第3回システムセキュリティ管理者向け研修（Q&A）

令和5年2月9日に開催いたしました第3回システムセキュリティ管理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	VPN装置のセキュリティ対策ですが、MFAやmTLS、VPNクライアントの機能で実装される接続元端末のMACアドレス制限などで、脆弱性はある程度緩和できると考えて良いでしょうか？	研修にご参加いただきありがとうございます。 ご指摘の機能で不正侵入は防げると考えますが、これらをバイパスするようなVPN装置に脆弱性が存在した場合は、攻撃が成功してしまいます。また、従いまして、ご指摘の設定に加えて、脆弱性対策の実施をお願い致します。
2	先週の内容で恐縮ですが、先週ご教示いただいたOfficeマクロ用の電子証明書による制限を行おうと思い、当院が使用している、証明書作成を行う認証サーバで証明書を作成したのですが、ユーザー指定の証明書でしたので複数ユーザーで登録ができませんでした。証明書を作成する上で注意点などございますでしょうか。また、証明書は個別に購入しないとならないものでしょうか。	研修にご参加いただきありがとうございます。 詳細な状況が分かりませんので、かみ合っていない場合は、改めてご連絡をお願い致しますが、証明書による署名の要件としては、①証明書の拡張キー（EKU:Extended Key Usage）にコード署名が存在する必要があります。ご使用の証明書にコード署名が入っているかをご確認ください。 また、自己署名証明書での署名も可能です。 https://support.microsoft.com/ja-jp/office/%E3%83%9E%E3%82%AF%E3%83%AD-%E3%83%97%E3%83%AD%E3%82%B8%E3%82%A7%E3%82%AF%E3%83%88%E3%81%AB%E3%83%87%E3%82%B8%E3%82%BF%E3%83%AB%E7%BD%B2%E5%90%8D%E3%82%92%E8%BF%BD%E5%8A%A0%E3%81%99%E3%82%8B-956e9cc8-bbf6-4365-8bfa-98505ecd1c01 ご参考ください。
3	システムベンダに共有フォルダを作らせると、平気でEveryoneフルコントロールを付けるので、まずはベンダ担当者の教育が必要では？	研修にご参加いただきありがとうございます。ご指摘は今後の参考とさせていただきます。
4	情報セキュリティ業界はなんでもかんでもインシデントって呼ぶので、CVSSはありがたいですね	研修にご参加いただきありがとうございます。 引き続き、よろしくお願い申し上げます。
5	「病院における医療情報システムのサイバーセキュリティ対策に係る調査」Q10 電子カルテシステムのバックアップデータの更新頻度について、当てはまるものを選択してください。 ①１か月以内に１回 ②１か月～３か月以内に１回 ③３か月～半年以内に１回 ④半年～１年以内に１回 ⑤バックアップデータを更新していない。 選択肢に１日（せめて１週間）がないことがおかしいです	研修にご参加いただきありがとうございます。 ご指摘ありがとうございます。フィードバックさせていただきます。
6	責任分界の話はありますが、ファームウェア更新をベンダ任せにして、後手に回るぐらいであれば、病院側でやってしまおうという議論があってもいいのではないでしょうか。 病院職員のスキルの問題はありますが、情シス担当として給与が支払われているのであれば、それぐらいの努力はしてもいいと思います。	研修にご参加いただきありがとうございます。 ネットワーク機器については、ご指摘通り、病院側で実施できる体制を持っておくことは重要かと思います。
7	「部門で独自に導入したネットワーク」がHISにルーティングされていること自体、ガバナンス上の問題がある組織だと思います。	研修にご参加いただきありがとうございます。 ご指摘、ありがとうございます。
8	VPN装置の脆弱性対策はインターネットVPNではもちろんの事ですが、	研修にご参加いただきありがとうございます。
