「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
1	全体		【意見の対象】 子ども・子育て支援金制度の賦課・徴収運用および料率改定時期について 【具体的な意見および要望】 料率改定タイミングの完全同期化 健康保険料率（および介護保険料率）の改定時期である「3月分」に、支援金の料率変更時期を統一することを強く要望します。1ヶ月のズレは、給与計算ソフトの「予約設定」ができない旧来型システムを使用している中小企業において、手作業による設定変更を2ヶ月連続で強いることになり、ヒューマンエラーによる徴収不足・過誤徴収のリスクを著しく高めます。事務コスト増大に対する定量的視点の欠如への指摘 制度設計において、既存の健保インフラへの「相乗り」による行政側の効率化は理解しますが、そのしわ寄せが民間の給与計算担当者の「工数増」として転嫁されています。数千万人規模の労働者の給与計算において、1ヶ月ずれた設定変更作業とそれに伴う従業員への説明、給与明細の修正にかかる社会的コスト（残業代、システムベンダーへの改修費）を考慮した、現場主導の運用ルールを策定すべきです。	ご意見として参考にさせていただきます。
2	全体		「個人情報漏洩」と言いますが、今 一番 個人情報を抜き出そうとしているのは、日本政府自身では ありませんか。任意のはずのマイナンバーカード・マイナ保険証を、既存保険証の廃止という強硬策まで執って 強制しようというのは、狂気の沙汰としか思えません。マイナンバーに紐付けられる電子カルテ情報には、情報の当人が 開示する相手・期間・範囲を指定できないという欠陥があります。この様な 個人の意思をないがしろにした政策は、やめていただきたい。	ご意見として参考にさせていただきます。
3	全体		本改訂は大幅な方針転換が多岐にわたるため、6.1版ではなく7.0版の方が良いと思います。	第7.0版としました。
4	全体		pdfのフォーマットについて、一部ファイルは文字情報が不完全のようです。検索するとヒットしなかったり、コピペすると不完全な文字列が表示されます。 本ガイドラインは利用者がAIに読み込ませる使い方をすることが想定されることから、ガイドライン内のテキストは機械可読にしてください。	ご意見として参考にさせていただきます。 公表形式については対応するようにいたします。
5	全体		文書の読みやすさ点から、いくつかの表現は短いものに置き換えたほうが良いと思います。これらはサイバーセキュリティのコンテキストでは一般的に使われているもので、本文書においても曖昧さなく使用できます。 ただし「セキュリティ」については、文脈によっては短くすると意味が通らなくなる箇所がある点にご注意ください。(例：情報セキュリティマネジメントシステム) インシデント　リスク　セキュリティ	ご意見として参考にさせていただきます。
6	全体		今となってはあまり使用しない用語は、最新のものに置き換えた方が読みやすいです。 脆弱性　ヘルスチェック	ご意見として参考にさせていただきます。
7	全体		複数の意味を持つ単語は、曖昧さの少ない表現に置き換えたほうが良いです。 利用者（人間を指している場合）/ アカウント(ユーザアカウントを指している場合)	ご意見として参考にさせていただきます。
8	全体		表記揺れがあります。 (右記のいずれか一つ)遺失 / 紛失	システム運用編について紛失にそろえました。
9	全体		これはセキュリティの分野では一般的な用語ですが、読者が用語を知らないことが想定され、かつ本文書の文脈によって誤解を与える可能性があるため、注釈等で補足しておいた方が良いと思います。 シャドーIT	用語集において対応させていただきます。
10	全体		文書の読みやすさの点から、箇条書きによって文が途切れているものは、箇条書きの前で文が終わるようにまとめた方が良いと思います。 Xは、例えば以下がある。 ・〇〇 ・□□	ご意見として参考にさせていただきます。
11	全体		「経営管理編」「企画管理編」「システム運用編」「保守委託機関編」のそれぞれについて、章構成、項構成の全体像が見えるように、フローチャートが欲しいです 章構成、項構成が見えるフローチャートを追加	ご意見として参考にさせていただきます。
12	全体		二要素認証の要求についてはパスワード認証の脆弱性を踏まえてこのようにしていると思います。もしそうでしたらパスキー等の最新技術も選択可能にした方がより安全だと思います。	パスキーについては、二要素認証として排除しているわけではありませんので、原案の通りでもパスキーの利用は可能です。原案の通りとさせていただきます。
13	全体		ガイドラインをもとに規制要求がなされているにも関わらず、ガイドラインという位置づけだけをタテにバブコメ期間が短く設定されている。 必要性と（改訂）内容に応じてバブコメ期間を設定すべき。	ご意見として参考にさせていただきます。
14	全体		現在ご提供いただいているPDFファイルには、しおり（ブックマーク）が設定されていないようです。 しおり付きのPDFにすることで、電子文書としての可読性や検索性が大幅に向上し、利用者が目的の情報にスムーズにアクセスできるようになります。 つきましては、今後の文書公開にあたり、最低限しおり付きPDFのご提供をお願い申し上げます。 これにより、より活用しやすく利便性の高い資料となり、関係者間の情報共有も円滑になると考えております。何卒ご検討のほどよろしくお願いいたします。	公表時に対応する予定です。
15	全体		事業者への委託推奨反対。	ご意見として参考にさせていただきます。
16	全体		令和8年度の診療報酬改定の医療事務作業補助体制加算において、RPAや生成AIを用いた業務効率化の要件の一部に『電子カルテ等と連動して医療情報を取り扱うものについては、「医療情報システムの安全管理に関するガイドライン」等（いわゆる３省２ガイドライン）に準拠していること』が求められているが、特に外部サービスや情報基盤との接続状態のもとで入力情報をベースに新たな文書や判断補助情報を提供する生成AIは従来の医療情報システムとは異なるセキュリティリスク（医療安全管理上のリスク）を有している。 すでに医療情報システムに生成ＡＩが導入され、利活用されている等、生成AIの医療分野での普及実態も踏まえ、生成ＡＩ固有のセキュリティリスクの評価・対策が重要な点を厚労省安全管理ガイドライン上でも明記すべきと考える。 また、生成ＡＩリスクの管理については事業者向けガイドラインとして経産省・総務省「ＡＩ事業者ガイドライン」に加え、26年に入り、総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン」、AISI「ヘルスケア領域におけるAIセーフティ評価観点ガイド」等が公開されている。 