第3回初学者・医療従事者向け研修（Q&A）

令和5年2月20日に開催いたしました第3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	オンプレよりクラウドやレンタルサーバーのほうが運用管理コストが低めになるとは思いますが、クラウドやレンタルサーバーの場合はオフラインバックアップをしてくれるサービスはあるのでしょうか？	あまり聞いたことはありませんが、オプションでそういったサービスを行っている場合もあるかもしれません。
2-セキュリティ対策に係る事項		
1	閉域網やVPNで、Windows7や8などのサポートが終了しているOSを使い続けるリスクはありますか。	たとえばVPNを使っていたとしても、VPNの脆弱性をつかれたら侵入されてしまうのでリスクはあります。システム構築・導入時にはOSのライフサイクルも意識しましょう。
2	セキュリティソフトを入れている場合、ソフトが更新されればインストールなりを促す連絡がくるものと思っていてよいですか。	セキュリティソフトによると思いますが、気が付かないこともありますので手動で確認することを習慣にするとより安全です。
3	説明をされていたら、大変な失礼をしてしまい申し訳ございません。メールの添付ファイルについて、暗号化されたZipファイルが先に来て、別送でパスワードが送られてきます（特に行政が多いです）。セキュリティのフィルターをすり抜ける場合があり、最近ではこのような送受信は推奨されていないと聞きました。このような送り方は、我々もしないほうがよいのでしょうか。また、大きいファイルの場合、セキュアな環境下でのファイル共有、アップローダーなど、おすすめはありますか？	暗号化されたファイルはウイルスチェックができないのがひとつ、もうひとつはそもそもメールが読まれてしまう状況で同じメールアドレスにパスワードを送るのではあまり意味がないのではということで最近ではアクセス権限をきちんと設定したクラウドストレージ（BoxやOne driveなど）を使う組織が増えています。ローカル保存しなければファイルを開くのはブラウザ上になりますので感染リスクも下がります。コストや運用方法にあったものを利用するのがよいと思います。
4	オンライン資格端末はVPNで接続されていますが、Windowsや顔認証端末のアップデートはどのように行われていますか。	組織のシステム管理者に確認いただくのがよいかと思います。組織が管理していないのであれば個人で端末のアップデートをする必要があります。 システム・セキュリティ管理者向けのコンテンツを確認していただけますと、各論が記載されていますのでそちらをご参考にしていただければと存じます。
5	以前厚生局個別指導で、医療情報システムの個々のPW変更について3月に1回変更を、といった指導を受けたことがあるのですが現在も同じ流れなのでしょうか？PWを推測されにくいものとし、あまり頻繁に変える必要はないような流れもあるといった話も聞いたことがあるのですが、もし分かればご教示いただければ幸いです。	オンラインで回答済み 定期的なパスワードの変更については現在は推奨されていません。 情報が流出した際はできるだけ早くパスワードを変更した方がよいですが、それ以外ではパスワードの使いまわしをしないこと、推測されにくい複雑で長いパスワードを使うことの方が重要です。
6	グーグルなどでの自動生成のパスワードを利用していいですか。	自動生成を利用する場合は英数字記号を使って桁数を10～12桁以上にするとよいかと思います。
7	昨日は興味深いお話をありがとうございました。 質問の要領がわからず、おそくなり、回答していただけなかった分ですが ⇒ グーグルなどのパスワード自動生成のシステムに頼っていもいいですか？ ⇒ パスワードは長いものとのことですが、何字ぐらいでしょうか。	
8	患者さまからUSBを預かり、医療機器（超音波エコー）に接続し、3Dを保存することがありますが、事前にその都度セキュリティスキャンはしていますが、問題ないですか？	USBメモリの場合、入手するまでに読み書きができてしまうため1度のみ書き込み可能なメディアと異なり注意が必要です。接続前にUSBメモリを2種類のセキュリティソフトでスキャンする、ファイル保存後に接続した端末もスキャンするとより安全でしょう。
9	システム管理者が日頃から気を付けておいたがいいことは何がありますか。	こちらが参考になると思います。 日常における情報セキュリティ対策（IPA） https://www.ipa.go.jp/security/measures/everyday.html
10	端末（パソコン）のセキュリティ対策について現在、各PCにウィルスバスターを入れてるのですが、昨今のランサムウェアによるサイバーインシデントの事例をふまえ、EDRというものを各端末にいれ対策をした方が良いとの話を聞きました。話の中で、ランサムウェアに感染したら情報は元に戻らないとの話しが少しありましたが、EDRだと感染後に復元可能との話を聞ききました。実際のところはどうなのでしょうかでし？？ 全くの素人で、ご質問場所が違うかもしれませんが、よろしくお願い致します。	一般的にはEDRで復号できるというのは聞いたことがありません。 EDRとはEndpoint Detection and Responseの略称で、EDRを導入することで侵入を検知することができるため、早期に対応しバックアップから復元することができるというお話だったのではないかと思われます。