医療機関における医療機器のサイバーセキュリティ確保のための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

医療機関における医療機器のサイバーセキュリティ確保のための手引書案について、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

医療機関における医療機器のサイバーセキュリティ確保のための手引書案について

No.	寄せられた御意見の概要	回答
1	(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に不足が疑われ、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。さらに、強調のための下線付き青字にしているが、一般的には、下線付き青字は、慣例としてハイパーリンクで多用されているため、ハイパーリンクであると思うかたが特にデジタルに明るい方には多いと思われます。このため、強調に下線付き青字を使うべきではないとデジタルに明るい方は感じるのではないかと考えます。	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。
2	(2) 本手引書(案)は、医療期間のサイバーセキュリティ強化に非常に重要な文書であると認識している。また、サイバーセキュリティに対する脅威及びその対策は、日進月歩で変化している。このような状況から、本書を常に最新の動向に合わせた改正が必要であり、その改正の体制、スキームを計画段階から明確にしておく必要がある。 本書においても、次回改正予定を明確に記載して、改正の遅れによる陳腐化、医療機関のサイバーセキュリティリスクを低減させるべきではないか。	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。
3	(4) 本手引書(案)は、IMDRF のガイダンスは 2020/4 発行の N60 文書だけを参考にしている。しかし、本書と対になり、同時にパブコメ開始した「医療機器のサイバーセキュリティ導入に関する手引書」では、IMDRF の N60 だけでなく、より実践的なアプローチを規定した追補 N70「Principles and Practices for the Cybersecurity of Legacy Medical Devices」(レガシー医療機器のサイバーセキュリティの原則及び実践) 及び追補 N73「Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity」(医療機器のサイバーセキュリティのためのソフトウェア部品表の原則及び実践) を取り入れた手引書(案)を公開している。この違いが発生してしまい、医療機器の製造販売業向けの手引書と整合していない部分が存在してしまっている。	ご意見ありがとうございます。 製販業者向け手引書との整合性については、今後の手引書の改正等を通じて対応を検討いたします。
4	(5) 医療機関においては、サイバーセキュリティを強化のために本書以外に医療法の施行規則の改正(概要版が 12/16～1/16 でパブコメ)中であり、安全管理ガイドライン第 6 版の作成も進行中だと認識している。さらに、NISC からは「サイバー攻撃被害に係る情報の共有・公表ガイダンス(案)」が作成中(12/27～1/30 パブコメ)である。 これらの関係をもう少し整理して提示した方が、医療機関にとって、何をどのように実施するかの検討に役立つのではないかと思います。	ご意見ありがとうございます。 今後も多くの文書が発出されると考えますが、他文書との関係性については、今後発出予定の通知等をご参照ください。

5	医療機関における医療機器及び医療情報システムは、ネットワーク上のひとつの構成要素である。その各構成要素間にて患者情報等の医療情報の送受信が行われている。医療機器事業者は各医療機器、情報システムのアクセス制御の一元化、一般的な情報ネットワークへの接続性の担保、セキュリティ対策の自動化（アップデート）といった「医療機器事業者が行わなければならない事象」が本手引書には、具体的に示されていない。 また、セキュリティを検討するにあたり、医療機器を利用したワークフロー、データフローが具体的に示されていなく、ネットワークインフラ上のハードウェアに対する対策、手引きに留まっている。医療機関対する具体的な手引書であるためには、医療機関と医療機器事業者だけをステークホルダにするのではなく、規制当局を含めた、より実践的で分かり易い社会的対策を含めるべきではないか。具体的には、脆弱性が見つかり次第、医療機器事業者に対して「改修」などを命じることや、医療機関に「警告」する義務を設けるなどである。本手引きは「医療機関における」とされてはいるが、医療機関、利用者側、特に医療機器を有する部門の負担が極端に増大しているように思える。より現実的にステークホルダを網羅した内容の手引き書が必要なのではないでしょうか。	ご意見ありがとうございます。 製販業者が行うべきサイバーセキュリティ対策については、製販業者向けの手引書を通知にて発出予定です。 またステークホルダを網羅した内容の手引書のご提案につきまして、今後の参考とさせていただきます。
6	(3) 73 行目 図 1 非常にシンプルにわかりやすく書かれた図であるが、非常にミスリードしてしまう図になってしまっていると考える。医療機関は、医療情報システムと医療機器のセキュリティ対策をすればいいように見えてしまうし、そのような対応がさまざまで行われていると認識している。 しかし、例えば、EU の ENISA では、 https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services?v2=1 において、Remote Care system, Mobile Client Devices, Identification Systems, Building Management Systems, Networking Equipment, Medical Devices, Clinical Information Systems, Industrial Control Systems, Professional Services, Cloud Services の類型(Type)に分類して、抜けが生じないような網羅性を確保している。 日本において、T 県の H 病院では医療機器、医療情報システムの分類に入りづらい Remote Service の ICT 機器の脆弱性が攻撃され、O 府の O 病院では、クラウドを利用した委託事業者のシステムが攻撃された。 せめて、医療機器、医療情報システム以外にクラウド、ICT 機器は追加すべき。 本書が、医療機関で使用する医療機器に特化することは構わないが、医療機関ではその抜けが生じないような方策が必要になる。	ご意見ありがとうございます。クラウドや ICT 機器についても、医療機器のシステム構成図に含まれるものについては、医療機器のセキュリティ対策において適切に対応する必要があると考えています。 また、医療機関における幅広い範囲のセキュリティ対策については、安全管理ガイドラインにおいて、対策すべき事項が記載されていると認識しています。
7	箇所：76 行 記述内容：医療機器：薬機法（＊6）の対象となるものが医療機器です。ヘルスソフトウェアのうち薬機法の対象となる SaMD（Software as a Medical Device）も対象となります。	ご意見を踏まえ、「契約により構成、導入される保守のためのネットワーク機器やシステムも本書の