さらに、民間団体でも医療AIプラットフォーム技術研究組合「医療・ヘルスケア分野における生成 AI利用ガイドライン」、日本デジタルヘルスアライアンス「ヘルスケア事業者のための生成AI活用ガイド」等、医療機関の立場/事業者の立場から、ガイドがかなり以前より登場している。 こうした官民の各ガイドラインを必要に応じて利活用すべき旨を例えば脚注で示唆し、医療機関に周知を図る等、医療AI固有のセキュリティリスク（安全管理リスク）にも適切に対応することの必要性をどこかで明記すべきと考える。 少なくとも今回の厚労省安全管理ガイドラインの改定内容のなかに、医療分野で加速度的に普及しているAI技術へのセキュリティ面での言及が一切ないことに対して大きな違和感がある。 このままでは、医療現場では生成AI等を実装した医療情報システムのセキュリティ対策を既存のシステムの延長線のみでしか検討できず、今後、本来あるべき生成AI固有のリスクを後回しで別途評価・対応せざるを得なくなるという点で、医療機関にとってネガティブな結果をもたらすことにしかならないおそれがあり、強い懸念を覚える。	ご意見として参考にさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
17	全体		医療情報は、個人の生命・身体に直結する極めて機微性の高い情報であり、かつ我が国の社会基盤を支える重要データであることから、安全管理措置においてはサイバーセキュリティの観点に加え、データ主権及び経済安全保障の観点等を明確に位置付けるべきであると考えます。 この点、医療分野におけるデータ利活用及び生成 AI の活用は急速に進展していますが、一方でサイバー攻撃の高度化や国家間のデータガバナンス競争が顕在化しており、こうした環境下では、単なる技術的・契約的な対策に留まらず、データの所在、統治構造、および AI の基盤そのものを含めた高度な安全管理が不可欠です。 また、本ガイドライン案では、クラウドサービスの活用や AI の利用を前提としつつ、主として契約・管理により安全性を確保する考え方を示していますが、海外事業者のサービスや AI 基盤モデルに依拠する場合、データの保存場所や事業者の準拠法・ガバナンスによっては、我が国の統制が及ばないリスクが残存します。 特に、米国の CLOUD Act 等の外国法令の適用を受ける環境においては、我が国の法制度や本人の意思に基づかない形で医療情報が開示される懸念や、事案発生時の実効的な統制、サービス停止、あるいは越境アクセスのリスクを否定できません。また、学習データや推論過程における情報の取扱いについても留意が必要と考えます。 加えて、海外製モデルへの過度な依存は、モデル提供の継続性や利用条件の変更に左右されるだけでなく、研究開発の知見や人材が国外技術基盤に依存する構造を招く恐れがあります。欧州におけるデータ主権の議論（GAIA-X 等）に見られるように、重要データについては域内での統制を重視する動きが進んでいます。我が国においても、独自の保険医療制度や診療報酬体系、科学的エビデンスに基づく診療ガイドライン、さらには日本の風土・文化的背景を十分に踏まえた国産 AI の重要性は高く、我が国の統制が及ぶ AI 基盤の活用を通じて、国内における技術・人材・ノウハウの蓄積を図るべきです。 最後に、医療情報は患者本人に帰属するものと認識しています。現状、医療機関ごとに分断されているデータを本人が一元的かつ継続的に把握することは容易ではありません。医療 DX の推進にあたっては、上述した安全性の確保と主権の確立を両立させつつ、本人が自らの医療情報を適切に取得・活用できる環境整備を進めることが極めて重要と考えます。 したがって、以下の点についてガイドラインへ明記すべきであると考えます。 1. 医療情報を「経済安全保障上の重要データ」と位置付けること 2. データの機微性・重要性に応じて、国内保管・国内事業者の活用を優先する旨の原則を示すこと 3. 外国法令の適用可能性および越境データ移転リスクについて、医療機関が評価・管理すべき事項として明確化すること 4. 特に高リスク領域（電子カルテ、診療情報、ゲノム情報等）については、国内完結型のシステム構成（クラウド、サーバー、AI 基盤を含む）を推奨又は要件化すること 5. 医療情報を取り扱う AI については、その基盤モデルの開発主体、管理体制および準拠法を踏まえ、我が国の法令・統治が及ぶ範囲で構築・運用されることを求める旨を明確化すること 6. 医療情報の取扱いに関しては、データ主権の観点に加え、本人による利活用の促進の観点も重要である。政府においてはマイナポータル等を通じた医療情報の閲覧環境の整備が進められているところであるが、現時点では閲覧可能な情報は一部に限られていることも踏まえ、医療機関においても過度にデータを院内に閉じるのではなく、患者本人に対し、電子的な形式により医療情報を閲覧・取得可能とし、かつ本人同意を前提として利活用しやすい形で提供する環境整備を推奨する旨を明確化すること	医療情報の保存場所については引き続き検討を進める予定ですので、 今回の改定では原案の通りとさせていただきます。
18	概説編	2	昨今、医療機関がグループを形成し、グループ単位でシステムを契約・管理・運用している場合があります。（例えば本部が管理している場合など） グループ単位で管理している場合の考え方など注釈があれば良いなと思います。	ご意見として参考にさせていただきます。
19	概説編	2．1	3行目 ・・・、本ガイドライン全てを遵守しているものとみなす。 「本ガイドラインを遵守しているものとみなす。」としてはどうでしょうか。 ＞ガイドラインの遵守すべき箇所を抜粋しているのが、「保守委託機関編」であるので、要求事項の全てではないためです。	ご指摘の修正案を踏まえて修正しました。
20	概説編	2．2	3行目 なお、医療機関等が作成した医療情報を患者の管理に委ねた場合は本ガイドラインの対象外となる。その後、当該医療情報について・・・・ 「＞　その後、当該医療情報について患者から提供を受けた事業者等の第三者が取り扱う場合に」と独立した文章にしてはどうか ＞前半は、ガイドラインの対象外になることを説明し、後半を独立させることにより、PHRを意識させることができます	PHRとの整理の関係も踏まえ、原案の通りとさせていただきます。