9	VPN装置の脆弱性対策はインターネットVPNではもちろんの事ですが、IP−VPN事業者閉塞網でも必要でしょうか？	研修にご参加いただきありがとうございます。 医療情報システムの安全管理に関するガイドライン 第 5.2 版では、「また、複数拠点の接続により内部ネットワークが拡張する場合、内部トラフィックにおける脅威の拡散を防止するために不正ソフトウェア対策ソフトのパターンファイルや OS のセキュリティ・パッチ等を適切に適用する等を行うことが求められる。」(p43) と指摘されています。対策をお願い致します。
10	前回もご質問させて頂きましたが、ウイルス対策ソフトについて、閉域ネットワークにおけるエンジンやパターンファイルの更新についてどうするのか、議論や検討をお願いしたい。	研修にご参加いただきありがとうございます。 多くのウイルス対策ソフトは、閉域網側とインターネット接続が可能な網側にパターン配付サーバーを設置し、USBやパーソナルファイアーウォールを設定したネットワークでパターンファイルやエンジンを更新する仕組みを持っています。導入ベンダーにご相談ください。
11	医療機器の承認審査機関のPMDAはセキュリティ観点の審査が入っているのでしょうか？組込ソフトが多いとはいえwindowsベースのものも沢山ありバックアップ機能を有していないものも存在している認識です。	研修にご参加いただきありがとうございます。ご意見ありがとうございます、まずは製造元ベンダに照会いただくのが良いと思います。

#	質問	回答
12	FWの更新を病院のシステム担当者が行うというのは心意気や良しなのですが、一般的な企業はどう対応しているのでしょうか。病院以外の業界のベストプラクティスを学ぶべきではないでしょうか。	研修にご参加いただきありがとうございます。 企業にもよりますが、いわゆる「医療」以外の重要インフラ事業者と呼ばれる「情報通信」「金融」「航空」「空港」「鉄道」「電力」「ガス」「政府・行政サービス」「水道」「物流」「化学」「クレジット」「石油」の13分野は、所轄官庁から指導があり、ネットワークやシステムの脆弱性管理は厳しく実施しています。インシデントが発生すると、所轄官庁への詳細な報告が求められるケースが多いようです。また、多くの分野で、インターネット接続が全くない完全な閉域網の維持や、データの持ち込み、移動に関して自らリスク分析を行い様々な対策を実施しています。 ご指摘の点は、今後の教材開発において、ご意見を参考にさせて頂きたいと思います。
13	資料はポータルサイトにアップロードされるとのことですが、そのポータルサイトのURLをご教示ください	研修にご参加いただきありがとうございます。 研修資料掲載については、現在準備中でございます。 掲載しましたら、ポータルサイトのTOPページの「お知らせ」からリンクにて掲載場所をお知らせいたします。
14	部門システムベンダーからウイルスバスターを導入すると動作が遅くなるといわれていますが、部門にセーフロック対策ソフトを導入すると対策は終了としてよろしいですかとなりますか。	研修にご参加いただきありがとうございます。 セーフロック対策ソフトとは、予め登録したアプリケーション（実行ファイル）のみ実行を許可するシステムであり、登録されていない外部から侵入したウイルス等のプログラムの実行を停止するものです。（ホワイトリスト方式などと呼ばれます。）ウイルス対策ソフトの稼働が困難なシステムで代替え的に使用されるものです。 ウイルス対策ソフトは、プログラムだけではなく、入出力されるDICOMファイルなどもチェックするため、動作に影響を与えてしまいますが、他方で、PCが取り扱うすべてのファイルをチェックしてくれるという意味で、より安全です。セーフロック対策ソフトを使用する場合は、DICOMファイルが保存されているサーバーで確実にウイルス対策ソフトを稼働させるなどの措置を講じる必要があると思います。ご使用の環境のリスクを十分に検討の上、導入の可否をベンダーとご検討ください。