	対応案：医療機器：薬機法（＊6）の対象となるものが医療機器です。ヘルスソフトウェアのうち薬機法の対象となる SaMD（Software as a Medical Device）も対象となります。薬機法対象の医療機器の運用に付随して構成、導入されるネットワーク機器やシステムも本ガイダンスの対象となります。 理由：機器の運用、保守のために構成されるネットワーク機器やシステムが安全ガイドラインの範疇としてあいまいにされているが故に、バックドアとなる VPN アクセスポイントを開設しながら合理的、妥当な安全管理を果たさないという事態が起こっている現実に対応するため、薬機法の認証には直接含まれないものであっても医療機器の運用に付随して構成、導入されるものには本ガイダンスの中で言及、対応すべき。	対象となります。」を追記いたします。
8	箇所：78 行 記述内容：医療安全：本書では患者安全を中心に、使用者、医療従事者等の安全も含めます。 対応案：医療安全：本書では患者安全を中心に、使用者、医療従事者等の安全も含めます。 理由：医療機器が同じネットワークに接続される他の機器やシステムに影響を及ぼすことで患者安全にリスクが生じる可能性も含めます。　　当該医療機器が踏み台にされ他のシステムに影響を及ぼし、医療安全に影響が及ぶといった視点が必要。	ご意見を踏まえ、「医療機器が同じネットワークに接続される他の機器やシステムに影響を及ぼすことで患者安全にリスクが生じる可能性も含めます。」を追記いたします。
9	箇所：92～93 行 記述内容：医療機関における医療機器のサイバーセキュリティ対策を確実に行い医療機器の医療安全を確保することを目的に、医療機関が主体的に実施することを示し、加えて医療機器事業者やサービス提供者等のステークホルダーと連携して実施する内容およびその役割と責任について説明します。 対応案：医療機関における医療機器のサイバーセキュリティ対策を確実に行い医療機器の医療安全を確保することを目的に、医療機関が主体的に実施することを示し、医療機器事業者やサービス提供者等のステークホルダーと連携して実施する内容およびその役割と責任について説明します。 また、医療機器事業者やサービス提供者においては、医療機関が安全確保を遂行するための手段の提供や提案が必要であること。 理由：医療機器事業者やサービス提供者等が医療機器および医療機器が使用される環境に対しての安全を確保するための情報や手段の提供が必要であることを示すべき。 医療機関が責任を果たす上で、サプライヤーはそのための手段、または達成するための情報を提供すべきであることを明示すること。 医療機器そのものだけでなく、医療機器を運用、保守する上で付随する汎用のシステムやサービスも含めてサプライヤーの対応が必要であることを示すべき。	ご意見を踏まえ、「また、医療機器事業者及びサービス提供者が、医療機関が安全確保を遂行するために実施する取り組みについても紹介します。」を追記いたします。
10	箇所：107～115 行	ご意見を踏まえ、「な