21	概説編	2．1	＞医療機関等とは、病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等を想定する。ただし、「保守委託機関編」の対象となる機関においては、「概説編」と「保守委託機関編」に対応することで、本ガイドライン全てを遵守しているものとみなす。 読者は「概説編」から読む始めると考えられるが、ここで「「保守委託機関編」の対象となる機関」のみの記載の場合、対象機関が不明瞭であるため、この箇所に「「保守委託機関編」の対象となる機関」を記載してみてはどうか。	3.1.5において記載しておりますので、原案の通りとさせていただきます。
22	概説編	2．3	下記の項目について気づいた点を提出します。概説編　2.3　医療情報システムの範囲　（第二段落　なお書き中）「なお、医療情報を含まない患者への費用請求に関する情報しか取り扱わない会計・経理システム等は、本ガイドラインにおける医療情報システムには含まない。」との記載があるが、いわゆる病院情報システムの運用の中で、レセプトコンピュータ等、費用請求、会計・経理システムにおいて「医療情報を含まない」システム運用はほとんど想定されないと考える。この一文によって、「レセコン」が、当該ガイドラインの対象外という誤解が（行政機関を含め）広がっているので、このなお書きの文面を修正する必要があるのではないか。　ご検討願います。	「医療情報を含まない患者への費用請求に関する情報しか取り扱わない」ものについて示しておりますので、原案の通りとさせていただきます。
23	概説編	3	概説編（案）のページ３から 本ガイドラインの構成、読み方　図の下部にある補足２について。「事業者がセキュリティアップデート責任を追うこと」と記載されていますが、「事業者がセキュリティアップデートの責任を負うこと」の表現のほうが適切ではないでしょうか。	ご指摘を踏まえて、「追う→負う」へ修正いたしました。
24	概説編	3	注釈 １．ここでいう「サーバ」は、医療情報の保存や主要な処理を担う機器を指す。原則としてPCやタブレット等のクライアント端末は含まない。ただし、電子カルテアプリ等を端末にインストールし、当該機器上で処理が完結する場合はPC等の端末も「サーバ」に含む。 「サーバ」について、「～主要な処理を担う機器を指す。」とあるが、物理的機器をイメージさせるため、以下のように修正してはどうか。 「～主要な処理を担う機器、クラウドサービスを指す。」	クラウドサービスの利用も含めた記載としておりますので、原案の通りとさせていただきます。
25	概説編	3	注釈 ２「事業者がセキュリティアップデート責任を追うこと」が、契約書や約款、サービスレベル合意書等に記載されている場合にのみ「YES 」を選択可能となる。記載がない場合や不明確な場合には医療機関側の責任となっている可能性がある。不明確な場合は必ず事業者に直接確認し、責任の所在を明確にすること。 １．「責任を追う」ではなく、「責任を負う」である。 ２．セキュリティアップデートの責任が医療機関等または事業者側のどちらなのかを明確にする意図であるなら、「医療機関側の責任となっている可能性がある。」という記載ではなく、以下のように修正してはどうか。 「記載がない場合や不明確な場合には必ず事業者に直接確認し、医療機関等と事業者双方において責任の所在を明確にすること。」	一つ目の点についてはご指摘の修正案を踏まえて修正しました。 二つ目の点については原案の通りとさせていただきます。
26	概説編	3	本ガイドラインは実務上の標準として広く参照される一方、項目が多岐にわたるため、現場において優先順位の判断が難しい場合がある。 医療機関の過度な負担や形式的対応を防ぐ観点から、各対策項目について、 ·①法令遵守上対応が求められる事項（Must） ·②推奨される事項（Should／Better） といった区分を、記号や分類により明確に示すことが望ましい。	ご意見として参考にさせていただきます。
27	概説編	3．1．5	3行目 ・・・対応することで本ガイドライン全体を遵守でき るものとみなす。一般的・・・ 「本ガイドラインを遵守できているものとみなす。」としてはどうでしょうか。 ＞ガイドラインの遵守すべき箇所を抜粋しているのが、「保守委託機関編」であるので、要求事項の全てではないためです。	ご指摘の修正案を踏まえて修正しました。
28	概説編	3．1．5	7～8行目 ・・・、クラウドサービス（特にSaaS型システム）を積極的に採用することで特別な契約を交わすことなく保守の委託を実現することを想定している。 「医療機関向けに提供しているクラウドサービス」としてはどうか。 ＞医療機関の利用を想定しないSaaSは、本ガイドラインの適用を考慮していない場合があります	医療機関等が医療情報を取り扱うために用いるクラウドサービスは本ガイドラインの対象としておりますので、原案の通りとさせていただきます。
29	概説編	3．1．5	3.1.5項にて、該当箇所をフォントで太字にしている理由が分からず、また、他の記述への注意が薄くなるので、太字解除を希望します。 （フォントの太字を解除する）	ご指摘の修正案を踏まえて修正しました。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
30	概説編	３．１．５	保守委託機関編や後続の文章で記載されているように、医療機関等において、リソース等の問題があり、システム担当者をおくことができず、かつセキュリティアップデートの責任を事業者に全て委託してしまっている医療機関等のために存在している「編」だと認識しています。指摘箇所については、本ガイドライン全体を遵守できているものとみなすための条件となる文章であるため、分岐を明らかにするためにも、図３－１の文言に合わせ、下記の表現としてはどうか？ ＜修文案＞ 本ガイドラインが対象とする医療機関等のうち、”専任のシステム運用担当者が不在かつ小規模で経営管理と企画管理の部門が区別されていない医療機関等で、「すべてのサーバの保守について、セキュリティアップデートの責任を事業者に全て”委託できている医療機関等」においては「概説編」と「保守委託機関編」のみを参照し、その遵守事項に対応することで本ガイドライン全体を遵守できているものとみなす。この一般的な保守委託機関編の対象”となる医療機関等としては、職員等が少なく、専任、役割の分離が困難な”小規模医療機関等を想定している。	保守委託機関編については、該当しない医療機関等が参照することを妨げておりませんので、原案の通りとさせていただきます。
31	概説編	３．１．５	助詞の間違いではないか？ ＜修文案＞ ～、専任のシステム担当者”が”配置されておらず、～	ご指摘の修正案を踏まえて修正しました。
