

アンケート質問項目一覧

		備考
1	姓、名、電話（ハイフンは不要）、メールアドレス 姓 名 電話（ハイフンは不要） メールアドレス	
2	設問1：取得している製造販売業の許可の区分は何ですか？ 第一種医療機器製造販売業 第二種医療機器製造販売業 第三種医療機器製造販売業 外国特例承認取得者（選任された製造販売業者を含む） なし	
3	設問2：製造販売業の範囲に含まれる構成員の人数は何名でしょうか？ 1～10名 11～20名 21～50名 51～100名 101～200名 201名以上	設問1で『なし』の場合、スキップし設問3へ
4	設問3：設問1 で「なし」を選択された方にお尋ねします。製造業（設計）の登録は行っておられますか？ はい いいえ	『いいえ』の場合、ここまで終了となります。
5	設問4：設計開発部門を有している場合、設計開発部門の構成員の人数は何名でしょうか？ 設計部門なし（0名） 1～5名以内 6～10名 11～20名 21～50名 51名以上	
6	設問5：製品（医療機器）は、国内製造、外国からの輸入、又は その両方 のいずれでしょうか？ 国内製造 外国からの輸入 国内製造と輸入の両方	
7	設問6：サイバーセキュリティ対策を要する品目（製造販売している又は製造販売は終了したが、使用が継続している）がありますか？ はい いいえ	『いいえ』の場合、ここまで終了となります。
8	設問7：サイバーセキュリティ対策を要するクラスⅠ一般医療機器の製造販売中の品目数を教えてください。 製造販売中の品目数： 新規の製造販売は終了し、サポート中の品目数：	
9	設問8：サイバーセキュリティ対策を要するクラスⅡ管理医療機器の製造販売中の品目数を教えてください。 製造販売中の品目数： 新規の製造販売は終了し、サポート中の品目数：	
10	設問9：サイバーセキュリティ対策を要するクラスⅢ高度管理医療機器の製造販売中の品目数を教えてください。 製造販売中の品目数： 新規の製造販売は終了し、サポート中の品目数：	

厚生労働科学研究「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に関する研究」
令和6年度 サーバーセキュリティ対策の対応状況アンケート(設問・選択肢)

11	設問10：サイバーセキュリティ対策を要するクラスIV高度管理医療機器の製造販売中の品目数を教えてください。 製造販売中の品目数： 新規の製造販売は終了し、サポート中の品目数：	
12	設問11：貴社の全製品（医療機器）のうち、サイバーセキュリティ対応を検討しなければならない医療機器のうち、対応が実施できている製品はどの程度ですか。 0%～20% 21%～40% 41%～60% 61%～80% 81%～99% 100%	
13	設問12：リスクマネジメント活動に従事できる力量を有する構成員の人数は何名でしょうか？ 1名～3名 4名～6名 7名～10名 11名以上	
14	設問13：社内体制に関する手順書（社内規定等）の整備は完了していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手）	
15	設問14：サイバーセキュリティ情報の評価体制の整備は完了していますか？ はい（入手した情報の評価、製品ごとの評価も整備済み） 準備中（一部未完了） いいえ（未着手）	
16	設問15：製造販売中の製品に対してSBOMの作成は完了していますか？ はい（すべて完了） 準備中（一部未完了） いいえ（未着手）	
17	設問16：製造販売が終了し、保守対象製品に対してSBOMの作成は完了していますか？ はい（すべて完了） 準備中（一部未完了） いいえ（未着手）	
18	設問17：製品のサイバーセキュリティに関して必要な力量を明確にし、教育・訓練を実施し、その後の力量の維持の仕組みを確立していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手）	
19	設問18：製品のセキュリティリスクに関する情報収集、分析、修正等、一連の市販後対応の仕組みを確立していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手）	
20	設問19：NVDやJVNに登録されている既知の脆弱性について、製品への影響を評価する仕組みを確立していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手）	
21	設問20：社外の第三者の発見者から製品の脆弱性について報告を受けることを想定して社内体制を整えていますか？ はい（完了） 準備中（一部未完了） いいえ（未着手）	

厚生労働科学研究「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に関する研究」
令和6年度 サーバーセキュリティ対策の対応状況アンケート(設問・選択肢)

