別紙 4

12 医療機関へのヒアリングシート

基本情報（病床数、施設基準、従業員数）

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）
   2）ネットワーク構成図の把握
   3）ネットワーク構成図は誰が作成して、誰が管理
   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か
   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）
   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
   7）IT-BCPを作成しているか
   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？

2. 医療機器のサイバーセキュリティ確保について
   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）をとっているか
   （医療情報システムとの違いがあるか）
   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
   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
   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
   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
   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、構築している場合は、その内容について
   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、人数はどうか
   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、人材配置はどう考えるか
   （院内の連携体制なども含めて）

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しているか（周知も含め、シナリオはあるか、提供可能か）

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、行っている場合は、その内容

14）医療機器のサイバーセキュリティ確保について、重要なポイントは何か（医療機器の日常的な点検で必要な項目など）

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。 盛り込んでいる場合は、その内容

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、している場合の具体的連携

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。していている場合は、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、契約書は提供可能か