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の一部を改正する件（案）に係る御意見の募集の結果について

令 和 ５ 年 ３ 月 １ 日
厚生労働省医薬・生活衛生局
医 療 機 器 審 査 管 理 課

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の一部を改正する件（案）について、令和４年 12 月５日から令和５年１月４日まで電子政府の総合窓口等において御意見を募集しましたが、お寄せいただいた主な御意見等の概要とそれに対する厚生労働省の考え方について、別添にとりまとめましたので、公表いたします。

御意見、御質問をお寄せいただきました方々の御協力に厚く御礼申し上げます。

別添

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の一部を改正する件（案）について

No.	寄せられた御意見の概要	回答
1	医療機器のサイバーセキュリティに関して、設計及び製造に関して基準を示した改正であるが、セキュリティの脆弱性が明らかになった場合は厚生労働省からの設計及び製造の変更を設計者及び製造者に命令できることを追記してはどうか。	薬機法第六十五条第一号において、同法第四十一条第三項の規定によりその基準が定められた医療機器であって、その性状、品質又は性能がその基準に適合しないものは、販売し、貸与し、授与し、もしくは販売、貸与若しくは授与の目的で製造し、輸入し、貯蔵し、若しくは陳列し、又は医療機器プログラムにあっては電気通信回線を通じて提供してはならない旨、既に記載されています。基本要件基準第十二条第三項では、サイバーセキュリティに係る危険性セキュリティの脆弱性について、特定、評価を行うと共に、危険性を低減する管理が行われていることを求めており、サイバーセキュリティの脆弱性が明らかになった場合は、このリスクマネジメントの中で対応することが必要であり、それらを満たしていない場合には、薬機法第六十五条に基づき、製造販売できない機器になり得るものです。 なお、「既承認品で流通後のもの」等について、脆弱性が明らかになった場合等についての対応については、今後通知等で示す予定

		です。
2	「プログラムを用いた医療機器の内、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および攻撃アクセス等が想定される医療機器については」であるが、「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および攻撃アクセス等が想定される医療機器」は必然的に「プログラムを用いた医療機器」であるので「プログラムを用いた医療機器の内」という文言は不要に思われる。	基本要件基準第十二条第一項及び第二項のいずれにおいても、冒頭に「プログラムを用いた医療機器」という文言を入れており、第三項においても、対象となる医療機器を明確化するため、本記載のままとさせていただきます。
3	激化するサイバー攻撃への対策が求められる状況において、医療機器の基準にサイバーリスク対策が盛り込まれることに賛同いたします。 医療機器においては遠隔医療や情報収集などで利用されるクラウドサービス上のセキュリティも重要であり、ハードウェア、制御ソフトウェア、ネットワークとともにクラウドサービスに対するセキュリティも重要であると考えます。 クラウドサービスも視野にいれたセキュリティ対策基準の設定を期待しています。	ご意見ありがとうございます。今後の改正時の参考意見とさせていただきます。
4	手引書の背景には「我が国においては、医療機器の製造販売を規制する「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」（昭和 35 年法律第 145 号。以下「医薬品医療機器等法」という）に紐づく「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	今後、通知において、本改正の趣旨等を解説する予定です。その中で、従来は基本要件基準第十二条第二項に紐付く JIS T 2304 に基づいた対応を求めてきたところ、これに加えて、今後は基本要件基準第十二条第三項に紐付く JIS T 81001-5-1 にも基づく対応を行いサイバーセキュリティの確保体制を整える必要があります。

	の基準」（平成 17 年厚生労働省告示第 122 号。以下「基本要件基準」という）によって、サイバーセキュリティを含むリスクマネジメントが求められ、使用者に対する情報提供や注意喚起を含めて最新の技術に立脚して医療機器の安全性を確保しなくてはならないこととされている。」と記載されている。具体的には、基本要件基準の「プログラムを用いた医療機器に対する配慮」の第 12 条 1 項及び 2 項において、サイバーセキュリティのリスクに関しても、抜け漏れなく実施する必要があることを示している。今回の案では、それをさらに強調させるために第 3 項を追加していると想定されるが、既存の第 1 項及び第 2 項との関係を明記したほうがいいのではないか。これにより、新規申請等の医療機器に関しては、3 項の実施を要求でき、既存に流通している医療機器に関しては第 1 項及び 2 項がサイバーセキュリティのリスクも含まれていることを再確認することが期待される。 （変更案） （プログラムを用いた医療機器に対する配慮） ３ 前 1 項及び 2 項において、サイバーセキュリティのリスクも考慮されなければならない。具体的には、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	「既承認品で流通後のもの」等については、今後通知等で具体的な対応を示す予定です。

