病院名	A病院
病床数	約400床
施設基準：主たる基準	≪基本診療科施設基準届出≫ ・一般病棟入院基本料1 急性期看護補助体制加算(50対１) 看護補助体制充実加算1 ・地域包括医療病棟入院料 看護補助体制加算(50対１) 看護補助体制充実加算1 ・回復期リハビリテーション病棟入院料3
従業員数：	
医師数	常勤49名
看護師数	211名
臨床工学技士数	10名
その他職種（メディカルスタッフと事務職等）	臨床検査技師22名、診療放射線技師20名、薬剤師15名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	情報室3名で対応。全員事務職　内医療情報技師2名。実務的には医師はほとんど関与していない。管理組織としての委員会に医師が入っているので、院長も把握はしている。委員会規程では、**部門システムの管理者や端末機器の管理者も定めている。**委員会の規程については、1年に1回は見直したいところであるが、実際には、監査や病院機能評価のタイミングで見直しをしている。その際には、他院の情報も取り入れながら、見直してをしている。他院の情報については、ベンダーを通して情報を入手している。システム保守についても、3名がオンコール体制で対応している。プリンタが詰まったということで、呼ばれることも。特に委託はしておらず、情報システム系の全てを対応している。端末機器の引っ越しなどの対応もしている。検診システム別システムであり、連携はしているが、別部署が管理している。
2）ネットワーク構成図を把握しているか？	情報システム更新後に把握するように改善した。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	委託業者に依頼して、ネットワーク構成図を作成。 情報システム自体も大手ではなく、地方のベンダーを利用
4）追加のシステムなどはどのように情報を入手して管理しているのか？	保守契約を行い、追加工事の際にも一括で委託業者が管理。無線は医局に1本引いているが別回線で使用。ただし、部門システムまでの構成図はできていない。部門システムやそれに接続する医療機器等については、構成図には反映できず、情報部門からは見えない状況にあるのが課題。各部門での管理となる。
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	開示していない。申請があれば、必要に応じてIPアドレスを払い出し。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	ニュースや県警などから情報を入手。県警と合同でセキュリティの勉強会も実施。警察が直接病院に来ていただき、講師として、情報セキュリティについて講習を実施。知り合い経由で警察に依頼したところ、実現となった。パッチなどは基本あてていない。情報システムの安定稼働を重視し、更新の際に最新にするような運用。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	IT-BCPがまだ作成できていない。作成する方法もわからないので、見本が欲しい。
2. 医療機器のサイバーセキュリティ確保について	

病院名	A病院
1）ネットワークに接続される医療機器についてどう管理しているか？	ネットワークに接続する際には、声をかけてもらうような運用。部門システムの責任者が対応することになっている。いただいた情報は**IPアドレスの払い出し情報とともに、台帳で管理（機器名、使用場所など）**。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	ネットワークに接続する機器については、情報システム課に報告することとなっている。選定は各部門で、実際の購入は総務が担当するが、職員同士連携して対応している。ベンダーからの連絡も多い。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	医療機器等については、ネットワーク構成図までに落とし込めていない。リモート接続は要件を出しているが、会社で対応できないということで、結果的には許可されている事例はない。どこまでを責任分界とするか指標が難しい。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	できていない。**診療側では知識がないので、わからない**。教育されていないので、言われても理解ができない。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	**情報が情報システム課にはあがってこない**。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	**ガイドラインについて知ってはいるが、見ているだけで具体のアクションはない。**今回の研究班によって始めて知った。**ビジュアルで分かるようにしてほしい。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	**このような情報があることを知らない。医療機器のサイバーセキュリティ確保に関する通知を病院団体から発出されたことを確認したことがない。医政局や保険局の事務連絡は通知されている。実働部隊がいない。**
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	メーカから提供はされない。聞いた事もない。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？構築しているようであれば、その内容をご教示いただきたい。	特に医療機器安全管理責任者と連携していることはない。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？また、その人材として必要な知識、技術、人数をご教示いただきたい。	できていない。OSの把握等について、医療機器に関しては把握できていない。
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	病院ごとの指標があるとありがたい。**医療機器についても、セキュリティを管理する責任者がいて、情報システムと連携して対応していけると良い。**
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	想定できていない。シナリオがあれば、こちらも欲しい。

病院名	A病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	できていない。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	わからない。
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	盛り込んでいる内容はない。
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	**医療機器メーカとの連携はない。メーカから情報を教えてほしい。物は売りにくるが、情報は持ってこない。卸からの情報もない。**見積もりや請求書は持ってくるのが早い。メーカからの情報をWEB上で情報共有ができる仕組みがあるとありがたい。
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	今回の研究班をきっかけに病院長と共有している。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	費用面の問題もあり、保守契約は結べていない。
その他意見	○インフラを整備する予算が不足している。今回の診療報酬改定でも、診療録管理体制加算が1から2に下がってしまった（バックアップのオフラインでの保管ができないため。）。補助金でも1/3補助とか2/3補助が現実なので、利益率1-2%の中で、補助金にも手が出せない。ネットワーク調査には補助金が使えたが、バックアップには使えなかったので、結果的に、1⇒2に下がってしまった。 ○実際に診療情報管理体制1を取得している病院の情報などが欲しい。現在は、過去の経験などを活かして人脈で情報を入手している。 ○**病床数や機能によって、対応が違うので、何をまねしていいのかも分からない。病院規模別、機能別の具体的な対策のひな形を望む。**
追加情報	○中央の情報システムは買い取り。サーバ保守が続く限り使用する。部門システムは別予算で更新。過去はネットワーク障害が多かったが、ネットワーク設備を更新することで、障害は減った。 ○電子カルテ端末からインターネットは使用できない。院内メールは電子カルテ端末で利用できるが、外部へのメール発信は別パソコンでの運用としている。 ○セグメンテーションを切って管理していないが、セグメンテーションを切って管理した方が良いか分からない。

病院名	B病院
病床数	約100床
施設基準：主たる基準	・一般病棟入院基本料　急性期一般入院料1 急性期看護補助体制加算(25対１) 看護補助体制充実加算2
従業員数：	
医師数	32名
看護師数	111名
臨床工学技士数	0名
その他職種（メディカルスタッフと事務職等）	172名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	情報管理室2名。病院システム全般的な管理。ウイルスソフトの管理画面で病院内のウイルス管理。 →**VPNの設置費用や管理については、設置したベンダーの責任で対応。**ワークステーションなどで費用なVPNは個別で対応し、**システム関係のVPNはひとつに統合**している。**情報系VPNの管理は電子カルテメーカーにお願い**している。検査系については、情報システムのVPNから入るようにしている。 **部門システムのメンテナンスは各部門で対応。**遠隔で保守する場合もある。手術部門システムは定期メンテの中でVerアップなどで対応している。（契約に含まれる。） 導入の際には各部門から情報管理室へ連絡がある。 **各部署の院内窓口を決めてもらっている。**ベンダーから見ると情報管理室、各部門窓口のどちらも病院の窓口として機能するようにしている。メインとサブというようなイメージ。 以前は担当者が短期間で交代していたため連携ができていなかったが、現在の担当者は10年以上の経験があるので、時間をかけて連携して対応ができるようになった。
2）ネットワーク構成図を把握しているか？	はい。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	ネットワーク業者が作成している。簡易版を病院で作成している。
4）追加のシステムなどはどのように情報を入手して管理しているのか？	システム関連の情報であれば、ベンダーから情報を入手します。
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	原則、開示していません。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	厚労省、全日本病院協会、ベンダーからの通知で入手しています。ルーターなどセキュリティ機器のファームウェアは常に最新状態。 →情報システム関係の脆弱性については、対応しているが、機器側については、どう対応すれば良いか分からない。情報システムについては、外のデータセンターにデータバックアップをしている。（市販のサービスを利用）リアルタイムバックアップが可能で、世代管理も実施している。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	可能です。※医療機器を特定した形では入っていません。シナリオを作成して随時アップデートを行う予定。 ※IT-BCPについて　協議会とともに医療機関用の訓練用ロールプレイングシナリオを作成中 →トラブル時のマニュアル自体の整備はしていないが、**サイバー攻撃に備えたアクションカード**をまとめて、これに沿って各部門で対応することとしている。
2. 医療機器のサイバーセキュリティ確保について	

病院名	B病院
1）ネットワークに接続される医療機器についてどう管理しているか？	情報管理室では、IP管理しています。 →検査、大型機器などは部門で管理。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	医療機器の管理は、メーカーとの連絡が密となるため、部署単位で行っている。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	放射線科ネットワークについては、**放射線科にてIPと設置場所など管理**している。（ＣＴ、ＭＲＩ、ワークステーション、エコー等）
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	医療機器のウィルス対策は病院側では行っていない。 ・OSバージョンアップは動作保証の問題があり、行っていない。（一部機器については、有償でのバージョンアップ対応が可能である。） ・**一部でベンダー側が脆弱性チェックを行う覚書を交わしている。** →覚書きに定期的に脆弱性のチェックをすることを明記。異常がある場合に連絡。対応については、ベンダー対応であるが、費用分担の記載はない。機器の保守契約の範囲であれば、ベンダーが対応する。今後、更新の際に、このような記載を横展開していく。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	メーカーからの通知を入手している。 内容を検討してバージョンアップなどの検討は行う。 メーカーからの無償パッチは、積極的に適用する。 →実際的には、機器側については、どう対応すれば良いかわからない。機器側トラブル→パソコン側で検知されると思っている。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	医療情報システムの安全管理に関するガイドライン　第6.0版 医療機器のサイバーセキュリティの確保に関するガイダンスについて →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**手引きも今回初めて見た**が、初めて見る内容が多い。**何をすれば良いのかわからないので、チェックリストなど具体のやり方を教えて欲しい。**手引きを読んでも全くわからない。玉を投げるだけでなく、拾いやすくして欲しい。
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	メーカーからも情報を入手していない。 →レガシー機器の対応については、10年ぐらいで更新をしているため、それほど問題とはなっていない。経営的には何とか更新できている。
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	メーカーからも情報を入手していない。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	医療機器に特化していませんが、**サイバーセキュリティ対策委員会を立ち上げて各部署連携**している。 →規約の中で、連携して対応するように明記している。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	各部署が対応を行い、問題発生時は情報管理室で対応にあたります。 **監視やインシデント対応、教育やセキュリティ対策などのセキュリティやネットワーク管理として法人で2名欲しい。**
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	SOC(監視）やCSIRT(インシデント対応やセキュリティ教育)を整備して、セキュリティ担当チームから、SOCや各部署との連携体制をとりたい。
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	動作不良など、初期対策で各部署とメーカで対応を行う。サイバーセキュリティの可能性があれば、IT-BCP発動へのシナリオへ移行。

