

医療機器の部

質問

- ① 日本におけるプログラムを用いた医療機器のサイバーセキュリティの確保については、基本要件基準第 12 条第 3 項への適合が必要となることは理解しました。

本条項への適合を示すためには、薬生機審発 0331 第 8 号により、総じて JIS T 81001-5-1 への適合性を確認すること、とされております。しかし、当該医療機器が、他の機器及びネットワーク等と接続して使用せず、かつ外部からの不正アクセス及び攻撃アクセスを確実に回避できる構造であれば、その旨を説明したエビデンス（報告書）をもって（JIS T 81001-5-1 への適合性を確認せずとも）、本条項への適合を示すことは可能でしょうか。

回答

下記の①、②を実施することで JIS T81001-5-1 に基づいて適合を示すことをお勧めします。実質的にはご質問内容の活動と差はないと考えています。

- ①当該医療機器が、他の機器及びネットワーク等と接続して使用せず、かつ外部からの不正アクセス及び攻撃アクセスを確実に回避できる構造であれば、

→JIS T81001-1-5-1 の 5.2/5.3 に基づいて、ソフトウェアの要求事項とソフトウェアの構造（データフロー図）を作成し、サイバー脅威を特定します。

- ② その旨を説明したエビデンス（報告書）をもって

→JIS T81001-1-5-1 の 7 に基づいて、脅威のリスク評価、低減をします。

→その結果として、サイバーリスクは試験をしなくても十分に需要可能であるということを結論付けます。

（JIS T 81001-5-1 への適合性を確認せずとも）、本条項への適合を示すことは可能でしょうか。

→規格に基づいたアプローチになっているかと思えます。