総研 35 号
2021 年 1 月 12 日

都道府県医師会
担当理事　御中

公益社団法人日本医師会
常任理事　　長島 公之

「医療機関の情報システムの管理体制に関する実態調査」実施のご案内

拝啓　新春の候、ますますご健勝のこととお慶び申し上げます。平素より当会の活動に格別のご厚情を賜り、深く御礼申し上げます。

さて今般、日本医師会総合政策研究機構（日医総研）において、医療機器センター附属医療機器産業研究所と合同で、医療機関の情報システム管理体制の状況を把握する目的で、調査研究を進めておりますので、ご了知いただきますようお願い申し上げます。

○調査名称：「医療機関の情報システムの管理体制に関する実態調査」

・全国の病院・診療所（病院 5,000、診療所 5,000 を無作為抽出）を対象に、ウェブ上に構築したアンケート調査システムを通じて回答いただきます。
・調査システムへのアクセス方法等を記載したご案内文書を、対象の病院/診療所の管理者宛に、1 月 7 日付で専用封筒にて郵送しました。
・併せて管理者宛に、日本医師会会長、医療機器センター理事長の連名でのご協力依頼状を同封しました。
・調査期間は、2021 年 1 月 7 日（木）以降、文書到着次第 ～2021 年 1 月 29 日（金）となります。

上記調査の開始にあたり、対象の医療機関宛に、書面にて医療機器センター附属医療機器産業研究所の下記担当窓口をご案内しておりますが、もしも上記に関連して貴会の窓口にお問合せがあった場合には、重ねて、下記事務局のご案内をお願い申し上げます。

ご多忙の折、お手数をお掛けし誠に恐縮ではございますが、宜しくご高配賜りますと幸甚です。

敬　具

記

「医療機関の情報システムの管理体制に関する実態調査」事務局
公益財団法人医療機器センター附属医療機器産業研究所
本田（ほんだ）／　松橋（まつはし）
TEL：03-3813-8553 (平日 10 時～12 時、13 時～16 時)
E-mail アドレス：mdsi-cyber@jaame.or.jp

以　上

２０２１年１月

院長　各位

公益社団法人 日本医師会
会長 中川 俊男
公益財団法人 医療機器センター
理事長 菊地 眞

『医療機関の情報システムの管理体制に関する実態調査』へのご協力依頼

拝啓　新春の候、時下益々ご清祥のこととお慶び申し上げます。平素より格別のご高配を賜り、厚くお礼申し上げます。

昨今、情報通信技術の発達やIoTの活用に伴い、サイバーセキュリティの重要性が増してきております。医療機関もその例外ではなく、情報システムの管理体制の構築と個別の医療機器も含めたサイバーセキュリティ対策が重要であると指摘されております。

医療機関におけるサイバーセキュリティ対策は施設毎に状況が異なり、課題も多く、解決策に関する情報も不足し、何をどこまですればよいのかという具体的対策も立てにくい状況下に置かれているものと考えられます。

そこで、日本医師会（日本医師会総合政策研究機構）と医療機器センター（医療機器センター附属医療機器産業研究所）は合同で、医療機関の情報システムの実施状況を把握するため、標記の実態調査を実施することといたしました。本調査結果に基づき、サイバーセキュリティ対策を講じる上での新たな課題などを抽出し、実効性の高いサイバーセキュリティ対策の具体化や充実化を臨産官が一体となって検討することを狙いとします。日本医師会総合政策研究機構では医療機関に向けた報告書、医療機器センター附属医療機器産業研究所では医療機器業者に向けた提言を目的とする日本医療研究開発機構委託研究報告書（別添参照）を、それぞれまとめる予定です。

つきましては同封の「実施状況とりまとめ用紙」をご一読頂き、皆様にぜひご回答頂きたくお願い申し上げます。ご多用中恐縮ですが、ご理解のうえ、ご協力のほど宜しくお願い申し上げます。

敬具

記

提出方法　：　同封した『実施状況とりまとめ用紙』を活用し関係部署へ確認を行って頂いた後、専用のWEBサイト（https://questant.jp/q/jmari-mdsi2020）から提出

提出期限　：　2021年1月29日（金）

守秘について

回答頂きました内容については、事務局内で守秘義務を厳守の上、調査のとりまとめを行い、本調査以外には使用致しません。また本調査における個別の回答内容については、事務局内のみでの取り扱いとし、施設名がわからないように加工あるいは一般化された内容のみ閲覧することができる状態とします。個別の回答内容を行政及び関連機関に報告することもありません。なお、日本医師会総合政策研究機構および医療機器センター附属医療機器産業研究所において、報告書執筆や学会発表、より良い医療の実現に向けた政策提言に活用させて頂く予定です。