	記述内容：医療安全についてサイバーセキュリティ上のリスクが懸念される医療機器を対象とします。具体的にはネットワークや機器との接続が可能であるプログラムを用いた医療機器であり、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（SaMD：Software as a Medical Device）を含みます。接続方法は有線、無線を問わず、接続対象の機器は他の医療機器、医療機器の構成品、USB メモリ等の携帯型メディアなどが含まれます。（図 2 参照） 対応案：医療安全についてサイバーセキュリティ上のリスクが懸念される医療機器を対象とします。具体的にはネットワークや機器との接続が可能であるプログラムを用いた医療機器であり、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（SaMD：Software as a Medical Device）を含みます。接続方法は有線、無線を問わず、接続対象の機器は他の医療機器、医療機器の構成品、USB メモリ等の携帯型メディアなどが含まれます。なお、医療機器事業者やサービス事業者が当該医療機器を保守するにあたって設置されるサーバや端末、ネットワーク機器などの医療機器認証に含まない周辺機器を含めて提供される場合においては当該医療機器を含む安全環境の維持に不可欠なものとして対象に含むべきものとする。 理由：医療機器事業者やサービス事業者が当該医療機器を保守するにあたって設置されるサーバや端末、 ネットワーク機器などの医療機器認証に含まない周辺機器を含めて提供される場合においては当該医療機器を含む安全環境の維持には不可欠なものとして医療機器に準じて周辺機器も含むべきものとする。	お、医療機器事業者やサービス事業者が当該医療機器を保守するにあたって、契約等によって設置するサーバーや端末、ネットワーク機器などの医療機器認証に含まない周辺機器を含めて提供される場合においては当該医療機器を含む安全環境の維持に不可欠なものとして対象に含むものとします。」を追記いたします。
11	該当箇所 113 114 115　図２ 本書で対象とする医療機器（イメージ）　について。 意見 ハードウェア有りについては、接続無し／接続有りで区別されている。一方ハードウェア無しの「医療機器プログラム（SaMD)」については、それをインストールする機器についての区別がされていないが、接続無しの機器にインストールされる可能性もある。「接続有りの機器にインストールする医療機器プログラム（SaMD)」としてはどうか。 意見（上記と同じ箇所） ハードウェア有りの医療機器について、接続無し／接続無しの区別は、通信機能の無し／有りでの区別と理解しても良いか。例えば、通信用のハードウェアを内蔵している機器及び接続ポートがある機器でも、通信機能が無ければ本書の対象外という理解で良いか。	ハードウェアの有無に関わらず、接続有りの医療機器が本手引書の対象となるため、図２に記載されていた「ハードウェアの有無」を削除いたします。 また、通信用のハードウェアを内蔵している機器及び接続ポートがある機器でも、接続が無ければ本書の対象外と考えています。
12	箇所：117～122 行 記述内容：医療機器に係るサイバー攻撃の被害により、医療安全に影響を	ご意見を踏まえ、「また、当該医療機器がサイバー

