第1回初学者・医療従事者向け研修 Q&A

令和4年12月20日に開催いたしました第1回初学者・医療従事者向け研修におけるQ＆Aについて、下記通り回答いたします。

#	質問	回答
1-バックアップ等に係る事項		
1	勉強になりました。 バックアップの重要性が強調され、その対策としてUSBメモリやクラウドバックアップが紹介されていました。いずれも電子カルテのバックアップとしては現実的でないように思います。電子カルテのバックアップとして推奨される方法をご教示いただければ幸いです。	大阪急性期Cを例にすればテープバックアップがあったので早期復旧が実現できました。そもそも電子カルテのクラウド化を行えばクラウド側での実現、設定ファイルや論文などの文書ファイルなどはUSBでも可能です。それぞれのデータや利用に応じてバックアップの形式や実施方法は異なるかと思います。
2	オフラインバックアップが重要との事でしたが、レンタルサーバーやクラウドとどう組み合わせればいいですか？	クラウドサービスやレンタルサーバだとしても同一ネットワークでのアクセスが可能な場合は攻撃者がアクセス可能なポイントとして判断されてしまう場合があります。またクラウドサービスであればサービス事業者側でのバックアップのメニューもあることでしょう。オフライン、オンラインでも攻撃者が到達しにくい、またはできない環境にバックアップを行うことが大切です。
3	オフラインバックアップにかわるものとしてイミュータブルストレージの利用はいかがでしょうか。	有効な手段の１つだと思われます。
4	オフラインにおいて、３つのSSDにバックアップをとっています。３世代残せるようにしています。手間を考えると日付を詰めるのも危惧するところではありますが、２週間ごとのバックアップで良いのか？迷うところです。何かご助言があればお願いします。	1週間ごとなど頻度が高いに越したことはありません。しかし、その頻度が上がればコストも高くなると思います。すべてのデータバックアップが望ましいですが、医療継続に特に必要なシステム、データをランク付けして、その大切な情報はバックアップの頻度を上げるなど、検討頂いた方がよろしいかと思います。
5	オフライン　テープバックアップが安全（感染被害なし）であることの確認は，どの様にして行うのでしょうか？	ネットワーク構成上侵入しえない、ランサムウェアによる暗号化が行われていない、不審なファイルがない、侵入形跡が無いなど、様々な要素があります。なお、データが改ざんされていなければファイルハッシュも合致するかと思いますので、ファイル同士のハッシュ確認によってデータが正しいと判断できます。
6	バックアップ自体が汚染されているケースがある、と言われていますがバックアップサイクルをどのように考えるべきでしょうか。	**ライブ中継で回答済み**
2-講演内容および資料等に係る事項		
1	要点をまとめた資料を頂けると助かります。上司、同僚などにお勧めなどもしやすくなります。ご検討をお願いします。	研修資料のサマライズ版の提供は、今後検討いたします。 研修資料の提供については、提供時期は未定ですが、管理者が伝達研修をできるような形で資料（講習資料）を提供できるように準備を進めております。 準備が整いましたらMIST（セキュリティ教育支援ポータル）サイトで提供いたします。
2	わかりやすい説明ありがとうございます。共有するために、本日の資料を頂くことは可能でしょうか。	
3	本日の資料はダウンロードかどうでしょうか？	
4	業者との保守契約の中に、サイバー攻撃等の責任は負わないというような文言がありましたが一般的でしょうか。	**ライブ中継で回答済み**
3-インシデント対応等に係る事項		
1	感染経路等の調査のため、サーバーやPCについて回収されると思いますが、どれくらいの期間がかかるのでしょうか？医療機関は1日でも早い復旧を目指すため、１日でも早くサーバーやPCを回収し再セットアップしたいと考えますが、いかがでしょうか？	対象のサーバやPCのフォレンジックを行った場合、少なくとも1か月は要します。そこからセットアップ等を行うとさらに時間がかかります。代替となるサーバやPCなどを用意しておくなどの準備が必要だと思います。
2	厚労省にインシデントについて連絡した場合、どのような対応をしていただけるのでしょうか？	**ライブ中継で回答済み** インシデントの初動対応については、無償となります。 サイバーセキュリティインシデント発生時に厚生労働省へご連絡いただき、厚生労働省の判断ものと、初動対応支援を発動いたします。 初動対応支援の内容は、以下の通りです。 ①医療機関へのヒアリングの実施 ②ネットワークや端末の遮断 ③データの保全、サイバー攻撃の痕跡データの保全 ④有償対応を行うベンダー候補の紹介
3	インシデントの対応については、有償なのでしょうか？	
4	初動対応をお願いした場合、どの程度の費用がかかりますでしょうか？	

