Cat	#	ご質問	回答
1　医療情報システムの有無			
	1	電子カルテの導入がまだですがその場合も同じまでのセキュリティ対策が求められるのでしょうか？	医療情報を取り扱う端末等があればセキュリティ対策は求められます。
	2	医療情報システムの範囲について。当院では電子カルテ、オーダリングリストを使用しておらず、紙カルテとレセコンをベースに運用している（一部訪問診療のみ電子カルテを使用）。日常の諸文書（議事録、マニュアル、紹介状、ワークシートなど）は院内のLANの中にNAS端末を設置し、それを各部署ごとのPC端末からアクセスし、作成更新を行っている。このような場合、医療情報システムに含まれるのはどの範囲をいうのか。	システムに依存せず、患者情報が含まれている環境は「医療情報システム」と考えられます。ここでは紹介状などもあることから患者情報があると推察され、記載の対象全て医療情報システムと思われます。
	3	個人歯科医院の開業医です 根本的で申し訳ないのですが、個人歯科医院において対策が必要な医療情報システムとは具体的にどのような物でしょうか？	患者情報が含まれる端末や機器などが対象だと推察されます。
	4	医事会計システムや給食システム、遠隔読影システムは「医療情報システム」に含まれますか？	患者情報が含まれているシステムは対象です。
	5	医療情報システムの範囲は医療機器に付随するPCも含まれる認識で良いでしょうか。	患者情報が含まれている機器やPCも対象です。
	6	①医療情報システムには医療機器も含まれるとのことでしたが、R5年度はサーバについて確認するので、末端にある医療機器は対象外とのお話もありました。ネットワークには繋がっているが、特にサーバ配下でも無い単独医療機器は調査対象ですか？（例：内視鏡の光源装置等） ②①対象の場合： アクセス制御やログ管理等はそもそも製品として採用されていないものでも、「いいえ」としてR5年度中に対応しなければならないのでしょうか。 ③②対応必要な場合： どのように対応すべきか、具体例を以って教えてください。仮にR6年度の対象である場合でも全く案が浮かびません。	①率先して確認すべきものとしてサーバとしていますので、対象外と言えますが、ネットワークにつながっている以上、他の機器やシステムよりリスクが高いと思われ、早期対応が望まれます。 ②以下をベンダーに確認し、Ｒ５年度についてはエビデンスとして保管して「はい」としてください。 ・そもそもアクセス制御（またはログ管理）ができない及び実施しなくてもよい理由を確認しましょう。 ・インシデントが発生したときはログがない状態でどのように対応をするのか。 ・OS標準で取得可能なログも存在しないのか。 ③以下をベンダーに確認し、Ｒ６年度についてはエビデンスとして保管して「はい」としてください。 ・上記②に変更方針はないか。 ・厚生労働省が求めている当該条項において、いつまでにログやアクセス制御の機能を実装する予定なのか確認し、共有を行ってください。
	7	チェックリストの対象となる医療情報システムの定義についてご教示ください。	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準じます。
	8	医療情報システムの定義は何か、病院内のシステムや機器をどこまでを含んでいるのか？	患者情報が含むもの全てです。
	9	「医療情報システム」の範囲について具体例をなるべく多くあげて教えていただきたい。	患者情報が含むもの全てです。
	10	レントゲンシステム事業者からレントゲンシステムはチェックシートやMDS/SDS等は対象外のため対応できないと言われました。レントゲンシステムは医療情報システムに入らないのか。	医療情報を扱っていれば入ります。
2　令和5年度中 ＞1 体制構築＞（１） 医療情報システム安全管理責任者を設置している。			
	1	①複数の医療機関を抱えている法人において、各事業所において医療情報システム安全管理責任者の配置が困難である場合、法人経営層に準ずる職員が、各事業所における医療情報システム安全管理責任者となることに問題はありますでしょうか。 ②当院では大学からの派遣医師が当直業務を行うことが多く、勤務開始直前に電子カルテアカウントを作成するよう要請されることがほとんどである。結果として申請書等の運用が有名無実となっている状況であり、きちんと管理できているとは言い難い。実効性のある運用とするために取り組むべきこととして何が挙げられますでしょうか。	①責任部門や責任者は組織によって異なると思われ、責任者が明確であることが重要であり、問題ないと思います。 ②派遣医師がある程度固定されているのであれば、事前に派遣医師毎にアカウントを割り当てる。固定されないのであれば使用するアカウントと勤務情報を紐づけるなど、追跡できる体制を確保すること等が考えられます。
	2	ガイドライン6.0には許可病床４００床以上の医療機関には専任の医療情報システム安全管理責任者を配置しないといけないとなっていますが、保健所の立入検査では「サイバーセキュリティー部門（新設）」という項目があり、部門とは専任で責任者を配置しないといけないのでしょうか。	厚生労働省からセキュリティ部門の新設という直接的な指示は出していません。CSIRT（Computer Security Incident Response Team）についてもあくまでも例示ですが、機能として有することが大切で専任の部門でなくとも仮想の部門や組織体で問題ありません。そのため、必ずしも専任で配置しなければならないわけではありません。
	3	医療情報システム安全管理者は経営層が望ましいとの事ですが、連絡体制図の例にある安全管理者がベンダー等に連絡することになっており、ここは経営層ではなく情報システム担当者がすることになる気がします。医療機関の体制に合わせて変更してもよろしいでしょうか。	組織によって権限も異なると考えられ、各医療機関の体制に合わせて頂いて問題ありませんが、内容的には現場責任者とも言えます。 大切なことは、インシデントが発生した際に迅速に責任者がシステムの停止やネットワークの遮断等が行える管理者であるかどうかです。
	4	個人歯科医院の開業医です ・機器台帳ですが、タブレットも記載が必要でしょうか？	患者情報が含まれれば対象です。
3　令和5年度中 ＞2 医療情報システムの管理・運用＞（１） サーバ、端末PC、ネットワーク機器の台帳管理を行っている。			
