版をご紹介したいと思います。SQL文を記述し、Security ログからEvent ID 4625の個数を数えるところから、必要な項目を抽出することも可能な、高速・高性能の製品です。まずは、こちらで4625等の検索を始めていただき、慣れてきたところで、各社製品のトライアルをされてはいかがでしょうか。 https://www.microsoft.com/ja-jp/download/details.aspx?id=24659 https://atmarkit.itmedia.co.jp/ait/articles/0610/27/news140.html
3	スライドP.29 参照系とはサーバー、端末のシステムとはクライアントアプリという理解でよろしいでしょうか。	ご指摘通りです。
4	ネットワークの体系を分けるとのお話でしたが、この時物理的なネットワークは同一で、アドレスの設定を分けるということでしょうか。同じHUBに繋がっている端末やサーバで、片方が10.XXX.XX.XX、片方が192.168.XX.XXというように設定し、お互いにアクセスできないようにするということでしょうか。	物理的なネットワークをルーターで分離して、分離されたネットワークごとに192.168.0.0/24、10.10.10.10/24といったIPアドレスを指定するものです。相互の通信可能なIPアドレスとプロトコルをルーターで指定します。
5	仮想サーバで構築されている場合、管理者権限で全て破壊される危険があります。 今日の研修内容以外で推奨される対策がありましたらご教示願います。	ご指摘通り、大阪急性期・総合医療センターも仮想基盤のサーバーが暗号化され全滅しました。このため、仮想基盤のサーバー群は、仮想サーバーやADサーバー、バックアップとも異なるセグメントに設置することが推奨されます。この場合、各仮想基盤サーバーのPWをユニークにすることは、他のサーバーと同様に重要です。
6	各クライアントすべてのパスワードをユニークにした場合に日々の運用に支障がでてくる可能性がありますが、運用事例や管理方法について何かあれば教えてください	例えばですが、コンピュータ名に区切り記号を入れたり、フレーズを追加することが考えられます。また、パスフレーズの先頭にフロア名や、フロア区分、診療科名などを付与してもよいでしょう。 例：4Fに設置されているコンピュータ名がWS1010の場合で、フレーズをTKhospitaとした場合 → 4FWS#1010TKhospita 例：透析内科に設置されているコンピュータ名がWS1010の場合 → WS10&10Nephrolo
7	昨年度研修で講師の板東先生からつよく刺激を受け、病院現場でかなり働きかけを行いました。しかしベンダ側担当者の意識も知識もよくなっていく兆しを見いだせず、燃え尽きかけておりました。どうしたらこの業界領域はよくなっていくのでしょうか？個人の努力ではどうにもなりません。	具体的なお困りごとをお知らせください。多少、お時間を頂戴する場合がありますが、ご一緒に課題を解決できるかもしれません。
8	膨大にあるセキュリティ製品の中で、「結局何を導入すればよいのか」、この点が大きな悩みであり、研修を受けても解決されない問題である。このところセキュリティ対策製品の営業電話が多くなっており不安を煽る営業手法が横行している。導入した方がよい製品の指定は難しいと思うが選択範囲を絞れるような仕組みが作れないかと思う。	重要なご指摘と受け止めております。一方で、セキュリティ製品は千差万別であり、使い処を謝ると何の役にも立たない場合があり、実際に専門家でも選択に苦慮する場合があります。また、管理者権限が付与されており、かつ、脆弱性管理がなされていない場合、万一、侵入を受けると、まったく機能しない場合が考えられます。このように、製品導入と運用は一体であり、不可分です。まずは、ネットワーク構成や、ウイルス対策ソフトの運用状況、管理者権限等の運用体制をベンダーに説明し、その上で、ベンダー製品を導入した場合の想定できるリスクを、ベンダーのSEに問い合わせてはいかがでしょうか。 誠実なベンダーのSEならば、病院の現状の課題を指摘し、製品の効果とともに、具体的なリスクも説明すると思います。
資料・アーカイブ		
1	説明資料を頂くことはできるのでしょうか？	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	参加できなかった分の講義はどこで視聴できますか？	
3	今年度の研修を受けさせて頂いており大変為になっております。しかし、振り返りなどをしたいときに資料がなく困っております。研修受講者に資料のご提供を頂けませんでしょうか？	
4	これまでも含めて、セミナで使われた資料を頂くことは可能でしょうか。	
5	当日参加できなかった職員やシステムベンダーと情報共有したいので資料をいただけないでしょうか。講義動画がベストですが難しいようでしたら説明用資料だけでもよいですし、閲覧は病院職員限定など、条件付きでも全く構いません。	
6	途中で邪魔が入り、視聴なくなってしまいました。後日改めて視聴することは可能でしょうか？	