	与えるリスクを対象とします。例えば、医療機器の性能に影響を与える（性能や機能の低下、誤動作、動作停止など）、診療活動に影響を与える（患者情報やオーダー情報へのアクセス停止など）、誤った診療につながる（情報の欠落や改ざんによる誤診断や不適切な治療など）、などによって医療安全が損なわれることが考えられます。 対応案：医療機器に係るサイバー攻撃の被害により、医療安全に影響を与えるリスクを対象とします。例えば、医療機器の性能に影響を与える（性能や機能の低下、誤動作、動作停止な　ど）、診療活動に影響を与える（患者情報やオーダー情報へのアクセス停止など）、誤った診療につながる（情報の欠落や改ざんによる誤診断や不適切な治療など）、などによって医療安全が損なわれることが考えられます。また、当該医療機器がサイバー攻撃の侵害に遭い同じネットワークに接続された他の医療機器やシステムに影響を及ぼし医療安全に影響を与えるリスクにも考慮が必要です。 理由：当該医療機器がサイバー攻撃の踏み台になり他の医療機器やシステムに対して悪影響を及ぼすこともリスクとして考慮する必要がある。	攻撃の被害を受けたことにより、同じネットワークに接続された他の医療機器やシステムに影響を及ぼし医療安全に影響を与えるリスクにも考慮が必要です。」を追記いたします。
13	●対象とするリスクについて ・箇所：117～122 行 ・意見：リスクに対する具体例で、Confidentiality, Integrity, Availability の I と A については考慮されているが、C に対する考慮は言及しなくてもよいか。 ●医療機器の導入までのリスクアセスメントについて ・箇所：184～185 行、225～267 行 ・意見：表１のステータス「医療機器の導入まで」において、医療機器事業者が提供する文書を元にリスクアセスメントを行い、リスク対応を検討する必要があると考えられるため、その旨追記すべきではないか。併せて、リスク対応として「サイバーセキュリティ対策が必要」などの説明があった方がよいのではないか。 ※表１の追記に合わせて４－２項も変更が必要と考え、箇所に 225～267 行も入れている。 ●リスクマネジメントの実施について ・269～278 行, 225～267 行 ・意見：「４－３．医療機器の導入後の管理、運用」の「1）リスクマネジメントの実施」において、「IT インフラの初期開発時」や「既存 IT ネットワークへの新規医療機器の統合時」といったステージでリスクマネジメントを実施することが求められる、と述べられている。「既存 IT ネットワークへの新規医療機器の統合時」は、「医療機器の導入時」に相当すると思われるため、「４－２．医療機器の導入時」にも記載すべきではないか（225～267 行）	対象とするリスクの具体例については、あくまでも例として示しているものであるため、原案のままとさせていただきます。 医療機器の導入までのリスクアセスメントに関して、サイバーセキュリティインシデントが発生した場合の対応手順について予め定めて関係者に周知することを明記しています。リスク分析結果に基づく対応（以下、リスク対応）については、主に医療機器の導入後に実施されるものですので、医療機器の導入までに行うべき対応への記載は控えさせていただきます。なお、医療機器の導入後に行うべきリスク対応として、協調的な脆弱性の開示等については明記し

		ています。 また、医療機器の導入前にリスク対応としてサイバーセキュリティ対策をとる必要があることは表１において明示されているため､｢サイバーセキュリティ対策が必要」という記載について追記することは控えさせていただきます。 ｢既存 IT ネットワークへの新規医療機器の統合時」につきましては、医療機器導入時点ではなく、医療機器導入後の内容ですので、原案のままとさせていただきます。
14	P6　3-2　ステークホルダーとの連携について、医療機器事業者は薬機法に従って、つまりこれから発行される予定の JIS T 81001-5-1 に従ったサイバーセキュリティの対策が必須となり、薬機申請では強制となるが、医療機関はこの手引書に基づいてサイバーセキュリティの取り組みを行うとなっており、医療機関での対応確認、実効性を第三者が確認する取り組みはあるのでしょうか？　　JIS T 81001-5-1 では製造業者、医療機関、規制当局及び脆弱性発見者の共同責任でサイバーセキュリティに取り組んでいく必要がありますが、サイバー攻撃を受けるのは医療機関となり、大病院からクリニックなどに至るすべての医療機関がその体制を整え、外部機関がチェックする体制が必要になると考えます。　医療法ではこのサイバーセキュリティに関する項目が追加となるのでしょうか？	幅広い範囲のセキュリティ対策については、安全管理ガイドライン等において、対策すべき事項が記載され、その他医療法施行規則改正が予定されています。
15	箇所：147～149 行 記述内容：医療機関に医療機器を導入する際、およびこれを運用・管理する 際には、医療機器事業者はもちろん、医療情報システムや医療機器の導入やメンテナンス等を担うサービス提供者との連携を図ることが重要です。 対応案：医療機関に医療機器を導入する際、およびこれを運用・管理する際には、医療機器事業者はもちろん、医療情報システムや医療機器の導入やメンテナンス等を担うサービス提供者との連携を図ることが重要です。一方で、医療機器事業者やサービス事業者は医療機関の要請に対して対応できるよう組織的な準備が重要です。 理由：医療機関の視点だけでなく、それに応じる事業者側の視点も併せて	ご意見を踏まえ、｢一方で、医療機器事業者やサービス事業者は医療機関の要請に対して対応できるよう組織的な準備をすることになります。｣を追記いたします。