【お問い合わせ窓口】　「医療機関の情報システム管理体制に関する実態調査」事務局
公益財団法人医療機器センター附属医療機器産業研究所　本田・松橋
E-mail：mdsi-cyber@jaame.or.jp　電話：03-3813-8553

写

別　添

令和２年度日本医療研究開発機構研究費（医薬品等規制調和・評価 研究事業）
医療機関における医療機器のサイバーセキュリティに係る課題抽出等に関する研究

医療機器センター附属医療機器産業研究所では、厚生労働省医薬・生活衛生局医療機器審査管理課及び医薬安全対策課からの依頼により、医療機関における医療機器のサイバーセキュリティに係る課題抽出等に関する研究（日本医療研究開発機構委託研究費（医薬品等規制調和・評価研究事業 研究代表者：当財団専務理事 中野壮陛））を 2019 年度から以下の研究班メンバーにより実施しております。

なお本調査の回答内容を取りまとめた結果は、本文記載の守秘義務を厳守の上で、報告書として国立研究開発法人日本医療研究開発機構(AMED)に提出します。

研究班メンバー

長島公之	公益社団法人日本医師会　常任理事
中村康彦	公益社団法人全日本病院協会　副会長（四病協）
久芳　明	一般社団法人日本医療機器産業連合会 サイバーセキュリティ TF リーダー
古川　浩	一般社団法人日本医療機器産業連合会 サイバーセキュリティ TF
松元恒一郎	一般社団法人日本医療機器産業連合会 サイバーセキュリティ TF
北村正仁	一般社団法人日本医療機器産業連合会 サイバーセキュリティ TF
谷口克巳	一般社団法人日本医療機器産業連合会 サイバーセキュリティ TF
中野壮陛	公益財団法人医療機器センター　専務理事　　※研究代表者

【オブザーバー】
厚生労働省医薬・生活衛生局医療機器審査管理課
厚生労働省医薬・生活衛生局医薬安全対策課
経済産業省商務情報政策局サイバーセキュリティ課
経済産業省商務・サービスグループヘルスケア産業課医療福祉機器産業室
独立行政法人医薬品医療機器総合機構（PMDA）医療機器審査第一部
独立行政法人医薬品医療機器総合機構（PMDA）医療機器審査第二部
独立行政法人医薬品医療機器総合機構（PMDA）医療機器品質管理・安全対策部
国立研究開発法人日本医療研究開発機構（AMED）創薬戦略部　医薬品等規制科学課

【お問い合わせ窓口】　「医療機関の情報システム管理体制に関する実態調査」事務局
公益財団法人医療機器センター附属医療機器産業研究所　本田・松橋
E-mail：mdsi-cyber@jaame.or.jp　電話：03-3813-8553

以上

写

公益社団法人日本医師会 日本医師会総合政策研究機構
公益財団法人医療機器センター附属医療機器産業研究所
合同調査
医療機関の情報システムの管理体制に関する実態調査

WEB 回答前の『実施状況とりまとめ用紙』

対象医療機関：ランダムに抽出した全国の病院(5,000 施設)・診療所(5,000 施設)を対象

回　答　者：貴院において「情報システムに詳しい方」

調 査 内 容：現時点（記入日）における医療機関の情報システムの管理体制と医療機器のサイバーセキュリティ対策の実施状況

提出方法：専用の WEB サイト（https://questant.jp/q/jmari-mdsi2020）から提出
※　本用紙は、サイバーセキュリティ対策の実施状況について貴院内の関連部署への確認などにご活用ください。提出は専用の WEB サイトからのみとなります。
右の二次元バーコードからもアクセスが可能です。

