

医療機器 三二解説

医療機器のサイバーセキュリティの確保について

- 医療機器には、無線又は有線により、他の機器、ネットワーク等と接続する医療機器があり、外部からの不正アクセス等によって医療機器の機能に支障が生じたり、安全性に懸念が生じたりするおそれがあります。そのため、厚生労働省の通知等により、製造販売業者に対し、適切なサイバーセキュリティ対策を実施することが求められてきました。
- 令和5年3月、医療機器に対するサイバー攻撃への対策を一層強化し、医療現場における安全性を確保するため、薬機法第41条第3項に基づく医療機器の基本要件基準※が改正され、第12条第3項にサイバーセキュリティに関する要求事項が定められました。

※ 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四十一条第三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）。医療機器が具備すべき品質、有効性及び安全性に係る基本的要件を規定したものの。

令和6年4月以降に製造販売されるプログラムを用いた医療機器のうち、他の機器及びネットワーク等と接続して使用する医療機器又は外部からの不正アクセス及び攻撃アクセス等が想定される医療機器については、基本要件基準第12条第3項への適合を確認する必要があります。

他の機器（医療機器、IoT機器、周辺機器、外部記録媒体（USB、SD、HDD、CD、DVD等）、電子カルテ、PC（外部からの持込みPC含む）、ネットワーク（院内システム、院外システム、グローバル）等に接続して電磁的情報のやり取りをする医療機器

基本要件基準第12条第3項

プログラムを用いた医療機器※のうち、他の機器及びネットワーク等と接続して使用する医療機器又は外部からの不正アクセス及び攻撃アクセス等が想定される医療機器については、

- 当該医療機器における**動作環境及びネットワークの使用環境等を踏まえて適切な要件を特定し、**
- 当該医療機器の機能に支障が生じる又は安全性の懸念が生じる**サイバーセキュリティに係る危険性を特定及び評価**するとともに、**当該危険性が低減する管理**が行われていなければならない。
- また、当該医療機器は、**当該医療機器のライフサイクルの全てにおいて、サイバーセキュリティを確保するための計画に基づいて設計及び製造**されていなければならない。

※医療機器プログラム又はこれを記録した記録媒体たる医療機器を含む。

第12条第3項への適合の確認とは？

設計・製造工程における取組だけでなく、医療機関との連携、脆弱性対策（市販後のアップデート等を含む）に係る計画等も踏まえ、それが達成できるように、また、問題点や脆弱性が見つかった場合に対応できるように設計・製造を行うことが求められている。

- JIS T 81001-5-1※等への適合性を確認**することにより、**基本要件基準第12条第3項への適合を確認**することが求められています。
- 製造販売業者は、JIS T 81001-5-1等により、**製品ライフサイクルにおける取組を通じたサイバーセキュリティ対策をより強化し、サイバーセキュリティに関するリスクを許容可能な範囲となるまで低減し、患者への危害の発生及び拡大の防止**に繋げる必要があります。

※JIS T 81001-5-1（ヘルスソフトウェア及びヘルスITシステムの安全、有効性及びセキュリティー第5-1部：セキュリティー製品ライフサイクルにおけるアクティビティ）

Check!

一般医療機器を含め、対象となる医療機器については、基本要件基準第12条第3項への適合が必要です。

製造販売業者においては、JIS T 81001-5-1等により、基本要件基準第12条第3項への適合を適切に確認してください。

最新情報の確認を

医療機器のサイバーセキュリティについては、厚生労働省や独立行政法人医薬品医療機器総合機構のWebサイトにおいて専用ページが作成されています。法令、通知等について常に最新の情報を御確認いただき、医療機器のサイバーセキュリティの一層の確保をお願いします。