	1	台帳管理の説明において、どの範囲なのか？という内容についてネットワーク接続をしている機器全てとして外部ネットワークに接続とも仰っておりましたが、院内ネットワークにつながっているものも全てという認識でよろしいでしょうか。	院内ネットワークにつながっているものも全てです。
	2	台帳管理のバージョン情報とは何でしょうか？	ソフトウェアのバージョン情報のことです。
	3	機器台帳に記載するソフトウェアは全てのソフトウェアを記載する必要があるのか。	原則は全てのソフトウェアですが、確認できる主要なソフトウェアから記載をしていきましょう。
4　令和5年度中 ＞2 医療情報システムの管理・運用＞（２） リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。			
	1	LAN接続されていないシステム（検査やリハビリ機器など）は独自のリモートメンテナンスが設定されていても、対象外と考えて良いか？	患者の診療情報等が含まれていれば対象内です。
5　令和5年度中 ＞2 医療情報システムの管理・運用＞（３） 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。			
	1	2023/9/13現在、MDS/SDSはVer5.2に対応だが、令和5年向けにはVer6t対応でなくてもいいのか	その時点で最新のバージョンのドキュメントをご利用ください。
	2	・医療機器において、機器を製造しているベンダーとそれを販売、保守をしているベンダーとありますが、この場合窓口となっている販売、保守ベンダーに対しての依頼はサービスを提供ということでSDSのみの回答を求める様になるのでしょうか。製造元のベンダーに対してMDSを出してもらうよう合わせて依頼するのでしょうか。	はい、ご記載の通りです。
	3	業者が、独自の視点で、MDMなどを記載し、統一した基準でチェックをしていない。どうしたらよいか？	必ずしもJAHIS等が定めた標準様式である必要はありませんが、医療機関が事業者から提供されているサービスのセキュリティについて標準様式に準じた内容を確認するようにして下さい。

Cat	#	ご質問	回答
	4	MDS/SDSのバージョンはガイドライン6.0に対応していませんが、古いガイドライン対応のものを使用して問題ないのでしょうか？	現時点では大丈夫ですが、更新を促してください。
	5	6.セキュリティ開示書（ＭＤＳ／ＳＤＳ）の提出があっても、全項目を満たさなければ、未実施となるのでしょうか。	本来は満たす必要があるものですが、対象外とならざるを得ない項目もあると思われ、適切に記入されベンダーから虚偽なく説明されるものであれば、未実施とはなりません。
	6	ＭＤＳ／ＳＤＳについては、独自様式で運用をしているチェックリストがある場合でも提出してもらう必要があるのか？	必ずしもJAHIS等が定めた標準様式である必要はありませんが、医療機関が事業者から提供されているサービスのセキュリティについて標準様式に準じた内容を確認するようにして下さい。
6	**令和5年度中 ＞2 医療情報システムの管理・運用＞（４） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。**		
	1	令和5年度の（4）（5）（6）についてですが、これはサーバのログイン時に使用するユーザーのことなのかそれとも電子カルテシステムのログインで使用するユーザーのどちらになりますか？それによって対応方法が異なります。	今年度についてはサーバ側のアカウントがメインとなり、R6年度は後者の電カルログインユーザも対象です。
	2	利用者のアクセス権限の設定の項目のところで１つお聞きしたいことがあります。「定期的にアクセス状況や棚卸を行う」とありましたが、ここでいう棚卸というのはどのようなものと理解すればよいでしょうか？もう少し詳しくご説明いただけるとありがたいです。	退職者が出た場合や臨時で割り当てる必要があったアカウントなどを、不要になった時点で見直しを行うこと等を想定しています。
	3	アクセス利用権限の利用者台帳は必要でしょうか？経営者への報告承認必要でしょうか？説明できるものはどのように作成しますか？	必要です。システムに取得できる一覧をベースに経営者に定期的に報告をしておくことが望ましいと思います。承認対応の粒度は組織によって異なりますが、経営者が認識していただいていることが望ましいと思います。
	4	令和5年度対象のエンドポイントというのはPC端末のことで医療機器や調剤機器などは対象外という認識でよいでしょうか？	R5年度は端末PCは対象外です。
	5	医療機関におけるサイバーセキュリティ対策チェックリストの（４）利用者の職種・担当業務別の情報区分ごとのアクセス利用権限を設定している。の項目の説明ではシステム（電子カルテ）の権限の話をされておりましたが、この項目についてはサーバについて、以下を実施している。と前置きがあるのでサーバへの権限の話(administratorなど）と考えるのですが、どちらの内容での回答が正しいものとなるのでしょうか？	今年度についてはサーバ側のアクセスやアカウントなどの権限です。
	6	「サーバについて、以下を実施している。(4)利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。」の項目ですが、これはサーバーOSのユーザー管理か、それともその上で動いているソフトウェアやアプリ（医療情報システム）のユーザー管理か、いずれが問われているのでしょうか？	今年度はサーバが対応の範囲です。
7	**令和5年度中 ＞2 医療情報システムの管理・運用＞（５） 退職者や使用していないアカウント等、不要なアカウントを削除している。**		
	1	令和5年度の（4）（5）（6）についてですが、これはサーバのログイン時に使用するユーザーのことなのかそれとも電子カルテシステムのログインで使用するユーザーのどちらになりますか？それによって対応方法が異なります。	今年度はサーバや管理者が対応の範囲です。R6年度はユーザー含む全てです。
	2	サーバについて以下を実施いるの項目について、 利用者の職種・担当業務別の情報区分ごとのアクセス利用権限、および退職者アカウントやLOG管理もそうですが、「カルテや部門ソフト使用するためのアカウント」と「サーバやNW機器のアカウント」の両方のことを指してますでしょうか？	いずれのアカウントも含まれますが、R5年度については後者です。
	3	2-(5)の退職者や使用していないアカウントについて無効にする場合でもセキュリティリスクはありますでしょうか。	適切にアカウントの無効化を行っていれば、セキュリティリスクは低いと思われます。