32	概説編	４．１．１	「医療情報が共有」と「継続した医療の提供」の因果関係の説明が抜けていると思われます。	ご指摘の箇所は並列的に重要性を示していますので、原案の通りとさせていただきます。
33	概説編	４．１．２	４行目 さらには一医療機関等を超えて、・・・ 「さらには、個々の医療機関等を超えて、・・・」としてはどうか ＞「一」は口語では良いが、文字にするの傍線のように見えます	ご指摘の修正案を踏まえて修正しました。
34	概説編	４．２	機密性の説明について、情報の「改ざん」や「破壊」は完全性に対応する概念で、可用性の説明にフォーカスできておらず、読者に誤った理解を与える可能性があります。とはいえ、単純にこれらを削除すると読者にリスクの大きさを認識させることができないため、バランスを取って「例えば許可していない者による情報システムの悪用によって」のような表現に変更するのが良いと思います。 「機密性（Confidentiality）」は、情報資産に対して、許された者のみがアクセスできることを指す。機密性が確保されていない場合、例えば許可していない者による情報システムの悪用によって改ざん、破壊などを含む、医療情報の不正な利用（参照、登録、改変）や漏えいが生じうる。	改ざんに関しては、作成権限権との関係では機密性に関連するものと整理しておりますので、原案の通りとさせていただきます。
35	概説編	４．２	順序に表記揺れがあります。 （関連：保守委託機関編 p.7,15,16ほか） 当該情報の真正性・見読性・保存性が確保されている必要がある。	ご指摘を踏まえ、真正性・見読性・保存性の順番に統一しました。
36	概説編	４．３	本章に書かれている「サイバーセキュリティ基本法（平成26年法律第104号）」の記述 左記の赤文字を全箇所削除してはどうか？同法が根拠法であるかようにようなに説読めます。 ２２行目に「本ガイドラインの直接の目的は個人情報保護法とe-文書法への対応である」と書かれているので、これらが根拠法だと明記していますので、混乱します。 サイバーセキュリティに対する要求は、同法を参考に記載することのみを明記してはどうでしょうか 全文の書き換えになるので、変更例は差し控えさせていただきます	本改定ではサイバーセキュリティ基本法を根拠法に加えておりますので、原案の通りとさせていただきます。
37	概説編	４．５	２～３行目 ・・・。この脅威としては、地震等の自然災害や、サイバー攻撃、システム障害などの環境要因によるもの、医療情報の漏洩や改ざんなどの人的要因によるものが挙げられる。 サイバー攻撃は、人的要因もしくはJISでいう技術的脅威ではないでしょうか？	ご指摘を踏まえて「技術的脅威」に修正しました。
38	概説編	４．５	「人的要因」とは誰の何であるかが読者に伝わりにくいので、情報処理推進機構の「組織における内部不正防止ガイドライン」の表現を参考にして「内部不正による」を追加した方が良いと思います。 参考：”組織における内部不正防止ガイドライン	情報セキュリティ	IPA 独立行政法人 情報処理推進機構” https://www.ipa.go.jp/security/guide/insider.html 安全に医療情報システムを管理し、医療情報を取り扱うに当たっては、安全を脅かす原因となる「脅威」を認識する必要がある。この脅威としては、地震等の自然災害や、サイバー攻撃、システム障害などの環境要因によるもの、内部不正による医療情報の漏洩や改ざんなどの人的要因によるものが挙げられる。	人的要因は内部不正に限らないという想定ですので、原案の通りとさせていただきます。
39	概説編	４．５ ４．７	修正の横展開漏れがあります。（漏えい vs 漏洩） 医療情報の漏えいや改ざんなどの人的要因によるものが挙げられる。 外部保存に際しては、外部と接続するネットワークを利用するという観点から、情報漏えいや不正アクセス等のリスクが生じる。	ご指摘を踏まえて「漏えい」に統一しました。
40	概説編	４．７	３行目 ・・・、外部の事業者に医療情報の保管を委託し、医療機関の外部に医療情報を保管することが となっている。・・・ 「保管ー保存」としてはどうでしょうか ＞題名も「保存」、各種法令も「保存」です ＞ここで保管に言い換える根拠を提示していただきたいです	ご指摘の修正案を踏まえて修正しました。
41	概説編	４．７	4.7項、「医療情報の外部保存」の定義があいまいです。本文記載の「診療録等の保存を行う場所について」〔医療法〕をたどれば分かりますが、ガイドラインなので、補足説明が欲しいです。 4.7項の冒頭に、「医療情報の外部保存とは、作成した病院又は診療所以外の場所における保存を指す。」を追加	ご指摘の修正案を踏まえて修正しました。
42	経営管理編	1	旧「経営管理編」p1に記載のあった＜医療機関等における情報セキュリティ＞に記載のあった『安全管理対策の実施を「コスト」と捉えるのではなく、質の高い医療の提供に不可欠な「投資」と捉え、その実施に必要となる資源（予算・人材等）の確保に努めることがも重要である。』という表現が改訂版では削除されているため、何らかのかたちで経営管理編に残すべきと考える。 理由としては、予算や人材等の資源（リソース）の確保がなければ、どれだけ現場の企画管理者やシステム運用者が努力しても実効的なセキュリティ対応は不可能であるからである。経営層がセキュリティを「無駄なコスト」ではなく、医療継続と患者安全を確保するための重要課題としてとらえ、適正なセキュリティ活動を支えるためのリソースを確保・配置し、全面に立って現場をリードしなければ、本来あるべきセキュリティガバナンスは実現されないため、削除された一文は非常に重要な意義を持っている。 そのため、「経営管理者はセキュリティに係るリソースを確保する責務がある（実務管理者等では対応できない事項のため）」という趣旨は経営管理編のどこかに残すべきと考える。 また、他の社会インフラ事業領域では当然視されている「サイバーリスクは経営上の重要リスクであること」を強調するため、たとえば「（サイバー）セキュリティリスクは単なるシステムの問題ではなく、患者安全や医療継続に直結する、経営管理上のリスクであること」をあわせて追記すべきと考える。	ご指摘の修正案を踏まえて修正しました。
43	経営管理編	１．２	1.2項、表1-1の中に責任を列挙していますが、本文中の＜説明責任＞＜管理責任＞などの項目名称との一致が取れるように統一をお願いします。 例：「＜説明責任＞管理方法・体制等に関する説明責任」 例：「＜管理責任＞管理及び監査を実施する責任」	ご指摘の修正案を踏まえて修正しました。
