医療機器のサイバーセキュリティ導入に関する手引書案に係る御意見の募集の結果について

令 和 ５ 年 ３ 月 31 日
厚生労働省医薬・生活衛生局
医 療 機 器 審 査 管 理 課

医療機器のサイバーセキュリティ導入に関する手引書案について、令和４年 12 月 26 日から令和５年１月 25 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

医療機器のサイバーセキュリティ導入に関する手引書案について

No.	寄せられた御意見の概要	回答
1	74 行に関して御意見申し上げます。 1.「医療機器製品」を「医用電気機器」及び「ソフトウェア」（プログラムも可）に変更する。 サイバー攻撃の対象となるのは，ガーゼ，ピンセットのような非電気製品ではなく，医用電気機器又はソフトウェアに限定されるため，誤解なきようにする。 2.「安全性と基本性能」を「基礎安全及び基本性能」に変更する。 医用電気機器の安全は JIS T 0601-1 によって「基礎安全」及び「基本性能」が確保されていることとされている。 「安全性と基本性能」では,「基本性能」が安全性に関係しない別の用語だと誤解される恐れがある。 3. 上記から巻末の「文献」に JIS T 0601-1 を追加する。 但し，この手引書の発行が JIS T 0601-1:2023(2 月頃発行）より後ならば，JIS T 0601-1:2023 とする。 4. 上記から巻末の「用語及び参考定義」に「基礎安全」と「基本性能」の 2 つを追加する。 「基本性能」が機器の「代表的な機能」と誤解されるケースが多いことから，JIS T 0601-1 に定義されている意味を持つことを明確に示す必要がある。 以上です。	1-1 サイバー攻撃を受ける対象が誤解されないよう「医療機器製品」を「プログラムを用いた医療機器」に修正します。 1-2 プログラムを用いた医療機器の安全性と有効性の両方を確保する必要があることから、「安全性と有効性」に修正します。 本手引書はプログラムを用いた医療機器全般におけるサイバーセキュリティ対策を講じることを目的とするものであり、医用電気機器固有の JIS 規格を参照することは適切ではないと考えます。
2	目次があった方が良い。 本改訂により、36 ページにもなり、このページ数になると目次がないと使いづらく、また目次を見ることで手引きの趣旨が把握できる。欧米及び IMDRF のサイバーセキュリティガイダンスにはすべて目次がある。	ご意見ありがとうございます。追加いたします。
3	(1)　行番号付きで公表され、コメントをする際、指摘箇所が特定しやすくなっていて非常に便利である。しかし、PDF で公開されているが、しおりがついていない。電子的な可読性を考慮するとしおり付き PDF が必須ではないかと思います。Word で見出しを適切に設定していれば、しおり付き PDF は、簡単に作成できる。これができていないと、デジタルのリテラシー不足が疑われ、内容に関してもデジタルのリテラシーがないのではないかと誤解を与える可能性がある。	ご意見ありがとうございます。今後の参考とさせていただきます。
4	(2)　前回の手引書(「医療機器のサイバーセキュリティの確保及び徹	前回の手引書との関

	底に係る手引書について」(令和３年 12 月 24 日付け 薬生機審発 1224 第１号、薬生安発 1224 第１号))との関係が全く記載されていない。最低限、前記の手引書の改訂である点、前回の版は今回の版で置きかわる点について明記すべきだと思います。例えば、50 行目の「～さらに国内運用における考慮事項を加えて改訂し」のあたりに追記する。	係については本手引書発出の際に示す通知にて説明いたします。
5	(3)　　前回の版との変更履歴付きの版も公表していただくと、前回の版で体制、システム等を構築している企業にとっては役にたつと考えます。）	ご意見ありがとうございます。今後の参考とさせていただきます。
6	p.1　16 ・「除去」とあるが、危険性を完全に除くことは難しく、その証明も現実的ではないため、「緩和」等の表現に修正してほしい。	原案のままとします。完全に除去することを求めるものではなく、ここでは、原則としてリスクの除去を行うように努める必要があることを示しています。
7	(4)　　48 行目：括弧が１つ余分になってしまっている。((以下、これら２つの追補を含めて「IMDRF ガイダンス」という）	ご意見を踏まえ、修正いたします。
8	44～52 行目：追補 N70 と N73 はまだ発行されていませんが、手引書はこれらが発行された後、その内容が適切に反映されていることを確認された上で、改訂されるのでしょうか。	IMDRF CS-WG での検討内容を踏まえて作成しています。
9	(5)　　60 行目：誤植「国立研究開発法人日本医療機器研究開発機構(AMED)」とあるが「機器」が余分である。つまり、「国立研究開発法人日本医療研究開発機構（AMED)」	ご意見を踏まえ、修正いたします。
10	p. 2　60-67 ・「この文書は、IMDRF ガイダンスの内容を基本としているが…我が国の状況にあわせて必要な編纂をしている。」とあるが、IMDRF との差異を明確化してほしい。	44-52 行に差異を記載しています。
11	75 行目：「患者等」の「等」に何が含まれるのか定義されていません。	患者だけでなく、使用者も含まれます。
12	(6)　　79 行目：「附属品」とあるが、本邦の医療機器規制の文脈では、「附」ではなく、「付」を用いて「付属品」との表記が使われている。	過去の通知等に揃え、「附属品」のままといたします。
13	箇所：77～80 行 記述内容：この文書は、無線又は有線により、メディア媒体を含む他の機器、ネットワーク等との接続が可能なプログラムを用いた医療機器（ソフトウェア単独で医療機器となる医療機器プログラム（Software as a Medical Device: SaMD）を含む）及びプログラムを用いた附属品（医療機器の薬事承認等範囲内の構成品）等に関するサイバーセキュリティを対象	ご意見を踏まえ、「また、医療機器の保守を目的として構成されるプログラムを用いた周辺機器についても契約等に応じて対