15	サプライチェーンには監査権を求めるようにはしてるのですが、中々同意をとれず結局は除外することが多いのですが、どのような進め方望ましいでしょうか。	研修にご参加いただきありがとうございます。 監査権が取得できない場合は、まず、責任分界点の明確化を求め、加えて、セキュリティ対策の実施要項や情報セキュリティ管理規程、運用規程の提出を求めてください。特に、脆弱性管理や、認証情報の保護について、具体的に情報を得ておくことが大事です。万一、インシデントが発生した際に、相手方の規程違反（過失）を指摘できるようにしておくことが重要と考えられます。これらの提出を拒む場合は、病院にとってリスクとなりますので、慎重な検討が必要となります。 一方で、セキュリティは協調領域であり、対立する領域ではありません。日常的に、友好的な関係を作り、セキュリティに関する情報交換を行うなど、相手方の意識を高めることも重要と思います。
16	講習会のパワーポイントのDL先をお教えください	研修にご参加いただきありがとうございます。 システム・セキュリティ管理者向け研修 e-learningのサイト(MinaSecure）よりログインしてダンロードください。 ※1：システム・セキュリティ管理者向け研修 e-learning受講申込みが未だの方は、受講申込の上、ダウンロードください。 ※2：共通研修のログインID/パスワードではダウンロードできません。 システム・セキュリティ管理者向け研修 e-learning受講申込は下記URLより申込ください。 https://www.saj.or.jp/form_agree/mist_e-learning-sys.html
17	以前の研修も含めて、資料はどちらにアップロードされているのでしょうか？	
18	こちらの資料もベンダーに見せたいため、前回に続きダウンロード可能としていただきたいです。	
19	これまでの講習会の資料を含めDL先をお教えください	
20	前回分も含めて資料のダウンロード先を教えて下さい。	
21	NW接続申請の様式があれば頂きたいです。	研修にご参加いただきありがとうございます。 ご指摘の様式は、今後の教材開発の参考にさせて頂きます。
22	「バックアップ」は、データのみのバックアップ、OSやミドルウェア等を含めた「同じハードウェアを用意するとOSインストール等を行わない方法で復元が可能なシステムセーブ」などが考えられますが、ここでは、どのような種類のバックアップと認識したらよいですか。	研修にご参加いただきありがとうございます。 バックアップは、OS、システム、データを含めたバックアップがあれば、復旧が早くなるメリットがあり、こちらをお薦めします。データだけの場合、システムの構成やバージョンの違いで、読み出すことができないなどの障害が考えられますので、ベンダーに確認をとる必要があります。
23	サプライチェーンの脆弱性管理について、ベンダ側のネットワーク機器の詳細(接続元IPアドレス制限されてるかやパスワードの強度等)を確認したくとも、ベンダ側の社内規則の都合で「イントラネットの構成が開示できない」という理由で提示を断られるケースがあります。こういった場合、どういう対応をするのが良いかをご教示いただけると有難いです。特に医療機器などは、予算の都合で保守契約締結ができないケースがあり、情報提供依頼がそもそもできない場合があります。病院側でサプライチェーン全体を把握するのは限界があると思っています。	研修にご参加いただきありがとうございます。 ベンダー側の構成については、調達時点で、多要素認証を要求したり、ID/PWの管理方法や桁数などを開示すること等の条件を付けることが重要です。開示されない場合は、次期更新で条件としてはどうでしょうか。 現行の仕様を開示しない場合は、責任分界点を明確化し、情報セキュリティ管理規程や運用規程の概要など、開示可能なものを求めるなどし、定期的にセキュリティに関する情報を交換する等、時間をかけて意識を高めることも必要ではないでしょうか。

#	質問	回答
24	接続元の正常性の保証証明というのは何をもって正常性と判断するのか。	研修にご参加いただきありがとうございます。 接続元でのインシデント発生が病院側に波及しないことが重要です。 ①機器やシステムの脆弱性管理の実施、②ウイルス対策ソフトの稼働、③Firewallの稼働、④多要素認証の導入や長いパスフレーズの採用、⑤個別のIDの採用などが最小限の目安になると思います。