期　限：２０２１年1月２９日（金）

【特記事項】

- 本調査は、公益社団法人日本医師会 日本医師会総合政策研究機構と公益財団法人医療機器センター附属医療機器産業研究所が合同で実施するものです。
- 本調査は、医療機関におけるサイバーセキュリティ対策の実施状況の全体像を明らかにするものであり、個別の施設の取組みについて議論をするものではありません。また個別の回答内容を行政及び関連機関に報告することもありません。
- 回答頂きました内容については、事務局内で守秘義務を厳守の上、調査のとりまとめを行い、本調査以外には使用致しません。
- 本調査における個別の回答内容については、事務局内のみでの取り扱いとし、施設名が特定されないように加工あるいは一般化された内容のみ閲覧することができる状態とします。
- 本調査の回答内容を取りまとめた結果は、「医療機関における医療機器のサイバーセキュリティに係る課題抽出等に関する研究（日本医療研究開発機構委託研究費（医薬品等規制調和・評価研究事業 研究代表者：(公財)医療機器センター 専務理事 中野壮陛)」の報告書として、国立研究開発法人日本医療研究開発機構(AMED)に提出します。また、日本医師会総合政策研究機構および医療機器センター附属医療機器産業研究所において報告書執筆や学会発表、より良い医療の実現に向けた政策提言に活用させて頂く予定です。
- 「＊」のある設問は、回答が必須の項目です。

※お問合せは、原則 E-mail にて、下記までお願い致します。
「医療機関の情報システム管理体制に関する実態調査」事務局
公益社団法人日本医師会　日本医師会総合政策研究機構　堤・坂口
公益財団法人医療機器センター附属医療機器産業研究所　本田・松橋
E-mail：mdsi-cyber@jaame.or.jp
電話：03-3813-8553((公財)医療機器センター附属医療機器産業研究所)

【Q1～Q6】
貴院について

Q1．貴院の開設者についてお答えください。＊

○ 個人
○ 医療法人
○ 医師会
○ 国（独立行政法人、国立大学法人を含む）
○ 都道府県・市町村（地方独立行政法人、公立大学法人を含む）
○ 公的医療機関（日赤、済生会、北海道社会事業協会、厚生連）
○ 社会保険関係団体（船員保険会、健保組合及びその連合会、共済組合及びその連合会、国保組合）
○ 公益法人（医師会を除く）
○ 私立学校法人
○ 社会福祉法人
○ 医療生協
○ 会社
○ その他の法人

Q2．貴院の病床数についてお答えください。＊

○ 無床診療所　（Q３へお進みください）
○ 有床診療所　（Q３へお進みください）
○ 病院　20～99 床　（Q４へお進みください）
○ 病院　100～199 床　（Q４へお進みください）
○ 病院　200～299 床　（Q４へお進みください）
○ 病院　300～499 床　（Q４へお進みください）
○ 病院　500 床以上　（Q４へお進みください）

※Q２．の回答による
Q３．Q２にて「診療所」の項目を選択された方にお伺いします。
貴院の主な診療科をお答えください（下記から１つだけ選択してください）。＊
○ 内科
○ 外科
○ 整形外科
○ 眼科
○ 耳鼻咽喉科
○ 小児科
○ 皮膚科
○ 泌尿器科
○ 精神科
○ 産科・産婦人科
○ 婦人科
○ 脳神経外科
○ その他（　　）

※Q２．の回答による
Q４．Q２にて「病院」の項目を選択された方にお伺いします。
貴院の施設の種類をお答えください。＊
○ 一般病院
○ 精神科病院

Q5．院長のご年齢について年代でお答えください。＊

○　３０歳代以下
○　４０歳代
○　５０歳代
○　６０歳代
○　７０歳代
○　８０歳代以上

Q6．令和３年（2021 年）３月から、「オンライン資格確認」（マイナンバーカードの個人認証や健康保険証の記載情報を用いて、オンラインで健康保険の資格確認を可能にする仕組み）が開始されます。貴院では、このオンライン資格確認のシステムを導入する予定かお答えください。＊

○　令和３年３月に導入予定である
○　令和３年３月には導入しないが、補助金の申請期限（令和５年３月３１日）までには導入予定である
○　導入する予定はない
○　検討中
○　わからない・知らない

【Q7～Q9】
貴院内のネットワークについて

Q7.　貴院の情報システムについて、取り扱っている範囲、並びに院内の接続状況(他のシステムやインターネット)についても合わせてお答えください。＊

なお、ひとつのシステムに複数の機能がある場合は、その機能に該当するシステムすべてに対してお答えください。
(例：電子カルテシステムが医用画像管理システムを兼ねている場合は、電子カルテシステムと医用画像管理システムの両方にお答えください)