44	経営管理編	２	経営管理編 ２．リスク評価を踏まえた管理 「対応方針を策定し」と「リスク管理方針を決定する」は意味が重複しています。片方を削った方が読みやすいです。 ①取り扱う医療情報に応じたリスク分析・評価を踏まえ、リスク管理方針（リスクの回避・低減・移転・受容）を決定すること。	ご指摘の修正案を踏まえて修正しました。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
45	経営管理編	2	本文書の用語では「リスク分析」→「リスク評価」→「リスク管理方針(管理措置)の決定」→「リスク低減/リスク回避/リスク移転/リスク受容」の順で実施するようなので、右記については順番に誤りがあると考えられます。 参考: "JIS Q 27000:2019 用語の定義にみる「リスクマネジメント」" https://www.ismwebstore.com/materials/archives/2118 ②リスク評価を踏まえたリスク管理が必要な場面の整理、対策として求められる体制、ルール等について、企画、整備、管理を、企画管理者に指示すること。 ③方針及びリスク評価を踏まえ、具体的にシステム面からの最適なリスク管理措置を検討し、実装、運用するよう、企画管理者に指示すること。	リスク管理方針について修正しましたので、この部分については原案の通りとさせていただきます。
46	経営管理編	2	句点の多用によって文の構造がかなり読み取りにくいです。 医療継続の必要性を考慮すると、医療機関等において選択される主なリスク管理方針は「リスクの低減」になると考えられ、リスク評価を踏まえたリスク管理方針の決定とその運用を継続的に実施する必要がある。	ご指摘の修正案を踏まえて修正しました。
47	経営管理編	2	医療情報システムの安全管理の強化は重要である一方、人的・財政的リソースが限られる中小規模医療機関においては、大規模病院と同一水準の対策を一律に求めることが困難な場合も想定される。 対策の未実施や形骸化を防ぐ観点から、医療機関の規模や機能、取り扱う情報の機微性に応じて、 ・①「最低限遵守すべき事項（ミニマムセット）」 ・②「段階的な対応ロードマップ（優先順位）」 ・③「コストを抑えた代替的な安全管理措置」 の具体例を示すことが望ましい。これにより、各医療機関の実情に即した実効性のある体制構築が促進されるものと考えられる。	ご意見として参考にさせていただきます。
48	経営管理編	2．1	「何が」が抜けていて、意味が読み取れませんでした。 このとき、例えば直接の作業をシステム運用担当者に実施させることを(○○は)妨げるものではない。	経営管理編においては、特段の記載がないものは経営管理者を想定しているので、原案の通りとさせていただきます。
49	経営管理編	3．1．2	「また、医療情報システム安全管理責任者は、経営層が担うことを想定しているが、企画管理者が医療情報システム安全管理責任者を兼務することも妨げない。」の件です。 原則が経営層の方と明記されていることは、組織のガバナンス強化の観点から理解できます。一方で、診療報酬改定における「電子的診療情報連携体制整備加算」等においては、「専任の医療情報システム安全管理責任者の配置」が施設基準として求められています。 実際の医療現場において、経営層（病院長、副院長等）やその任に就く上位の企画管理者は、院内の管理業務のみならず、学会の役員・業務、大学等での講義、公的機関の会議委員などを日常的に業務していることが多々あります。 このような実態がある中で、経営層が「医療情報システム安全管理責任者」に就任した場合、外部の業務等を業務した状態のままで、診療報酬における「専任」の要件を満たすと解釈してよいのか、現場では大きな疑問と混乱が生じています。 上記の懸念を踏まえ、以下の点について見解をお示しいただくようお願いいたします。 ・経営層や企画管理者が、学会業務、大学の講義、公的機関の委員等の院外業務を業務した状態で「医療情報システム安全管理責任者」に就く場合、診療報酬の算定要件である「専任」として認められるのか、明確な解釈をお示しください。 ・もし「専任」と認められるためには一定の条件（エフォートの割合や、実務を補佐するシステム運用担当者の配置義務など）が存在する場合は、医療機関が体制構築において迷わないよう、ガイドラインの解説や関連Q&A等で具体的な基準を明記してください。	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。
50	経営管理編	3．1．5	【遵守事項】該当文：「情報セキュリティインシデントの未然防止策として、通常時から医療情報システムに関係する脆弱性対策やEOS（End of Sale, Support, Service：販売終了、サポート終了、サービス終了）等に関する情報を収集し、迅速に対策を講じることが可能な体制を整えるよう、企画管理者やシステム運用担当者に指示すること。」 EOSを迎えたシステムや情報機器について、経営層は担当者に「体制を整えるよう指示する」だけでなく、収集された情報や提案に基づき、「費用を伴うシステム更新（予算確保）」や「対象機器の運用廃止」といった最終的な『経営判断』を行う責務がある旨をガイドラインに明記していただきたいです。「指示をする」という記載のみでは、経営層が現場からのEOS報告を受け取るだけで具体的な予算措置や運用見直しの決断を下さず、結果として現場に責任が押し付けられたまま脆弱なEOS機器が放置される（サイバー攻撃の起点となる）リスクがあります。経営層が自らの責務として投資判断を行うべきであることを明確にする必要があります。 上記の懸念を踏まえ、当該箇所の記載（または解説部分）に以下の趣旨を追記することを提案いたします。 追加案：「経営層は、企画管理者等からEOS等の対象機器に関する報告を受けた場合、医療提供の継続性やサイバーセキュリティ上のリスクを総合的に評価し、システム更新のための予算の確保、補完的対策の承認、または当該システム・機器の運用廃止等について、責任をもって経営判断を行うこと。」	ご指摘の修正案を踏まえて修正しました。
51	経営管理編	3．4．2	修正の横展開漏れがあります。(関連：p.8) EOS（End of Support：サポート終了）	ご指摘を踏まえて修正しました。
52	経営管理編	3．4．2	緊急連絡網を速やかに整備することと読めてしまうため、下記の表現へ修正すべき。 ＜修文案＞ ～、初動の対応が重要であることから、速やかに情報共有”する”ための緊急連絡網 ～	ご指摘の修正案を踏まえて修正しました。