病院名	B病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	病院スタッフへは情報セキュリティ研修を行う。佐賀県警セキュリティ研修や全日病DX人材育成プログラムの内容から研修動画を作成する。11月に行う予定。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	医療機器の正常な動作を確認する。
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	新しく契約を更新しているものから、内容を盛り込んでいる。
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	動作不良など判明した時点でメーカーと対応する。
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	医療機器に限らず、動作不良やシステム不良時は状況を院長・事務部長と情報共有している。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	医療機器のサイバーセキュリティ保守契約は結んでいないが、脆弱性のチェックに関しては横展開するように今後は追加する予定。
その他意見	○**現実的には一人で対応することはできない**。情報システムから見ると部門システムは専門外。部門システムから見ると情報システムは専門外。**お互いわからないところがある**ので、必要時に連携して対応するしか方法がない。 ○**サイバー攻撃はコロナよりかかりやすく、部門システムから入りやすい。**職員にも浸透させる必要がある。 ○**輸液ポンプやシリンジポンプがネットワークに繋がるような認識はない。**今後業者とも話し合う必要がある。 ○**医療機関向けの第三者的なセンター**が欲しい。**メーカーとつなぐ、情報を流通して整理するようなところ。公的な集団**が欲しい。医療機関では、**セキュリティに関する人材は集められない。給与も低い。** ○**医療機器まで含んだ院内規程の参考となるものが欲しい。**
追加情報	○放射線関係のシステムは部署長が管理を担当することになる。機器の選定をしているので、その流れでシステムについても管理担当となっている。 ○手術室のシステムについては、麻酔科医師と連携して対応している。手術室を担当する主任看護師がメンテナンスなどを対応することになる。その他の部門システムについては、気がついた時に対応している。経験が長く、医療機器安全管理責任者としても対応している。 ○検査部門のシステムは主任が対応を任命されている。 ○サイバー攻撃の対応訓練として、関連病院を中心に、**協議会の支援を得て、訓練をサイバーセキュリティ対策委員会を中心に机上訓練**を実施予定。 →セキュリティ対応については、専門家でないので、何をどうすれば良いかわからない。地域セキュリティ協議会は、医療だけでなく、警察、セキュリティの専門家、大学の情報管理部門の関係者が集まり協議会を設置。医療介護系のセキュリティ強化を目的に、非営利に近い団体。ネットワークを作り、BCP、サイバー対策の相談窓口としても機能することを目指している。 →1-2時間で1つの部署完結で行うような訓練。病院関係者がいないと説得力がないということで、病院関係者が理事として、協議会に入っている。**セキュリティのプロと現場をなじませる。共通言語を作る等、現場に落とし込む形での訓練を実施し、それを横展開**していくことを考えている。厚労省のガイドラインの解釈の違いについても、相談に乗っている。 ○全日病でも個人情報の研修会があり、その中でセキュリティに関する内容も入っているが、セキュリティ単体の研修はない。 ○診療放射線技師会では、情報セキュリティに関する勉強会はあるが、養成課程では情報セキュリティに関する内容はほとんどない。臨床検査技師も同じような状況。 ○看護師教育では、セキュリティ内容も入っている。医療情報に関する内容もカリキュラムに入ってきている。

病院名	C病院
病床数	約500床
施設基準：主たる基準	一般病棟入院基本料(急性期) 急性期充実体制加算 急性期看護補助体制加算 2(25対１) 看護補助体制充実加算
従業員数：	
医師数	
看護師数	
臨床工学技士数	
その他職種（メディカルスタッフと事務職等）	
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	職種：情報部長の医師1名（兼任）、事務職員3名（専任）、外部委託業者7名 役割：医療情報に関わる導入、運用、保守、ヘルプデスク →医療情報システム系はある程度、医療情報部で抑えているが、**医療機器については、契約で購入しており、抑えていない。ベンダーと各現場とのやりとりで対応しているのが実情。HIS側は何とかなるが、医療機器までは到底対応できない。** 部門システムの管理は各部門の管理者が行っている。情報管理委員会はあるが、しばらく開催していなかったので、今後開催して、IT-BCPの承認などを得ていく予定である。また、医療機器に関する動きも情報共有していく。外部委託者はヘルプデスクと運用を行う。ネットワークの検知まで行うが、トラブル対応はベンダーにお願い。情報部は橋渡し的な役割。
2）ネットワーク構成図を把握しているか？	ネットワーク構成図のうち物理構成図はシステム更新時に作成し、必要に応じて更新を行っているが、必ずしも最新版ではない。理論構成図に関しては、設定変更の度にネットワーク業者より更新データが納品される。また、現状、構成及び機能などを全て把握できているわけではない。 →情報部範囲のネットワーク構成図はあるが、その先は各部門での管理。各部門でもそれほど認識は高く無い。その場でやっている感じ。リモートメンテの希望が多い。申請ベースで管理しているため、使わない時でも残ってしまう。**ネットワーク資産の棚卸しをどうするかが課題。**
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	ネットワーク構築業者が作成し、納品したものを使っている。その後の変更等も業者に依頼した場合は、完成図書を納品してもらっている。
4）追加のシステムなどはどのように情報を入手して管理しているのか？	HIS系ネットワーク及び情報系ネットワークに接続するシステムの場合、接続するためには、情報部が管理しているIPアドレス、証明書などの情報がないと接続できない仕様になっている。そのことから、必然的に新たなシステムを導入する際は、事前に情報部に相談いただく流れとなっている。
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	医療機器メーカーには基本的に開示していない。求められれば、必要に応じて部分的に開示することはある。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	（入手先） ・厚労省、県庁及び協議会からの通知 ・IPAからのメール配信 ・電子カルテベンダー及びネットワークベンダー等の業者からの連絡 ・県警からの情報提供 （活用） ネットワーク機器等に脆弱性情報に合致するものがあるか確認し、合致するものがある場合は、速やかに対象ベンダーへ対策依頼を行う。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	現在、初版を作成中。完成後の提供は問題ない。現時点では、医療機器に関してはほぼ出てこない状況で、ベンダーに協力を得て感染している・していない、対策を依頼するフローとなっている。
2. 医療機器のサイバーセキュリティ確保について	

病院名	C病院
1）ネットワークに接続される医療機器についてどう管理しているか？	厚労省のサイバーセキュリティ確保事業を契機に現在洗い出しをし、脆弱性のチェックをしようとしている。 →IPを払い出しているのみで、細かいところまでは把握していない。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？ （医療情報システムとの違いがあれば。）	現時点では、電子カルテなどの医療情報システムは医療情報係が管理し、部門調達の医療機器（医療機器に付随するシステムを含む）は契約係で契約・管理、各部門で運用をしている。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	医療機器は含まれていないネットワーク構成図はある。※一部は理論構成図（ＩＰアドレス管理）は存在する。 →**機器までの配線管理はできていない。**
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	医療機器に関しては、契約係で調達していることもあり、契約係とディーラー間で対応を行っている。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	ディーラーからの報告等で把握しており、必要がある場合は対応を行っている。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	・医療情報システムの安全管理に関するガイドライン6.0 ・セキュリティ教育支援ポータルサイト ・ほか医療機関のIT-BCP ・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き書 →手引き書を見てはいるが、**最もな事を書いている反面、今全部やれとなるとパンパワーがない。今までの流れを考えるとレベルが高く、実際やるのが難しい。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	現時点では管理できていない。MDS/SDSに関して昨年度末に開示を求めた。
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	医療情報係で調達したシステム等は、MDS/SDSに関して昨年度末に開示を求めた。部門システム（レガシー医療機器を含む）は、把握できていない。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	まだできていない。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	医療情報システム障害発生時連絡体制図に沿って、動く想定だが、人材として必要な知識、技術、人数はまだ試算できていない。 また、現時点では医療情報システムが主であり、医療機器を含めたものについては、別の管轄部署と調整しながら今後行う必要あがると考えられる。
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？ （院内の連携体制なども含めて）	現在は、医療情報システムと医療機器の調達管理担当部署が異なっており、情報が共有されることが少ない状況である。そのため情報共有できる体制を作る事が望ましいと考えている。なお、現状、医療機器調達担当及び医療情報システム担当者は事務職員が担っているため、セキュリティを含む必要な知識を持った人材を配置することが望ましいと考える。
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？ （周知も含め、シナリオがあればご恵与願いたい）	現在、医療情報システムに関しては、IT-BCPを作成中。他院のIT-BCPを参考にしている。今年度中には病院情報システムに関するIT-BCPを作成予定であり、その後医療機器もふまえた内容に改訂していく必要があると考えられる。

病院名	C病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	（職員向け） ・医療従事者：1回/年の情報セキュリティに関する研修を必修としている →医療に関わるところより、一般的なセキュリティ教育。一般的なセキュリティ研修　県警職員が講師。協議会研修会でサイバーセキュリティ対策講習 机上訓練を実施（一般的なサイバーセキュリティ訓練） （在宅患者） ・在宅患者さんには、**レンタル会社などから酸素やポンプなどが貸し出されているが、サイバー攻撃の影響が考えられるものがないと思われる。** ・在宅患者さんには研修などは行っていない。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	・医療機器の一覧を最新にしておく運用をする ・ＯＳやバージョンを最新にしておく運用をする ・通常のログ状態の把握と異常の検知 ・IT-BCPのブラッシュアップと訓練
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	現状、保守範囲や個人情報の取り扱いに関しては、契約書等で定めているが、**サイバーセキュリティ確保に関する責任分界点は定めていない。**
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	連携のルールなどは定められていない。現状は必要に応じてディーラーから担当者に連絡されている。
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	IT-BCP、遠隔地バックアップなど個別には共有することがあるが、全体として共有はできていない。医療機器に関しては、必要に応じて、供覧・起案等で情報共有を行っている。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	結んでいない。
その他意見	○**ベンダーもピンキリであり、会話にならないところもある。**何のこと？と言いながら**勝手に接続していることもある。**外資系はしっかりしているが、**今後契約で縛り、外部との接点は1本化していく必要がある。** ○**IT資産台帳が必要。**勝手に接続すると警報が出るような仕組みがあると良い。しかし、**誰が管理するかが課題。** ○**サイバーについての契約をしていないので、有事の時に協力が得られるか**も課題。 ○**資産台帳と紐付けて、サイバーリスクを管理できるような台帳が必要。** ○現状把握が大変であり、ネットワーク資産の棚卸し、ログの管理が難しい。**セキュリティと医療情報分野は別に管理**することでも良いのではないか。**良心的なコンサルが指南してくれ、仕組み作りをサポート**いただけると良い。 ○素人でもさわりが分かるようにしてもらわないとお手上げ。専門の人に丸投げする場合、検証ができないことも怖い。**セキュリティの仕様書のひな形ができると便利**であり、最低限これだけやるようなことがあると良い。ただ、固めすぎると参入業者が来なくなり、費用も高くなるので難しいところ。 ○医療機器の**認可の段階で標準的な仕様で開発**してもらい、セキュリティが問題ない機器を販売してもらわないと困る。**広まった段階で何とかせよと言っても対応できない。** ○**セキュリティができる人材は取り合い。**
追加情報	○HIS系、インターネット系、学術系で分けている。 ○2020年7月にHISはリプレース。次回は2027年予定。今年度基本方針を策定予定。部門システムについても要望が上がってくれば、同時に更新する。 ○厚労省の支援事業として、今年の春ぐらいに、**外部との接点や脆弱性のチェックを行ってくれる事業があったので、参加している。**各部門のベンダーが見えなかったので、契約の方に、ベンダー各社の情報を出してもらって、そこにメールで一斉配信して、外部接点について確認しているところ。おおよそ返答があり、リスト化できつつある。厚労省の事業で、委託側との接点の調査と脆弱性のチェックをしつつ、現場確認や診断結果をいただけるような事業。外部接点があるかどうかの確認が主目的で、それにぶら下がる端末機器や医療機器等は今後の検討となる。放射線や検査関係が多かった。情報部が把握していない**20～30の外部接続の可能性が確認できた。** ○機器更新は比較的できており、古くなったOSと言うようなコメントもあり、レガシー機器については、更新で対応できている。保守が切れるからというのが更新理由で多い。フルメンテが多い。移転した際にほぼ新規で購入した。