22	設問21：使用者（医療機関等）から、自社の製品かを問わず広くサイバーセキュリティに関するインシデント情報を入手していますか。 入手していない 入手している 入手したいが方法がわからない	
23	設問22：脆弱性等に関する報告（IPA）、セキュリティリスク等に関連する不具合等報告に該当する仕組みを確立していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業経由で対応している	製造業で『はい』とされた場合のみ表示
24	設問23：使用者（医療機関等）への通知（情報提供）の方法を決定し、情報提供する仕組みを確立していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
25	設問24：製品のEOL、EOS（責任移転）に関する情報を決定し、通知（情報提供）する仕組みを確立していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
26	設問25：製造販売中の製品（医療機器）に対してEOL、EOSを定めている状況を教えてください。 はい（すべて完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
27	設問26：製造販売が終了した、保守対象である製品（医療機器）に対してEOL、EOSを定めている状況を教えてください。 はい（すべて完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
28	設問27：製品（医療機器）のサイバーセキュリティに関連する社内プロセスに問題がないことを確認する仕組みを確立していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手）	
29	設問28：製品（医療機器）のセキュリティポリシーを定めていますか？ はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業のものを受け入れている	製造業で『はい』とされた場合のみ表示
30	設問29：製品（医療機器）のセキュリティポリシーを使用者（医療機関等）に開示する仕組みを確立していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応している	
31	設問30：侵入試験等で、第三者試験を利用したことはありますか？ はい（頻繁） はい（数回） いいえ	

厚生労働科学研究「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に関する研究」
令和6年度 サーバーセキュリティ対策の対応状況アンケート(設問・選択肢)

32	設問31：開発段階で、製品ソフトウェアの保守計画を作成する手順を確立していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手）	
33	設問32：製品ソフトウェアの保守計画を使用者（医療機関等）に提示していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手）	
34	設問33：製造販売中の製品（医療機器）に対して使用者（医療機関等）への情報提供体制の整備は完了していますか？ はい（すべて完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
35	設問34：製造販売が終了し、保守対象となる製品（医療機器）に対して使用者（医療機関等）への情報提供体制の整備は完了していますか？ はい（すべて完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
36	設問35：セキュリティパッチ等のアップデートを定期点検以外のタイミングで実施したことがありますか？ はい（頻繁） はい（数回） いいえ 自社は製造業であり、製造販売業で対応している	製造業で『はい』とされた場合のみ表示
37	設問36：市販後の製品の脆弱性管理として、収集又は報告された脆弱性等の分析結果（対応の判定結果）について記録がありますか？ はい（完了） 準備中（一部未完了） いいえ（未着手）	
38	設問37：脆弱性等に関するアドバイザリー情報を使用者（医療機関等）に提供していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
39	設問38：脆弱性等に関する使用者（医療機関等）への情報提供について、PSIRT等の製品セキュリティインシデント対応組織を設置していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手）	
40	設問39：セキュリティリスクを扱うリスクマネジメントを実施する仕組みを確立していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手）	
41	設問40：脅威分析等に基づき製品の信頼境界を決定し、使用者（医療機関等）に提示していますか？ はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

厚生労働科学研究「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に関する研究」
令和6年度 サーバーセキュリティ対策の対応状況アンケート(設問・選択肢)

42	設問41：製品のソフトウェア開発では、ソフトウェア構成管理等を含むJIS T 2304を適用した上で、サイバーリスクを扱うために必要なアクティビティを実施することが求められています。ソフトウェア開発で、アウトソース先がある場合、SBOM等ソフトウェア構成管理、脆弱性管理に必要な情報が入手可能な契約になっていますか？	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	
43	設問42：使用者（医療機関等）から、脆弱性に対する対応状況の問合せ又はマルウェアによる感染確認等の依頼を受けたことがありますか？	
	はい（頻繁） はい（数回） いいえ	
44	設問43：製造販売業としてのQMS対象である製造業・委託先の管理について、製造業・委託先におけるサイバーセキュリティに関する対応状況を把握していますか。	
	製造業者および委託先まで含めて全て把握 製造業までを把握している（委託先は把握していない） 把握していない 自社は製造業であり、求めに応じ製造販売業者へ情報を提供している	製造業で『はい』とされた場合のみ表示
45	設問44：サイバーセキュリティに関する問い合わせ先を明確にし、使用者（医療機関等）に対して情報提供していますか。	
	公開している 今後公開する予定 公開していない 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
46	設問45：明確にしている場合、医療機関から問い合わせはありましたか？	
	あった なかった 自社は製造業であり、製造販売業経由で問い合わせがあった	製造業で『はい』とされた場合のみ表示
47	設問46：問い合わせがあった場合、どのような内容ですか？	設問45で『あった』とされた場合のみ表示、それ以外はスキップして、設問48へ 記載ください
48	設問47：問い合わせがあった場合、問い合わせに対して十分な対応ができましたか？	設問45で『あった』とされた場合のみ表示、それ以外はスキップして、設問48へ
	できた できなかった	
49	設問48：製造販売時におけるサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供していますか。	
	提供している 要求があれば提供する 提供していない 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
50	設問49：製造販売時におけるサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供している場合、どのような方法で提供していますか。（複数選択可能）	
	自社WEBサイト 添付文書 取り扱い説明書 契約書 技術資料 サイバーセキュリティに関する特別文書 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している その他（具体的にご記入ください）	製造業で『はい』とされた場合のみ表示