53	経営管理編	3．4．3	＞なお、ランサムウェア攻撃においては、暗号化された情報の復号と引き換えに攻撃者から金銭を要求されることがある。「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」（令和４年 11 月 10 日付け厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室・厚生労働省政策統括官付サイバーセキュリティ担当参事官室事務連絡）3では、金銭の支払いは、犯罪組織に対して支援を行うことと同義であり、厳に慎むべきとしている。そこで、このような場合には、独自の判断をせず、事前に厚生労働省等と相談することが強く求められる。 →「事前に厚生労働省に相談すべき」という趣旨を強めるために、金銭を支払って状況が改善した場合と支払っても改善しなかった場合の両方を入れておくべきだと考える。 （修正案） なお、ランサムウェア攻撃においては、暗号化された情報の復号や、窃取された情報の不正公開の停止と引き換えに、攻撃者から金銭を要求されることがある。 一部の事案においては、金銭を支払わなかった結果として患者等の情報の不正公開が継続したものの、最終的に金銭を支払うことで当該公開が停止されたとされる事例が報告されている。一方で、金銭を支払った場合であっても、暗号化されたデータが確実に復旧される保証はなく、要求が更にエスカレートするなど、状況が必ずしも改善しない可能性も指摘されている。 「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」（令和４年11月10日付け厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室・厚生労働省政策統括官付サイバーセキュリティ担当参事官室事務連絡）においては、金銭の支払いは犯罪組織に対する支援と同義であり、厳に慎むべきものとされている。 これらを踏まえ、ランサムウェア攻撃を受けた場合においては、金銭支払いの可否を含む対応について医療機関等が独自に判断するのではなく、事前に厚生労働省等の関係機関と十分に相談・連携を行うことが強く求められる旨を、より明確に記載することが望ましい。 2） （P21） ＞そのため、利用する医療情報システム・サービスに関連する情報機器等の管理がどの主体にあるのかを明確にし、安全性の確保の対応の役割分担についても明らかにする必要がある。情報機器の所有者、設置責任者、その安全管理措置のための保守管理者等がそれぞれ異なることもあり、事前に明確にすること。 →これでは不十分と考える。安全管理措置として、保守契約に必要な項目（OSのアップデート間隔、脆弱性対策、ペネトレーションテストの指摘事項に対する改修作業等）が含まれているか確認した上で、現状の契約が不十分といういうことであれば契約の見直しを指示すること。 （修正案） そのため、利用する医療情報システム・サービスに関連する情報機器等の管理主体を明確にするとともに、安全性確保に係る対応について、各主体の役割分担をあらかじめ整理し、文書等により明確化する必要がある。情報機器の所有者、設置責任者、並びに安全管理措置の実施に係る保守管理者等が異なる場合も想定されることから、これらの責任の所在を事前に確認しておくことが求められる。 さらに、当該安全管理措置が実効的に担保されるよう、保守契約等の内容についても十分な確認を行う必要がある。具体的には、OSやミドルウェア等のアップデートの実施方針・頻度、既知の脆弱性に対する対応内容、ペネトレーションテストや脆弱性診断により指摘された事項への改修対応の範囲および対応期限等が、契約上明確に含まれているかを確認することが重要である。 その結果、現行の契約内容が安全管理措置として不十分であると認められる場合には、必要に応じて契約内容の見直しや追加を行うよう、医療機関等から委託先に対して指示・調整を行うことが望ましい。	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
54	経営管理編	３．４．３	「緊急対応体制」について。 ①CSIRTはチームなので、体制ではありません。 ②CSIRTの日本語名は定着したものがないので、企画管理編のように単にCSIRTと記載するのが良いと思います。 （案1）CSIRT（Computer Security Incident Response Team） （案2）CSIRT（Computer Security Incident Response Team（緊急対応チーム）） （案3）CSIRT（Computer Security Incident Response Team（インシデント対応チーム）） （案4）CSIRT（Computer Security Incident Response Team（緊急対応組織）） （案5）CSIRT（Computer Security Incident Response Team（インシデント対応組織））	CSIRTについては、体制として位置づける説明がされる例もありますので、原案の通りとさせていただきます。
55	経営管理編	３．４．３	①個人情報保護法に基づく報告は、情報漏えいが確定していなくても必要です。 ②医療情報でなくても、個人情報であれば報告が必要です。 参考:“漏えい等報告・本人への通知の義務化について ｜個人情報保護委員会” https://www.ppc.go.jp/news/kaiseihou_feature/roueitouhoukoku_gimuka/ （案1）また、インシデントの発生によって個人情報の漏えいのおそれがある場合には、個人情報保護法に基づく報告等が必要である（同法第 26 条、同法施行規則第 8 条）。 （案2）また、インシデントの発生による個人情報の漏えいが否定できない場合には、個人情報保護法に基づく報告等が必要である（同法第 26 条、同法施行規則第 8 条）。	ご指摘の修正案を踏まえて修正しました。
56	経営管理編	４．２	①「発見」的措置の説明なので、「仮に被害が発生しても」は「仮にインシデントが発生しても」の方が発見したニュアンスが伝わりやすいと思います。 ②インシデントや発見的措置の種類によっては「防止」と言えるほど効果を発揮できない場合があるので、もう少し控えめな表現のほうが良いと思います。 発見的措置は、仮にインシデントが発生しても、速やかに検知をすることで、被害の拡大を最小限にコントロールするための措置である。	ご指摘の修正案を踏まえて修正しました。
57	経営管理編	４．２	発見的措置を実施すべきだと考えらえるため、望ましいではなく、下記の表現にしてはどうか？ ＜修文案＞ ～、あるいは攻撃された痕跡を検知するなどの発見的措置も、適宜組み合わせること。	ご指摘の修正案を踏まえて修正しました。