	4	令和5年度対象のエンドポイントというのはPC端末のことで医療機器や調剤機器などは対象外という認識でよいでしょうか？	エンドポイントは末端の端末を意味しており、PC端末や各種機器を指しています。
	5	・退職者アカウントに対し、学部教授会から「大学で雇用していなくても医局には所属しており、研究で必要だから、使わせろ」と言われているが、この場合でもアカウント削除は必要でしょうか？	個別のケースなので対処方法を正確にお答えするのは難しいです。
	6	退職者、使用していないアカウントを削除ではなく無効にしている場合、セキュリティリスクは上がりますか	適切にアカウントの無効化を行っていれば、セキュリティリスクは低いと思われます。
	7	退職者のIDを削除せよとのレセコンでメディコムでは削除できないとの事でした。どうすればいいのでしょうか。	まずは担当窓口ではなく本社部門にご確認をお願いします。それでもアカウント管理もできない製品であれば改善を求めます。
8	**令和5年度中 ＞2 医療情報システムの管理・運用＞（６） アクセスログを管理している。**		
	1	令和5年度の（4）（5）（6）についてですが、これはサーバのログイン時に使用するユーザーのことなのかそれとも電子カルテシステムのログインで使用するユーザーのどちらになりますか？それによって対応方法が異なります。	今年度についてはサーバ側の対応を求めています。
	2	また、システムベンダーへのチェックリストやアクセスログ関連の協力依頼が難航している場合、厚労省からの何かしらのサポートは期待できるでしょうか？	医療機関が事業者に対策の状況を確認するよう求めており、厚労省からの個別ケースに対するサポートはございません。
	3	サーバのアクセスログは、部門システムも含めるか?	部門システムが医療情報を管理または医療情報システムと接続されていれば含まれます。
	4	アクセスログ管理は対象は電子カルテシステム連携している部門システムにも及びますか？	医療情報システムの範囲において全てです。
	5	②アクセスログの管理について、こちらは電子カルテや医事システムおよび部門システムやUTMなどの機器へのアクセスをそれらのシステム上で取得できればよろしいでしょうか？それとも端末すなわちOSつまりWindowsへのアクセス管理も必要でしょうか？	医療情報システムの範囲において、対象の機器やシステムのログが必要です。
	6	2-6について、ログの管理について具体的な方法、手順、対象を示してほしい。PC端末のログインやログアウトまで分かればいいのか、電子カルテをだれが開いてだれが書き込みだれが閲覧したのかまでわかるべきなのか。Windowsの標準機能で取得できるものでよいのか、電子カルテ等基幹システムや部門システムに個別にアクセスログ管理機能を実装する必要があるのか。一言で「ログを管理する」ではあいまいだと思います。	具体的な取り組みは各医療機関で費用や実装方法は異なるため、どこまでどの製品を用いて等の言及は控えさせて頂きます。なお、サイバー攻撃や内部不正などが生じた場合に追跡できるような環境構築が必要です。
	7	⑦アクセスログの管理はつききっりでしょうか？ログリストはどのようなものでしょうか？ログが取れてるとは何でしょうか？	ログはいつ、誰が、どこに、どのようなアクセスをしたのかがわかる情報が取得できているかです。定期的にログを確認し運用状況を確認したり、製品からのアラートが飛んでくるように設定しておくことが必要です。ログリストとは、取れているログのリストです。Windows、Active Directory、ウイルス対策ソフト、ファイアウォールなどの組織が導入している製品やソリューションで取得しているログの一覧化したものです。
	8	11.医療機関によってはマンパワーの問題から、ログのレビューまでできる余裕がない場合、自組織のセキュリティポリシーで求められている期間のログが保存されている体制がとれていれば、「アクセスログを管理」できていると整理してよろしいのでしょうか。	最低限、組織で導入しているセキュリティ製品がログを取得、できる限り長い期間保管できている設定になっているか、そしてアラートを通知してくれる設定になっているかなどを確認をしましょう。定期的にログを確認し、組織で起きているサイバー攻撃の状況などを関係者で共有しましょう。
	9	ログを取得するところでwindoewsへのログインは標準ユーザーの1アカウントで、閲覧機能やオーダ権限等の認証はログイン後のアプリでしか行っていない場合アクセスログとしては電子カルテのアクセスログを取得し確認すればよいのか教えてください。	具体的な確認項目等に関しては、ご提示頂いた内容だけでは判断できず、回答することは難しいです。大変申し訳ございませんが、ご理解頂けますと幸いです。

Cat	#	ご質問	回答
9　令和5年度中 ＞2 医療情報システムの管理・運用＞（７） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。			
	1	令和5年度の（7）についてチェックリストではネットワーク機器が対象と思いますが、今回の説明ではネットワーク機器とサーバが対象と言われていました。サーバは令和6年度の対応と思いますが、どちらが正しいのでしょうか？	ネットワーク機器が対象で、サーバも令和6年度の対象です。しかしながら、セキュリティ対策の構築上、仮想アプライアンス等で構築しているものはサーバも対象となります。
	2	閉域網を利用した環境でのOS/ソフトウェア等のバージョンアップに関して、適切な方法はあるでしょうか？	オフラインでの更新方法も準備されていますので、ご利用製品の企業サイトをご確認ください。
	3	ネットワーク機器には、ルータやスイッチ、APなど多くの種類があります。ファームウェア更新は、全てのネットワーク機器が対象か？	対象です。
	4	セキュリティパッチ関係で、ネットワーク機器とは具体的に何を指しますか。	昨今の攻撃で用いられているファイアウォール（VPN機能を有する）機器はもちろんのこと、ルータなどのネットワーク機器も対象です。
	5	①パッチの適応について、現状電子カルテや医事システムおよび部門システムについてはWindows updateを止めているのが現実です。こちらはベンダーに対して我々医療機関以外からも厚労省から働きかけなどは行われるのでしょうか？	医療情報システムや機器の更新を促すためのガイドライン更新や通達などは行っています。またベンダーによっては検証後アップデートを行っているベンダーも存在します。Windows updateを止める前提の設計になっているようであれば、当該ベンダーと協議頂き、脆弱性対応を行うよう促進ください。