	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。	
5	「危険性」と表現しているが、少し誤解を招きやすい表現に思えます。 特定、識別するのは危害の大きさで、評価するのはその確率も考慮したリスクで、そのリスクの低減が望まれる。「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」(平成３０年７月２４日付け薬生機審発０７２４第１号、薬生安発０７２４第１号)においては、「サイバーリスクとは、そうした安全性や信頼性が損なわれ、危害(harm) が生じるリスクと考えられる。」と記載され、現在作成中の手引書においては、「サイバーセキュリティに関するリスク」と表現している。 さらに、「医療機器におけるサイバーセキュリティの確保について」(平成２７年４月２８日付け、薬食機参発 0428 第１号、薬食安発 0428 第１号)においては、「サイバーリスクについても既知又は予見し得る危害としてこれを識別し、」と記載している。 これらとも整合のある記載にしたほうがいいのではないか。 (変更案) 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害を特定及びそのリスクを評価するとともに、当	リスクマネジメントにおいては、「危害」の他にも「ハザード」や「危険状態」の特定を行いますが、それらを代表して「危険性の特定及び評価」と表現しているところです。また、基本要件基準において、一貫して「リスク」を「危険性」と記載しており、これらと整合をとるため「危険性」については元の記載のままとさせていただきます。

	該リスクが低減する管理が行われていなければならない。	
6	3 項の規格引用は、JIS T 14971、JIS T 2304 にしてほしい。 【理由】現行製品は、既に発出済みの通知に従い、JIS T 14971、JIS T 2304 に組み込んでサイバーセキュリティ対応を実施している。それらの現行通知との連続性、継続性が必要となるため。	基本要件基準第十二条第三項の適合については、今後、通知において、これから発行予定の、医療機器のサイバーセキュリティに関する規格：JIS T 81001-5-1 に基づき、具体的な対応内容を示す予定です。 なお、JIS T 14971 と JIS T 2304 のいずれも、サイバーセキュリティ体制を確保する上で、その基盤として既に対応しているべき規格であり、本改正においては、追加として JIS T 81001-5-1 への対応を求めることになります。
7	経過措置期間 1 年間は、3 年間としてほしい。 【理由】詳細な対応内容が示されないまま、現時点で、1 年間の経過措置期間は合理性、納得性がない。経過措置は、具体的対応策が示された時点で、実現可能性を見積もったうえで、適切な経過措置期間を、通知等で示すべきである。	医療機器のサイバーセキュリティについては、基本要件基準に基づき、医療機器に関するサイバーリスクに対する適切なリスクマネジメントを実施し、必要な対応を行うよう、従来から関係事業者等に周知してまいりました。 また、今年度中に通知において、これから発行予定である医療機器のサイバーセキュリティに関する規格：JIS T 81001-5-1 に基づき具体的な対応内容を示す予定です。JIS T 81001-5-1 は、基本要件基準第十二条第二項の適用を示す手段として既に用いられる規格：JIS T 2304 に従って開発を進める上で実施するサイバーセキュリティに関する取り組みを規定する規格となります。 以上から、新規の製品について、従来から求めてきている対応内容

		との連続性の観点から、経過措置期間を１年間とすることに関して、適切と考えています。
8	情報通信技術の発展に伴い、複雑化・巧妙化するサイバー攻撃に対して、医療機器の安全性の確保が必要不可欠です。御省では、平成 27 年 7 月に「医療機器におけるサイバーセキュリティの確保」でセキュリティ対応の考え方を示されましたが、今般、医療機器のサイバーセキュリティ確保の重要性や各国のサイバーセキュリティ対策の実情等を踏まえ、国際医療機器規制当局フォーラム(IMDRF)において、サイバーセキュリティ対策の国際的な調和を図ることを目的として、「医療機器サイバーセキュリティの原則及び実践」が取りまとめられ、これを踏まえ、医療機器プログラムにおける基本要件基準の改定が行われたことは、誠に時期を得たものであります。弊社としては、今回の基準改定に賛同致します。 引き続き、弊社は、IT とサイバーセキュリティの力で、社会的課題に立ち向かい、国の発展を支え、人々の暮らしを守ってまいります。	ご意見ありがとうございます。引き続きご協力の程、よろしくお願い致します。
9	経過措置期間が 1 年間(令和 6 年 4 月 1 日義務化)と理解したが、基本要件基準の詳細な内容、手引書との関連、更に経過措置期間の設定の背景や根拠の説明がないため、拙速に過ぎると考える。しかし、サイバー被害増加の現状に鑑みて、行政と業界と一丸となって、合理性を確保した上で早期の結論が必要と考える。全体像を明確にして、実施項目の優先順位を検討し、各通知等で、実情	医療機器のサイバーセキュリティについては、基本要件基準に基づき、医療機器に関するサイバーリスクに対する適切なリスクマネジメントを実施し、必要な対応を行うよう、従来から関係事業者等に周知してまいりました。 また、今年度中に通知において、これから発行予定である医療機器のサイバーセキュリティに関する