58	経営管理編	５．１．２	文書の構成として「プライバシーマーク制度」に並ぶのは「ISMS」ではなく「ISMS認証制度」です。 個人情報保護に関しては「JIS Q 15001 個人情報保護マネジメントシステム」（プライバシーマーク制度と呼ばれる）があり、情報の安全管理に関しては「JIS Q 27001 情報セキュリティマネジメントシステム」（ISMS認証制度と呼ばれる）などの規格により、システム関連事業者における情報管理等の安全性を確認することができる。	ご指摘の修正案を踏まえて修正しました。
59	経営管理編	５．１．２	下部　注4 【意見内容】 以下の文言を追加する。 「なお、「クラウドセキュリティ認証等」プライバシーマーク認定や ISMS 認証と同等の認証や評価も企画管理編に記述され、これに代えることも可能である。ただし、これら認証の取得をもって、サービスそのもの安全管理水準を満たすわけではないことに留意する必要がある。システム等の安全管理の妥当性については、対象事業者内部の独立した監査部門や第三者機関2Iが評価を行っていることを確認することが望ましい。 【理由】 この記述は、２省ガイドライン４．３および４．４の趣旨に沿って書き換えると、実際の運用として有効なガイドラインとして活用できる。	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。
60	経営管理編	５．１．２	パスワードが記憶要素であることを経営層にも提示するため、下記の表現にしてはどうか？ ＜修文案＞ ～、”記憶要素である”パスワードに加えて”、記憶要素でない”別の要素を組み合わせる二要素認証を採用に可能な限り迅速に対応すること。	ご意見として参考にさせていただきます。
61	経営管理編	５．２．２	法の要件として個人情報保護法のみに限らない可能性があるため、下記の表現にしてはどうか？ ＜修文案＞ ～特に海外のシステム関連事業者を再委託先とする場合には、個人情報保護法”をはじめ国内法が”求める要件を具備しているか十分留意する必 要がある。	ご指摘の修正案を踏まえて修正しました。
62	企画管理編	２．１．５	約款契約におけるリスク表示および明示合意について、医療機関が確認すべき最低限の記載要素が不明確である。 民法第548条の2との関係を踏まえ、必要とされる記載内容および推奨される様式を明確に示されたい。	ご意見の内容は個別事案の内容かと存じますので、原案の通りとさせていただきます。
63	企画管理編	3	【意見2】クラウド利用・外部委託における「責任分界」の可視化 該当箇所：第3編（企画管理編）及び第5編（保守委託機関編） 意見の要旨： 医療DXの進展に伴いクラウドサービスの活用が一般化する中、医療機関とサービス事業者との間における責任の所在が不明確となることによる対策漏れが懸念される。このため、実務上のリスク低減の観点から、以下の点について記載の充実が望ましい。 （１）責任分界点の明確化： SaaS／PaaS／IaaS等の形態ごとに、医療機関と事業者がそれぞれ担うべき管理責任の範囲を、モデル図等により明示すること。 （２）契約実務の支援： 契約締結時に確認すべき事項として、セキュリティ要件、障害発生時の対応体制、データの移行性（ポータビリティ）等について、標準的なチェックリストを提示すること。	クラウドの責任分界の考え方は、システム運用編において示しているところですので、原案の通りとさせていただきます。
64	企画管理編	３．１．２	小規模の診療所、薬局、介護系小規模事業者等では、専任CISOの配置や独立したCSIRTの構築は現実的でない場合が多い。現行案のままでは、大規模組織を想定した体制整備が事実上の前提と読まれ、小規模医療機関が「何を最低限実施すれば適合的か」を判断しづらい。 本文は、非常時に必要な対応として「影響範囲や損害の特定」「被害拡大防止」「復旧」「再発防止」を挙げていますが、これらは必ずしも専任CISOや独立CSIRTがなくても、役割分担と外部支援の確保で代替可能です。小規模組織向けの実施可能なモデルを明示する方が、実効性と普及性が高まります。 追加案。 小規模の医療機関等において、専任の情報セキュリティ責任者（CISO）の配置又は独立したCSIRTの構築が困難な場合には、企画管理者、システム運用担当者、院長又は管理者、委託先事業者の連絡責任者その他必要な者により構成される「非常時対応責任者体制」又は「緊急時対応連絡体制」を整備し、初動対応、被害拡大防止、外部連絡、復旧判断及び再発防止の役割分担をあらかじめ定めること。 また、外部専門事業者、地域医療連携先、都道府県等の支援窓口その他の外部支援先を含めた連絡網を整備し、平時から利用可能な支援体制を確保すること。	ガイドラインでは、CSIRTの必須化は求めていないため原案のままといたしました。
65	企画管理編	３．２．２	システムとして認識されず、機器等にメンテナンス用の回線が含まれることがあるため、下記の表現にしてはどうか？ ＜修文案＞ 昨今、各部門が独自に調達したシステムや”医療情報システムに含まれない機器等、”それに伴う回線が、～	シャドーITの対象を広く禁止する観点から、原案の通りとさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
66	企画管理編	３．２．２	P18 ＞また、多数の外部接続点が存在することは、それ自体が管理を困難にし、VPN 装置等の脆弱性が放置されるリスクが増大する。新たに導入するシステムに保守回線が必要な場合は、医療機関側で集約した回線を利用可能な事業者を選定する等、管理の実効性を高めるための対策を講じること。 ーVPN事業者によるVPNのリモートメンテナンス回線を通じてランサムウェアに侵入されるケースが増えている。また、VPNの脆弱性を放置されるリスクを減らすには保守契約に当該の内容を盛り込むべき。それらを踏まえて以下のように修正案を提示する （修正案） また、多数の外部接続点が存在することは、それ自体が管理を困難にし、VPN 装置やリモートアクセス機能等に存在する脆弱性が長期間放置されるリスクを高める。特に、システム事業者等が保守・運用のために設置する VPN 等のリモートメンテナンス回線を経由して、不正侵入やランサムウェア感染に至った事例が増加しているとの指摘もある。 新たに導入するシステムにおいて保守回線が必要となる場合には、医療機関側で外部接続点や回線を集約・把握可能な構成とするとともに、当該回線を利用する事業者を適切に選定するなど、管理の実効性を高めるための対策を講じることが求められる。 