	6	2-7 サーバに対してのパッチ適用について、ベンダーの許可がない限り難しいと思いますが、どうすればよいのでしょうか？	契約形態にもよりますが、医療情報システムの委託元としてセキュリティ対応を行うよう促していく必要があります。またクラウドサービス等においてもどのような適用状況になっているのか、確認を求める必要があります。ベンダーとしてのセキュリティ姿勢を確認し、病院としての方針を伝えセキュリティ強化を行いましょう。
	7	事業者にサーバーのセキュリティパッチについて確認したところ、「外部ネットワークに接続していないため、セキュリティパッチの適用は不可。」と回答がありました。どうすればよいでしょうか。	2年連続で発生しているランサムウェア事案は、閉域網というベンダーのセキュリティの思考停止から発生しています。閉域網の利用、リモートメンテナンス状況、システムベンダー（サプライチェーン）を通じてもアクセスができない完全な閉域網なのかを確認と証明を求めましょう。
	8	ｼｽﾃﾑ上OSの更新が困難な場合はソフトウェアやセキュリティパッチの更新のみでも良いのでしょうか。また、閉域網あるいは別の要因に伴う機器の改修が大々的に必要な環境でありながら運営上その回収が困難な場合、猶予期間あるいは免除措置などは今後予定しているのでしょうか？セキュリティが必須であるというのは理屈としてわかりますが、現実的に現在の事業を継続しつつそこに人員を割くことが困難な医療機関等は必然出てくるかと思います。そういった対象への救済処置はあるのでしょうか？現状その対策としてアクセスログやリモートPCなどのセキュリティ確認をそれを担うベンダーが管理するようにと案内されているように思いますが、それが困難な場合の対策および実務が具体的に提示されていないように感じました。	医療情報システムに接続するネットワークのトラフィックにおける脅威の拡散等を防止するために、OSのセキュリティパッチ等、リスクに対してセキュリティ対策を適切に適用して下さい。チェックリストでは、令和5年度中はネットワーク機器を対象にしております。
	9	サーバーOSを更新する場合、冗長構成でないものはシステム停止が必要となると思います。停止時間の予測も立てづらく、ベンダーからもシステムへの影響が読めないと言われ見送ってきました。定期的な更新を行なっている医療機関があれば環境など教えていただきたいです。	そもそも冗長構成になっていないことが大幅なリスクですが、一般的には参照環境を用いたり、計画停電時に更新を行ったり作業を行っています。またWSUS（Windows Server Update Services）を用いて更新を行っている医療機関もあります。
	10	本日はご講演ありがとうございました。セキュリティパッチの適用について、オンプレ型の電子カルテについてシステムのバージョンが古いため、最新のセキュリティパッチに適応しておらず更新ができておりません。最新のセキュリティパッチを適応するためには電子カルテシステムのバージョンアップが伴い、多額の費用が発生することになります。現状電子カルテの更新を待って最新化を図ろうと検討しておりますが、良い方法はありますでしょうか。	オンプレの電カルシステム更新では今後も同様の課題が伴うため、クラウド型の電子カルテの活用を検討するなど、BCPの観点からも是非、ハードウェアやカスタマイズしたソフトウェアを医療機関で保有しない環境づくりの検討をしてください。
	11	セキュリティパッチの適用は24時間365日稼働が必要な病院経営の構造上、非常にリスクの伴う行いである。患者の受け入れを止める事は経済的損失も伴う行為でもある。代替案や特定の条件下においては不要と判断できるような案がもしあれば教えていただきたい。	BCPを鑑みてシステムを冗長化したり、クラウドサービスの利用によって改善・解消できると思われます。
	12	OSの更新をするようにとのことでしたが、オンプレの電カルで（リモート有の閉域網）セキュリティに多くの費用を使えない中小の病院でも、簡単にできることなのでしょうか。	各医療機関のシステム、構成、契約等によっても異なります。まずは運用・保守の契約がどのようになっているか確認してください。
	13	令和5年度対象のエンドポイントというのはPC端末のことで医療機器や調剤機器などは対象外という認識でよいでしょうか？	エンドポイントは末端の端末を意味しており、PC端末や各種機器を指しています。
	14	セキュリティパッチについては、どこまでが求められるのでしょうか。IEしか動作しないようなシステムもあり、アップデートの対応が出来ないような場合は、次回更新時などの対応予定日になっても良いのでしょうか。	医療情報を取り扱う、全てのシステムや機器が対象です。動作しないような環境であればリスクをきちんと把握し、次の対応時期を決定してください。チェックリストの対応予定日は定期的な確認目的でもあるため、年度内に設定してください。
	15	2.ＯＳ更新はシステムの停止が必要となるが、救急受入等実施している医療機関において運用面に課題がある場合、半年に１回程度の定期的なパッチ適用でも良しとする整理でよろしいでしょうか。	頻度については病院毎の運用もあるため言及できませんが、適用できていないパッチによってどれくらいのリスクがあるのかは把握しておく必要があります。
	16	3.ＯＳ更新により、電子カルテ等の重要な情報システムの挙動が保証できない場合等、セキュリティと運用のバランスについてはどのような見解となりますでしょうか。	まずは保証できないとしている技術的・組織的な理由などを、既存の契約を踏まえ確認しましょう。基本的には脆弱性や古いソフトウェアは更新を行い、安全な状況で利用して頂くことが必要です。保証しない理由が検証をしないということであれば、検証を促していただく必要があります。また古いソフトウェアを利用するのであれば推奨はできませんが、完全な閉域網の中で利用するのであれば、外部侵入されるリスク、さらには侵入されても脆弱性が悪用されるリスクは低いため、そのような環境を構築し利用しているか確認することが必要でしょう。
	17	12.パッチの更新はインターネット経由で行うことが原則であるとおっしゃっておりましたが、発言の真意についてご教示いただけますでしょうか。	昨今のソフトウェアそのものがネットワーク接続していない環境での使用を想定していません。また頻度高く更新するのであればセキュアにネットワーク接続を行い、更新の方法を検討する方が現行の閉域網で何もしないとしている状況よりセキュアであるという趣旨です。