	記述しておくべき。	
16	p.6　153　3-3. 製品ライフサイクル全体（TPLC）とリスクマネジメント p.7　184-185　表 1：医療機関と医療機器事業者がサイバーセキュリティ対策・インシデント対応で行うこと（概要）　「レガシー状態での対応」 ・「『4-5. レガシー医療機器への対応』3）サポート終了への対応（EOS 以降）」の内容と一致させるため、EOS 以降は当該医療機器のセキュリティを管理する責任及びサイバーセキュリティ EOS 日以降も使用を継続することによって発生し得るリスクを医療機関側が引き受けることを上記 2 項目中に追記し、明確化してほしい。	ご意見を踏まえ、3.3 に、「提示された EOS 以降も使用を継続することによって発生し得るリスクは、医療機関が引き受けてマネジメントしていくことになります。」を追加いたします。また、表 1 の「レガシー状態での対応」に「サポート終了後、使用を継続することに対するリスクマネジメントの実施」を追加いたします。
17	箇所：155～156 行 記述内容：また医療機器事業者からは　EOL（製品寿命終了）/EOS（サポート終了）などに関して、医療機器の製品寿命およびサポート条件に関する情報も提供されます。　医療機器事業者からは EOL（製品寿命終了）/EOS（サポート終了）などに関して、医療機器の製品寿命およびサポート条件に関する情報も提供されます。 対応案：また、医療機器事業者は自社開発部分だけでなく、稼働するプラットフォーム（ハードウェアや OS、ライブラリ等）についてサプライチェーンとライフサイクル全体を通じて、リスク情報の提供や、コントロール策についての情報も考慮が必要です。 理由：OS のセキュリティアップデートやセキュリティ対策の併用など、現実的に必要とされるリスク低減策と、その維持が不可欠である。	他のコメントによる修正がされているため、原案のままとさせていただきます。
18	箇所：185 行 記述内容：表 1 医療機器の導入まで｜導入前の準備医療機関｜医療機器事業者（その他ステークホルダーを含む）＞顧客向けセキュリティ文書（MDS2、 SBOM、等） 対応案：顧客向けセキュリティ文書（MDS2、SBOM、等）にて、想定リスク、リスク分析結果の提示を含めること。昨今のサイバー攻撃を踏まえ内部に脅威が侵入する前提を考慮すること。 理由：医療機関の行うべきものだけでなく、事業者側が行うべきことも整理して記述しておくべき。想定リスク、リスク分析結果の提示を含めること。想定は内部に脅威が侵入する前提とする。	製販業者向けの手引書は別途通知で発出予定です。 また、想定リスクについては、サイバーセキュリティインシデントが発生した場合の対応手順について予め定めて関係者に周知することを明記しています。 リスク分析結果の提示については、主に医療機器の導入後に実施されるものですので、医療機器の導入までに行うべき対応

		への記載は控えさせていただきます。なお、医療機器の導入後に行うべきリスク対応として、協調的な脆弱性の開示等については明記しています。
19	箇所：185 行 記述内容：レガシー状態への対応 対応案：導入前の準備において、予め合意しておくべき項目としておくべき	ご意見を踏まえ、レガシー状態への対応を念頭に、導入前の準備に「●アップデートオプション、保守計画の確認」を追記いたします。
20	箇所：190～193 行 記述内容：IT インフラを整備しこれを維持管理するための方針や情報共有についてのポリシーを明確にするとともに、医療セプター等の ISAOｓ（情報共有分析機関）からの情報を常に確認し、自施設で必要になる対策があれば実施すること、および対策が必要になる可能性について医療機器事業者等に確認することが求められます。 対応案：IT インフラを整備しこれを維持管理するための方針や情報共有についてのポリシーを明確にするとともに、病院情報システム・ネットワークを構成するすべての機器、関連する部門全てにおける共通理解が求められます。医療機器を構成するアプリケーション部分だけでなく動作環境のソフトウェアや、医療機器以外の周辺装置についても脆弱性の最少化、安全性の維持に努め、管理していくことが重要となります。 医療セプター等の ISAOｓ（情報共有分析機関）からの情報を常に確認し、自施設で必要になる対策があれば実施すること、および対策が必要になる可能性について医療機器事業者等に確認することが求められます。 理由：サイバーセキュリティを維持する上での重要なポイントを明示する。	本手引書は病院情報システム・ネットワークを構成するすべての機器を対象とするのではなく、接続有りの医療機器を対象にするものであること、また動作環境や周辺装置を整備することの重要性については本手引書内でも複数回に渡り言及しているため、原案のままとさせていただきます。
21	箇所：249～251 行 記述内容：医療機器の意図する使用及び使用環境に対して設計したセキュリティ機能を俯瞰可能な、製造販売業者による医療機器セキュリティ開示書（Manufacturer Disclosure Statement for Medical Device Security： MDS2） 対応案：医療機器の意図する使用及び使用環境に対して設計したセキュリティ機能を俯瞰可能な、製造販売業者による医療機器セキュリティ開示書（Manufacturer Disclosure Statement for Medical Device Security：MDS2）については、接続するネットワーク内に脅威が侵入する可能性を考慮したものとすること。 理由：昨今のサイバー攻撃を想定したものにする。	MDS2については、接続するネットワーク内に脅威が侵入する可能性を考慮する必要があることは自明のことであるため、原案のままとさせていただきます。
22	箇所：253～256 行	ご意見を踏まえ、「医療機