	とする。 対応案：この文書は、無線又は有線により、メディア媒体を含む他の機器、ネット ワーク等との接続が可能なプログラムを用いた医療機器（ソフトウェア単独で医療機器となる医療機器プログラム（Software as a Medical Device:SaMD）を含む）及びプログラムを用いた附属品（医療機器の薬事承認等範囲内の構成品）等に関するサイバーセキュリティを対象とする。また、医療機 器の運用や保守を目的として構成される各種周辺機器についても薬事承認の 範囲内の構成品に準じて対象とする。 理由：医療機器単体のセキュリティ確保だけでなく、その機器を導入、運用する際に構成される周辺装置の設計、運用において十分な安全確保が行われていないケースが多く、病院システム全体にダメージを与える事案が頻発している。病院システム全体へのダメージは患者の医療安全リスクにも影響を及ぼすインシデントと考えるべきであり、医療情報システムの安全管理に関するガイドラインに押し付けず、医療機器の導入、運用に関する範囲の中で求めるべきことを示すべき。 その一つであるリモートアクセスに関しては、表 1. 医療機器 150 の設計における検討事項に対する設計原則 にも示されているわけなので、目的の部分できちんと示すべき。	象とする。」 を追加いたします。
14	p.4　108 ・「脆弱性修正」とあるが、『5.2　TPLC に関するリスクマネジメント原則』における「リスクを受容可能なレベルまで低減する」という目標に合わせるため、「脆弱性緩和」に修正してほしい。	原案のままとします。 ここでは、原則として脆弱性がなくなるように修正して行うように努める必要があることを示しています。
15	p.4　110 ・「継続的な情報共有及び連携」とあるが、24 時間体制で監視する必要があるとも読めるため、「定期的な情報共有及び連携」に修正してほしい。	過去から現在までの一連の情報共有・連携が必要であることから「継続的」としており、原案のままといたします。
16	箇所：117～119 行 記述内容：製造販売業者は、国際整合化の背景及び「共同責任(Shared Responsibility)」における自らの責任を理解し、サイバーセキュリティベースラインを構築した上で、医療機関、使用者、規制当局及び脆弱性発見者等のステークホルダーと連携可能な体制を整備する。 対応案：　製造販売業者は、国際整合化の背景及び「共同責任(Shared Responsibility)」における自らの責任を理解し、サイバーセキュリティベースラインのセキュリティアシュアランスケース（セキュリティベースラインがどのような利用環境におけるリスクを想定しているかの明確化及	セキュリティアシュアランスケースの考え方は非常に重要ですが、様々な機能、情報接続の形態を有する医療機器において、全ての品目についてセキュリティアシュアランスケース

	び、その合理的十分性の説明）を構築し、医療機関、使用者、規制当局及び脆弱性発見者などに開示し、ステークホルダーと連携利用環境におけるリスクマネジメントに十分な情報を与える目的で開示し、連携可能な体制を整備する。 理由：サイバーセキュリティ対策は、医療機関、使用者において、利用環境においてのリスクマネジメントの一部としてリスクがコントロールされていなければならない。そのため、サイバーセキュリティベースラインは、医療機関、使用者においてのリスクマネジメントに必要となる情報を適切に開示する必要があるため。	の確立を求めることは難しいと思われます。 ここでは、セキュリティベースラインの構築とステークホルダーとの連携体制の整備が重要であることを記載するものであり、原案のままといたします。 セキュリティアシュアランスケースは全てのプログラムを用いた医療機器ではなく、セキュリティベースラインの構築とステークホルダーとの連携体制の整備が重要であることを記載するものであり、原案のままといたします。
17	(7)　150 行目表 1 データ保護：「例えば、パスワードは、暗号化によって保護されたハッシュとして保存する。」は、原文では For example, passwords should be stored as cryptographically secure hashes. なので、「例えば、パスワードは、暗号的に安全なハッシュとして保存する。」のほうがいい。	ご意見を踏まえ、「暗号学的に安全なハッシュとして保存する。」と修正いたします。
18	(8)　150 行目表 1 機器の完全性：「製造販売業者は、データの否認防止を確保できる設計特性の要否を判断するために、監査ログ機能のサポート等、システムレベルのアーキテクチャーを評価する。」は、少し日本語的に不自然に思える。変更案として、「製造販売業者は、監査ログ機能のサポート等のデータの否認防止を確保できる設計特性の要否を判断するために、システムレベルのアーキテクチャーを評価する。」	ご意見を踏まえ、「製造販売業者は、監査ログ機能のサポート等のデータの否認防止を確保できる設計特性の要否を判断するために、システムレベルのアーキテクチャーを評価する。」と修正いたします。
19	(9)　150 行目表 1 ソフトウェア保守：「安全でないバージョンの OS」は少し正確ではないのではないか。医療機器の規制上では、「安全」は	ご意見を踏まえ、「古いバージョンの OS」に