	18	ＯＳのアップデート作業で非常に高額は費用（２千万円超）を請求されるが、実施すべきなのか？	作業や請求内容が不明なため、お答えしかねます。
	19	サーバーへのセキュリティパッチ適用とあるが、OSのパッチなのか、インストールしているウイルスチェックソフトのパターンファイル最新化なのか区別が分からない説明だった。 今も分からず終いで混乱している。RedHatやLinuxでも影響あるものと無いものの切り分けはユーザー側では判断できない。（しにくい）	双方です。ソフトウェアはできる限り最新のものを利用してください。
	20	・セキュリティパッチの範囲ですが、OSの更新プログラムとウイルスパターンの更新では影響範囲がかなり違うと考えます。重要なOSのパッチは充てるべきでしょうが、常に最新を充てる必要はないと思いますし、現実的に作業費用や検証費用を考慮すると難しいと思います。どのように考えればよろしいでしょうか。 必要があると思います。	基本的にソフトウェアの考え方から、重要なパッチは適用すべきであり、サポートされている最新の状態を維持する必要があります。なお、パッチがあたってい（あてられ）ない場合は、脆弱性をつくサイバー攻撃を確認できる体制確保が必要です。昨今の動向を踏まえると脆弱性やソフトウェア更新対応が必要な国際的な動向となっており、対応を促していただく必要があります。さらにこれまでの閉域網は閉域網とは言えず、いわばオープンな環境であるため、クラウドの活用など基本のネットワーク構成などの見直しを行っていきましょう。
10　令和5年度中 ＞2 医療情報システムの管理・運用＞（８） 接続元制限を実施している。			
	1	2.送信元の制限については、結局どこまで実施すれば〇となりますでしょうか。MACアドレス制限、IP制限、地域制限など具体的に教えてください。	組織によってどこまでというのは異なりますが、外部からの不要なアクセスを制御できている環境（アクセスする環境のIPアドレス制限、地域制限等の実施）であれば、問題ありません。

Cat	#	ご質問	回答
11 参考項目（令和６年度中）＞2 医療情報システムの管理・運用＞（９） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。			
	1	バックグラウンドで動作する不要なソフトとの表現がありましたが、例えばどのようなソフトのことでしょうか。ご教示ください。	環境に依存するためこれが不要とは言及しがたいですが、例えば、医療情報を取り扱うパソコンでゲームのソフトは不要であり、削除の対象です。
	2	チェックシート2(9)不要なソフトウェア・サービスにはWindows本体のサービスも対象になるのか、また単純にサービスが使用しているポートをファイアウォール機能でブロック、あるいは通信先を制限する対策ではだめなのかご教示ください。	対象になります。どのポートやプロトコルを制限しているかはわかりませんが、通信制御の1つの方法として相違ありません。
12 その他			
A 機器の区分けに関する事項			
	1	「サーバー」と「端末ＰＣ」の具体的な違いを教えて下さい。「サーバー」とは「サーバーOS」、「端末ＰＣ」とは「クライアントOS」のことを指すのでしょうか？またクラウドシステムはどちらに入るのでしょうか。	サーバはADなどの管理系のサーバやデータを格納しているファイルサーバなどが対象です。端末PCは取り扱うパソコンや機器などが含まれます。クラウドは享受しているサービスによって異なりますが、DaaSであればクライアント、SaaS、IaaS、Paasなどであればサーバとして考えてください。
	2	・「ネットワーク機器について、以下を実施している。」とありますが、ネットワーク機器とはどこまでの範囲でしょうか。院内のスイッチやハブ、無線AP等を含めると相当な数になります。外部と接続されている機器（VPNルータやファイアウォール等）を考えておけばよろしいでしょうか。	優先すべきはファイアウォール、VPN等のセキュリティ機器ですが、記載のネットワーク機器も対象です。
B チェックリストの回答に関する事項			
	3	予算等の関係で本年度中どうしても実施不可能なものがある場合にも今年度中の対応予定日を記入する必要があるのでしょうか。	2回目の実施目標としても期限入力をお願いします。
	4	OSのパッチやVPNの接続元制限をできないのは、ベンダー側の理屈の方が通っています。 説明の内容は病院側に責任を押し付ける逃げでしかなく、全く納得がいく内容ではありませんでした。 なぜ、利用者側の病院でなく、サービスを提供する事業者側に義務付けないのでしょうか。 現在のままでは、永遠に解決できないと思います。 これについてはどうお考えでしょうか。	医療情報システムを利用する利用者としての責任、または委託元としての責任があり、システムを使う以上、各組織で対応をしていく必要があります。また既にガイドラインに準拠する必要性があり、医療機関もベンダーも当該ガイドラインに準じた対応が必要です。
	5	チェックリストの提出を求める事業者の対象はシステムベンダーのみでしょうか？それとも医療情報システムに接続されている医療機器ベンダー等もすべて対象となるのでしょうか？	患者情報を有するシステムや機器は対象です。
	6	実際に小規模病院で対応可能なのか？	チェックリストに基づくご対応をお願いいたします。
	7	自組織のサイバーセキュリティ対策チェックリストは、令和6年度から提出義務化されるのでしょうか。	サイバーセキュリティ対策チェックリスストは医療法に基づく立入検査の際に使用されます。
	8	オフラインでレセコンを運用していて、院内にインターネット回線がきていない、というときは、チェックリストは不要となりますか？	回線がないのであればネットワークの部分については該当しませんが、その他の部分はチェックリストへの対応が必要になります。
C ペナルティに関する事項			
	9	ずっとセキュリティー対策が構築されずにいた場合の罰則等はあるのでしょうか？	現状罰則はございませんが、立入検査で指摘があった内容について改善がみられない場合等において、法第24条第２項における改善命令が出されます。
	10	チェックリストで「いいえ」とした項目について、目標日を記載しますが、2回目のチェックタイミングはこの目標日にするということでしょうか。また、2回目も「いいえ」の場合ペナルティ等あるのでしょうか。	2回目のチェックのタイミングは必ずしも目標日に行うものではなく、医療機関で実施できるタイミングで行って頂ければと思います。また2回目も「いいえ」の場合、3回目以降も実施して頂き、令和５年度中に全てのチェッ