#	質問	回答
4-セキュリティ対策に係る事項		
1	PC購入時にMicrosoft Defenderがすでに入っておりましたがセキュリティソフトはこれで十分でしょうか、また、別に必要なら推奨のものがありますか？	最低限のウイルス対策としては問題ないと思います。運用が行えるようであればEDRのようなソリューションも必要です。しかし、高価で運用負荷も高いため、まずはPowershellやマクロの無効化など、使わない機能は無効化するなど、PCの設定にお時間を割くべきだと思います。
2	当院はオンプレで、オンライン資格端末導入でネットにアクセスすることで攻撃されやすくなるのではないかと不安です。	オン資は当該システムを経由しない限り侵入できないと思われ、オン資側の対策に依存するかと思います。なお、インターネットにアクセスしているとのことで不安なようであれば、接続ポイントを限定する。海外とは接続させないようにするなど、FW等で行える対策もありますので、まずはそのような対策を実施頂くのは1つかと思います。あとは端末側のセキュリティ対策を強化することです。
3	サイバー攻撃を受けてしまったと仮定して、(医療の継続を含めて)医療従事者がどのような対応をとったらよいか、訓練できる機会があれば参加してみたいです。そのような研修等はありますでしょうか?	医療従事者向けの演習は今後、整備を行って参ります。なお、システム担当者のインシデント対応訓練という視点ではNICTが提供しているCYDERなど、既に演習があります。
5-運用保守契約等に係る事項		
1	ベンダー側にセキュリティーに関して情報を提供し、安全性を守る義務はないのでしょうか？またはそういった契約をすることは可能でしょうか？	ライブ中継で回答済み
2	厚生労働省で、標準的な契約書のひな型を提供していただけないでしょうか？	ご意見ありがとうございます。 厚生労働省検討し、年度内にMIST（セキュリティ教育支援ポータル）サイトで回答いたします。
6-国の施策等に係る事項		
1	個々の医療機関ではセキュリティ対策にかけられる予算と労力に限界があります。 マイナンバーカードを利用した医療情報の共有化も検討されている昨今、「国を挙げて医療情報を守る」ために検討されている施策があれば教えてください。 ※例えば国主導で医療情報クラウドを各医療機関向けに提供するなどの施策があれば安心できると、お話を聞いて思ったのですがいかがでしょうか。(素人考えで誠に恐縮です)	１　国民の生命・健康を守る医療機関が、サイバー攻撃により、その機能を失うことがないよう、サイバーセキュリティ対策の強化が不可欠であり、医療機関において、 ・PCやネットワーク機器、情報システムの脆弱性に対する措置 ・診療の継続や早期の業務復旧に必要なデータや情報システムのバックアップの確保 ・災害対策と同様に、サイバー攻撃やシステム障害等の非常時を想定した訓練の実施 などの対策を継続的に行うことが重要であると考えています。 ２　厚生労働省では、医療機関に対策を求めるだけではなく、令和４年度診療報酬改定において、診療録管理体制加算の中で医療情報システム安全管理者の配置や職員に対する研修等の実施状況とともに、医療情報システムのバックアップの確保状況等について届出を求めております。 ３　また、 ・サイバーセキュリティ対策に関する研修や研修資材の提供 ・サイバーセキュリティインシデントが発生した医療機関の初動対応支援 など、医療機関に対するセキュリティ対策の強化に必要な支援を行っているところです。 ４　引き続き、医療機関の現状を踏まえ、サイバーセキュリティ対策を強化するために必要な対応を行ってまいりたいと考えております。
2	ベンダー側に、３省ガイドラインや厚労省セキュリティガイドライン遵守を強制的に促す（保守契約記載）のはありですよね。	ご意見ありがとうございます。 現在は、3省2ガイドラインとなっております。
7-クラウド等に係る事項		
1	クラウド型のサーバが攻撃されるリスクというのはないのでしょうか？（オンプレとの安全性の比較について、データなどはあるのでしょうか？）	ライブ中継で回答済み
2	クラウド・インターネットが安全で、オンプレが安全ではないという誤認識でしょうか？	運用をされていないオンプレのシステムが多いのが実情で、そのような環境であればオンプレの方が安全ではないという意味です。 クラウドサービスの利用形態などによっても異なりますが、基盤部分は事業者側が運用しているのであれば、利用者の運用負荷は下げられます。しかし、クラウドの場合は設定などは利用者に依存するため、その部分での運用は負荷がかかります。 適切に運用がされていればオンプレでも安全ですが、全ての機器の脆弱性管理や脅威情報の収集や対応などを行うのは難しいと思い、クラウドを選択肢としてお示ししている次第です。

#	質問	回答
8-感染に係る事項について		
