#	ご質問	回答
#	**質問**	**回答**
1	警察が介入し各種サーバや機器を回収するまでにやっておくべきことはありますか	ネットワークケーブルを抜線し、電源を切らない、ウイルス対策ソフト等でスキャンしない、操作等を一切行わない、などが適切な対応と考えます。保全は、ハードディスクの保全とメモリの保全があり、ウイルス対策ソフトでスキャンすると、メモリ上に常駐しているウイルスがスキャンを検出し自分自身を消去するケースがあります。そうした場合、ワクチンの作成が困難になる、フォレンジック調査を行っても原因が判明しない等の影響がありますので、ご注意ください。
2	タイムスタンプの確認とありましたが、昨今のランサムウェアにタイムスタンプ改ざんの懸念は無いのでしょうか？なにかツールを使って詐称の判別は可能ですか？	設定ファイル（テキストファイル）の再利用においては、タイムスタンプの改ざんや、内容の改ざんの恐れはゼロではありません。従って、テキストファイルの内容を確認し、想定外のスクリプトの実行等がなされないようにすることが重要です。残念ながら当該のツールは存在しないため、目検以外に方法はないと思います。なお、実行形式ファイルの再利用は原則禁止ですので、ご注意ください。
3	ウイルス対策ソフトについて、当法人はサーバーやクライアント端末にウイルス対策ソフトを導入しています。そのため、更新する必要がありインターネットに繋がっています。やはりそれは危険でしょうか？	一般的なご家庭や企業での使用を見ても、インターネット接続が即ち危険ということはありません。ウイルス対策ソフトのエンジン、パターンの更新は、極めて重要な正しい対策と考えます。ただし、脆弱性管理ができないサーバーや端末、医療機器が同じネットワークに存在する場合は、外部からの攻撃が考えられます。従って、Firewall等でウイルス対策ソフトのエンジン、パターン更新先などの必要最小限の通信のみ接続を許可する等の設定を施すことが重要と考えられます。
4	RDPの待ち受けポートをデフォルトから変更しているとのことだが、全マシンでランダムに変更しているのか？ 全マシンでランダムであれば運用負荷が高くなると思われる。 一方でデフォルトから変更しても、全マシンで共通のポート番号であれば1台のマシンにポートスキャンをしかけ、変更後のポート番号が分かってしまえば全マシンにログオン試行が出来ると思われる。	RDP接続対象マシンで3389/TCPから特定の一意のポートに変更しており、残念ながら全数をユニークにはしていません。 Lockbit 、 Phobos、Snatch等のグループは3389/TCPの調査のためにスキャナーを使用しますが、全ポートスキャンの事例は存じ上げません。また、大阪急性期・総合医療センターでは、3389/TCP固定のスキャナーが確認されています。 これには、いくつかの理由が考えられますが、nmap等による全ポートスキャンを行うことで、侵入検知システムやEDRで検出されることを恐れているのではないかと考えています。 ポート変更は万全ではありませんが、多層防御の一つとしてお考えいただくのが良いと思います。
5	管理者IDとパスワードの保管は、どのようにするのが安全でしょうか。	必ず、長い推測困難なパスフレーズを設定し、ファイル名からPWが保管されていることが推測できないようにします。また、保存するフォルダーのアクセス権限を限定してください。ノートや手帳等に記録した場合は、鍵のかかるロッカー等に保管する等をお願い致します。
6	今回は、大阪急性期・総合医療センターの感染経路が給食センター経由ということでしたが、その給食センターに接続しているのは総合医療センターだけではないと思います。 他の医療機関が感染しなかったということは、パスワード、権限の管理が正しく行われていたからだと判断してよろしいでしょうか。	他の医療機関がどのようにセキュリティ対策を行っていたか等不明のため、お答えすることは難しいです。
7	大阪急性期医療センターではHIS系ネットワークはそもそもインターネット抜けしていなかったのですか？	大阪急性期・総合医療センターのHIS系はインターネットに直接は接続されていません。ただし、保守やファイル交換のためのVPN経由で接続してくるベンダー側のネットワークは、インターネットに直接接続、もしくはベンダー側のネットワークが閉域網であっても、VPN等で間接的に接続が可能な状態にありました。
8	海外モダリティベンダーは、リモート回線はベンダー独自以外は各社許容しないと言われている。また容易なパスワード変更機構もなく、セキュリティパッチの常時最新適用は難しいとの説明で、医療機関側でそれぞれ相当な費用、工数をかけて調整をしており、ベンダーに義務と責任を課していただきたい。	医療機器規制の国際調和を目指すIMDRF（国際医療機器規制当局フォーラム）から「医療機器サイバーセキュリティガイダンス（以下 IMDRF ガイダンスという）」が発行され、本年3月には「医療機関における医療機器のサイバーセキュリティ確保のための手引書」が公表されています。この中で、「医療機器事業者やサービス事業者が当該医療機器を保守するにあたって、契約等によって設置するサーバーや端末、ネットワーク機器などの医療機器認証に含まない周辺機器を含めて提供される場合においては当該医療機器を含む安全環境の維持に不可欠なものとして対象に含むものとします。」とされており、リモート回線等を含む保守におけるセキュリティ体制も、必要情報の提供が医療機器事業者（その他ステークホルダーを含む）に求められています。また、「脆弱性に関するセキュリティアドバイザリー情報、修正や指示等の提供」、「協調的な脆弱性の開示」も求められていることから、手引書におけるベンダーの対応状況の説明を求めることが必要です。今後は、調達時点での手引書対応等を選定基準に入れ、安全な機器等の導入の目安にされることをお勧めします。