病院名	D病院
病床数	約600床
施設基準：主たる基準	特定機能病院
従業員数：	1574人
医師数	443人（医師　435人、歯科医師8人）
看護師数	648人
臨床工学技士数	24人
その他職種（メディカルスタッフと事務職等）	459人
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	職種：医師、看護師、医療情報技師、事務職員、技術補佐員 人数：13人 役割：病院情報システムの運用・保守 →上記は基本、情報システム本体の対応。**部門システムについては、部門で対応**いただいている。各部門とは、調整会議で連携を図っている。情報部は情報部+学術管理部門　併せて13人。委託業者は入っていない。放射線関連のシステムは診療放射線技師が対応。副技師長を担当として任命している。副技師長の中で適任者を選任している。 小さい部署については、情報部でもサポートしている。基本的には、ネットワークに接続する際は、情報部へ連絡が来ることになっている。仕様策定の段階で情報部も加わる。 情報部ではHIS系のネットワークと学術系のネットワーク両方を管理している。 放射線機器や検査機器以外の医療機器については、基本的にはネットワークには接続していない。切り離して使用しているのが現状。接続する場合には、情報部に相談して対応。**メーカと臨床工学部門、情報部の三者協議で対応している。**
2）ネットワーク構成図を把握しているか？	ネットワーク完成図、統合管理システムのマップ上で把握 →HIS系や学術系の配線図は、情報部で管理している。最新化については、都度、新システム導入時に都度委託業者が対応。情報システム系については、委託している。部門システムの配線図は各部門での管理。部門システムで電子カルテに繋がらないものやリモートメンテに必要な接続は学術系のネットワークで対応。内容によって対応している。以前は別の配線を引いていたこともあったが、HISの更新の際に、一本化して現在は、**基本外部からの接続は統一し、集約化している。大阪の事例があった後、リモート回線を調査せよという指示もあったが、既に一本化しており、問題はなかった。**
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	ネットワーク契約時に情報部にて構成図の仕様を作成。情報部にて管理している。
4）追加のシステムなどはどのように情報を入手して管理しているのか？	追加希望の部署から情報部へ依頼があり、当該部署、情報部、当該ベンダーにてヒアリングを行っている。（要件定義の整理）
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	開示していない。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	以下URLを適宜参照し、必要に応じてベンダーと協議している JVN:　https://jvndb.jvn.jp/ IPA: https://www.ipa.go.jp/security/vuln/index.html
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	病院情報システム運用継続計画　IT-BCP作成済み（医療機器は含まれていない）。 →作成したばかり。バックアップについての規程などは定めていない。今の話題は、**バックアップ取っているが、有事の際に本当に戻せるかどうかが課題。メーカでも検証が難しい。** →大学が作成したひな形を参照して作成している。ＢＣＰとも整合性を取る形で作成。ＢＣＰの際に紙カルテ運用対応を想定して作成している。一部印刷して、準備、またはダウンロードして使えるように準備している。大学とも連携するような連絡体制を作っている。実際に事が起きれば、ＢＣＰとも連携して動くような体制を組み込んでいる。 →IT-BCPの中では部門システムについては記載はない。**部門システムのことは記載はあるが、医療機器に特化した内容は今後の課題。**
2. 医療機器のサイバーセキュリティ確保について	

病院名	D病院
1）ネットワークに接続される医療機器についてどう管理しているか？ 2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	医療情報システムに接続する機器はMACアドレス管理。 部門システムに接続する機器は、医療情報システムとはVLANを切り分け部門管理している。部門システムのリモート保守は一元管理し、医療情報システムのVPN経由でしか接続しないようにしている。 →新規接続や機器更新の際には、**部門から情報部に申請して、MACアドレスを登録しているが、実際の細かい管理は部門側で行っている。両方で管理しているのが現状。**
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	部門システムのネットワーク構成図は設置時に提出。新規案件で接続機器が増える際は、ヒアリングを行っている。医療機器のセキュリティ状態、OS、通信形式などは把握するように努めている。 →情報部で構成図をもらえるところはもらっているが、管理まではしていない。**情報部の構成図までには落とし込めておらず、各部門で管理している。** →情報部の立場としては、**部門システムは部門システムというくくりで接続して、その中のことは現場にお願いするしかない**という立場。あとは、その**境界での対応をどうするかを整理**しているようなイメージ。振る舞い検知機能を導入したいと思っているが、高価なため最初に削減されてしまう。 →ICUのシステムについては臨床工学部門でも構成図等は把握しておらず、メーカが対応している。導入する際に、情報部門では提出を求めている。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	**導入時にのみ**確認
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	**未着手** →メーカから他院での**脆弱性があったような情報提供**はあるが、**何もしていない。どうすれば良いか分からない。** 改修が入るような不具合があれば、対応するが、**脆弱性だけだと対応方法が分からない。**
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	医療情報システムの安全管理に関するガイドライン →**医療機器の手引きは知らない。** →ガイドラインを遵守するだけでも大変 →**周知を図り分かりやすい物が必要。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	機器の上流にFWを設置するなど、必要以外の通信が発生しないように徹底。
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	必要な都度、依頼することにより提供 →更新が遅れている部分も有り、メーカからＯＳのサポート終了の連絡が来ても、致し方ないということで、対応しているのが現状。メーカから、ＯＳ対応についての連絡は１年から2年前にくることが多いので、それで更新の検討をするような形で対応。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	月一回、各部門（事務含む）との調整会議を実施している。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	基本的に情報部が主体となって把握、対応している。必要に応じて調整会議メンバーに協力依頼。全体となって動く人材は情報処理安全確保支援士　１名、医療情報技師　５名（内上級１名）
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	CSIRT同様に事務部門とも連携し、医療情報部門は問題対応のみに特化できる体制が望ましい。
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	病院情報システム運用継続計画　IT-BCP「サイバーインシデント発生時の連絡体制図」に基づき対応

病院名	D病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	行っていない。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	医療機器は多種多様となるため、個々の機器把握は難しいと感挙げる。今後は通信状態の振る舞い検知などを徹底して行っていきたいと考える。
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	→接続について指示することと、ファームウェアの更新などは契約に盛り込んでいないもののお願いしている。
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	リモート接続をしている装置の場合、装置からシーメンスのリモート端末にVPNで接続いており、一般のインターネット回線とは違う系統を使っている。また、リモート時に使用しているルーターについても、セキュリティソフトを含めた最新のバージョンに定期的に更新を行い、万全を期している。基本的に装置と一般のインターネット回線とは違う系統に直接つながっている為、ウイルス感染した場合の補償などについては、想定していない。 →契約の中に書いているわけではない。
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	マルウェアに起因して、対象装置が不稼働又は動作不安定になった場合は、保守の実施可否は都度協議のうえ決定することとしている。 →ある機器では、契約に含まれている。保守の除外要件として。 →ある装置ではデータ送信するだけで、メーカサイドからの送信機能はないことから、不正アクセスなどの可能性はないとの回答。
その他意見	○現在は、医療機器メーカが接続できるようになりましたとか、ぜひ接続してくださいとか売り込んでくる事が多いが、実際話しを聞いてみると、**ＩＤとかパスワードを変えているかなど聞いてみても、業者が理解していない**ことが多い。**営業担当者ベースであるが、医療機器だからパソコンと違ってウイルス感染しない**と言うような説明を平気でしてくる。カタログ情報を見るとリナックスとか記載があり、その**リスクなどを営業ベースでは把握しておらず、不確かな情報を医療機関に伝えている。それによって、医療現場が混乱することもある。** →このような機器でも接続する場合には、VLANで切って、境界で遮断するようにして、通信許可するしかない。 ○**インフラを整備するインセンティブが必要。**評価に対してつけて、チェックする必要。 ○部門システム管理する側からすると、**専門の診療業務以外の負担が大きい。**セキュリティIT人材がいるとはいえ、管理体制の強化のためには、教育面も重要であり、人材を専従させるのも難しい。現状はなかなか難しい。ベンダーさんや情報部にお願いしているところも多い。**属人化にならないようにする必要**がある。資格などについては、個人レベルでの対応。自己学習のレベルで。医療情報技師を3名程取得しているが、人員配置までには繋がっていない。 ○**医療情報技師を雇用するにも人材がいない。IT系の人材が不足。資格とっても、自己満足のレベルになってしまう。せめて学会行けるぐらいのインセンティブが必要。**
追加情報	○県警からもサイバーセキュリティに関して一度連絡あり。情報提供は随時されている。 ○有事の際は全学とも連携して、全学の方でも対応をしてくれると想定している。現在も毎週ＷＥＢでカンファで情報交換している。 ○**病院と学術が一緒で管理されており、大学本部とも連携している。** ○**医療機器については、資産台帳とは別に医療機器の安全管理システムでシリアルNoまで管理**している。そこに入力した機器は固定資産台帳の備考にも記載して相互で管理できるようにしている。10年以上前に導入しているが、別々運用とはなっているが、相互に連携を必ずしている。臨床工学部門で管理している機器はMEで、それ以外は事務的に登録している。安い機器やどこまでを管理するかが課題。納品する際に医療機器登録票をメーカに提出依頼をしている。 ○**大型の部門システムを持つ部署については、IPアドレスを渡して、部門の方で割り振り。**放射線関係だと、保守管理用の機器台帳や配線図にIPを記録して管理しているが、見直しなどはせず。 ○一般的な接続確認しているが、その程度。仮想攻撃をテストすることはない。 ○セキュリティの問題で、更新する必要などの連絡はない。エンドオブサポートの段階で連絡がくる。OSが原因で使用期間が短くなっているような感覚はない。
	○超音波装置については、業者にお願いして調査を行った。台数、検査可能内容、プローブは管理し、更新計画、台帳管理をしている。通信しているかどうかは管理できていない。2023年10月～11月調査、報告書が12月完成 ○要望者が出た段階で、台帳をみながら更新計画に落とし込んでい区作業を事務で行っている。