1	仮にWEBやUSBから感染した場合、実害がでるまでどれくらいの時間がかかりますか？	攻撃のされ方に寄って異なりますが、、、接続先からバックドアのようなウイルスをダウンロードした場合は、攻撃者として利用したい視点から実害迄には時間を要すると思います。感染と共に拡大をさせるようなウイルスであればその被害はすぐにでも生じる可能性があります。
2	セキュリティソフトやOSの更新するには、インターネットなどに接続する必要があると思いますが、外部との接続をしない環境でどのようにして更新をすればよいのでしょうか	オフラインでも、別環境でモジュールをダウンロードして、安全なUSBを経由して端末で更新をして頂く方法があります。（環境がわからないため大雑把ですが）オフライン、対象のソフトウェアをキーワードに検索頂くと、更新方法が出てくるかと思います。
9-メンテナンス等に係る事項		
1	メンテナンス用リモート接続の安全性を確認、担保するにはどのような方法がありますでしょうか？	まず対象のIPアドレスだけの制限を行うこと、それ以外の特に海外のアクセスは認めないようにすることです。検疫のような仕組みもありますが、費用面で厳しいと思われます。常時接続ではなく、接続する際にその時のOSやセキュリティ対策ソフト、検索エンジン、パターンファイルなどのバージョン情報を取得するように申請させるというのが現実的な手法ではないでしょうか。
10-事例に係る事項について		
1	半田病院はオンプレだったのでしょうか？？	ライブ中継で回答済み
2	半田病院では身代金を払って鍵を教えてもらったと噂で聞いたのですが、それは本当ですか？また2018のバックアップからどのようにして電子カルテのデータを最新の状態に戻したのでしょうか？	半田病院が身代金を支払った事実は確認されていません。ただフォレンジックにお願いした事業者が復元を行っており、どのように対応されたかはその事業者にしかわかりません。事業者が信頼できるかどうか、チェックシートなどを用いて確認を行っていただければと存じます。（https://www.draj.or.jp/news/check-sheet/）
3	「PCの動作がいつもと動作がおかしい」や「インシデントかも」となる基準や事例などはございますでしょうか	CPUやメモリなどの負荷がいつもより掛かっている、設定が変更されている、インターネットの接続が遅かったり切断される、迷惑メールが増えた、個人情報の悪用があったなど、サイバー攻撃以外の原因も考えられますが、原因は様々です。
4	半田病院や大阪急性期病院では電子カルテサーバだけが被害にあったのですか？画像や生理検査データなど放射線科、検査科など他部門で設置しているサーバも閲覧できなくなったのですか？	詳細は報告書などでご報告をいたしますが、今回給食システム経由ですので給食サーバを始めとした一部の部門システムでの被害が出ました。
5	国内の医療機関（診療所・クリニック）でサイバー攻撃にあわれた事例はありますか？ある場合は、どのような事例でしょうか？	宇陀、半田、大阪急性期と残念ながら国内でもランサムウェアをはじめ様々なサイバー攻撃が確認されています。
11-その他、ご意見等		
1	ハッキングに対する保険制度などはありますか？個人情報漏洩に関してはありますが、保険会社さんに事業再生までの諸費用を保証する制度ですね	ここで指しているハッキングの詳細が不明瞭なので、回答があいまいかもしれませんがサイバー保険というものがありますので、当該保険を販売しているまたは提供元にご確認頂くのが良いかと思います。フォレンジックなどの調査費も負担して頂ける仕組みです。
2	バックアップの復旧方法、時間をベンダーがきちんと教えてくれるところがほぼないのですがベンダーにもきちんと指導してほしい。	ご意見ありがとうございました。
3	物にもよりますが、パスフレーズが長く忘れた場合にシステムに入れない（可用性として×）ことがありますが、やみくもに長くするのではなく天秤にかけることが大切ではないでしょうか？	例えば、重症・急性期患者情報システムなどは長くできないといった事情もあるシステムもあるかと思います。その場合は共通化したい、長くできないなどといったご要望もあることでしょう。その場合は、その端末のセキュリティ対策や監視を強化するなど、ご指摘の通り、組織置いて天秤にかけて頂き、セキュリティ対策をご検討頂くことがとても大切です。
4	放射線システムは○○企業、検査システムは××企業など複数の企業がかかわっている場合はどう対策すればよろしいでしょうか	サプライチェーン管理としてそこまでの管理が求められています。まずは外部接続ポイントの洗い出し、電子カルテシステムと接続しているベンダーなどステークホルダーの可視化が必要です。全てを把握するのは時間がかかるかと思いますが、外部接続や重要なシステムなどから棚卸をして頂くのが良いかと思います。