別添4 :第4回初学者・医療従事者向け研修（Q&A）

令和5年3月3日に開催いたしました第4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	**バックアップに係る事項**	
1	PC本体に接続した状態の外部記録媒体にバックアップをしていますが特に問題はないでしょうか？	外部記録媒体をPCに接続したままでいると、PCが感染した場合、外部記録媒体も感染しますので、バックアップ時以外は外した（オフライン化する）方が安全です。
2	**インシデント対応等に係る事項**	
2	インシデント発生時には厚労省への届け出だけで十分ですか？IPAへの届け出は不要ですか	IPAへの届け出は義務ではありませんが、被害の拡大・再発防止などの理由から届け出がされています。なお、個人情報漏えいの報告については、個人情報保護委員会の資料をご確認ください。 https://www.mhlw.go.jp/content/10808000/000943451.pdf
3	**セキュリティ対策に係る事項**	
1	いわゆるEDAというものは必要なのでしょうか。	EDRについて質問されている前提で回答しますと、EDRはEndpoint Detection and Responseの略で不正な挙動などを検知するものです。万が一侵入された場合にその挙動を素早く検知し、対応するためのものですので、対応するという運用が必要になります。EDRをいれただけで安全というわけではありません。
2	ファイアウォールとアンチウイルスソフトだけでは、不十分ですか？	システムの規模によります。たとえば個人利用であればそれだけでよい場合もありますが、規模が大きくなればそのほかの対策も検討した方がよいでしょう。
3	脆弱性の情報をいち早く知るためにはどのような手段があるでしょうか。	セキュリティ全般ではなく脆弱性の情報、という枠でいうと、内閣サイバーセキュリティセンター（NISC)やIPA、JPCERT/CC、またIPAとJPCERT/CCが情報を発信しているJVN脆弱性レポートのTwitter情報をみたり、JPCERTのWEBサイトを定期的に確認するとよいと思います。
4	クラウド型の電子カルテをしようしております。ファイアウォールは設定しないと使えないようになっている状態です。メールなどを電子カルテと同じPCでみていますが、これは感染としてはかなりリスクの高い状態でしょうか？クラウド型カルテの場合で気を付けることをおしえてください	クラウド型の電子カルテの利用でファイアウォールが設定できないというのはどのような仕様なのか不明なのでその部分には回答できないのですが、「感染」という点のみで回答すると、クラウド型のカルテは常時接続でデータをローカルに保存していないと思われますので、クラウドサービス上のデータは端末が感染してもクラウドサービス側のセキュリティにて守られていれば問題ないといえるでしょう。それ以外のリスクとしては、万が一、端末に侵入されて電子カルテのサービスにログインしたままになっている場合は情報を抜かれてしまうリスクがあると考えます。
5	先き程の訂正クラウド型の電子カルテをしようしております。ファイアウォールは設定しない状態でしか使えないようになっている状態です。メールなどを電子カルテと同じPCでみていますが、これは感染としてはかなりリスクの高い状態でしょうか？クラウド型カルテの場合で気を付けることをおしえてください	
6	IDやパスワードですが、次回入力を省略するため、端末に記憶させることは問題ないでしょうか？	ブラウザに記憶させたままにしていて侵入された場合はそのままログインされるリスクがあります。また、保存されたIDとパスワードを表示することができる場合は、アクセスする権限をもっていない人が端末からIDとパスワードを知ることができる（内部不正を可能にする）というリスクもあります。
7	Windows以外のOSを使ってみたら少しは安心できるものでしょうか。（MacOSとかLinuxとか）	MacOSやLinuxを狙う攻撃者もいますので、Windowsより少ないからという理由で気持ち的に安心できても、リスクがなくなったり安全になるわけではありません。
8	セキュリティソフトにUTMという機器を併用する方法でも危うくエモテットに感染しそうになった事例がありました。どんな方法でも使う人の意識の隙があれば大きな穴になると思いますので職員の教育が大事だと思います。しかし、疎い人にわかりやすく説明するのはとても難しいです。	万能薬はないですし、薬であっても扱いを間違えれば危険になることもありますので、理由もなくただこれをしないとダメ、これをしてはダメ、というより、「何のために」この対策をして「何を」守っているのかを知ってもらえたらと思います。
9	電子カルテと他のPCをハブで分けてますが、ルーターは同じです。どこまで分ければいいのかよくわかりません。	ルーターが同じということは、ネットワークは同じということになるので、より安全にということであれば電子カルテは物理的に別のネットワークにわけた方がいいでしょう。
10	ウイルス対策ソフトの検知はクライアントにメッセージは出ますが、管理者は管理コンソールにつなげないと、その情報には気づきません。挙動検知のアラームを管理者にタイムリーに伝えるソフトを導入した方がよろしいでしょうか？	クライアント端末から管理者へ通知をおこなったり、管理ツールなどで管理者に通知をすることができるものもありますので、まずはお使いのソフトで管理者通知ができるか確認してみるとよいと思います。
4	**その他**	
1	オンライン資格確認のIP-VPNに侵入された場合、IP-VPNがレセコンにつながっているとレセコンにつながっている電子カルテに侵入されると思います。厚生労働省はどのように対応を考えておられますか。	「オンライン資格確認・医療情報化支援基金関係医療機関等向けポータルサイト」https://www.iryohokenjyoho-portalsite.jp/ というのがあるので、そちらでご確認ください。 サイトの掲載資料には、オンライン資格確認ネットワークから医療機関内ネットワーク方向に侵入できないようにする対策が類型化して提示されているので、自分の医療機関のシステムベンダーと確認していただくのも良いでしょう。