病院名	E病院
病床数	約500床
施設基準：主たる基準	地域医療支援病院 救急告示病院 第二次救急指定病院・第三次救急指定病院 地域災害拠点病院指定 エイズ診療拠点病院 地域周産期母子医療センター指定 医師臨床研修指定病院 歯科医師臨床研修指定病院
従業員数：	
医師数	118名、研修医　26名
看護師数	583名
臨床工学技士数	25名
その他職種（メディカルスタッフと事務職等）	391名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	セキュリティ対策基準に体制図を明記。システム委員会の委員長、情報セキュリティ管理者として、副院長を当てている。事務局として事務部　情報システム課を置いている。**各部門（病棟も含めて）にもセキュリティ担当者を置き、本社にもセキュリティ担当者を報告している。** **本社からひな形が送られそれに沿って、各病院で、作り込んでいる。システム委員会の委員長がセキュリティ責任者となる。**病院毎でも違うが、小さい病院では兼務となっているところもある。 **サイバーセキュリティ関係の問題が生じる前から、セキュリティ対応をしている。** 規程などはガイドラインや本社のひな形を参考にして作成している。最初は平成27年10月に作成。 電子カルテの障害対応はリモート対応、修正資源配布もリモートで対応。リモート回線の集約化は今後検討課題。1ベンダー1回線で対応しており、回線契約は病院で行い、管理は業者が行う。VPNなどは病院側で管理。**MDS（「製造業者による医療情報セキュリティ開示書」）などももらうようにしている。昨年度は、保健所の監査をきっかけに集めたが、業者が提出してくれなかった。今年度は今集めているが、問題なく提出してくれている。**MDSで【いいえ】の部分を【はい】にできるように意識している。 5人で対応。セキュリティマネジメントやITPを持つ者もいるが、無資格の者もいる。5人の内、セキュリティに関しては課長をふくめて3名で対応。残り2名は運用、メンテ専従で対応している。外部委託はしておらず、内製化して対応。課長職については、数年ごとに交代することもあったが、**現員の2名は、入社してから異動したことがない。**病院長としては、**技術職だからという認識**がある。
2）ネットワーク構成図を把握しているか？	把握している。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	委託業者が作成。管理は委託業者と情報システム課で行っている。各種サーバーや無線AP、スイッチ系を管理。**市販のネットワーク監視システムを入れて、故障やループ配線などの場所も確認できるようにしている。無線APの電波到達範囲も管理。基本は日勤帯での対応。**
4）追加のシステムなどはどのように情報を入手して管理しているのか？	**新規システムの要望はシステム委員会での検討が必要**であり、情報システム課が知らないシステムが入る事はない。システムが導入される度に配線図は最新化している。契約ではなく、ネットワークの配線については、病院が把握しなければならないという前提で、各社に最新化してもらい提出してもらっている。
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	開示していない。申請があれば、IPを提供している。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	脆弱性情報はベンダーから入手し、適用作業については、相談しながら実施している。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	バックアップシステムを今年度導入予定であり、併せてIT-BCPも作成予定。本社から素案が配布されて、それを基に作成予定。夏頃にひな形連絡あり。最終ひな形はまだ。**訓練シナリオも本社から届く予定。** 単体バックアップ　バックアップBCP→市販システムを導入。 院内にNAS→ランサム用。２本立てで計画
2. 医療機器のサイバーセキュリティ確保について	

病院名	E病院
1）ネットワークに接続される医療機器についてどう管理しているか？	**各部門で機器については、管理。各部門でリスト化して管理。USBを使う場合の注意点などは情報システム課から運用ルールを周知。**
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	各部門で管理。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	各部門で管理。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	各部門で管理。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	各部門で管理。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	情報システム課では把握していない。**臨床工学課では、医療機器の手引きを把握。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	医療機器ではないが、**診断書システムの企業からは、メールでセキュアな環境でダウンロードできる形でのMDSの送付**されてくることもある。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？構築しているようであれば、その内容をご教示いただきたい。	情報システム委員会やセキュリティ担当者として、医療安全管理者や医療機器安全管理責任者が関与していないが、インシデントが発生し、患者安全にも影響を及ぼす場合には連携して対応することが想定される。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？また、その人材として必要な知識、技術、人数をご教示いただきたい。	なし
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	なし
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	なし

病院名	E病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	なし
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。（医療機器の日常的な点検で必要な項目などあれば。）	なし
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	**情報システム本体の契約の中でも、まだ盛り込まれていない。**
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	医療機器メーカより院内の医療職の方の意識が高い。職員については、イーラーニングを実施しているが、一般的な内容である。**システム導入に関して、関わる内容を毎年、導入毎に各部門の担当者に周知し続けてきた結果、セキュリティに関しても文化が醸成された。**
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	部門システムについては、情報システム課が窓口となり、経営層にも情報提供している。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	なし
その他意見	○規模が小さい医療機関では、**医療安全の部門にぶら下げる形でのサイバーセキュリティ対応**も考えられるのではないか。 ○**大きな医療機関でどこまでできるのか、理想像を把握した上で、小さい医療機関に落とし込む必要があるのではないか。** ○医療機器のサイバーセキュリティに関する情報については、**3年間など期間を決めて、メーカから医療機関へ提出させるなどのキャンペーンが必要ではないか。**それをどう活用するかについては、その後検討する必要があるのではないか。各医療機関のレベル間を見据えて検討する必要がある。 ○セキュリティの確保等も含めて、情報システムの運用・管理については、**人海戦術で対応しており、評価される部分も少ない。**各医療機関でのモチベーションを保つ意味でも、**評価する仕組みが必要ではないか。** ○**メーカから提出されるセキュリティに関する見積もりも複雑すぎて、メーカ自身が把握していない**場合もある。5年使用するような前提のシステムでも、ウイルス対策ソフトのライセンスは1年だけしか見積もっていないなど、不備があることも多い。
追加情報	○グループ病院でも各病院で対応している部分も多いが、同じグループ病院なので、電話でいろいろ相談できる体制となっている。係長研修や課長研修で全国のグループ病院の担当者と一緒になることも多く、そこで顔をつなぎ、情報収集も可能となっている。 ○他のグループ病院ではリモート回線の集約なども行っている。 ○**部門システムも含めてリスト化して管理しており、約7年間隔ぐらいで、更新計画を作成して、委員会へ答申**している。9年間隔では更新できるように検討している。毎年、**11月くらいに翌年度の更新リストと更新タイミングを検討して、更新計画をたて予算確保**をしている。電子カルテの更新に合せるか、合せないかも検討を行う。情報システム課から各現場に相談した上で、更新計画を挙げてもらっている。 ○地方病院だと、メーカ直接ではなく、卸がフォローアップすることも多い。**卸にサイバーセキュリティに関する知識がない**こともある。 ○情報システム課の方で、**導入するシステムについては、どこにどういう方式でデータが蓄積されるのかを確認して、病院側から接続方式を提案することもある。しかし、それを対応してくれるような場合は少ない。ペースメーカの遠隔モニタリングシステムを導入する際には、メーカと打ち合わせをしたうえで導入している。**
	○モバイルLTE回線でリモートを行いたいという提案があった際には、病院側からは、**専用回線を提案したが、結局受入れてもらえず、通信内容がログだけということもあり、許可**したこともある。中身を精査したうえで、対応している。

病院名	F病院
病床数	約200床
施設基準：主たる基準	保険医療機関 労災保険医療指定機関 生活保護法指定医療機関 指定自立支援医療機関
従業員数：	常勤職員210名、非常勤合せて250名
医師数	常勤　10名程度、非常勤23名（外来のみ10名）
看護師数	
臨床工学技士数	0
その他職種（メディカルスタッフと事務職等）	
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	情報システム管理者として病院長を置き、安全管理責任者が事務長、企画管理者として医事課長代理を置いている。 **管理に関するガイドラインにそって作成。各部署野帳を運用責任者としておいている。**（検査、薬局、訪問、医療相談、医師など） IT-BCPは今年の6月に作成（診療録管理体制加算の取得のため。） **パソコンなどのOS管理は一元的に管理できるサーバを導入して対応している。**情報システムのサーバーについては、各メーカにお願いして対応している。HIS系の通信やアプリについては、許可されたものだけ使える仕様となっている。現在ではPCは200台前後使用している。 ネットワークに接続する機器が少ない。各部門システムもほとんどない。リモート接続については、現時点では使用しておらず、電子カルテの業者のみ外部に接続されていない、専用回線で接続して、対応する形になっている。 将来的にも必要があれば、**既に導入されているシステムを利用することで、外部からセキュアに接続できる**と考えている。担当者は主に一人で、企業でのSE経験を経て入職。
2）ネットワーク構成図を把握しているか？	**委託業者が作成。**初期の段階からネットワーク構築に関与している業者であり、イントラネット、インターネットの接続、ネットワーク保守、ハードウェア保守、設定変更の対応などしている。 配線図は変更があるたびに、最新化している。無線LANとかの設計・施工なども対応。保守契約の中に入っている。 セキュリティパッチの最新化は機器やソフトウェアの保守として対応している。設定変更などについては、現地作業やリモートで対応し、都度支払いで対応している。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	
4）追加のシステムなどはどのように情報を入手して管理しているのか？	**申請が上がってきたら対応。**技術的なところは、**ネットワーク保守委託業者と直接システム業者で対応。**
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	していない。開示する必要がある場合にも、委託業者と相談して決定。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	脆弱性については、**委託業者やメルマガ、ウイルスバスターからの情報提供**などがあるが、**期限を決めて、パッチを当てて対応**している。テスト端末にパッチを当て、**問題がなければ、全端末に展開**している。この作業は院内の担当者が実施している。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	作成済み。**医療機器に特化した内容は入っていない。**
2. 医療機器のサイバーセキュリティ確保について	