	Safety を示す場合が多い。ここでは文脈からは secure とか outdated とかにしたほうがいい。変更案「古いバージョンの OS」	修正いたします。
20	(10)　150 行目表 1 物理的アクセス :「未承認者による医療機器へのアクセスを防止する手法」は、未承認者が、少しわかりにくい。(変更案)「許可されていない者による医療機器へのアクセスを防止する手法」	ご意見を踏まえ、「許可されていない者」に修正します。
21	(11)　150 行目表 1 物理的アクセス :「ポートを物理的にロックする、ポートへのアクセスを物理的に制限する又は必要な認証なしに物理ケーブルを用いたアクセスを禁止する等の手法を検討する。」は、少し日本語が不自然に思える。(変更案)「～又は必要な認証なしでは物理ケーブルを用いたアクセスを禁止する等～」	明確化のため、「ポート」を「ネットワークポート」に修正いたします。 また、「必要な認証なしに物理ケーブルを用いてアクセスすることを禁止する等」に修正いたします。
22	(12)　150 行目表 1 リモートアクセス :「また、医療機器として使用するネットワークポートとは異なるポートを使用する、又は別の LAN 回線を使用する等専用の接続手段を用いる。」と記載されているが、リモートアクセスへの侵害が医療機器の機能に影響を与えないためには有効な場合が多いが、別ポート、別 LAN にすることにより守るべき箇所が複数になる(通常、病院では多数の医療機器が管理されている)欠点もある。このため、別にすることを必須になるような記載にすべきではない。 (変更案) また、医療機器として使用するネットワークポートとは異なるポートを使用する、又は別の LAN 回線を使用する等専用の接続手段を用いることにより、リモートアクセスが侵害されたときに医療機器の機能への影響を小さくできる場合がある。しかし、複数のポート、LAN 等を管理しなければいけないデメリットもある。これらのような検討を実施する。 (A)　150 行目表 1 信頼性及び可用性 :「SaMD 以外のソフトウェアの入れ替えが比較的少ない医療機器への利用に適している」と記載されているが、複数の区切りで読めてしまう。特に「SaMD 以外」がどこにかかるか読みづらい。 SaMD 以外の～医療機器への利用に適している (B)　SaMD 以外のソフトウェア～ (C)　SaMD 以外の～入れ替え ここでは、ホワイトリスト型は適している場合を記載されているので、SaMD を記載をわけたほうがよりはっきりするのではないか。 ホワイトリスト型はソフトウェア入れ替えが少ない場合に適している。 SaMD は、一般 PC 等に実装した場合、実行環境のソフトの入れ替えが多い場合が多い SaMD でも他の医療機器に実装した場合は、ソフトウェアの入れ替えが少ない場合が多い。 (変更案)	ご意見を踏まえ、「また、汎用で使用するネットワークポートと同じポートだが異なるネットワークポート番号を使用する、又は別の LAN 回線を使用する等、専用の接続手段を用いる等のリスク低減策の他、使用環境に必要なリスク回避策を講じる。」に修正いたします。 ご意見を踏まえ、「SaMD 以外の」を削除いたします。

	ソフトウェアの入れ替えが比較的少ない医療機器への利用に適している。SaMD は汎用 PC 等に実装した場合は、その実行環境のソフトウェアの入れ替えが多い場合が多く向いていない場合が多い。	
23	150 行目、表 1（ソフトウェア保守）：ソフトウェアの更新/パッチの適用については、共同責任があります。 ソフトウェアのパッチ/更新を作成するための製造業者の役割と責任は明確されていますか。 さらに、医療従事者、患者、消費者の役割と責任もサイバーセキュリティ エコシステムで定義し、メーカーが提供するソフトウェアのパッチと更新を適用するべきです。	製造販売業者の責任については表 1 にて明確にしておりますが、医療従事者・患者・消費者の役割と責任についての定義づけは本手引書では行っておりません。 いただいたご意見について、今後の参考とさせていただきます。
24	箇所：P.7 表 ソフトウェア保守 記述内容：製造販売業者は、定期的なアップデートの実施プロセスと展開プロセスを確立し、そのアップデート情報を共有する。 対応案：製造販売業者は、定期的なアップデートの実施プロセスと展開プロセスを確立し、そのアップデート情報を使用者である医療機関へ共有する。 理由：アップデート情報の共有対象が不明確。ユーザーに情報提供することを明示すべき。	ご意見を踏まえ、「そのアップデート情報を医療機関及び使用者へ共有する。」に修正いたします。
25	箇所：P.7 表 ソフトウェア保守 記載内容：製造販売業者は、オペレーティングシステム（以下 OS という）、オープンソース等のサードパーティ製ソフトウェアのアップデート手法及び管理方法について検討する。また、製造販売業者は、ソフトウェアのアップデートや、安全でないバージョンの OS 上で動作する医療機器ソフト ウェア等、サポートが終了し、管理対象外となった古い OS 環境への対処方法計画を立案する。 対応案：製造販売業者は、オペレーティングシステム（以下 OS という）、オープンソース等のサードパーティ製ソフトウェアのアップデート手法及び管理方法について検討する。また、製造販売業者は、ソフトウェアのアップデートや、安全でないバージョンの OS 上で動作する医療機器ソフトウェア等、サポートが終了し、管理対象外となった古い OS 環境への対処方法計画を立案、使用者である医療機関へ情報を共有し、対応方法を協議する。 理由：使用者である医療機関に対して情報提供、提案することを前提とした検討を求めるべき。実施におけるコストが生じることは否めないが、説明がなされずうやむやにされる状況は許されるべきではない。	ご意見を踏まえ、「立案し、医療機関及び使用者へ共有する。」に修正いたします。
26	箇所：P.7 表 リモートアクセス 記述内容：製造販売業者等は、運用支援、医療機器の保守点検、修理等の	ご意見を踏まえ、「また、医療機器として使