25	先日、検査業者（大手）がシステム管理者で無断でリモート接続機器（携帯回線）を設置していたことが判明しました。現場の検査技師に了解とったと思われるのですが、その機材でないと遠隔保守できないとのこと。システムベンダだけでなく、当局から検査業者等への教育も行って欲しいです。	研修にご参加いただきありがとうございます。 ご指摘のリモート接続機器の設置は多くの病院で見受けられるようです。この場合、パスワードの桁数が短い、脆弱性管理がなされていない、などの課題も見受けられますので、まず、病院からこれらの確認を求めることが重要です。 ご指摘の検査業者等への教育については、今後の参考とさせていただきます。
26	院内NWであってもウィルス対策ソフトを入れるべきとのことですが、この時リアルタイムでパターンファイ等を更新するのは	研修にご参加いただきありがとうございます。 リアルタイム更新については、各ウイルス対策ソフトベンダー閉域網に対するソリューションを持っていますので、導入ベンダーにお問い合わせください。
27	ベンダーにバックアップ取得、脆弱性修正手順、作成、動作テストを依頼とのことですが、無償での対応していただけるベンダーはないと思います。	研修にご参加いただきありがとうございます。 有償での対応となると思います。今後の予算計画に反映頂ければと思います。
28	ネットワーク構成図の具体的な完成図があれば、ご教示ください。	研修にご参加いただきありがとうございます。 今後の教材開発で検討させていただきます。内容的には、機器の型番、役割、IPアドレス、サブネットマスク、空いているポートなどが考えられます。また、ルーターの場合は、セグメント間でのルーティング情報などが必要です。
29	院内NWであってもウィルス対策ソフトを入れるべきとのことですが、この時リアルタイムでパターンファイル等を更新するのはどうしたらいいですか。	研修にご参加いただきありがとうございます。 リアルタイム更新については、各ウイルス対策ソフトベンダー閉域網に対するソリューションを持っていますので、導入ベンダーにお問い合わせください。
30	接続元IPアドレス制限をかけてあれば、悪意のある者からは接続されないと言えるのでしょうか。悪意のある者が接続元のグローバルIPアドレスを詐称して接続してくることはあり得ないのでしょうか。	研修にご参加いただきありがとうございます。 悪意あるものが接続元のグローバルIPアドレスを詐称することは可能ですが、どのネットワーク機器が接続元制限をしているのか、つまり接続先のIPアドレスを知る必要があります。ケースとしては、接続元に侵入して接続先の認証情報を得るなどが必要です。 接続元が侵害された場合は、ご指摘のケースは成立してしまいますが、それ以外は、悪意ある接続を防ぐという意味で効果的です。
31	医療ITのガイドラインをはじめとして様々な対策を取るべき指標は出されていますが、そもそもとして電子カルテ他HIS系システムベンダーに厚労省のほうから指定内容を満たすシステム構成を取らせるよう指示・許可等させればいいのではないでしょうか。病院側で全てを確認させるというのは正直やり方として破綻しているように思います。今回や前回の内容など、ベンダーに話しても全く理解できないような、レベルの低いシステムベンダーも現実多い認識です。	研修にご参加いただきありがとうございます。 ご指摘は今後の参考とさせていただきます。
32	VPN装置について、SSL-VPN機能を使用していないため対策不要との回答をしたベンダーが居ましたが、その通りなのでしょうか。	研修にご参加いただきありがとうございます。 SSL-VPN機能を使用していないから対策不要と回答するベンダーは多いようですが、それ以外の脆弱性があるため、攻撃される可能性が高まります。非常に危険な状態ですので、脆弱性対策を実施するように求めてください。
33	複数の無料サービスのご紹介がありました。公的支援でもない限り、無料には無料なりの理由があると思いますが、なぜ無料で利用可能なのかご教示頂ければ幸いです。…というのも、突然有料化されると、公的医療機関は迅速な予算措置が難しく、行き詰まってしまうおそれがあるためです。	研修にご参加いただきありがとうございます。 無料サービスの多くは、スポンサー企業の存在や、利用者からの寄付で運営されています。サイトを訪問の上、ご確認いただき、利用の可否についてご検討ください。