病院名	F病院
1）ネットワークに接続される医療機器についてどう管理しているか？	ほとんど接続されていない。接続される場合には、無線ＬANなどで接続したいなど申請があれば、MACアドレスで管理している。**安全を確認したうえで許可**している。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	情報システムと同じ。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	ほとんど接続されていない。検査については、外注しており、データだけが別回線で送られてくる。送られてきたデータを運用ルールにそって、セキュリティを担保したUSBを用いて、HISに取り込んでいる。また、仮にUSB経由でウイルスが入るような場合でもOSロックの仕組みを導入しているため発症せず、**不要なアプリを使っての攻撃ができないようなシステムも導入**している。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	なし
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	なし
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	**把握していない。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	なし
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	なし
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？構築しているようであれば、その内容をご教示いただきたい。	なし
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？また、その人材として必要な知識、技術、人数をご教示いただきたい。	なし
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	なし
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	なし

病院名	F病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	なし
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	なし
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	なし
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	なし
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	医療機器に関わらず、**事務長レベルが俯瞰的に把握**している。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	なし
その他意見	○**セキュリティに関するシステムの導入は医療機関の考え方によるところが大きい。**実際的には、まだ導入されていないところが多いのではないか。この病院では、**企業側からの提案もあり、経営層レベルでもサイバーセキュリティ確保を認識したうえで導入されている。** ○**端末から感染するか、外から感染するかがほとんどであるが、それらをブロックするシステムを中心に投資**していることで、有効的な対策ができていると考えている。 ○セキュリティシステムについては、**医療機関の身の丈にあったものを導入する必要があるが、どの程度のレベルが必要かが分からない。** ○**最後の理想像だけ目標にしても、段階的に導入していかないと難しいのではないか。事業者でも提案に迷う事が多い。**規模感によってかなり変わる。 ○**医療機関の規模や特性にあったセキュリティシステムが必要ではないか。それを判断する基準がない。** ○ネットワークを開放しても、ウイルスに対して対応できるようになれば良い。全てが最新にものになっていれば安心できる。 ○**電子カルテによってはアップデートを許してくれないので、ゼロトラストの考え方が適用できない。** ○**NDR（Network Detection and Response）というツール**もあるが、なかなか、導入するのは難しいのではないか。 ○**医療機器のサイバーセキュリティ確保については、初めて知った。浸透させていくには、サイバーセキュリティ本体の対応を同様にチェックリストや監査などで対応していくしかないのではないか。** ○**医療機器側でも最新のセキュリティ対策の考え方に沿って、製品開発が必要ではないか。クラウドと接続を前提とした製品開発として、医療機器側でも認識を変える必要があるのではないか。** ○**ある一定の医療機器に特化した通信基準を作る必要もあるのではないか？または、個々の医療機器の対策と言うよりは安全な環境を作る方策を検討した方がよいのではないか？多層防御の方法も合せて検討する必要があるのではないか？**
追加情報	○当院では、20年以上前からIT化を進めてきた。精神科では多職種の情報共有が重要であることから、グループウェアの導入や電子カルテなどの導入を進めてきた結果、ネットワークの構築についても取り入れてきた経緯がある。USBの使用制限なども進めてきたが限界があり、現在は、守ることだけではなく、**内部の環境を最新化して、ウイルスから守ることを進めている。** ○段階的に導入してきたこともあり導入できている。**電子カルテがないと、若い看護師の採用ができない。** ○セキュリティ関係に費やす予算は技術レベルによって、キリがないので、**企業から提案いただくときには、松竹梅の提案をしてもらい、必要な対応について説明が付くレベルを担保できるように検討**している。ランサムウェアの対策システムも導入済み。 ○入口、出口の対策、ランサムウェア対策（設定を書き換える）もすぐに対応している。**ゼロトラストの考えや仕組を導入**している。 ○今後、**クラウド化を見据えて、新たな設備投資が不要となるように対応を進めている。** ○ネットワーク更新については、委託業者から上がってくる。**事故が起こった時に説明ができる範囲で検討**している。

病院名	G病院
病床数	約400床
施設基準：主たる基準	日本医療機能評価機構認定病院 リハビリテーション病院、一般病院2、高度・専門機能：リハビリテーション（回復期） マンモグラフィ(乳房エックス線写真）検診施設 臨床研修協力施設 下肢静脈瘤に対する血管内焼灼術の実施基準による実施施設
従業員数：	819名
医師数	91名
看護師数	293名
臨床工学技士数	10名
その他職種（メディカルスタッフと事務職等）	272名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	法人全体の責任者を理事長として、連絡協議会（法人内の情報管理）を設置。**病院の情報管理責任者は院長として、システム委員会を設置。各部門の長を委員に任命し、月1回情報システム連絡会議を開催。報告事項が中心であるが、機能追加や要望などの導入可否も判断している。** 電子カルテの更新は7年を想定しており、部門システムは別々に対応している。部門システムはハードの保守が受けられる上限期間で更新を検討している。 事務局として情報システム部門で対応、法人全体で6名、法人内9施設を病院で一括で対応している。 **病院機能評価、保健所の立入の結果、関連する規程を整備し、法人として承認している。**
2）ネットワーク構成図を把握しているか？	**業者に入ってもらって把握している。年間保守も契約している。** 拠点間ネットワークはVPN業者が入っている。**電子カルテ系で2系統引いている。インターネット系については、各市施設で1本づつ引いているが、最終的に1本化して、ファイヤーウォールを入れて管理している。** **リモートメンテなどに使用する回線が上記とは別に、各ベンダー毎にVPNを準備してもらっている。接続するルールを徹底し、バージョンアップなどは業者の責任で行ってもらっている。サービスの契約書の中で盛り込んでいる。病院として1本化はしていないが、接続回線は全て把握するようにしている。**
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	**3年前に作成。かなりの時間がかかった。**現在は業者に入ってもらって年間保守契約の中で管理している。 **外部接続が必要な場合には、情報システム課が必ず関与し、接続方式等を含めて確認して、リスト化している。**勝手に設置されないように監視を強める方法も検討中である。
4）追加のシステムなどはどのように情報を入手して管理しているのか？	**サーバーは１つのベンダーなので、対応できるが、端末となるとコントロール不能。**
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	聞いてくるメーカもない。開示していない。**接続情報の申請がくれば、IPを払い出している。**
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	JPCERTや医療セプターから入手。**部門システムベンダーからの情報はほとんどない。対応すべきものがあれば対策するが、目をつぶって使うしかないこともある。**
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	**システムダウン時のマニュアルを策定ずみ。30分以上止まるか止まらないかで紙カルテ運用にするか否かを判断基準として示している。**ダウン後の各現場での動きは各現場で対応するように示している。今年に入り、２回地域の停電があり、その経験に基づき改めてまとめなおした。停電感知でシャットダウンしてサーバー停止の際の復旧方法の確認がそのタイミングでできた。自家発電に切り替わることが前提であったが、うまく切り替わらず、シャットダウンとなった。**実際の停電を経験して、気づいたことをマニュアルに盛り込んでいる。**
2. 医療機器のサイバーセキュリティ確保について	

病院名	G病院
1）ネットワークに接続される医療機器についてどう管理しているか？	**サーバーは１つのベンダーなので、対応できるが、端末となるとコントロール不能。** **アップデートの連絡もこない。**
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	**IPの払い出しのみの管理。**ネットワーク配線図までには落としていない。ネットワーク接続する医療機器の調達には関わっている。物によっては、古い機器で自主点検の範囲で使用しているものもあるが、使用頻度も低くい場合にはレガシー機器でも許容せざる得ない。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	**ウイルス対策については、インストールできる端末であれば情報システム側で対応。**パターンファイルについても手動で移し替えている。USB接続は制限している。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	特に連絡はない。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	**知らない。読み手側が読み解けて納得の上対応できるのかも疑問。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	**データ収集はできていない。情報システムに関しては、立入検査のために対策しているが、医療機器については、できていない。**
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	ない
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	**現場からもOSが古いなどの相談はない。OSの概念がない。**
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	なし
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	なし
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	なし

病院名	G病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	なし
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	なし
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	なし
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	なし
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	**理事長からは気にかけてもらっており、理解いただいているのでシステム導入ができている。**
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	なし
その他意見	○医療機器までとなると無数にあり、どこにセキュリティホールがあるのかすらも分からない。大きな課題である。全く手つかずの状態である。 ○**メーカのサービスマンがメンテナンスのためにノートパソコンを医療機器等に接続する場合などについても対策が取られているのか？そのような責任分界点についても、契約の中に入っていない。そのような契約を結んでいる医療機関はほとんどない。** ○**医療機関の中でもとこまでが守備範囲なのかが、体制としてとられていないところが多い。**システム担当がいないところも多い。医療機器までは掌握できていない。 ○1242病院のアンケート調査でも、電子カルテの導入していない病院は10%以下であった。**中小病院でも情報システムの導入が広がっている。中小関係の病院ではシステム関係の部署もなく、今後危険な状態も危惧される。** ○オンライン資格確認システムについても、補助金で導入後1-2年でシステムに合わないから買い換えてくれとも業者から平気で言われる。国の施策だから仕方ないと。病院側は言われたら買い換えるしかない。ささいな話しであるが、業者も医療機関も素人の域をでていない。補助金で購入すると、使わなくてもしばらくは放置しておかなければならない。 ○厚労省からも五月雨式にDXに関する補助金などがでてくるので、病院側もタイミングをみている。 ○電子カルテの更新経費も高騰している。今までは1床100万程度だったが、200-300万円程度になっている。10億円以上かかっているところもある。しかし、**セキュリティには1242病院のうち2割は全く投資していない。無回答、よく分からない回答も多い。どこまでがセキュリティにかかる費用かも判断できない状況**にはあるが、**赤字がすすむにつれて、セキュリティにかかる費用は削られるのではないか。** ○**専門部署がある故に、現場からの問い合わせも多く、各部門はお客さん的に対応を迫られる。知識のアップデートも必要であるが、時間がさけない。** ○**自己評価できる指標が必要。どこまで費用をかければ良いか分からない。今までなかった仕事、新しい対策として、どう評価するかが課題。** ○**資格に対して報酬をあげることができないので、細かく言及することができない。評価する仕組みがなく、資格を取っても変わらないので、モチベーションを上げる仕組みが必要である。各法人の努力の範囲で対応している。施設維持する人員として確保するようにしないと各医療機関のレベルはあがらない。** ○**モニタリングシステムにしろ、次世代型のウイルス対策にしても費用が高額。ウイルス対策だけで言うと固定費となるが、以前は年間で1台1000円のところ、現在は10倍以上。抱え込むにも限度がある。**
追加情報	○**今年度ネットワークセキュリティ対策として、ダークトレースを導入。ネットワーク情報をモニタリングして、AIが危険性を判断してアラートを出してくれるようなシステム。**デバイス1台あたり年間5000円程度から利用可能で、ネットワークスイッチ配下に置いてモニタリング。IP管理ベースで対応。ランサムウェアの被害が他病院であり、その対策として導入。3ヶ月ほどテスト運用して導入した。NDR（Network Detection and Response）。**EDRについては、端末にインストールするタイプなので、医療機器には対応できない。NDRはデバイスに依存しない。**検知・報告の未導入。上位オプションとして、自動遮断できるような機能もある。24時間運用も可能。端末毎遮断できる。リモートデスクトップ接続などの検知も可能。導入から半年であるが、危険なものは検知されていないが、普段使っていない端末からのアクセスなどがチェック・確認できるようになった。人の手だけでやるのは無理がある。メール、スマホで確認可能。それを契機に管理画面で確認している。電子カルテ系については、リモートデスクトップの作業程度の報告であるが、インターネット側の端末については結構なイベント報告がある。岡山の病院で導入していたので検討した。怪しい動きがあれば、部門担当者に連絡して協働で対応している。 ○**大阪の私立病院の情報連携あり。**月1回IT部会あり。事務長会の下部組織として。大阪のみの取組み。京都でも同じような取組みあり。大阪と京都で交流できないか相談中。IT部会でもNDRの導入病院はまだ少ない。テストを始めた病院もある。 ○**法人内の勉強会という形でセキュリティの勉強会をした。個人情報の保護は医療安全の範囲で対応しているが、セキュリティについては、現状難しい。勉強会をしても、我々の守備範囲ではないという意見もある。** ○**セキュリティを担当する人を増やすことが難しい。財政的にも人材的にも。採用できるチャンスが巡ってきた時には、ITリテラシーを確認した上で採用している。単価が見合わないので採用できないこともある。**