	機能・効率向上のため、リモートサービスを利用して遠隔地からアクセスして作業を行う場合がある。この場合、アクセス経路のセキュリティ確保に加え、医療機器におけるアクセスログ等の収集、作業終了に関する医療機関等の責任者による確認等のための手法を検討する。また、医療機器として使用するネットワークポートとは異なるポートを使用する、又は別の LAN 回線を使用する等専用の接続手段を用いる。 対応案：製造販売業者等は、運用支援、医療機器の保守点検、修理等の機能・効率向上のため、リモートサービスを利用して遠隔地からアクセスして作業を行う場合がある。この場合、アクセス経路のセキュリティ確保に加え、医療機器におけるアクセスログ等の収集、作業終了に関する医療機関等の責任者による確認等のための手法を検討する。また、医療機器として使用するネットワークポートとは異なるポートを使用する、又は別の LAN 回線を使用する等専用の接続手段を用いることはリスク低減方法の一つであってリスク回避にはならないことに留意する。 医療機関からの求めに応じてセキュリティの管理状況について説明出来るようにする。 理由：踏み台端末、踏み台サーバを介して医療機器や HIS 内部ネットワークに接続するケースでもサイバー攻撃による侵害が発生しうることを意識する必要がある。事業者によって設置されたアクセスポイントとその関連機器についての管理状況について説明を求めても情報開示しない事業者が存在するため、必要に応じて情報開示すべきことを示すべき。	用するネットワークポートとは異なるポートを使用する、又は別の LAN 回線を使用する等、の専用の接続手段を用いる等の リスク低減策の他、使用環境に必要なリスク回避策を講じる。 製造販売業者は、作業開始前、終了後において、その内容及び結果について、医療機関に対して説明を行い、医療機関の求めに応じてセキュリティの管理状況についても説明できるようにする」に修正いたします。
27	p.8　170　5.3 セキュリティ試験 ・設計開発においてどのようなセキュリティ試験を行っていれば十分と判断できるのか考え方を示してほしい。	設計におけるリスクコントロールを評価できる試験を意図しており、個別の製品によって異なるため、考え方を示すことは控えさせていただきます。
28	該当箇所 5.3. セキュリティ試験 187 意図する使用及び予見可能な誤使用に起因する危険性を評価し、合理的に実行可能な限り除去した上 188 でもなお、脆弱性が悪用された場合に予見可能な患者の安全に対する影響が大きい製品は、侵入試験を実 189 施する場合もある。これらの試験について、経済産業省が策定した「情報セキュリティサービス基準」に 190 適合したと認められた事業者の脆弱性診断サービス（IPA 提供）や同省に登録された登録認証機関による 191 第三者試験も利用可能である。	これらの試験では必ずしも第三者試験を要求しているわけではなく、事業者のコンピテンスが適切であれば、認定機関の適合証明書等を利用することで差し支えありません。

	意見 これらの試験について、経済産業省が策定した「情報セキュリティサービス基準」に適合したと認められた事業者の脆弱性診断サービス（IPA 提供）や同省に登録された登録認証機関による 第三者試験も利用可能である。」とあるが、『平成 27 年 1 月 20 日薬食機参発 0120 第 9 号　医療機器の製造販売承認申請書添付資料の作成に際し留意すべき事項について』の 4.　設計検証及び妥当性確認文書の概要のなお書き「International Laboratory Accreditation Cooperation(ILAC)若しくは Asia Pacific Laboratory Accreditation Cooperation(APLAC)に加盟する認定機関による国際標準化機構の定める試験所並びに校正機関の能力に関する一般要求事項(ISO17025)適合の認定を受けた機関若しくは工業標準化法(昭和 24 年法律第 185 号)第 57 条第 1 項に基づく登録(JNLA 登録)を受けた機関によって規格への適合が確認されている場合は、その旨記載の上、その適合証明書を添付することで差し支えないこと。」は当該セキュリティ試験についても適用との理解で良いか。	
29	●5.3 セキュリティ試験（187 行～189 行） 本手引書では、患者安全に大きな影響がある製品は、侵入試験を実施する場合もある、と記載され、侵入試験は、患者安全に大きな影響がある製品に限定し、かつ必ずしも実施しなくても良いような表記になっている。いっぽう、基本要件基準に適用予定の JIS T81001-5-1 では、以下のように医療機器の設計開発プロセスに従って異なるタイプの試験を実施する要求事項になっている。5.7.1～5.7.3 が設計検証に相当し、5.7.4 が攻撃者視点でのセキュリティの最終確認である設計バリデーションに相当する内容である。 5.7.1 セキュリティ要求事項試験　⇒セキュリティ要件の実装確認 5.7.2 脅威軽減試験　⇒個々のセキュリティリスクコントロール手段の実装及び有効性の確認 5.7.3 ぜい（脆）弱性試験　⇒潜在的な脆弱性（既知の脆弱性が主体）を検出する各種のセキュリティ試験 5.7.4 侵入試験　⇒製品の連鎖した脆弱性を突くなどして、攻撃者が実際に侵入できるかどうかという点に着目して検査を行う試験 同規格には、侵入試験に対して実施の条件などは付けられていない。また、本手引書のベースである IMDRF のガイダンスや FDA サイバーセキュリティガイダンス（2022 年発行のドラフト）にも侵入試験に対する実施条件は付けられていない。国内（薬機法下）及び国際間でのセキュリティ規制は整合（調和）すべきと思う。 （変更提案） その１：187 行～189 行を削除し、以下を記載する。	手引書は、侵入試験を含めた各試験の必要性について記載をしているものではないことから、原文のままといたします。

	『侵入試験を実施する。但し、侵入試験を実施しない妥当な理由がある場合は、その理由を文書化する。』 その２：侵入試験を含むセキュリティ試験は、JIS T81001-5-1 の規格書本文及び附属書 B に詳細が記載されているので、手引書では、同規格を参照する体裁とし、必要な情報のみを補足する。	
30	p.9　189-191 ・利用可能な試験に、国際的に認められた機関である CREST や、NIST 等の国際規格に則った試験も含めていただきたい。 ・本手引書中に利用可能な機関等を明確なリストとして記載していただきたい。	そのような試験を行うことは問題ありません。現時点では具体的な試験や試験機関のリストの作成は検討していませんが、今後の参考とさせていただきます。
31	p.10　209 ・「このような場合」とあるが、使用する汎用 OS 等ソフトウェア汎用部品の EOL が市販前にわかっている場合を想定していると思われるので、「使用する汎用 OS 等ソフトウェア汎用部品の EOL がすでに明確な場合に限って、開示する」と明確にしていただきたい。	EOL は市販前の段階で予め計画されているべきものであり、EOS が EOL に先行する場合には、世代の異なる部品の使用又は部品の切替えを含むアップデート等を市販前に計画し、顧客又は規制当局に開示できるようにすることについて記載しています。従って、EOL が明確か否かで開示の有無が決まる訳ではないため、原案のままといたします。
32	箇所：218～219 行 記述内容：意図する使用環境、使用者の遵守事項（概要）、要求された環境外で使用した場合のリスク等 対応案：意図する使用環境、使用者の遵守事項（概要）、要求された環境外で使用した場合のリスク等。長期間にわたる運用の中では OS 等システムを構成するソフトウェアにおいてセキュリティパッチの適用が必要になることが想定され 理由：セキュリティパッチすら適用すると保守から外れるといわれるケースが多数である。医療機関の環境を現実的に捉えた想定環境設計をする必要がある。	市販前に、セキュリティパッチの適用等の長期間運用の計画を立てることで、保守から外れないものとなるため、原案のままといたします。