	11	どう考えても、「いいえ」の項目が多数。令和6年度でも対応できない場合は、どのようなペナルティが課されるのか。	現状罰則はございませんが、立入検査で指摘があった内容について改善がみられない場合等において、法第24条第２項における改善命令が出されます。
	12	チェックリストがすべて「はい」にならず、その後改善がなされない場合の行政行為は「医療法第第24条第２項における改善命令」に留まるのでしょうか。	ご指摘の通りで、現状罰則はございませんが、立入検査で指摘があった内容について改善がみられない場合等において、法第24条第２項における改善命令が出されます。
	13	チェックリストは最終的に「いいえ」となった場合は、どうなるのでしょうか？	現状罰則はございませんが、立入検査で指摘があった内容について改善がみられない場合等において、法第24条第２項における改善命令が出されます。
D 事業者（ベンダー）に関する事項			
	14	ベンダーに照会した事項について、回答が「はい」となっているものをどこまで信用すればよいのか迷うところがあります。どのように対処すればよいでしょうか。	ベンダーと協議して疑わしい点を確認するか、第三者に助言を求めるようにしてください。
	15	チェックリストをベンダーに提出し、提出依頼をしても返答がない。ベンダーの変更を検討するべきか。医療機関だけでなくレセコンや電子カルテ取扱業者に対しても意識改革の取り組みを強化してもらえないだろうか	医療機関は事業者にサイバーセキュリティ対策の状況を確認するよう求めてください。
	16	「簡単な設定変更」が保守の範囲外といわれることがかなり多いです。（足元を見られている気がする）病院の職員では保守範囲内外を見極めるのが難しいのですが、何か手立てはあるでしょうか。	通常の保守であればシステムが正常に稼働できる状態を維持することが本体の目的であり、維持できない運用は保守とは言い難く、保守の範囲をまずは協議しましょう。また、ガイドラインに遵守するのは医療情報システムとしては必要であり、ガイドラインに順じた対応ができているのか確認してください。
	17	専門的な知識を持つシステム管理者がいないので、ベンダーとの交渉ができなかった場合の対応を教えてほしいです	医療機関は事業者にサイバーセキュリティ対策の状況を確認するよう求めてください。
	18	閉域網での、サーバやルータへのセキュリティパッチの更新はベンダーへ依頼することになるかと思いますが、エンドポイントのWindowsUpdateなどはどう考えればいいのでしょうか	環境にもよりますが、各自更新をお願いします。大規模環境であれば一元的に管理できる仕組みを検討しましょう。
	19	電子カルテベンダーを通して部門システムを導入しています。保守の契約も電子カルテベンダーが代表で行っています。この場合、部門システムの事業者確認用チェックリストは電子カルテベンダーに提出をお願いするべきでしょうか。部門システムベンダーからは直接の契約がないため対象外との回答がありました。	保守契約を電子カルテベンダーが行っているのであれば、電子カルテベンダーの責任で収集頂く必要があります。なお、インシデント発生時のベンダー側の対応も確認しておきましょう。
	20	コースの内容と直接関連しませんが、今回のチェックリスト作成に関して、事業者から書類提出の費用を求められた場合、医療機関はどのように対応するのがよいでしょうか。できれば、ポータルサイトに掲載いただければと存じます。	既存の運用確認として用いるものであり、費用追加は想定していません。
	21	①ベンダーにチェックリストの回答をもらっていますが、ベンダーにはいをつけてもらっただけではだめでしょうか？立ち入りで説明になるでしょうか？	なぜ「はい」となったのか、根拠を確認いただき、説明できるようにしておいてください。
	22	・患者情報は匿名だからとか患者情報は扱わない（勤務管理システム等）のでチェックリストは作成しないというベンダーでも、ネットワークで直接接続しているシステムは、チェックリスト作成の対象外なのでしょうか？	患者情報があれば対象ですが、患者情報を取り扱わないようであればチェックリストとしては対象外です。しかしながら、医療機関のガバナンスという視点ではすべてのシステムやネットワークを組織として把握しておく必要があります。
	23	5.事業者用のチェックリストは、医療情報システムの保守契約をしている事業者が対象となるのか。	はい、その通りです。

Cat	#	ご質問	回答
	24	病院には立入検査として強制力を持ってセキュリティ向上を求めているが、国からシステムベンダー側への強制力を持ったアプローチは無いのか？病院によっては情シス人員が1人以下というところもあり、例え立入検査の項目にサイバーセキュリティ関連内容が入ったから、急に病院側が情シス人員を増やしたところでマンパワーとして使えるものでは無く、チェックリストにある「令和5年度中、6年度中」にやるべきことの助けにはならない。 そのため、国からシステムベンダー側への強制力を持ったアプローチが無いと達成は難しいと思うがどうか。	医療機関は事業者にサイバーセキュリティ対策の状況を確認するよう求めてください。
	25	マルチベンダーの場合、特にセキュリティパッチ対応は、どのベンダーも「他のベンダーシステムの動作確認までは面倒が見れない」といって拒否されるのはどうしたら良いでしょうか？ また、ベンダー（保守）側のアカウントが複数人での共有アカウントでないと困ると言われているが、それは良いのでしょうか？	医療機関は事業者にサイバーセキュリティ対策の状況を確認するよう求めてください。
	26	保守サービスを結んでいるが、事業者用のチェックリストの提出は対象外との返事など、医療情報システムのネットワーク内で患者情報等をやり取りしているベンダーから返答がある場合に法的な根拠としてはどの部分を示していけば良いか教えていただければ助かります。	医療機関は事業者にサイバーセキュリティ対策の状況を確認するよう求めてください。
E	**その他**		
	27	立入検査とは保健所が行う検査ですか	保健所等が行う検査です。