病院名	H病院
病床数	グループ全体で6000床以上
施設基準：主たる基準	グループ病院で違いあり
従業員数：	グループ全体で30000名以上（常勤）
医師数	
看護師数	
臨床工学技士数	
その他職種（メディカルスタッフと事務職等）	
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	**SE45名以上が本部に在籍**し、本部所属で各病院へ派遣している。一人やめても穴埋めができるように3年前くらいからチーム体制を取っている。システム開発、データセンター事業（中央で部門システムのサーバを管理）、PC・機器レンタルサービス（仕入れ、設定、設置までサービス提供）、病院支援常駐サービス（SE35名は病院常駐）一人3病院ぐらいを担当。情報機器貸し出し実績　5000台以上。セキュリティ対策については、ランサム対策などを導入。センターサーバ方式への切替、センター側でランサムウェア等のサイバー対応に関してサーバに導入。すべてを拒否して例外で許可する。オフラインバックアップについては、単独の病院だと2500万円ぐらいするので、中央化してサーバに導入。18病院分のバックアップを実施（オフライン） **放射線機器を導入する場合いは企画の段階から診療放線技師が関与。臨床工学については、立ち上がったばかりで現在対応中。システム関係は情報システムで対応している。** 病院個々でセキュリティ対策をするというよりは、**本部から下ろす形で対応。** 定例で毎月部会を開催。ガイドライン検討部会やＢＣＰ、**ネットワーク全体を医療機器含めたＢＣＰの策定を企画中。**部内で検討し、事務長会などで発信。反対意見に対しては本部を悪者として、本部主導で対応してもらう。 **今まではネットワークに接続される医療機器については、部門任せになっていたところもあるが、今後は情報システムの方に集約する形で検討を開始**したところである。**ネットワーク構成図なども、放射線機器メーカが作成し、部門で保管しているものの、情報システムとは共有されていない状況にあったが、それを情報システムにも集約化する方向で検討**している。 情報システム安全管理責任者：情報システム課長、医療機器安全管理責任者：臨床工学科長
2）ネットワーク構成図を把握しているか？	情報システム課が主幹で管理している。完成図書として、メーカが作成して、情報システム課へ納品してもらっている。末端の細かいところは病院で作成しているが、ネットワークの大元に関しては、保守契約を結んで対応している。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	情報システム課
4）追加のシステムなどはどのように情報を入手して管理しているのか？	**導入企画段階で情シスが関与しており、導入確定したものもすべて把握できるフローになっている。価格交渉や接続方式を確認した後に導入。** 接続する際には情報システム課に連絡が来るようになっている。30万円以上のシステムは連絡がくる。年度末などでは駆け込みの連絡も多い。関連病院も含めて、全ての調達情報が情シスに集約。システムで管理しており、５年前から運用。申請、決済　管理、もシステムで対応している。内製で作成。**価格や機能によっては、メーカ差替えなども提案している。**
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	これまで事例がない。**出すことがリスク。**
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	厚労省HP、ベンダーからの情報提供 IPAからのメーリングリストからの情報。警察などからも情報がある。 ベンダーからはほとんどない。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	作成している。**医療機器は含まれていない。リスト化と連絡体制を取りまとめる予定。**夜間常駐していないところについての小さい病院での対応が課題。 ソフトウェアサービスのシステムについては、リモートで接続。電子カルテはベンダー毎でリモートでも対応できるようになっている。
2. 医療機器のサイバーセキュリティ確保について	

病院名	H病院
1）ネットワークに接続される医療機器についてどう管理しているか？	各部門で医療機器安全管理責任者の責任の基、台帳管理（管理システムをエクセル等で管理）を行っている。　今後情シスで集中管理をするべく議論している。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	各ベンダーより情シスに依頼し主幹部署が得て、情シス管理の台帳に反映するように依頼している。 ＩＰを払い出しているのみで実際何が接続されているかのフィードバックが今後の課題。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	部門システムまでは反映されているが、末端の機器までは盛り込めていないのが実情。現状できていないがIPやゲートウェイ情報はもちろんのこと、通信で使用するサービスポートなどは把握すべきと思う。今はそこができていない。変更の際にも連絡が来るようになっているが、知らないところで増えているような不安もある。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	アプリケーションの動作保証の問題もあり、OSのバージョンアップはできていないのが実情、ウイルスソフトは導入しているものもあるが、パターンファイルが更新されているか把握できていない。透析管理システムはウイルス対策は未導入、単独LANの可能性あり。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	各メーカに情報収集、対応を委ねているのが実情。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	医療除法システム安全ガイドラインを参考にしている。 医療機器については、知らない。あるのであれば、一緒の方が分かりやすい。
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	医療情報と同様、取り始めているところである。取得したものは内容を確認して問題ないことを確認している。 作り方についても？な部分もあり、どうすれば良いかもどうつかえが良いか不明。ＳＢＯＭの部品表から脆弱性が分かると良いが、第三者がやってくれる方が良い。業者も出してくれるところとだしてくれないところもある。出してくれても本当に正しいのかも疑問。
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	業者も出してくれるところとだしてくれないところもある。出してくれても本当に正しいのかも疑問。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？構築しているようであれば、その内容をご教示いただきたい。	医療情報とのどうようの流れで、MDS/SBOMは専門知識の高い情シスにもチェックしてもらい、 問題点がないかを確認するフローを構築している最中である。課題があれば、委員会に挙げたり、関連部門と協働で対応する。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？また、その人材として必要な知識、技術、人数をご教示いただきたい。	情報システム課が主体で動き、情報も情シスに全て集約化、課題となるポイントは安全管理責任者、委員会にも共有するながれ。リスク分析ができ、対策案を検討できる人材が必要と考えられるが判断に迷う際は、法人本部の医療情報部門とにも連携しながら、随時検討している状況。知識、技術という点では情報システムと同じ観点で良いと考えられるため、兼務で良いのではないかと考える。報酬で点数をつけて兼務が現実的。
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	配置したいところであるが、人が来てくれない。他分野に流れてしまう。医療資格を持っている経験者でITやっていきたい人や、子育て世代のお母さんなどを採用している。リモート環境も考えたが、現地へいかないと難しい。
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	原則、IT-BCPで策定した流れに準じて対応する流れで考えている。最終的にはメーカなので、いかに情報伝達を早くできるか？課題。電子カルテは止まっても診療を継続できる場合もあるが、医療機器については、診療を止めなければいけないのが大きな違い。

病院名	H病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	実施に至っていない。情報システムについては実施しているが、**医療機器についてはできていない。**
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	**機器の導入時にリスクを評価することが大前提**で、リスクのあるものないものに分類し、ネットワークに接続され、汎用OSソフトが導入されているものがある場合には、情報システムと同様、侵入経路の確認やウイルス検知ログの点検が必要。また、**保守回路系については、最新のファームウェアが提供されているのか確認などができることが望ましいのではないか。**
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	盛り込んでいない、**メーカ側もどこまでが対応範囲かが明確にできていないところではないか。**
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	なし
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	**本部のトップはセキュリティについては理解があるが、予算の確保は別の話しとなっている。トップが納得できる内容を提案はしているが、自院がどれくらいまできているかわからない。分かりやすい指標で評価できると良い。**
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	サイバーセキュリティ確保に特化した条文は特段設けていない。**責任範囲などが不明確な中、また、影響範囲をどこまでに設定するかなど、定義が難しい部分**ではないかと考えている。
その他意見	○**サイバーセキュリティに関して契約として書き込むと費用に跳ね返ってくるので、曖昧の中で紳士協定として対応**しているのがほとんどではないか。**責任分解を話しても平行線となり、押し付け合い**となってしまう。 ○**IPやゲートウェイ情報はもちろんのこと、通信で使用するサービスポートなどは把握すべきと思う。** ○**医療機器に関するサイバーセキュリティの手引きがあるのであれば、安全管理ガイドラインと一緒になっていた方が分かりやすい。分かりやすく伝える工夫が必要。** ○**ＳＢＯＭの部品表から脆弱性が分かると良いが、第三者がやってくれる方が良い。** ○**病院として、可能な範囲で業者とも協力して守り合うことが重要。** ○**医療機器メーカがガイドライン準拠しているといっても信頼性が薄い。どのようにチェックすれば良いか分からない。医療機器を接続したときにも信頼性が担保できないことも多く、閉域で対応できるところは閉域で対応している。** ○**専門部署があれば良いが、専門家がいないと対策についての判断も難しい。収入にもならない対策なので、点数をつけてもらわないと成り立たなくなる。ＤＸを進めても、セキュリティができていないのが課題。** ○**インフラを更新しても診療報酬が手厚くなるわけでもなく、物価も高騰し、保守費も高騰している。人口減少に入る中、どこに集約すべきかを検討する必要がある。**
追加情報	○**取引先500社前後に医療機器等の接続に関して、独自調査を実施。他院で被害の実例が起こったことをきっかけに実施。**侵入経路をつぶすため。医療機器の中身については、何もできないので、業者が責任を持ってもらうとして、侵入経路を確認するために調査。侵入経路となりうるネットワークの構成確認を医療情報システム・医療機器問わずグループと取引のある協力会社　約500社に対して脆弱性、調査接続方法、セキュリティ方式、暗号化方式などを調査。検査機器、放射線モダリティも含めて調査。 →**インターネット経由での接続が多く、国内業者については、別方法での接続で対応してもらった。国外事業者については、一部許容している。** ○**ウイルス対策については、医療機器については対策できていない。課題である。医療機器は薬機法で手出しができないのが実情。** ○**ランサムウェア対策についてもほとんどできていなかった。** アンケート結果については、グループないの医療の質向上委員会で企画を立てて発表。事務長会でも報告し、インターネット経由から閉域ネットワークにした際の費用捻出についても説得してきた。 ○**端末についてはウイルス感染しても、バックアップ機器で何とか対応できるが、医療機器については難しい。** ○**サイバーセキュリティのみならず、経営、運営は本部主体で各病院へ一本化**している。 ○診療情報や機能に対しては医療の質向上委員会で各部門の長、医療情報代表者が決定→**グループの答えとして、それに従うようなガバナンス体制となっている。決定したルールは守らせる。守っているかどうかは各病院の部門が後追い調査を実施し担保している。本部機能が充実し、本部が掌握している。病院の診療機能毎にレベル分けはしておらず、統一基準で対応している。**