33	P.11　234　5.5.2 顧客向けセキュリティ文書 ・「顧客向けセキュリティ文書」とあるが、図１の記載「セキュリティ開示文書」とあえて違うワードを使用しているのか。同じ意味であれば用語を揃えてほしい。 ・図１の「セキュリティ開示文書」では顧客向け文書として MDS が含まれているが、5.5.2 では MDS について触れられていない。MDS を顧客に提供する必要があるのかを 5.5.2 の中で明確にしてほしい。	医療機器のセキュリティの状態を開示するための文書（MDS2、SBOM）が含まれることを表すために「セキュリティ開示文書」というワードを使用しています。MDS は医療情報セキュリティにかかる顧客向け文書であり、本手引書で扱う医療機器セキュリティとは違うことから、図１を削除するとともに、記載から削除いたします。
34	P.11　236 ・図１では「セキュリティ開示文書」として MDS、MDS2、SBOM の三つが挙げられているが、「運用環境のための技術的要求事項等」はどの文書を指しているのか、用語を整理してほしい。	「運用環境のための技術的要求事項等」については、5.5.2 に記載しています。
35	P.11　237-257 ・図１では「セキュリティ開示文書」として MDS、MDS2、SBOM の三つが挙げられているが、237-257 の各情報が図１のいずれの開示文書に含まれるべきか明確にしてほしい。	MDS2,SBOM については 5.5.2 に記載しています。 図１は MDS を整備することで医療機器サイバーセキュリティの開示書となるような誤解を招く可能性がありますので、削除します。
36	箇所：245～245 行 記述内容：・医療機器製品に実装されている自製（開発委託したものも含む)、オープンソース及び市販のソフトウェア部品（製品コンポーネント）の透明性を確保するための SBOM 対応案：・医療機器製品に実装されている自製（開発委託したものも含む)、オープンソース及び市販のソフトウェア部品（製品コンポーネント）の透明性を確保するための SBOM ・医療機器製品に実装されている自製（開発委託したものも含む)、オープンソース及び市販のソフトウェア部品（製品コンポーネント）についての脆弱性修正プログラム（セキュリティパッチ）を適用するための方針、原則	SBOM だけでなくアドバイザリー情報の提供を求めています。SBOM を含む医療機関における医療機器の情報については、医療機関におけるインデント対策等の構築に用いることと今後発出する医療機関における医療機器のサ

	理由：SBOM を提供すれば医療機関が後は全て調べるもの、ということになると医療機関側の負担が大きすぎるため、事業者側から情報提供はもちろん、適用方針、せめて基本的な考え方について示すべき。	イバーセキュリティ確保のための手引書で示すものです。
37	箇所：268～273 行 記述内容：合理的に予見可能な実使用環境を考慮した上で、使用者のフィードバックを反映させながら、医療機器製品の注意事項等情報、取扱説明書及び顧客向けセキュリティ文書を更新し、拡充する。さらに、在宅医療機器等、患者自身が操作することを意図している医療機器については、通常の使用方法に加えて、基本的なサイ バーセキュリティに関するトレーニングを患者に対しても行うことが求められるので、製造販売業者は、これを支援できるレベルの情報提供が必要となる。 対応案：重要な前提条件なので、235～236 行の段落で示したほうが良いと思われる。 理由：重要な点をより分かりやすく示すことが期待される	当該記載を 5.5 の下へ移動します。
38	P.12　276-282 ・具体的な関係法令が定まっていないため以下の記載の削除を希望する。 276 「リスクマネジメント活動に基づき、次の文書を提出することとなるが、」 277 「(承認申請書、STED、SBOM、MDS2 等がこれらに含まれる)」 278-282 「セキュリティに関連する…セキュリティ文書」	具体的な文書の内容については、現時点では定まっておらず、追って通知等により示す予定です。従って、ご指摘の記載箇所については削除いたします。
39	p.13　299 ・「MDS2 及び SBOM 等の顧客向け文書」とあるが、「等」に何が含まれるのか不明瞭なので明確にしていただきたい。	5.5.1、5.5.2 に記載されている文書が含まれます。
40	312 行目：ISAO/CERT について、日本における組織を具体的に示してください。	JPCERT/CC、医療セプターを本手引書内で紹介しています。
41	(13)　325 行目：「既知のインシデント情報」とあるが、IMDRF の原文では「Confirmation of incidents (e.g. “Are you seeing this too?”)」となっていて異なった意味になってしまっている。原文では、インシデントの確認方法とあるので、こちらに合わせたほうがいい。 (変更案) インシデントの確認方法(何があらわれているか？)	ご意見を踏まえ、「インシデント発生時の確認事項」に修正いたします。
42	336 行目：規制当局等について、「等」に含まれるものを具体的に示してください。	規制当局以外の経済産業書等の行政機関、工業会、JPCERT/CC 等があります。
43	箇所：368～370 行 記述内容：製造販売業者は、緊急性を伴う場合で、迅速な対応が困難と判断した場合には、一時的な機能の使用停止、設定変更等の応急的な処置に	ご意見ありがとうございます。本手引書は医療機器の製造販売