	貴院内の他のシステムやインターネットとの接続はしていない	インターネットとは接続していないが、貴院内の他のシステムと接続している	貴院内の他のシステムとは接続していないが、インターネットと接続している	貴院内の他のシステムとインターネットの両方に接続している	このシステムは使っていない
医事会計システム（レセコン）	○	○	○	○	○
電子カルテシステム	○	○	○	○	○
オンライン請求システム	○	○	○	○	○
医用画像管理システム	○	○	○	○	○
オーダリングシステム	○	○	○	○	○
診療予約システム	○	○	○	○	○
健康診断システム（健診・人間ドック等の受診者管理システム）	○	○	○	○	○
遠隔診療システム(オンライン診療システムを含む)	○	○	○	○	○
地域医療連携システム（医療連携、医療・介護連携のシステム）	○	○	○	○	○
その他　(具体的な情報システムの名称については次問(Q6)にてご回答ください)	○	○	○	○	○

※Q7．の回答による
Q8．Q7にて「その他」を選択された方にお伺いします。
その他の具体的な情報システムの名称をご記入ください。

Q9.　貴院内のすべてのネットワークを外部に説明できる資料（ネットワーク構成図）を持っていますか。
また、その資料の更新のタイミングと共にお答えください。＊

○　資料を持っており、計画的に見直しや更新を行っている
○　資料を持っており、ネットワークの追加・修正のあるタイミングで見直しや更新を行っている
○　資料を持っているが、見直しや更新は行っていない
○　資料は持っていない

【Q１０～Q１２】
貴院のサイバーセキュリティ対策への取り組み（組織体制）について

Q１０.　貴院の情報システムの管理体制について、もっともよくあてはまるものをひとつ選んでお答えください。＊

- ○ 専任の担当部門がある
- ○ 専任の担当部門はないが、委員会等を設置している
- ○ 専任の担当部門や委員会等はないが、専任の担当者がいる
- ○ 専任の担当部門、委員会等や専任の担当者はいないが、兼務の担当者がいる
- ○ 上記のような管理体制はなく、院長が自ら管理している

Q１１.　貴院の情報システムのメンテナンス活動を現場にて行っている方についてお答えください。＊

- ○ 内部スタッフ（院長含む）により実施している
- ○ 外部の業者のサービスを利用して実施している
- ○ 内部スタッフ（院長含む）および外部の業者のサービスにより実施している
- ○ 実施していない
- ○ わからない

Q１２.　貴院では、サイバーセキュリティ対策に関する費用を計画的に用意していますか。＊

- ○ 計画的に使えるように用意している
- ○ 計画的ではないが、必要に応じて使えるように用意している
- ○ 用意していない

【Q１３～Q１９】
貴院のサイバーセキュリティ対策への取り組み(運用)について

Q１３．厚生労働省の「医療情報システムの安全管理に関するガイドライン」(最新版は【第５版】)を把握・活用しているかお答えください。＊

○ 活用している
○ 知っているが活用していない
○ 知らない

Q１４．サイバー攻撃を受けた際は厚生労働省 医政局 研究開発推進課 医療情報技術推進室に連絡することをご存知かお答えください。＊

○ 知っている
○ 知らない

Q１５．マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口が独立行政法人 情報処理推進機構 情報セキュリティ安心相談窓口であることをご存知かお答えください。＊

○ 知っている
○ 知らない

Q１６．患者・受診者情報が保管されている貴院内の情報端末（ＰＣやタブレット等）の管理ルールについてお尋ねします。下記の（１）～（５）の各ルールの徹底度合いに対するご認識についてお答えください。＊

	ルールがあり、徹底されている	ルールはあるが、徹底されているかどうか、自信がない	ルールはあるが、徹底されていない	ルールはない
(1) 端末の持ち出し時のルール	○	○	○	○
(2) 外部媒体(USBメモリ等)と接続するときのルール	○	○	○	○
(3) インターネットに接続するときのルール	○	○	○	○
(4) 端末から離席するときのルール	○	○	○	○
(5) 端末を廃棄する際のルール	○	○	○	○

Q１７．ＵＳＢメモリ等の外部媒体の管理ルールについてお尋ねします。下記の（１）～（３）の各ルールの徹底度合いに対するご認識についてお答えください。＊

	ルールがあり、徹底されている	ルールはあるが、徹底されているかどうか、自信がない	ルールはあるが、徹底されていない	ルールはない
(1) 持ち込み・持ち出し時のルール	○	○	○	○
(2) 貴院内のPC等と接続するときのルール	○	○	○	○
(3) 廃棄する際のルール	○	○	○	○