病院名	I病院
病床数	約300床
施設基準：主たる基準	急性期一般入院料4 療養病棟入院基本料1 救急医療管理加算 診療録管理体制加算1
従業員数：	541名
医師数	32名
看護師数	看護師　219名（助産師　12名、看護師173名、准看護師34名）
臨床工学技士数	11名（ME5名、透析6名）
その他職種（メディカルスタッフと事務職等）	290名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	医療情報システム管理者　他２名、医療機器安全管理責任者（臨床工学技士）、放射線科技師長 **情報システムの管理は合計3人で対応**している。**部門系システムについては、書式があり、作業依頼の連絡が来た際に、確認した上で、ネットワークへの接続などを許可**している。**接続の影響度も確認した上で許可**している。 セキュリティ対策として現在は、松竹梅の梅と理事長には話しており、**松までは計画をたてて実施することで話し**をしている。**元SEが配置されたことで、改革**が進んでいる。 **リモートメンテナンスなどで、勝手に接続されることはない。**リモート端末接続用に3台準備して、ポートのID、パスワードを与えて、対応している。入ってくるところで防御している。**セキュリティ単独では難しく、更新などのタイミングで実施**している。**サイバーセキュリティの責任分界点までは入札仕様書の中にいれていない。**意識すれば良かったが、そこまではできていない。**保守にも盛り込めていない。**
2）ネットワーク構成図を把握しているか？	はい ただし、**細かいところまでは把握できていない。細かいところは記憶などで対応しているが、メインの部分については、大まかな状態を管理している。**中央棟は10年ほど前にその段階で配線図を業者の方が作成している。その他、４病棟　西、南、東などがあるが、フロアスイッチ配置されていないことから、はっきりとした配線図はなし。概要的な配線の資料はある。配下までの細かいものはない。記憶などで対応。ネットワーク保守については、**保守契約を結んで外注していたが、設置機器の脆弱性対応やバージョンアップに関しての情報提供がなく、トラブルがあった**ので、違うベンダーに変更して、現在はアップデートできるような体制となっている。（自動アップデートでなく、確認後、手動アップデートする体制。）
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	ベンダーが作成、室＋ベンダーで運営
4）追加のシステムなどはどのように情報を入手して管理しているのか？	各ベンダーからシステム導入時
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	していない
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	IPA、またはベンダーから。 **対応する場合には、限定的な端末で評価して、運用上問題ないことを確認したうえで、修正モジュールを端末に配信するようにしている。**
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	はい 医療機器に関しては、外部アクセスのネットワークに接続していないので表現していない。 **バックアップデータがあれば、何とか復旧が可能なので、通信ポートを1方向として、バックアップデータを保持できるようにバックアップシステムを構築**している。 訓練シナリオなども作成して、訓練計画を策定している。メールのセキュリティ訓練も実施している。
2. 医療機器のサイバーセキュリティ確保について	

病院名	I病院
1）ネットワークに接続される医療機器についてどう管理しているか？	室＋ベンダーで運営 システム運用は室となるが、物理的な機器の管理は各部門で対応 導入の際に連絡がこなかったこともあり、購入した後に連絡がきたこともあるが、**現在では、指導的に対応していることもあり、接続する際には連絡がくることがおおよそ徹底**されている。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	各ベンダーからシステム導入時
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	室からIPアドレスを払い出している。 **事務端末はHISとは別系統とはなっているが、セキュリティレベルが低く、接続端末についても把握しきれていない。**
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	ベンダーに任せているが行っていない。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	臨床工学技士会の安全情報や機器メーカ（ベンダー）からの通達
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	特になし。IPA
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	なし
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	ME、放射線部では該当なし。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	ME、放射線部では該当なし。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	ME、放射線部では該当なし。 情報システムも含めてセキュリティ確保のためには、**人数ではなく個々のスキルが重要**である。しかし、**病院の給料では待遇が合わず採用が難しい**。**事務職の給与体系の延長であるため、スキルが高くなったら、給与が増えるような仕組み**が必要である。
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	ME、放射線部では該当なし。
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	障害が発生した場合は、室へ連絡。

病院名	I病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	ME、放射線部では該当なし。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	日常点検表はあるが、サイバーセキュリティに関しては行っていません。
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	販売メーカ書式の売買契約書内には盛り込まれておりません。
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	販売メーカのサービスと保守契約を締結していますが、サイバーセキュリティ連携の項目はない。
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	ME、放射線部では該当なし。情報システムについては、共有している。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	サイバーセキュリティ連携の項目はない。
その他意見	○毎日のようにいろいろな情報が流れてくるが、**インターネット関係の人達は相手が同じレベルで受け取っていると思っているが、現場では受け取れていない。**拒否反応を示す職員も多い。**厚労省では通知などは出すものの、実際の現場まではとどいておらず、単なるアリバイ作りをしているのでは？** ○当院にはSEのスペシャリストがいるが、そのような**人材を配置している医療機関はない。IT業界の給与を考えると病院には来てくれない。** ○MEの教育レベルを上げて、**上級の人がサイバーを含めてできるようにするような職種の教育体制を強化することも必要ではないか。学生の時からの意識付けも重要である。セキュリティ対策の職種として担うのはMEではないか。** ○**以前は電子カルテにトラブルがあっても紙運用もできた**が、**現在は複雑になり、サイバー攻撃などで停止した場合には被害が大きい。** ○**病院側で全て対応するのは難しい。供給側で何とか対応してもらい、かかる費用について補助金などの対応も必要。** ○**ベンダーは言えば情報を出すが、言われなければ情報は出さない。情報が流れてくればベンダーに確認できるが、IPAの情報があってもそれが、自分の病院に関係するか理解できない病院が多いのではないか。ベンダーがイニシアティブを持って対応しないと解決しない。** ○**通信内容をパケットレベルで中身を解析して、モニタリングするような製品も販売されている。そのようなものを政府主導で導入して院内の設備を可視化できると分かりやすい。**どこからどう攻撃されるかも実態がわからない。**セキュリティがない状態で走っているのが危険。** ○**セキュリティ関係は投資しても売り上げにはつながらないため、費用補填の仕組みが必要。** ○**人材がいないなかでどうやって守り合うかが重要。**病院の担当者と話していてもSEレベルの話しについては、ついてこれないことも多い。 ○**サイバーセキュリティ確保に関する業者との責任分界点については、国のガイドラインなどでサンプル案を示して欲しい。この仕様を記載できるスキルがある職員がいないことが多い**ので、そのほうが対応しやすい。**病院側に不利益とならないように病院側が主体で作成**して、広めて行く必要がある。セキュリティに関しては、**底上げだけでなく、上層部を教育するような仕組み**も必要。
追加情報	○他病院との情報交換はとくにない。**今までの経験をふまえて提案**している。検討する委員会もない。 ○担当責任者は4年前に着任し、ベンダーの技術者から病院職員となった。 ○関連法人全体の管理を室で対応している。看護学校などについても、病院とは直接的にネットワークには接続されていないが、管理・設計をしている。

病院名	J 病院
病床数	約200床
施設基準：主たる基準	二次救急病院
従業員数：	521名
医師数	49名
看護師数	203名
臨床工学技士数	5名
その他職種（メディカルスタッフと事務職等）	264名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	病院長を責任者として、**システム安全管理責任者として、室長が対応。室長が委託業者やベンダー等のチャンネルを持っていて、やりとりしながら対応している。各部門毎に部門の責任者がシステム担当者**として管理体制図に入っている。**室長含めて、6名でシステム管理を対応。**グループ組織の方はグループの方で専従者が配置されている。ネットワークについては、兼務で対応している部分もある。情シスがもともとあって、ネットワーク周りを管理していた。その後、スマホ導入の際に、DX推進室が設置され、現在はDX推進室と情シスが一体となって動いている。 その都度ガイドラインを遵守しているかどうか確認し、ベンダーとも相談して作っている。費用対効果をみながらセキュリティレベルをどこまで導入するかを検討している。その後、サイバーセキュリティの通知が出たので、情報管理の体制だけでなく、セキュリティ関係の体制を構築。 **セキュリティに関しては各社に支援いただき、相談しながら、コスト的にはも実務的にも運用できるレベルで進めている。**部門システムとしては、PACSやエコー画像、動画サーバ、同意書スキャン、薬袋発行システム、生理検査系（心電計）、内視鏡など。院内LANの更新（3年前）の際に、ネットワーク監視を導入。変な動きがあれば、シスログが飛んでくる仕組み。振る舞い検知やEDRまでは入っていない。**何千万円のオーダとなるので、簡単には導入できない。** **情報系の担当6人については、スマホ導入の際に増員され、その後も増員してもらっている。IT知識が豊富な人ではなく、パソコン好きな人を集めて、教育しながら育成している。魅力もなく、給与も高くないので、なかなか集まらない。放射線技師や臨床工学技士も興味を示してくれない。仕事が増えても給与は上がらない。**
2）ネットワーク構成図を把握しているか？	**スマホ導入の課程の中で、セキュリティも含めて最適と考えられる構成**を構築した。 リモート回線接続については、以前は各ベンダーの責任で接続していたが、**新規は病院側がVPNアカウントを払い出して対応。**管理も病院側であるが、以前から接続がある回線は、ランサムの被害が他院であった後、調査してベンダーにしっかりとした管理をお願いしている。**調査に3ヶ月くらいかかったが、知らない間に接続されている回線もあった。**現在は新規接続は申請がある仕組みとなっている。**医療機器メーカにも確認した。**
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	委託業者
4）追加のシステムなどはどのように情報を入手して管理しているのか？	購買より情シスへ連絡あり
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	必要な場合のみ提供
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	ベンダーより連絡あり
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	作成中 厚労省のテンプレートを参考にしながら進めている。
2. 医療機器のサイバーセキュリティ確保について	