厚生労働科学研究「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に関する研究」
令和6年度 サーバーセキュリティ対策の対応状況アンケート(設問・選択肢)

51	設問50：市販後においてサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供していますか。 提供している 要求があれば提供する 提供していない 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
52	設問51：貴社は、製品（医療機器）に関するソフトウェア部品表（SBOM）を使用者（医療機関等）に対し、開示していますか。 提供している 要求があれば提供する 提供していない 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	設問50で『提供していない』とされた場合のみ表示、それ以外はスキップし、設問53へ
53	設問52：提供していない場合、ソフトウェア部品表（SBOM）の提供には何か課題があると考えていますか。（複数選択可能） 知的財産の流出の懸念（提供先からの情報漏洩） ソフトウェア関連の改良・改善と情報開示のタイミングのズレ どこまで公開するのかわからない（標準フォーマットが不明） 社内での部門まで対応しないといけないかわからない（資材、開発、生産部門など） サードパーティやオープンソフトウェアの妥当性検証の懸念 開示しても顧客（医療機関等）側が適切に理解するかが懸念（合理性のない対応を求められる懸念）	
54	設問53：納品時、ネットワークに接続して使用することを使用者（医療機関等）に確認していますか？ 確認している 確認していない 自社は製造業であり、製造販売業で対応している	製造業で『はい』とされた場合のみ表示
55	設問54：ネットワークに接続して使用する場合には、サイバーセキュリティ確保のための対応が必要であることを使用者（医療機関等）に通知していますか？ 通知している 通知していない 自社は製造業であり、製造販売業で対応している	製造業で『はい』とされた場合のみ表示
56	設問55：使用者（医療機関等）のネットワーク構成図を把握していますか？ 把握している 把握したいが把握できない（医療機関側から開示されない） 把握していない 自社は製造業者であり、把握したいが把握できない（製販業者側から共有されない）	製造業で『はい』とされた場合のみ表示
57	設問56：製品（医療機器）について、SBOMを作成していますか？ 作成している 一部作成している 作成していない	
58	設問57：SBOMを作成していない場合、その理由は何ですか？（複数選択可能） 作り方がわからない 作れる人がいない 作る意味がない その他（具体的にご記入ください）	
59	設問58：製品（医療機器）について、MDS2を作成していますか？ 作成している 一部作成している 作成していない その他（具体的にご記入ください）	

厚生労働科学研究「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に関する研究」
令和6年度 サーバーセキュリティ対策の対応状況アンケート(設問・選択肢)