	関する情報をセキュリティアドバイザリーとして医療機関へ提供する。 対応案：製造販売業者は、緊急性を伴う場合で、迅速な対応が困難と判断した場合には、一時的な機能の使用停止、設定変更等の応急的な処置に関する情報をセキュリティアドバイザリーとして医療機関へ提供する。医療機器の導入に伴い併せて導入される周辺機器やソフトウェアについても同様とする。 理由：薬機承認の医療機器に限った対応ではなく、併せて導入される周辺機器、OS やソフトウェアなども対象とするのが現実的。	業者を対象とするものであり、ご指摘の内容は本手引書に含めるべきではないと考えます。従って、原案のままとさせていただきます。
44	箇所：405 行 記述内容：D. 医療機器の誤動作又は不正動作 対応案：D. 医療機器の停止、誤動作又は不正動作 Availability への影響として停止も追加。 理由：遅延（使用に耐えない遅延）は不正動作の範疇として考えるか、別途書き足す。	ご意見を踏まえ、「医療機器の機能停止、誤動作又は不正動作」に修正いたします。
45	箇所：410～411 行 記述内容：パケットフィルタリング等が強化されたファイアウォール（表 3 参照）等によって防御する。 対応案：パケットフィルタリング等が強化されたファイアウォールや IPS（侵入防御システム）（表 3 参照）等によって防御する。 理由：許可されたポートで攻撃が展開される場合にはファイアウォールでは無力であり、ネットワーク IPS も選択肢として考えられる。	「パケットフィルタリング等が強化されたファイアウォール、IPS（表３ 参照）等」に修正します。
46	396～439 行目：顧客には、サイバーセキュリティのインシデントやイベントを報告するため、または通常の顧客サポートチャネルを通じて提出するために、医療機器メーカーの連絡先情報を提供する必要はないでしょうか。	医療機器製造販売業者の連絡先情報については、個別の医療機器の添付文書に示しています。
47	429~435 行目：製造販売業者は、JPCERT/CC に必ずコミュニケーションしなければならないのでしょうか、それとも別の CERT 組織にコミュニケーションすることでもよいのでしょうか。	JPCERT/CC については、ソフトウェアに脆弱性が発見された場合の脆弱性情報の登録、及びスムーズな脆弱性情報の収集に利用できる組織の一例となっております。必ずしも JPCERT/CC のみに限定するものではありません。
48	p.19　464 表 2 各マイルストーンにおける医療機関に提供する情報 ・図１ではセキュリティ文書の中に MDS2 と SBOM が含まれているが、表 2 では「セキュリティ文書」と「MDS2、SBOM」が別のものとして記載されている。用語及び定義の整理をしてほしい。	表２で示すセキュリティ文書には SBOM や MDS２に関する記載がされるべきですが、当

	・MDS や添付文書の記載が表 2 から抜けていることは問題ないか。 ・表 2 の「アップグレード計画」は 5.5.2 の顧客向けセキュリティ文書に含まれていないため、整合を図っていただきたい。	該文書だけではなく、SBOM や MDS２本体についても医療機関に対して情報提供する必要があると考え、表２には分けて記載しています。従って、原案のままとさせていただきます。
49	(14)　473 行目：「～不具合等に関する情報収集義務（医薬品医療機器等法 68 条の２の５第１項)」とあるが、現時点の法では、「法 68 条の２の６第１項」にしたほうがいいのではないか。	「法 68 条の２の６第１項」に修正します。
50	(15)　490 行目：「～その仕様及び設定情報は、顧客向け文書に含める(5.5.1)。」とあるが、(5.5)を参照したほうがいい。5.5.顧客向け文書、5.5.1. 注意事項等情報及び取扱説明書、5.5.2. 顧客向けセキュリティ文書	医療機器がレガシー状態となった際に、限定的サポート段階の延長を行うための補完的対策について示した文章であり、5.5.1 の注意事項等情報及び取扱説明書で記載する「ファイアウォール等の補完的対策に関連する装置の設置・設定に関する情報」を指しているため、原案のままとさせていただきます。
51	p.22　558 ・「6.6.3 補完的リスクコントロール」とあるが、p.20 図 3 中の「補完的対策」と同じ意味を指しているのであれば、用語を統一してほしい。	表３の補完的対策を補完的リスクコントロールに修正いたします。
52	箇所：559 行 記述内容：ファイアウォール等の補完的リスクコントロール手段 対応案：ファイアウォールや IPS 等の補完的リスクコントロール手段 理由：IPS を追加	ファイアウォール等の「等」に IPS も含まれるため、原案のままとさせていただきます。
53	(16)　562 行目：「表 3 は、補完的リスクコントロールに対する一般的な推奨事項を示す。 実施にあたっては、特定の機器及びその運用環境に依存し、機器の臨床的な意図する使用を損なわないよう考慮する。」の「特定の機器及びその運用環境に依存し、」が少し不自然な日本語になってしまっている。 (変更案)「実施にあたっては、補完的リスクコントロールは特定の機器	ご意見を踏まえ、「補完的リスクコントロールが、特定の機器及びその運用環境に依存し、機器使用時の臨床的な意図を損なわ