病院名	J 病院
1）ネットワークに接続される医療機器についてどう管理しているか？	機器の管理は各部署。購買課→情シスに連絡があり、**IPアドレスを払い出し**。最近はベンダーの方からウイルス対策をどうするかなどの相談も多い。どちらが準備するとか。ベンダーがなんでも良いスタンスであれば、病院側指定のウイルス対策を推奨している。**ワークフローで購入申請が回ってきて、リストとして追加しているが、除却までは管理できていない。同じIPを使い回している可能性**はある。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	各部署管理
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	**IPをまとめて渡して対応してもらっている。細かいところまでは把握できない。** **医療機器メーカが持ち込んだ閉鎖系のネットワークもあり、なかなか見えない。モニタ関係は閉鎖系で各ベンダーが責任を持って対応している。スマホなどで院外から生体情報を確認できることが有用であるが、実際的にはモニタからの情報はネットには出してくれない。**
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	ベンダーマター 部門にはそのような認識はない。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	ベンダーマター 部門にはそのような認識はない。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	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について（令和５年３月31日） 手引き書については、**MEから情報提供があったが、ひも解いて情報展開できていない。読んでもできる人がいない。MEが手をつけてくれるとありがたい。現員では対応できない。しかし、MEも自分ところしか見えていないので、ME、検査、放射線、医療機器などという形で取り纏めないと進まない。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	**SBOMを読み取れる人が医療機関にはいない。納品時にSBOMを見た記憶はあるが、特になにもしていない。提供されていない可能性もある。** **MDSの提出を求めているが、システムベンダーからは提出されるが、医療機器については、提出してくれない。検討中が多い。メーカから連絡があれば、対応するが、最初のアクションの連絡が来ていない。**
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	**医療機器メーカから連絡はない。システムベンダーからは連絡があるが、医療機器は連絡はない。古い機器については、接続するなとも言えず、更新時に対応するしかない。**
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	**医療安全とはリンクしていない。システムの安全確保だけで手一杯。**個別に各部門と案件ごとにやりとりしている。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？ （院内の連携体制なども含めて）	**資産の見える化が言われているが、IPの管理までが限界。それ以下の詳細まで管理するのが難しい。情報機器の資産管理が課題であり、継続して行うことが難しい。日常的な運用だけでも難しい。**
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？ （周知も含め、シナリオがあればご恵与願いたい）	

病院名	J 病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	保守契約までは対応てきていない。
その他意見	○**リスクはゼロにはできないが、成果が明確でなく費用対効果が見えない**ので、なかなかスマホ導入などを進めるのが難しいところがある。 ○地元の業者だとネットワーク1つとっても、**VLANの意味も分からず話していることもあり、業者のリテラシーも千差万別。** ○事務職だけでは対応できないので、**支援してもらえるような仕組みが必要**。 ○**セキュリティの要求が上がってきている。MDRは導入しているが、EDRを導入するとなるとコストがかかる。将来的には診療データに価値を創出して、その収入でセキュリティ費用を担保するような仕組みも必要。** ○所属団体などで、**ボリュームディスカウントできると良い。機構では商材の一括購入を行っており、ウイルス対策ソフトなどもそこから購入**している。EDRも現在交渉中。 ○**セキュリティを担当する人材の評価**が必要。 ○**医療情報技師の知識はベースとしてあった方が良い。ベース知識を持った人が対話型の生成AIなどで指導してもらって解決ができるような仕組みが必要。人材育成は難しい。** ○**昔は情シスがトラブルの切り分けをしていたが、スキルがなくなってきている。**今はベンダーにお願いしているのが現状であり、情報システム自体、**自前で対応することが難しくなってきている。**電カルベンダーがネットワークの切り分けなどを行っている。 ○**セキュリティ対策をやっていることを評価してくれるような仕組みがないと、なかなか進まない。**動機付けが必要。診療報酬での誘導など。**必要だからやってくれだと対応が進まない。セキュリティ対策のゴールが見えない。他院との差が見えない。コストをクリアしないと新たなシステムが導入できない。経営者にも伝えられない。** ○**サーベイは受けなければならない。立ち位置評価のためにも。第三者評価があると病院は助かる。そうしないと、DXするにもベンダーも一歩踏み出せない。守りに入る。病院側にたって、伴走してくれるような組織が必要。監査ではなく、助言が必要。**
追加情報	○麻酔システムとして外資系業者が入っているが、システムに関する情報開示などはしてくれている。救急系は入っていない。 ○機構にシステム部会があり、半年に1回オンラインでの勉強会があり、ベンダーからのプレゼンなどで情報収集している。

病院名	K病院
病床数	約200床
施設基準：主たる基準	
従業員数：	
医師数	常勤10名、非常勤35名
看護師数	常勤65名、非常勤12名
臨床工学技士数	1名
その他職種（メディカルスタッフと事務職等）	常勤56名、非常勤12名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	システム委員会と電子カルテの運用を検討する委員会がある。 システム委員会→委員長は統括課長（事務）、ハード系が主。サイバーセキュリティ担当者が主に参加　ほとんど事務系で構成。セキュリティ関係も含む 電子カルテ委員会→委員長は病院長　医師、事務、外来師長で構成　運用面がメイン 双方8名づつの委員構成で、月1会程度開催。 電子カルテシステムは保守契約をしている、ハード系は業者と保守契約。セキュリティ関係の話はない。定期アップデートについては、セキュリティよりは利便性向上のため。 セキュリティパッチについては、新規導入の際に対応する程度。 **担当者は臨床工学技士として5年前に採用され、高校が情報系ということもあり、セキュリティ関係の業務を併任している。** 周知が必要な情報については、システム委員会で共有して回覧や月1回の院回会議（常勤医師全員とそれぞれの代表が集まる会議）で周知。 UTM（Unified Threat Management）を設置し、設定は担当者が自前で行っている。
2）ネットワーク構成図を把握しているか？	**電設係やそれぞれのメーカが作成。それを集めて把握**している。絶対に提出されるような仕組みではないが、ネットワーク接続の会話の中で収集している。 リモートメンテについては、回線は病院側で準備して、ルータの設定管理などは業者にお願いしている。過去には勝手に接続していたこともあるが、担当者が5年前に赴任した以降は病院側で管理している。不明な接続回線もあるが、それは目をつぶっている状態。ルータは6台程度。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	**それぞれが作成した物を担当者が収集して把握**
4）追加のシステムなどはどのように情報を入手して管理しているのか？	ネットワーク接続する際の会話の中で収集
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	なし
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	**ネットの情報やベンダーからの情報。関係があれば対応するが、安定性をみて対応。テストした後、安定性が保てない場合には対応できない。**業者から持ち込まれる事例はないが、セキュリティパッチを当てるような事例が発生した場合には、CDから病院側で対応するか、業者に来院してもらって対応することを想定している。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	作成中。システム委員会で事務的なたたき台を作成してもらった後、担当者が手を加える予定。
2. 医療機器のサイバーセキュリティ確保について	

病院名	K病院
1）ネットワークに接続される医療機器についてどう管理しているか？	**パソコンについては、OSを10に切り替え、11に切り替えられるものは変えている。**相互互換性がなく、不便だったため切り替えを行い、システム委員会で管理している。勝手に接続できないようになっている。ベンダー側でも把握していないことが多く、病院側で管理している。外部ネットワークに直接接続されている医療機器等は2-3台、遠隔診療用の機器。閉鎖回線には200-300台接続されている。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	**管理というより知っている程度。**管理まではできていない。ログは取っている。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	**メーカ任せ。こちら側は触れない。メーカ側が言ってくれれば対応する。**
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	**ハードに関する脆弱性を知っていても、動かなくなることが怖いので、何もできない。メーカ検証の上であれば、対応はできる。**
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	ない。**あったとしても誰が理解できるかが不明**。**院内教育用の資材**もほしい。
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	**最近、輸液ポンプをWiFiにつないだが、メーカからは特にそのような情報はなかった。保守点検のデータ抽出で利用している。今回のヒアリングで初めてそのような情報があることを知った。**
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	**ない。**
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？構築しているようであれば、その内容をご教示いただきたい。	**医療機器安全管理責任者がサイバーセキュリティ担当者を兼ねている**ので、連携をしているといえばしている。ネットワークに接続する医療機器は現在は少ないが、クラウドに移行した場合には多くなると想定される。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？また、その人材として必要な知識、技術、人数をご教示いただきたい。	**サイバーセキュリティ担当者１名。詳しく知っているというよりは、高校で情報関係を卒業したレベル。**
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	**各部門に一人は欲しい。事務が幹線のネットワークを把握してくれるのが理想。**
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	システム委員会で連絡網の作成などを整備予定。**医療機器に特化する場合には、パターンが多すぎて、マニュアル化できない**ことに悩んでいる。

病院名	K病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	在宅での医療機器はない。**患者への説明が必要な場合には、オンライン診療のシステムを流用して行うことを想定**している。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	**UTM、ディフェンスルータの設置、セキュリティソフトの導入。MDRも導入したいができていない。** **医療機器にネットワーク接続ケーブルが何本刺さっているか把握が必要。ITパスポート程度の用語の理解が必要。**
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	なし
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	なし
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	**している。システム委員長に報告し、連絡窓口、周知を行う。レポート対応などが必要であればシステム委員長が対応。現場のトップとして統括する立場であるが、専門的な知識があるわけではない。医事課を纏めている方が担当している。その後、事務部長→院長→理事長へ情報があがっていく。**
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	ない
その他意見	○**医療版ISACも整理されておらず、予算もバラバラ。予算が分散化されてばらまいているので、各医療機関レベルになると数万円程度にしかならない。慢性期病院でも赤字が拡大しているので、サイバーセキュリティまでの予算が確保できない。情報システムも1床250万円の世界が、400万円以上となり、立ちゆかない。病院が1つの空間の中で公的に守ってもらえるような仕組みが良い。** ○**勉強資材として、病院事務系のセキュリティ関係のものがあると良い。**
追加情報	○**セキュリティ関係で他院とのつながりはない。**新規導入する際に声をかけるぐらい。 ○臨床工学技士としては、呼吸器18台、輸液ポンプや麻酔器の日常点検などを実施。**臨床工学技士として採用された移行、徐々に情報系の仕事が増えていき、3：7で情報系の仕事が多くなっている。**コロナきっかけやランサム被害が増えてきたこともあり、情報系の仕事が増えている。診療放射線技師は関わっていない。 ○**自前でやっているので安くすんでいる。後任として、事務の人員を育成しているが、後任の確保が課題。情報交換する先もない。**