第2回初学者・医療従事者向け研修（Q&A）

令和5年1月20日に開催いたしました第2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	オフラインのバックアップについてですが、テープの他に事例はありますでしょうか？できるだけコストを抑えた事例をご存じでしたらご教示ください。	組織の大きさにもよりますが、最近のハードディスクは大容量のものもありますので、保存したいデータの容量によってはHDDにバックアップをとることも可能かと思います。
2	電子カルテデータのバックアップ（オフライン）は最低何日（何世代）分を保存すべきでしょうか。	厚生労働省の医療情報システムの安全管理に関するガイドラインにでは少なくとも第３世代確保し、遅くとも3 世代目以降はネットワーク的あるいは論理的に書き込み不可の状態にする等の対策が必要とされています。
2-講演内容および資料等に係る事項		
1	とても為になる講演をありがとうございました。ストリーミング配信等されるご計画はございますか？	現在、動画配信の予定はございません。 オンライン研修の動画提供のご要望がありました旨は、厚生労働省へ共有し、 今後検討させていただきます。
2	他の職員に説明をしたいのですが、スライドの提供は可能ですか？	研修資料の掲載については、現在準備中でございます。 掲載しましたら、医療機関向けセキュリティ教育支援ポータルサイト(MIST)のTOPページの「お知らせ」に掲載いたします。
3-セキュリティ対策に係る事項		
1	メールアドレスでも怪しいものはすぐにメールを消したりしていますが、メールを誤ってひらいてしまった場合はどういう対応がよろしいでしょうか？	多くの場合、メールを開いただけでは何も起こりません※。添付ファイルを開いたり、メール内のリンクをクリックしたりすることで感染したりフィッシングサイトに飛ばされたりします。HTMLメールなどで開いただけでウイルスに感染するものもありますが、セキュリティ対策ソフトなどで防げる場合もあります。不安な場合はまずセキュリティ対策ソフトでフルスキャンをし、その後担当部署に報告、相談しましょう。 ※：可能性としてゼロではないのでご留意ください。
2	ノートンパワーイレーサーでのチェックで日本の行政のアプリが発行元証明書云々でひっかかりますが、どう理解したらいいのですか？ ノートンの質問者ですが、ラップトップPC　Win10です。	ノートンパワーイレーサーはセキュリティ対策ソフト（ウイルス対策ソフト）ではなく駆除ツールです。こちらに関してはノートンにお問い合わせいただくのが一番確実かと思います。
3	Webメール（Gmail等）は仕事では使わない方がいいでしょうか？	**ライブ中継で回答済み** 組織のセキュリティポリシーにしたがってください。
4	サードパーティー製のウィルス対策ソフトウェアは絶対に必要ですか？はじめからWindowsに入っているWindowsディフェンダーなどでもよいですか？	**ライブ中継で回答済み** ウイルス対策のみであればWindowsディフェンダーでもよいと思いますが、セキュリティ対策ソフトはウイルス対策以外にも機能があるのでそういった部分も考慮して導入されるのがよいと思います。
5	院内LANに接続している機器は、普段からオフラインにできるものはそうしておくほうが無難でしょうか。	**ライブ中継で回答済み** 基本的にはオンラインにしておく必要がない機器に関しては、オフラインにしておくとよいと思いますが、手間やリソース、費用とのバランスを考慮して実施いただければと思います。
6	パスフレーズ類推されにくいというのは、単語の組み合わせでも安心できますか？例：bananarinngo	**ライブ中継で回答済み** 単語の組み合わせがパスワードなので、文章の組み合わせにしたパスフレーズを利用する方が推測されにくくなります。
7	他院からの照会患者さんの診療情報がデジタルメディアで提供されますが、それらを起点としたセキュリティ障害の事例はありますか。	メディアの種類によりますが、具体的に医療機関の事例ではありませんが、USBメモリやスマートフォンをつなぐことでマルウェアに感染することは知られています~~あります~~。
8	あるセグメントのPCが感染した場合、セグメントを切ってるるだけで、他のセグメントに感染しないのでしょうか？	セグメントを切るだけで安全になるわけではなく、セグメントを切ることで必要なセキュリティの設定が（アクセス制限など）行いやすくなりますので、セグメントを切った上で感染しないようしっかり設定をして対策をしてください。
9	非常に分かりやすく、参考になるお話ありがとうございました。 セキュリティ対策について、EDRなどを業者から勧められることが多いのですが、エンドポイントの対策ソフトのみでは不十分でしょうか。	EDRを導入するとシステム侵害の発見が早くなりますが、運用できる体制があるかどうかというところも検討する必要があります。アラートが出てもそれがどういう意味なのか理解して対応できる体制が用意できるかもあわせて検討してください。
10	クロムでの自動生成パスワードの安全性と、個人のパスフレーズはどちらが安全ですか？	自動生成パスワードは文字列を長くすることでさらに予測しにくくなりますが、同時に覚えておくのが困難になります。自動生成してパスワードマネージャーのようなツールを利用すれば覚えておく必要がなくなるので、それも1つの方法かと思います。覚えておく必要があるからパスワードの使いまわしをしてしまうので、それをさけるためには、パスフレーズを使うのがよいと思います。

#	質問	回答
11	Macはウイルスに感染しないというのは本当ですか。「Macだから、ウイルス対策ソフトは不要」という理由は成り立ちますか。	結論から言うと、Macもウイルスに感染します。Macを標的にしたウイルスも数多くありますし、攻撃者にとってはすべてのOSがターゲットですので、Macだからセキュリティ対策が不要ということにはなりません。
4-クラウド等に係る事項		
1	オンプレよりもクラウドのほうが安全と最後の方にありましたが、明確な根拠ってありますでしょうか？	オンプレよりもクラウドの方が安全というのは、自分たちで管理しきれないオンプレを使うよりも、事業者が設定してくれるクラウドを使う方が安全ということです。物理的にネットワークを分離し、必要なデータやシステムのバックアップを頻繁に行い、セキュリティ対策を行い、適切な管理が行えるのであればオンプレでも安全な運用はできると思います。
5-その他、ご意見等		
1	とても勉強になりました。	お参加いただきましてありがとうございます。 本研修が皆様方の一助となれば幸いです。
2	施設の管理者が費用をかけたがらない。この必要性を納得させるとか、費用をかけざるを得ないような法律のような利用できる情報や外部の圧力はありますか？	対応を検討します。