令和７年度医療機器等基準評価検討部会
～医療機器のサイバーセキュリティ対策への理解促進に向けた検討～

資料４－２

１．背景

○　コンピューターシステムやネットワークに対する攻撃は、業種を問わず、その対象となっており、実際にサイバー攻撃を受けた医療機関のインシデント調査報告書において、医療機器に関する問題点が指摘されている。
- 医療機関は閉域網の中にあるので安全だという誤解があった
- 既にサポートが切れた OS の利用なども確認された
- リモートメンテナンスに対する対策の未実施　等

○　また、厚生労働科学研究※１で、医療機器製造販売業者のサイバーセキュリティ対策の理解不足と遅れも報告されている。

○　医療機器が備えるべき品質、有効性及び安全性に係る基本的要件の基準※２が令和５年４月に改正され、制度としてもサイバーセキュリティへの対応が求められている。

※１　令和６年度　医療機関における医療機器のサイバーセキュリティの確保等のために必要な取組の研究

※２　医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第 41 条第 3 項の規定により厚生労働大臣が定める医療機器の基準（平成 17 年厚生労働省告示第 122 号）

医療機器におけるサイバーセキュリティ対策が急務

２．令和７年度及び令和８年度の取組み

令和７年度の取組み

○　検討に先立ち、医療機器のサイバーセキュリティの専門家を招き、現状や課題について意見交換を行った。
- 製造販売業者からの情報提供が不十分
- 医療機器の保守・メンテナンス時のセキュリティ対策の重要性　等

○　府内医療機器製造販売業者（約 360 件）における対応状況の把握を目的としたアンケート調査をオンラインシステムで令和８年２月から３月にかけて実施。

令和８年度の取組み（予定）

○　アンケート結果を取りまとめ、課題や問題点、取組み事例等を整理する。

○　これを踏まえ、サイバーセキュリティの理解を深め、対策の参考となる資料等を作成し、周知する。

３．医療機器のサイバーセキュリティに関するアンケートの概要について

○　インシデント調査報告書や本部会での検討を踏まえ、製造販売業者に特に確認いただきたい事項を抽出し、アンケートを作成した。
- 設計段階における、セキュリティ対策の実施
- 脆弱性等に関するアドバイザリー情報の提供
- 医療機器の保守・メンテナンスに使用する機材におけるサイバーセキュリティ対策　等

なお、アンケート回答後も項目が確認できるように、質問票を郵送にて送付する。

○　全 41 問で構成しており、主な内容は以下のとおり。
また、対象製品の製造販売がない事業者にもサイバーセキュリティ対策を意識付けるため、医療機器の販売・受注システムにまで内容を広げた。
- 基礎情報（業態や医療機器の取扱い状況等）
- サイバーセキュリティに関する対応状況（製品自体の対策、顧客等との連携、教育訓練や記録の状況等）
- 販売・受注システムへの対策状況

【アンケート項目の例】

問１：脆弱性等に関するアドバイザリー情報を顧客（医療機関等）に提供していますか。
- はい
- いいえ

「設問のポイント解説」と「用語の説明」を記載

「アドバイザリー情報」とは、公開された脆弱性について、自社製品への影響の内容、アップデートやその他の緩和策を記述した情報を指します。ソフトウェア部品表や脆弱性情報、アップデートの有無などを記載したセキュリティアドバイザリーは、製造販売業者が適切な方法で速やかに提供することが重要です。また、医療機器が複数の国・地域で使用されている場合、国内のインシデントであっても、各国の規制に応じた情報共有が求められることがあります。

問２：「いいえ」と回答された方にお尋ねします。
提供していない理由について、該当するものを選択してください。（複数回答可）
- 提供方法や体制を準備中である
- 顧客（医療機関等）から情報提供の要求がない
- どの情報を提供すべきか判断が難しい
- その他（自由記述）

対応できていない理由を確認し問題点を抽出