	28	管轄の保健所より立入検査時に、サイバーセキュリティチェックリストは大きな病院の為のものであり、個人でやっているような診療所はしなくてもいいという回答を得たという話を伺いました。研修を受けた印象は、電子カルテシステム等で患者様の情報を扱っている医療機関は大小関わらずしなければならないと認識いたしましたが、保健所からの説明は正しいのでしょうか？ご教示ください。	いいえ、全医療機関が対象であり、保健所の回答は適切ではありません。
	29	ソフトウェアの更新やセキュリティパッチの適用など、ベンダー側に対応してもらわなければいけない項目が多いが、国として利用する施設側ではなく、医療システムを販売するベンダーに対して販売するためのチェックリストや対応しなければいけない基準等を設ける等、ベンダーに対する指導、研修を行うことはないのか。	医療機関は事業者にサイバーセキュリティ対策の状況を確認するよう求めてください。
	30	対象になっている医療情報システムの範囲がどこまで及ぶのかが難しい。外部ネットワークとのつながりはなく、レントゲンなどの画像を電子的に保存するのみの院内ネットワークの場合はどこまでのチェックリストを満たせば良いかわからない。ベンダーの質が様々だと思うが、この研修を受けたベンダーは一定信用できるといったような認証制度はないでしょうか。	患者情報があるシステムやネットワーク、機器はすべて対象となり、全ての事業者確認が必要です。また閉域網だと思っていも設定によってはオープン化されている場合もありますので、既存のネットワーク環境の確認も行ってください。ご指摘の通りベンダーの質次第ですが、ご記載の認証制度については現状ございません。
	31	以前、教えてもらったサイバー攻撃を受けた場合の厚生労働省の連絡先 医政局　研究開発振興課　医療技術情報推進室 03-3595-2430 は、今回、教えてもらった連絡先に変更になったのでしょうか？	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html 医療機関等がサイバー攻撃を受けた場合の厚生労働省連絡先 医政局特定医薬品開発支援・医療情報担当参事官室 TEL：03-6812-7837 MAIL：igishitsu×mhlw.go.jp ※迷惑メール防止のため、メールアドレスの一部を変えています。 「×」を「@」に置き換えてください。
	32	医療機器において、必要時に電子カルテとネットワーク接続する機器がありますが、これらも対象となりますでしょうか。	対象です。
	33	個人歯科医院の開業医です 今回の研修では主に電子カルテを使用している医療機関向けの対策だったと思うのですが、個人歯科医院は電子カルテではなくレセコンがメインとなっております。その場合今日のような対策は必要なのでしょうか？	医療情報を含む端末や機器があればすべてが対象です。
	34	個人歯科医院の開業医です オンライン資格確認のシステムはサイバーセキュリティ対策を行わなければならないでしょうか？インターネットを介さないシステムだと伺っておりますが、いかがでしょうか？また、サイバー攻撃が行われた場合その責任の所在はどこにあるのでしょうか？	オンライン資格等システムにおいてもサイバーセキュリティ対策を実施頂ければと思います。また、オンライン資格確認等システムを運営する実施機関または医療機関等の利用者の責任範囲は、「オンライン資格確認等システム利用規約」に定められております。医療機関等におかれては、医療情報システムの管理や運用を適切に行う責任があります。
	35	インシデント発生時の外部連絡先優先順位を具体的に教えていただきたい。大阪の事例で警察に連絡すると証拠保全のため端末を触ることができなかったなどの報告があったため。	ケース等によって外部連絡先が異なってくるため、お答えすることが難しいです。
	36	サイバーセキュリティ対策チェックリストで確認した結果、機器更新の検討が必要となった場合の費用の面での補助は国としてあるのか。また、診療報酬上の加算などは検討されているのか。	現状、チェックリストの項目で機器更新を求めていないため、補助はございません。
	37	立ち入り検査で、はいの回答にたいして、どのような質問が想定されるでしょうか？	保健所の対応のため回答いたしかねます。
	38	サーバーのアカウントとは何でしょうか？	サーバを管理する管理者のアカウント等があるかと思いますので、ご確認ください。
	39	医療機関用のチェックリストは医療機関全体で一つで良いか、それともシステムごとに必要でしょうか？	事業者向けはシステム・契約毎で、当該情報を参照し医療機関として１つのチェックリストを
	40	医療機関として事業者が提出してきたチェックリストが妥当か確認するためにも、事業者確認用チェックリストの解説をしたマニュアルが必要と考えますが今後作成される予定はございますでしょうか。	現状、ご指摘頂いたマニュアル作成の予定はなし
	41	令和７年度のチェック項目が変わった場合であっても、令和５年度～令和６年度で未実施となっている項目については、引き続き立入検査での確認をされる整理でしょうか。	R7年度のチェックリストについては今後の検討事項であるため、現時点ではお答えができません。
	42	サイバーセキュリティ対策については専門的な人材が少なく、検査実施者によってチェックの粒度が異なってしまうのではないかと思われますが、その点についてどのような見解でしょうか。	保健所職員にも研修を受けて頂いています。

Cat	#	ご質問	回答
	43	MDS/SDSは医療情報システム事業者に契約病院等へ提出させるように、厚労省通知を発出させればよいと考えます。病院等及び医療情報システム事業者の負担が激減されると思いますが、いかがお考えでしょうか。本研修は医療情報システム事業者にこそ見ていただきたい内容です。サイト等で公開される予定はございますでしょうか。 既存の設定を変更する、保守契約に追加する、セキュリティの専門家に依頼する、これだけでも病院等によっては億千万単位の費用がかかります。またこの内容を行うとすると電子カルテシステムを導入したいと考える医療関係者はいないと考えますが、セキュリティ対策に補助金等財政支援が必要かと考えますが、病院が支出する費用増について、研修の打合せの際に厚生労働省とは話をされたのでしょうか。医療法による立入検査ではなく、貴協会のような専門事業者に厚生労働省が委託し、監査・アドバイスを行うほうがよほど日本国全体のセキュリティレベルがあがると考えますが、いかがでしょうか。 ケーススタディでログの取得方法については解説がありましたが、解析については話がありませんでした。解析こそ職人技でITSSの高レベル人材が活躍するフィールドですが、一般の病院等職員で行える方法があるとお考えでしょうか。