9	あるサーバをhis系、情報系両方のネットワーク内で使用したい場合のセキュリティ対策の例をご教示いただけないでしょうか サーバを2NICにするだけではかなり危険なのはわかりますが、どう対策すればわからないためよろしくお願いいたします	別途、softwareisac.jp に具体的なネットワーク構成とルーティングの方法を解説するページを用意いたしますので、しばしご猶予ください。
10	踏み台サーバを使用したVPN接続では、複数のベンダーが同時に作業できないと思われる。踏み台を複数用意することは、コスト高・管理煩雑になり、民間病院ではハードルが高い。低コストで利便性の高い方法は無いか？	踏み台サーバーを使用した場合は、ご指摘通り、複数の同時接続は困難です。一方で、ベンダーがいつでも自由な時に接続できてしまうことは、一つの懸念事項ということもできます。VPN接続にあたっては、事前申請とし、時刻を定めて作業をしてもらうことが重要と考えます。
11	スライド16に「LTO装置のハードディスクも暗号化されていた」とありますが、LTOはテープなのに「ハードディスク」とあり、何を意味するのかが不明なので教えてください。 スライド26に「16桁のパスワード」とありますが、公表するのはいかがなものかと思います。桁数は13桁以上であり充分な長さかもしれませんが、桁数を公表すると特定されるリスクは上がります。また、他施設が「当施設は13桁だ。12桁だ。」と公表してしまう可能性を考慮すると桁数は公表すべきでなく「充分な長さの桁数」などの表現が適していると考えますが、いかがでしょうか。	LTO装置には内蔵HDDが存在しています。マニュアル等では、ファームウェアという表現が多いと思いますが、組み込み用 Windows が動作しており、こちらが被害を受けました。 スライド26ですが、8桁~10桁程度では、昨今のコンユーティング能力の向上を考えるとご指摘の懸念が残ります。一方で、16桁のPWの総組み合わせ数を考えた場合、キーボードに刻印された文字が95種使えるとすると、最大で95の16乗（4.40126668651766E+31）という膨大な組み合わせ数になります。これは1秒間に1億回総当たり攻撃を行っても1京年以上かかるため、単純な繰り返しなどが行われていない限り、桁数を開示しても実質的なリスクにはつながらないと考えております。

#	ご質問	回答
12	大阪急性期病院様では、システムのサーバー、パソコンを初期化された際、ベンダーにより２０２２年１１月当時の最新セキュリティパッチを適用された、との説明でした(現地見学会で医療情報部長先生よりご教示あり)。 最新セキュリティパッチを適用するとシステム動作が保証できない、何が起こるかわからない、保証できない、というベンダーの定型句的な回答を大阪急性期病院様はどのように回避されたのか教えていただきたいです。 最新セキュリティパッチを適用した状態でシステムの動作検証を予めメーカーが実施した、という理解で正しいでしょうか?	ご指摘通り、最新のセキュリティパッチを適用し、動作検証を行いました。最新パッチの適用で、特段の不具合や動作不良についての報告は受けておりません。多くのベンダーは納品時点の最新のパッチを適用して出荷していることから、パッチ適用が実質的な動作不良を引き起こす可能性は極めて少ないと判断しています。 一方で、OSのバージョンアップは、デバイスドライバの互換性がない等の影響があるため、実施できない場合があります。
資料・アーカイブ		
1	今回の公演資料を提供していただくことはできないのでしょうか。	本事業終了時（年度末頃）に、公開予定です。 公開した際には、MISTサイト（ https://mhlw-training.saj.or.jp/ ）からお知らせいたします。
2	パワポの資料はいただけますか？特に踏み台サーバーとVLANによる構成図を確認したいです。	
3	毎回感じるのですが、セミナー資料がダウンロードできるようにして欲しいです。大変参考になる情報があるのですが、所属部署内で共有することが難しいからです。ご検討のほどよろしくお願いいたします。	
その他		
1	前回、突発事項により受講できませんでした。再受講することは可能でしょうか？	システム・セキュリティ管理者向け研修は、各回異なった内容でご提供しております。そのため、同じ内容を再受講することができません。全オンライン研修終了後にアーカイブ配信を予定しております。アーカイブをご利用をお願いいたします。 アーカイブ配信については、随時MISTサイト（https://mhlw-training.saj.or.jp/）からお知らせいたします。
2	院内のセキュリティレベルを調査、報告頂けるようなサービスがあれば、紹介頂けますでしょうか。	現時点で、病院のセキュリティレベルの調査等について、ご紹介できるようなサービスは存じておりません。