	記述内容：医療機器の保守・サービスは医療機関の責任において行うことになり、その一部を委託する場合でも管理責任の主体はあくまでも医療機関になります。医療機関等の管理者は、患者に対して、受託する事業者の助けを借りながら、「説明責任」、「管理責任」、「維持・改善の責任」及び「善後策を講じる責任」を果たす義務を負います。 対応案：医療機器の保守・サービスは医療機関の責任において行うことになり、その一部を委託する場合でも管理責任の主体はあくまでも医療機関になります。医療機関等の管理者は、患者に対して、受託する事業者の助けを借りながら、「説明責任」、「管理責任」、「維持・改善の責任」及び「善後策を講じる責任」を果たす義務を負います。それに対し、医療機器事業者は医療機関がこれら「説明責任」「管理責任」「維持・改善の責任」及び「善後策を講じる責任」を果たせるよう情報の提供や対応の提案などが求められます。 理由：医療機関が保守を委託する上で、リモートアクセス環境を構築されることは現実として一般化している。しかし、ここで医療機関に管理責任があるといいながら、医療機関からの情報開示請求に応じない事業者が多いことも現実である。事業者は医療機関が安全管理責任を全うできるだけの情報開示、安全対策の維持について協力する義務を負うべきである。	器事業者は医療機関がこれら「説明責任」「管理責任」「維持・改善の責任」及び「善後策を講じる責任」を果たせるよう情報の提供や対応の提案などを行います。」を追記いたします。
23	箇所：317 行 記述内容：協調的な脆弱性の開示（CVD） 対応案：医療機器を構成するソフトウェアは事業者が開発するアプリケーション部分だけでなく、動作環境となる OS 等のソフトウェアもサイバーセキュリティ対策において重要な構成要素です。医療機関が適切に判断できるようにするため構成要素それぞれに関する脆弱性情報の提供がもとめられます。 理由：医療機関の行うべきものだけでなく、事業者側が行うべきことも整理して記述しておくべき。	アプリケーション部分のみならず、動作環境を整えることも重要であり、各々に対して脆弱性情報の提供が必要であり、本手引書にはそれらを医療機関もしくは製販業者が行うべきものとして、区別して記載すべきとのご意見と承りました。 P.11の③協調的な脆弱性の開示において、医療機関と製販業者がどのように連携を取って脆弱性情報の提供を行い、対策を講じるべきかについて記載されているため、原案のままとさせていただきます。
24	p.11 328-329 ・「医療機関では、医療機器事業者が提供するアップデートをインストール手順に従って適用することが期待されます。」とあるが、アップデートは製造販売業者が実施することがある。そのため、製造販売業者がアップ	本手引書は医療機関におけるサイバーセキュリティ対策について記載していること、また製販業者

	デートを行う場合についても追記してほしい。	向けの手引書において製販業者の行うアップデートに関する記載があることから、原案のままとさせていただきます。
25	参考資料 ・IMDRF ガイダンスだけでなく、「医療機器のサイバーセキュリティ導入に関する手引書」で引用されている「医療機器・ヘルス IT 共同セキュリティ計画（Joint Security Plan)のベストプラクティス」も参考資料として追記してほしい。	Joint Security Plan は製販業者向けものであり、医療機関向けのものではないため、原案のままとさせていただきます。