	及びその運用環境に依存することに留意し、機器の臨床的な意図する使用を損なわないよう考慮する。」	ないよう考慮する」に修正いたします。
54	p.23　567　表 3：補完的リスクコントロール手段の例 ・「表 3：補完的リスクコントロール手段の例」を実施する主体が製造販売業者か医療機関なのかを明確にしてほしい。なぜなら、「物理的アクセスの制限」は医療機関が実施していただかなければならず、一方でファイアウォール、マルウェア対策等は製造販売業者でなければ実施できず、各補完的リスクコントロール手段を実施すべき主体が不明確であるため。 ・表 3 を EOS 前後で分けてほしい。なぜなら、EOS 以降は顧客に責任が完全に移転するため、EOS 前後での責任の所在を明確にするため。また、EOS 以降は製造販売業者による全てのサポートが終了となるが、現在の表では EOS 以降も製造販売業者が補完的リスクコントロール手段を講じる必要があるように読めてしまうため。	補完的リスクコントロールについては、製造販売業者と医療機関が協力して実施するべきものと考えています。個別の事例によって、各対応についての実施元が異なることが予想されるため、実施元についての明確な線引きは控えさせていただきます。 また、表３を EOS 前後で分けるご提案につきまして、EOS 以後は製造販売業者によるサポートは終了するものの、それを見越して EOS 前に補完的リスクコントロールの手段を取っておくことが求められていることから、EOS 前後で分けた記載は適切ではないと考え、原案のままとさせていただきます。
55	箇所：567 行 記述内容：表 3：補完的リスクコントロール手段の例 対応案：IPS（侵入防御システム）ネットワーク・ブリッジとして配置し、経路上の不正な通信を検知、設定に従って当該通信を遮断、防御する。機器の前段への配置し機器自体の脆弱性を保護する、リモートアクセスポイントの内側に配置し外部からの脆弱性攻撃から保護する、部門システム境界に配置し HIS 全体への攻撃拡散を防ぐ、といった方法がある。 理由：IPS を追加	IPS は表３に含まれています。
56	箇所：596～598 行 記述内容：販売業者は、製造販売業者、他の販売業者及び医療機関との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者より共有された SBOM、MDS2 その他 CVD に必要となる情報を他の医療機	6.2 で製造販売業者が使用者等との間でセキュリティパッチに関する情報提供を行

	関又は販売業者への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。 対応案：販売業者は、製造販売業者、他の販売業者及び医療機関との情報共有を行うために必要な体制を整備する。必要に応じて SBOM、MDS2 その他 CVD に必要となる情報提供やセキュリティパッチの適用等を適切かつ遅滞なく実施できるよう、必要な処置を行う。 理由：パッチ適用に関する情報は重要なので明示する	うことと明記されており、また 7.1 で製造販売業者は単一又は複数の販売業者を介しセキュリティパッチの適用を適切かつ遅滞なく実施できるよう必要な処置を行うことと明記されています。従って、原案のままとさせていただきます。
57	箇所：599～603 行 記述内容：修理業者は、医療機器の脆弱性情報等の情報共有を行う等の CVD に必要な情報共有が製造販売業者から得られるよう、適切な体制を構築する。また、医療機関及び販売業者と情報共有を行うために必要な体制を整備する。なお、必要に応じて、製造販売業者より最新の SBOM、MDS2 その他 CVD に必要となる情報を取得するとともに、医療機関又は他の販売業者への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。 対応案：修理業者は、医療機器の脆弱性情報等の情報共有を行う等の CVD に必要な情報共有が製造販売業者から得られるよう、適切な体制を構築する。また、医療機関及び販売業者と情報共有を行うために必要な体制を整備する。必要に応じて SBOM、MDS2 その他 CVD に必要となる情報提供やセキュリティパッチの適用等を適切かつ遅滞なく実施できるよう、必要な処置を行う。 理由：パッチ適用に関する情報は重要なので明示する	同上
58	箇所：618～621 行 記述内容：販売業者は、医療機関、製造販売業者、他の販売業者及び貸与業者との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者、貸与業者又は他の販売業者より共有された SBOM、MDS2 その他 CVD に必要となる情報を医療機関、他の販売業者又は貸与業者への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。 対応案：販売業者は、医療機関、製造販売業者、他の販売業者及び貸与業者との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者、貸与業者又は他の販売業者より共有された SBOM、MDS2 その他 CVD に必要となる情報提供やセキュリティパッチの情報等を医療機関、他の販売業者又は貸与業者への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。 理由：パッチ適用に関する情報は重要なので明示する	同上
59	箇所：622～625 行 記述内容：貸与業者は、医療機関、製造販売業者及び販売業者との情報共	同上

	有を行うために必要な体制を整備する。必要に応じて、製造販売業者又は販売業者より共有された SBOM、MDS2 その他 CVD に必要となる情報を医療機関への共有（販売業者を含む場合もある）を適切かつ遅滞なく実施できるよう、必要な処置を行う。 対応案：貸与業者は、医療機関、製造販売業者及び販売業者との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者又は販売業者より共有された SBOM、MDS2 その他 CVD に必要となる情報提供やセキュリティパッチの情報等を医療機関への共有（販売業者を含む場合もある）を適切かつ遅滞なく実施できるよう、必要な処置を行う。 理由：パッチ適用に関する情報は重要なので明示する	
60	箇所：626～630 行 記述内容：修理業者は、医療機器の脆弱性情報等の情報共有を行う等の CVD に必要な情報共有が製造販売業者から得られるよう、適切な体制を構築する。また、医療機関及び販売業者との情報共有を行うために必要な体制を整備する。なお、必要に応じて、製造販売業者より最新の SBOM、MDS2 その他 CVD に必要となる情報を取得するとともに、医療機関及び貸与業者への共有（販売業者を含む場合もある）を適切かつ遅滞なく実施できるよう、必要な処置を行う。 対応案：修理業者は、医療機器の脆弱性情報等の情報共有を行う等の CVD に必要な情報共有が製造販売業者から得られるよう、適切な体制を構築する。また、医療機関及び販売業者との情報共有を行うために必要な体制を整備する。なお、必要に応じて、製造販売業者より最新の SBOM、MDS2 その他 CVD に必要となる情報やセキュリティパッチの情報等を取得するとともに、医療機関及び貸与業者への共有（販売業者を含む場合もある）を適切かつ遅滞なく実施できるよう、必要な処置を行う。 理由：パッチ適用に関する情報は重要なので明示する	同上
61	箇所：646～650 行 記述内容：販売業者は、医療機関、製造販売業者、他の販売業者、貸与業者及び中古医療機器を取扱う販売業者との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者、他の販売業者、貸与業者及び中古医療機器を取扱う販売業者より共有された SBOM、MDS2 その他 CVD に必要となる情報を医療機関、他の販売業者、貸与業者又は中古医療機器を取扱う販売業者への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。 対応案：販売業者は、医療機関、製造販売業者、他の販売業者、貸与業者及び中古医療機器を取扱う販売業者との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者、他の販売業者、貸与業者及び中古医療機器を取扱う販売業者より共有された SBOM、MDS2 その他 CVD に必要となる情報提供やセキュリティパッチの情報等を医療機関、他の販売業者、貸与業者又は中古医療機器を取扱う販売業者への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。	同上