Q１８．　下記のようなサイバーセキュリティに関わるインシデントが発生した時の明文化された対応手順やルールの有無についてお答えください。＊

	明文化された対応手順やルールあり	明文化された対応手順やルールなし
(1) 貴院内のサーバや情報端末に、ウイルス感染や不正アクセスがあった場合	○	○
(2) ホームページの改ざんや乗っ取り等のハッキング被害があった場合	○	○
(3) 患者・受診者の個人情報の漏えいがあった場合	○	○
(4) 患者・受診者への直接の危害があった場合	○	○

Q１９．　サイバーセキュリティ保険への加入状況についてお答えください。＊

○　サイバーセキュリティ保険に加入しており、保険の内容も知っている
○　サイバーセキュリティ保険に加入しているが、内容はよく知らない
○　サイバーセキュリティ保険に加入していないが、検討したい
○　サイバーセキュリティ保険に加入しておらず、検討予定もない

【Q２０～Q２１】
貴院のサイバーセキュリティ対策への取り組み（現場状況）について

Q２０．　過去３年間において、貴院では、以下のような経験がありましたか。経験があるものをすべてお答えください。
＊（複数選択可）…注：調査画面上は（複数選択）と表示。以下、同じ。

□　経験がない　（Q２２へお進みください）
□　貴院内のサーバがウイルス感染した。
□　貴院内の端末（PCやタブレット端末）がウイルス感染した。
□　従業員が院内システムを使って、貴院内ルールに違反してインターネットにアクセスした。
□　従業員が貴院内のＰＣやタブレット端末から、フィッシング（詐欺）サイトにアクセスさせられた。
□　貴院のホームページが改ざん・乗っ取りされた。
□　患者・受診者の個人情報にアクセスできる端末が、なりすましメール（迷惑メールなど）を受信した。
□　患者・受診者の個人情報が漏えいした。
□　従業員の個人情報が漏えいした。
□　上記以外の情報が漏えいした。
□　貴院内のシステムに外部からの不正ログインがあった。
□　業務用のノートPC・スマートフォン・タブレットの紛失・盗難があった。
□　USBメモリ等の外部媒体の紛失・盗難があった。
□　患者・受診者の個人情報が含まれるメールの誤送信があった。
□　患者・受診者の個人情報が含まれるFAXの誤送信があった。
□　情報システムや医療機器等へのサイバー攻撃により患者に直接の危害があった。
□　その他（　　）

※Q２０．の回答による
Q２１．　Q２０にて、いずれかの経験があると回答された方にお伺いします。
発生したインシデント情報をどのレベルまで把握し、対応できているかについてお答えください。＊

○　インシデントの原因分析と今後の対応まで整理できている
○　インシデントの原因分析まで整理できている
○　インシデントが発生したという事実まで整理できている
○　その他（　　）

【Q２２～Q２４】
貴院のサイバーセキュリティ対策への取り組み(教育)について

Q２２．　サイバーセキュリティ対策に関する教育の実施状況についてお答えください。＊

○　半年から１年に１回程度実施している
○　１年から３年に１回程度実施している
○　３年から５年に１回程度実施している
○　実施していない(Q２５へお進みください)

※Q２２．の回答による
Q２３．　Q２２にて「実施している」と回答された方にお伺いします。
教育の対象者についてお答えください。＊

○　全職員に対して実施している
○　担当の部門に対して実施している
○　希望者に対して実施している
○　わからない

※Q２２．の回答による
Q２４．　Q２２にて「実施している」と回答された方にお伺いします。
貴院における教育の方法について当てはまるものをすべてお答えください。＊ (複数選択可)

□　専門家を招いての講習会を用いて実施している
□　行政等から出されているガイドラインを用いて実施している
□　担当部署内で作成した教材を用いて実施している
□　専門機関の講座を用いて実施している
□　e-learning講座を用いて実施している
□　市販されている教材を用いて実施している
□　その他（　　）

【Q２５～Q２６】
貴院のサイバーセキュリティ対策への取り組み（要望）について

Q２５.　サイバーセキュリティ対策にあたって、このようなことがあればよいと思う選択肢をすべてお答えください。
（複数選択可）

□　自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み
□　インシデント・アクシデント発生時の相談先
□　サイバーセキュリティ対策の体制構築を検討する際の相談先
□　サイバーセキュリティ対策を学べる場所
□　自施設内のサイバーセキュリティ対策を担う人材
□　サイバーセキュリティ対策の費用面での公的支援
□　その他（　　）