34	VPN装置のファームウェア更新について、「ベンダに依頼してもお金を払わなければやりません。」という姿勢の会社がほとんどです。VPN装置のファームウェア更新について、情報システム部が無い病院の素人職員でも行えるような研修を行って欲しいです。	研修にご参加いただきありがとうございます。 今後の教材開発で検討させていただきます。
35	ベンダーは金がないと動かない、定期的なセキュリティcheckをお願いしたらどれだけ保守料とられるかわからない	研修にご参加いただきありがとうございます。ご指摘は今後の参考とさせていただきます。
36	病院に直接接続する業者側のリモート端末は安全性が高いと伺っていますが、そこへ外出先からリモート接続して接続していると伺っています。	研修にご参加いただきありがとうございます。ご指摘は今後の参考とさせていただきます。
37	リモートメンテ用のVPN装置が３０台以上あります。各ベンダーが推奨する機器構成のため機種や構成はバラバラで、それぞれの機器の脆弱性を把握したり、不正アクセスのログ監視は量的に難しいです。よい解決方法はありますでしょうか？	研修にご参加いただきありがとうございます。 リモートメンテナンスのVPN機器1台に集約し、そこから各機器にVLANをはる構成が考えられます。残念ながら、一部ベンダーは、自社システム以外の接続方式を認めない場合があります。この場合は、責任分界点の明確化、セキュリティ仕様や規程の開示、脆弱性管理体制、接続元IPアドレス制限の設定、認証情報の保護体制、ログ監視での状況報告を求めることが重要です。多くは、病院からベンダーへの情報送信というケースが多いですが、VPN装置の認証情報が脆弱であれば、第三者からの侵入を許すことになります。

#	質問	回答
38	カルテ・部門システム間でファイル共有式の連携を行う際には、カルテ側で単一のIDを払い出すケースをよくみかけるのですが、各システムごとに個別のID・パスワードを払い出すのが望ましいということでしょうか。	研修にご参加いただきありがとうございます。 システムの作り方で異なると思いますが、単一のID払い出しは、ランサムウェア攻撃に対して脆弱といわざるを得ません。導入ベンダーとどのような保護方法があるか、ご検討いただければと思います。
39	病院に直接接続する業者側のリモート端末は安全性が高いと伺っていますが、そこへ外出先からリモート接続して接続していると伺っています。 この場合でも問題ないということになりますか？	研修にご参加いただきありがとうございます。 担当者が自社にVPNで接続し、そこから病院側のVPNに接続している、という状況を前提にご回答いたします。（もし違っていたらお問い合わせください） この場合、自社のVPN装置に接続する際に、自社端末の認証を行っているかが重要です。どのような端末からでも接続を許可しているようでは安全性が担保できません。 ベンダーの管理している端末しか自社VPNに接続できないこと、多要素認証を導入している、もしくは長いパスフレーズを使用している、などの確認が必要と考えます。
40	クローズドネットワークにNGFW（UTM）を設け、そこでそのNGFWが提供するDNSを用い、FQDN指定でそこだけクローズド内のサーバ・クライアント等からアクセスできるように設定した場合は、安全性高くできると考えてよろしいでしょうか。クローズド内のアンチウイルス定義更新等はそのようにできればよいのではと考えています	研修にご参加いただきありがとうございます。 詳細な構成が分からないと、正確なご回答ができませんが、UTMがインターネットに接続でき（HIS系とはルーティングしない）、UTMのパターンやシステムの更新が可能であれば、一定の安全性は確保できるかもしれません。
41	オフラインバックアップに最適な製品を紹介してほしいです。	研修にご参加いただきありがとうございます。 特定の製品を推薦することはむずかしいですが、「WORM バックアップ」「WORM ストレージ」「イミュータブルバックアップ」などで検索すると、様々な製品が紹介されると思います。それらから、電子カルテベンダーとご一緒に健闘されてはいかがでしょうか。