	理由：パッチ適用に関する情報は重要なので明示する	
62	理由：651～659 行 記述内容：中古医療機器を取扱う販売業者等（貸与業者が兼ねる場合もある）は、医療機関及び製造販売業者との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者又は販売業者より医療機関向けに共有される SBOM、MDS2 その他 CVD に必要となる情報を医療機関へ適切かつ遅滞なく共有（販売業者も含む場合もある）できるよう、必要な処置を行う。なお、中古医療機器を取扱う販売業者等は、使用された医療機器を他に中古販売する際、医療機関において適切なセキュリティ対応がとられるよう、使用された医療機器が EOL 又は EOS までの段階においては、製造販売業者（販売業者を含む場合もある）と必要な連携をとり、使用された医療機器の品質等に係る注意事項等の必要な処置について、使用された医療機器の製造販売業者から指示を受けた場合には、医療機関に対し提供をする。 対応案：中古医療機器を取扱う販売業者等（貸与業者が兼ねる場合もある） は、医療機関及び製造販売業者との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者又は販売業者より医療機関向けに共有される SBOM、MDS2 その他 CVD に必要となる情報提供やセキュリティパッチの情報等を医療機関へ適切かつ遅滞なく共有（販売業者も含む場合もある）できるよう、必要な処置を行う。なお、中古医療機器を取扱う販売業者等は、使用された医療機器を他に中古販売する際、医療機関において適切なセキュリティ対応がとられるよう、使用された医療機器が EOL 又は EOS までの段階においては、製造販売業者（販売業者を含む場合もある）と必要な連携をと り、使用された医療機器の品質等に係る注意事項等の必要な処置について、使用された医療機器の製造販売業者から指示を受けた場合には、医療機関に対し提供をする。 理由：パッチ適用に関する情報は重要なので明示する	同上
63	箇所：660～665 行 記述内容：修理業者は、医療機器の脆弱性情報等の情報共有を行う等の CVD に必要な情報共有が製造販売業者から得られるよう、適切な体制を構築する。また、医療機関及び販売業者との情報共有を行うために必要な体制を整備する。なお、必要に応じて、製造販売業者より最新の SBOM、MDS2 その他 CVD に必要となる情報を取得するとともに、医療機関又は他の販売業者（中古医療機器を取扱う販売業者等を含む場合もある）への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。 対応案：修理業者は、医療機器の脆弱性情報等の情報共有を行う等の CVD に必要な情報共有が製造販売業者から得られるよう、適切な体制を構築する。また、医療機関及び販売業者との情報共有を行うために必要な体制を整備する。なお、必要に応じて、製造販売業者より最新の SBOM、MDS2 その他 CVD に必要となる情報やセキュリティパッチの情報等を取得するとともに、医療機関又は他の販売業者（中古医療機器を取扱う販売業者等を	同上

	含む場合もある）への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。 理由：パッチ適用に関する情報は重要なので明示する	
64	(17)　720 行目：「～表 A-2 の要素を含むことが望ましい。」とあるが、表 2 は存在していない。表 3 の誤植。	図表は連番とし、表 4 に修正いたします。
65	(18)　722 行目表３「コンポーネントハッシュ」は、IMDRF の Cybersecurity の SBOM の追補版の案ではオプションになっている。必要性は理解できますが、IMDRF の趣旨でもある、国際的な規制調和の観点を尊重し、今回は IMDRF に合わせてオプションにしたほうがいいのではないかと思います。	ご意見を踏まえ、オプションに修正いたします。
66	(19)　745 行目：「表 A-2 に示す要素を表形式で表すと例えば表 A-4 の～」と記載されているが、表 A-5 の誤植。	図表は連番とし、表 5 に修正いたします。
67	(20)P16 用語及び参考定義（五十音順）の PSIRT PSIRT Services Framework 1.0 日本語版のハイパーリンクが表示だけでなく、リンクも 2 行にわかれてしまい、クリックしてもそこが開かない状態になっている。 https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Fra mework_v1.0_jp.pdf	ご意見ありがとうございます。パブコメ版ではリンクを削除していましたが、発出版ではリンクを反映いたします。
68	(21)P16 用語及び参考定義（五十音順）のファジング https://www.ipa.go.jp/security/vuln/fuzz_faq.html は、表記はあっているがクリックしても URL が適切でなく、所望の Page に飛ばない。	ご意見ありがとうございます。パブコメ版ではリンクを削除していましたが、発出版ではリンクを反映いたします。
69	●EOL の定義（811 行） 『製品のライフサイクルにおいて、製造業者が定めた有効期間を超えた製品の販売を終了し、製品について正式な EOL プロセス（顧客への通知等）を実施する段階。』 EOL は製品のライフサイクルの特定の段階を定義するものだが、有効期間という用語は、個々の医療機器の使用期限や耐用年数のイメージがある。また、IMDRF 原文から、製造業者が定めるのは、有効期間ではなく、EOL と解釈できる。 （変更提案） 以下のように記載する。 『有用な期間を超えた製品の販売を終了し、製品について正式な EOL プロセス（顧客への通知等）を実施する、製造業者が定める製品のライフサイクルの段階。』	製造業者が製品の有効期間を定めた上で EOL の時点も決定されること、また製品の有効期間については耐用年数等を考慮して設定されるものであることを考慮し、原案のままとさせていただきます。