	に合った段階的な経過措置期間の設定を望む。なお、内容が不明のため、適正期間のコメントが出来ず、代わりとして懸念事項を参考として記載する。 【懸念事項(参考)】 ＜懸念-1＞現在開発中の新規申請の品目対応 大型診断・治療機器(以下、大型機器)の場合、設計開発に2?3年を要する場合がある。既に開発中で、申請が令和6年4月以降に計画されているものは、既に開発済みプログラムの遡及的な対応が必要になり、再設計や追加検討による申請延期、及び上市時期の遅延が想定され、患者への医療機器の提供に影響を及ぼすことが懸念される。特に、JIS T 81001-5-1は、新規であり企業側の準備がないため、今回の基準引用を止めるか、仮に引用した場合、大幅な経過措置(例えば3年)の設定が必要である。加えて、海外メーカによる輸入医療機器への対応の配慮が必要である。 ＜懸念-2＞現在製造販売している品目対応 基本要件基準の改正のため、現行の製造販売している品目にも適用が必要と想定される(第65条)。大型機器の場合、開発サイクル(製品ライフサイクル)が長いため、過去の設計ドキュメントを再レビューして基本要件基準への対応が想定される。現行で製造販売している品目が多い場合(例えば、数十品目)、設計開発部門は、上記＜懸念-1＞の作業に加えて同時並行して、現行品の遡及対応の作業が必要となり、適切な経過措置期間の設定がなされない場合、	規格：JIS T 81001-5-1に基づき具体的な対応内容を示す予定です。JIS T 81001-5-1は、基本要件基準第十二条第二項の適用を示す手段として既に用いられる規格：JIS T 2304に従って開発を進める上で実施するサイバーセキュリティに関する取り組みを規定する規格となります。 以上から、新規の製品について、従来から求めてきている対応内容との連続性の観点から、経過措置期間を1年間とすることに関して、適切と考えています。 本改正の根拠として、国際医療機器規制当局フォーラム（IMDRF）からIMDRF N47及びN60文書が発出されており、海外メーカも原則としてこれに準じた対応が求められているものと考えています。 一方で、「既承認品で流通後のもの」等については、今後通知等で具体的な対応方針を示す予定です。 なお、End of Support (EOS)/End of Life (EOL)の告知は個別の製品に関して行うものであり、従来の販売においても個別の製品に対して実施されてきているものであることから、行政機関等において掲示するのではなく、医療機器製造業者が医療機器のサポートの一環として告知するものと考え、PMDA のホームページ等への掲載は行わない予定です。

	対応が厳しいと想定される。大型機器の製造販売の一時的な中止も想定され、安定供給の側面でも懸念が生じる。 ＜懸念-3＞EOS の告知方法について 大型機器の耐用年数は、メーカ設定で 5？10 年程度で、実際の医療機関の買い替え年数は平均 13 年※である。これら機器に、サイバー対応として、EOS 情報提供のみ実施すると仮定しても、対象品目数と納入台数の長期間の累積となり、膨大な対応が必要となる。上記＜懸念-1,-2＞の作業を行いながら、この作業に対応することは、現実的でない。解決案として、PMDA 添文ホームページ等に EOS 情報を掲載することで告知とすれば、個別の医療機関への対応が省け、医療機関側も、すぐに EOS が参照可能になり、双方ともに業務軽減が期待できる。 ※: JIRA DATABOOK 2022	
10	サイバー攻撃対策として、メーカ側から医療機関側に対して、一方的に EOS 情報を提供しても、医療機関側にその制度の理解や対応協力(設備やコスト負担)が無ければ、実質的な効果は期待できず、逆に混乱を生じる懸念がある。円滑な運用のため、経過措置期間中に、行政側からも、医療機関側への十分な説明と、法制度の周知・理解の啓発を行っていただきたい。	医療機関におけるサイバーセキュリティの確保については、今年度中に通知等を発出し、周知する予定です。
11	改正後欄の５行目「等」は、機器、ネットワーク以外の何が含まれるのか。	ＵＳＢやＨＤＤ、ＣＤ、ＤＶＤ等の外部記録媒体が含まれます。
12	改正後欄の７行目「等」は、動作環	ファイアウォールやシステムアッ

	境、使用環境以外の何が含まれるのか。	プデートを含むＩＴセキュリティ対策状況が含まれます。
13	改正後欄の１２行目「全て」は「すべて」のほうがよい。第９条第７項「すべての廃棄物」、第１８条第１項「すべてのデータ」の例と同様に。	法令における漢字使用は常用漢字表によるものとなっており、平成22年の常用漢字表で「全て」が追加されたことから､本改正では｢全て」と記載いたします。