セキュリティパッチ等の適用は電子カルテシステムベンダが拒否する、または高額の費用を請求するようになっていますが、本状況を打開するにはシステム更改のタイミングでベンダを変更するくらいしか無いように思います。このような業界の状況で令和６年度までにどう対策すればよろしいでしょうか。 ここまでセキュリティに不安があるのであれば、総務省が日本年金機構の事件をきっかけに自治体セキュリティ強靭化を行ったようにすればよいかと思います。厚生労働省が主導し手始めにLGWANと同じ思想のWANで医療等の業界が活動すれば一気にセキュリティリスクは減りますが、このような大規模WANについて、メリット・デメリットはいかがお考えでしょうか。 情報セキュリティが大切であれば、唯一の独占名称資格である情報処理安全確保支援士の採用など、セキュリティ人材の確保について、診療報酬や補助金でインセンティブをつけるといった手段がありますが、そういった方法についてはどうお考えでしょうか。 経営層にセキュリティへの投資を促すため、総務省がマイナンバーカード普及の際に各首長へ書簡を送ったように、厚生労働大臣から書簡を送るというやり方もあります。このような方策について厚生労働省に提案するなど、委託事業者の視点から活動していることはございますか。	ご意見として承ればと思いますので、何卒宜しくお願いします。
	44	基本的な質問で申し訳ありません、「立入検査」は具体的に何を指しておられますでしょうか。	医療法第25条第1項に基づく医療機関への立入検査です。
	45	Q1.いろいろやれば良いのはもちろんわかりますが、具体的な攻撃の詳細がわからないためどの対策をまずやるべきか、費用(手間)対効果も含めてわかりません。優先度の検討のためにも教えていただきたいのですが、例えば半田病院、大阪急性期のケースでは、windowsのセキュリティパッチを適用をしていればランサム被害を防げたのでしょうか。その場合、いつ公開されたパッチが適用されていれば防げたのでしょう。	大阪急性期例でいえば、院内に侵入された理由はRDP通信を常時接続していたことであり、給食事業者が侵入を許してしまったのはFWの脆弱性の放置、または漏洩されていた脅威情報の収集ができておらず漏洩したIDやパスワードを使用続けたことが根本的な技術的な原因があります。すなわち適切な制御とFWの脆弱性対応、IDとパスワードの適切な運用がまずは必要でしょう。
	46	Q2.同様に、半田病院、大阪急性期において、(FWの脆弱性とRDPによる操作は別の問題として)、各端末あるいはサーバへのランサム被害は、ウイルス対策ソフトで防げるか局所化できたのではないかと思っています。閉域では手動アップデートをせざるを得ませんが、1週間に1回のパターンファイルアップデートでは遅いほどのゼロデイだったのでしょうか。	攻撃者は管理者権限を悪用して、セキュリティ対策ソフトは無効化、アンインストールした上で攻撃を行うため、セキュリティ対策ソフトや更新の有無によって感染可否が変わった攻撃ではありません。
	47	Q3.講演中「windows7が動いているのが悪いのではなく、それを把握していないことが問題」との表現がありました。その場合、令和6年度のセキュリティチェックリストの2(7)が「いいえ」となり、立入検査上問題と指摘されそうです。どのような対策をすればwindows7をオンラインで使っても問題ないと考えられますでしょうか。	古いOSをオンラインで利用し続けることはリスクが高く、使用し続けることは望ましくありません。古いOSを利用しているリスクを受容し、インシデントが起きた際にどのように対応するのかなど、リスク受容に対する説明をお願いします。
	48	古いOSは論外として、大手のセキュリティソフトを使用するとWindows Defender の機能が制限されてしまうため慎重に導入する方が良いのでしょうか？ セキュリティソフトを検証する第三者機関である、世界的に有名な「AV TEst」や「AV-Comparatives』においてはwindows10 の中盤以降でのWindows Defender は 他の大手セキュリティソフトと比べ、総合評価にて圧倒的にトップでした。 Windows Defender の機能を最大限に活用する設定をした方が好ましいかと考えます。 もちろん怪しい添付ファイルを開かない、詐欺メール対策などへの教育を徹底するなどは常識的に行ってことはどちらにしても必要ですが。	具体的な製品についてはコメントできませんが、各種セキュリティ機能を有効活用した対策が必要です。
	49	サイバーセキュリティに関する院内規定等を作成しないといけないのでしょうか？また参考になる資料等はございますでしょうか？	既存の規程類にセキュリティの項目を追加いただいても、新たにセキュリティの規程を作成頂いても問題ありません。中小企業向けではありますが、IPAが公開している文書を共有します。 （https://www.ipa.go.jp/security/guide/sme/about.html）
	50	・チェックリストの「はい」は、まずはリスクの確認ができていればよろしいでしょうか。サーバやPCの設定変更やパッチの適用には、別途作業期間と費用がかかります。令和５年度中のチェック項目についても、事業者用も含めすべて年度内に対応するのは難しいと考えます。さらに令和６年度中の中身については、完璧に対応する場合サーバやPCの買い替えが発生し、複数年の計画を立てなければ、対応は難しいのではないかと思います。セキュリティを軽視するわけではないですが、現実的な計画の下で更新を進める必要があると思います。	それぞれの項目によって異なりますが、実施できている状況が基本的には「はい」です。 記載のような状況であり、計画的に対応していくことを立入検査等で説明できる状況にしておいてください。
	51	立ち入り検査はいつありますか？	各都道府県の対応によって異なりますので、具体的な時期はこちらではわかりません。
	52	私がITリテラシーが比較的高いということと、IT企画部門ということで医療情報システム安全管理責任者となる見込みだが、今回の研修をみると電子カルテ停止を判断・打診できる権限がないといけないように見受けられたので、そういった権限が必要であることを経営層に対して説明して同意を得る必要があると理解したが、その通りでよいか。	迅速に対応するためには基本的には前もって停止できる体制（権限）を確認しておくことが望ましいです。一方で、経営層と迅速に連携ができる形でも問題はありません。各組織の背景によって体制は異なりますが、大切なことは救急同様、迅速に対応できる体制の確保です。