Q２６.　サイバーセキュリティ対策にあたって、最も優先度が高いと考える選択肢をひとつお答えください。

○　自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み
○　インシデント・アクシデント発生時の相談先
○　サイバーセキュリティ対策の体制構築を検討する際の相談先
○　サイバーセキュリティ対策を学べる場所
○　自施設内のサイバーセキュリティ対策を担う人材
○　サイバーセキュリティ対策の費用面での公的支援
○　その他（　　）

【Q２７～Q３２】
医療機器に関するサイバーセキュリティ対策の実態について

本調査で対象とするのは、サイバーセキュリティ対策が必要な医療機器です。
具体的には、通信機能・ネットワーク(Bluetooth、Wi-Fi 等)への接続や USB・CD/DVD ドライブ等のある医療機器を指します。
例えば、PACS などの医療用画像管理システムに接続される透視装置・CT・MRI 等、テレメトリー式心電計、バイタルモニタ機器、輸液ポンプ、麻酔器・モニタ機器類や人工呼吸器・透析装置といった医療機器です。

Q２７．　サイバーセキュリティ対策が必要な医療機器があることをご存知かお答えください。＊

○ よく知っている
○ 知っている
○ あまり知らない
○ 知らない　(Q３０へお進みください)

※Q２７．の回答による
Q２８．　Q２７にて「よく知っている」、「知っている」、「あまり知らない」と回答された方にお伺いします。
個別の医療機器に関するサイバーセキュリティの情報をどこから入手されているかについて当てはまるものをすべてお答えください。＊(複数選択可)

□ 医療機器のメーカ
□ 医療機器の販売業者
□ セキュリティ会社
□ 医療情報システム会社
□ 医師会
□ 所属する病院団体
□ 行政
□ 入手していない　(Q３０へお進みください)
□ わからない　(Q３０へお進みください)
□ その他（　　）

※Q２８．の回答による
Q２９．　Q２８で、いずれかから情報を入手していると回答された方にお伺いします。
入手した個別の医療機器に関するサイバーセキュリティの情報の理解度についてお答えください。＊

○ 対策・対応の必要性の判断ができるレベルで理解している
○ 用語は理解できているが、対策・対応の必要性の判断はできない
○ 用語についても理解できない

Q３０．医療機器を購入した際に、販売業者から医療機器のサイバーセキュリティに関する説明があったか、また、貴院での理解度についてお答えください。＊

○ 説明があり、内容も十分に理解できた
○ 説明はあったが、内容は理解できなかった
○ 説明はなかった
○ わからない

Q３１．貴院のサイバーセキュリティ対策を検討するにあたって、個々の医療機器に施されているサイバーセキュリティ対策の情報※が必要か当てはまるものすべてお答えください。＊(複数選択可)

※　医療機器内に組み込まれたセキュリティおよびプライバシー対策機能に関する標準化された情報やソフトウェアコンポーネント(部品表・構成表)の情報など。このような資料を製造業者開示説明書(MDS2)と呼びます。

□　購入検討時に必要
□　購入時に必要
□　購入後、契約更新に応じて必要
□　購入後、求めに応じて必要
□　必要ない
□　わからない

Q３２．「レガシーメディカルデバイス※」という言葉をご存知かお答えください。＊

※　レガシーメディカルデバイスとは、サイバーセキュリティ対策を検討しなければならない医療機器のうち、既に市販済みの製品であって、設計段階等においてサイバーセキュリティの検討がなされていなかった医療機器であり、当該製品単独では今後もサイバーセキュリティの脅威に対して合理的に保護できないと考えられる医療機器を指す。

○　知っている
○　知らない

【Q３３～Q３４】
ご意見、ご要望等

Q３３.　最後にサイバーセキュリティに関連するご意見、ご要望等がありますか。

Q３４.　ご回答頂いた方のお立場をお答えください。
複数兼務している場合は、メインの役職をひとつ選んでください。＊

- ○ 理事長
- ○ 院長
- ○ システム担当
- ○ 事務長
- ○ その他（　　）

お忙しいところ、ご協力頂き誠にありがとうございました。
頂いた内容は、より良い医療政策の実現に向けた
調査研究と政策提言のために活用させて頂きます。

医療機関の情報システムの管理体制に関する実態調査

日本医師会
Japan Medical Association

公益財団法人
医療機器センター