60	設問59：MDS2を作成していない場合、その理由は何ですか？（複数選択可能）	
	作り方がわからない 作れる人がいない 作る意味がない その他（具体的にご記入ください）	
61	設問60：製品（医療機器）のサイバーセキュリティに関して、どのような情報を医療機関に通知していますか。（製造業の場合は、製造販売業経由で通知する情報を選択してください。）（複数選択可能）	
	SBOM MDS2 EOL EOS 脆弱性情報 レガシー医療機器に関する情報 通知していない その他（具体的にご記入ください）	
62	設問61：製品（医療機器）のサイバーセキュリティに関する情報として、SBOM、MDS2を通知している場合、医療機関にどのような内容を通知していますか。（製造業の場合は、製造販売業経由で通知する情報を選択してください。）（複数選択可能）	
	SBOMの意義 SBOMの管理方法 SBOMの使い方 MDS2の意義 MDS2の管理方法 MDS2の使い方 その他（具体的にご記入ください）	
63	設問62：製品（医療機器）のサイバーセキュリティに関する情報を医療機関のどの部署に通知していますか。（複数選択可能）	
	事務（購買）部門 事務（総務）部門 使用する診療科・部門 医療安全部門、医療機器管理部門 医療情報管理部門 自社は製造業であり、製造販売業で対応している その他（具体的にご記入ください）	製造業で『はい』とされた場合のみ表示
64	設問63：製品（医療機器）のサイバーセキュリティに関する情報はどのようなタイミングで医療機関に通知していますか。（複数選択可能）	
	入札時、納品時 医療機関からの求めに応じて 脆弱性などの情報がわかったとき サイバーセキュリティ対策（脆弱性等）が必要となったとき EOLの時期が決まったとき EOSの時期が決まったとき レガシー医療機器が発生したとき 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している その他（具体的にご記入ください）	製造業で『はい』とされた場合のみ表示
65	設問64：製品（医療機器）のサイバーセキュリティに関する情報（EOL/EOS）はどのようなタイミングで医療機関に通知していますか。	
	EOL/EOSの2年前 EOL/EOSの1年前 EOL/EOSの半年前 EOL/EOSの3ヶ月前 EOL/EOSの1ヶ月前 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している その他（具体的にご記入ください）	製造業で『はい』とされた場合のみ表示
66	設問65：レガシー医療機器のサイバーセキュリティの確保に必要な情報については、どのようなタイミングでどのように把握していますか？	
		記載ください

厚生労働科学研究「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に関する研究」
令和6年度 サーバーセキュリティ対策の対応状況アンケート(設問・選択肢)

67	設問66：レガシー医療機器の対応については、どのような内容を医療機関に通知していますか？（複数選択可能） 使用継続のリスク 使用継続のための費用 ネットワークから遮断する方法 ファイヤーウォールなどの対応 とくに通知していない その他（具体的にご記入ください）	
68	設問67：SBOMに含まれるソフトウェアに関連する脆弱性情報などは、どのようなタイミングでどのように把握していますか？	記載ください
69	設問68：製品（医療機器）のサイバーセキュリティに関する情報を医療機関に渡す想定で、添付文書、取扱説明書や保守点検マニュアルに記載していますか？（複数選択可能） 取り扱い説明書に記載している 保守点検マニュアルに記載している 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している 記載していない	製造業で『はい』とされた場合のみ表示
70	設問69：記載している場合、どのような内容を記載していますか？	記載ください
71	設問70：医療機関からサイバーセキュリティに関するどのような情報を求められますか？（製造業の場合は、製造販売業からの要求で提供する情報を選択してください。）（複数選択可能） 求められない ネットワーク構成図 SBOM MDS2 EOL EOS 脆弱性情報を含むアドバイザリー情報 レガシー医療機器に関する情報 その他（具体的な情報を記載してください）	
72	設問71：医療機器のサイバーセキュリティ確保に関して、医療機関との連携の課題についてお答えください。	記載ください
73	設問72：医療機関と製造販売業者との情報共有について、具体化する等の意見をお答えください。	記載ください
74	設問73：医療機器サイバーセキュリティに関する保守契約を医療機関と締結していますか？ 締結している 締結していない 自社は製造業であり、直接締結していない	製造業で『はい』とされた場合のみ表示
75	設問74：締結している場合、信頼境界及び責任分界点はどのような内容で、どのように決めていますか？	記載ください

厚生労働科学研究「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に関する研究」
令和6年度 サーバーセキュリティ対策の対応状況アンケート(設問・選択肢)

76	設問75：販売業者、修理業者に対して、サイバーセキュリティ対策の確認や指導を行っていますか。 定期的に指導等を行っている 不定期に指導等を行っている 行っていない 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
77	設問76：医療機器のサイバーセキュリティ対策についての課題と感じていることを選択してください。（複数選択可能） 専門家の確保 専門家以外の教育 対策費用等 医療機関との連携・情報共有 リスクマネジメントの具体的方法 その他（具体的にご記入ください）	
78	設問77：医療機器のサイバーセキュリティ対策について課題と感じていることをご記載してください。	記載ください
79	設問78：医療機器の基本要件基準第12条第3項の適用について、課題又は懸念等がありましたらご記載ください。	記載ください