あわせて、VPN 装置やリモートアクセス機能に関する脆弱性が適切に管理されるよう、保守契約等において、脆弱性情報の継続的な把握、セキュリティアップデートの実施方針および実施期限、設定変更や緊急対応を含む運用管理の責任範囲等を明確に定めておくことが望ましい。これらの内容が契約上担保されていない場合には、契約内容の見直しを含め、必要な対応を講じることが重要である。 P10 ＞特に委託先事業者が再委託を行う場合、再委託先事業者において生じた漏えい等の情報セキュリティインシデントの責任も、委託元の医療機関等の責任となりうることから、再委託先事業者の管理だけではなく選定などについても、委託先事業者と適切に分担することが求められる。また、医療機関等が購入した機器等については、別途、事業者と当該機器についての保守契約を締結しない場合には、原則、管理責任は医療機関等にあり、事業者との間での管理責任の分担は生じない。 ー医療機関に対して保守契約を締結しないリスクがこれでは伝わりにくい。リスクを伝えて、医療機関に保守契約の締結を促すために以下のように修正を提示する。 （修正案） 特に、委託先事業者が再委託を行う場合には、再委託先事業者において生じた情報漏えい等の情報セキュリティインシデントについても、委託元である医療機関等の責任が問われる可能性があることから、再委託先事業者の管理のみならず、その選定方針や管理方法についても、委託先事業者と適切に役割分担を行うことが求められる。 また、医療機関等が購入した情報機器等について、当該機器に関する保守契約を別途事業者と締結していない場合には、原則として当該機器の管理責任は医療機関等に帰属し、事業者との間で管理責任の分担は生じない。この場合、機器に対するセキュリティアップデートの実施、脆弱性への対応、障害発生時の迅速な復旧対応等が十分に行われないおそれがあり、結果として情報セキュリティリスクが高まる可能性がある。 これらのリスクを踏まえ、医療機関等においては、購入した機器等について適切な安全管理措置が継続的に確保されるよう、必要に応じて事業者との間で保守契約を締結し、その内容に管理責任の範囲や対応内容を明確に定めておくことが強く望まれる。	ご意見として参考にさせていただきます。
67	企画管理編	３．２．２	「また、多数の外部接続点が存在することは、それ自体が管理を困難にし、VPN 装置等の脆弱性が放置されるリスクが増大する。新たに導入するシステムに保守回線が必要な場合は、医療機関側で集約した回線を利用可能な事業者を選定する等、管理の実効性を高めるための対策を講じること。」の箇所です。 現実の医療現場においては、多くの部門システムベンダーや医療機器メーカー、あるいは診療情報を扱う前提のスマホ回線事業者や生成ＡＩ事業者が、システム導入やリモート保守の必須要件として「自社専用のIP-VPN等による閉域網の敷設」と「自社指定ルータの設置」を強く要求してきます。 高度な医療機器や特定領域の部門システムにおいては、事実上代替となる事業者が存在しない（あるいはリプレースのハードルが極めて高い）ケースが多く、ガイドラインに記載されている「集約した回線を利用可能な事業者を選定する」ことが現実的に不可能な場面が多々あります。 結果として、医療機関の意図に反して安全とされるはずの閉域網が乱立し、管理不能な多数の外部接続点が生じているのが実情です。医療機関側の「選定」という自助努力のみでこの問題を解決することには限界があります。 上記の現状を踏まえ、以下の点についてガイドラインへの追記、あるいは関連省庁（経済産業省・総務省等）の事業者向けガイドラインとの連携による対応をお願いいたします（または、これらの場合の対応方法についてご教示ください）。 ・ベンダーに対する要請の明記　医療機関側の対策としてだけでなく、「システム関連事業者（医療機器メーカー含む）は、自社専用の回線敷設を前提とするのではなく、医療機関側が集約・統合したネットワーク回線やVPNインフラを利用したセキュアなリモート保守の仕組みに積極的に対応すること」といった、事業者側への要請・指針となる文言を追加してください。 ・やむを得ない場合の責任分界の明確化　代替手段がなく、やむを得ずベンダー指定の専用閉域網及びVPN装置を導入せざるを得ない場合において、当該外部接続点（ルータやVPN機器等）の脆弱性監視およびセキュリティアップデートの実施責任が「システム関連事業者側（ベンダー側）」にあることを契約上明確にさせるなど、責任分界のあり方に関する具体的な記載の追加を提案します。	ご意見として参考にさせていただきます。
68	企画管理編	３．２．２ ８．２	■ 意見の要旨 医療機関のサイバーセキュリティ対策体制をより実効性のあるものとするため、専門的な技術知見を有する「臨床工学技士等の専門職種」の役割を明記することを提案します。特に「通信機能を備えた生命維持管理装置等の医療機器」のリスク管理において、これらの専門職種をセキュリティ担当者として位置づけるべきです。 ※生命維持管理装置の操作及び保守点検を行うことを業とするのは臨床工学技士のみ ■ 修正案 【現行案】 「企画管理者は、医療情報システムの安全管理のうち特に技術的な対応を行う担当者を任命し、経営層の承認を得る必要がある。」 【修正案】 「企画管理者は、医療情報システムの安全管理のうち特に技術的な対応を行う担当者を任命し、経営層の承認を得る必要がある。その際、医療機器を専門的に扱う臨床工学技士等の専門職種を、各部門のセキュリティ担当者や連携担当者として適切に位置づけること。」 ■ 理由 現在のガイドライン案においても医療機器安全管理責任者等との連携は示唆されていますが、近年の医療機器の急速なIoT化に伴い、ネットワークに接続された生命維持管理装置等へのサイバー攻撃は、単なる情報漏洩にとどまらず「患者の安全」に直結する事態となります。 生命維持管理装置の可用性を確保し、インシデント発生時にも医療継続を維持するためには、機器の工学的知識と臨床現場の運用の双方を熟知した臨床工学技士の関与が不可欠です。情報システム部門のみでは把握しきれない医療機器固有の挙動やリスク、保守運用や契約内容を、専門職種が現場の目で管理することで、初めて実効性のあるセキュリティ対策になり極めて重要であると考えます。	ご指摘の内容ですが、今般の改訂において「医療機器安全管理責任者」に関する記載を示して、その趣旨を示しております。
69	企画管理編	7	「f　プライバシーマーク認定又はISMS認証の取得」に以下を追記 「f　プライバシーマーク認定又はISMS認証の取得又は一般社団法人保健医療福祉情報安全管理適合性評価協会の民間事業者による医療情報に係るクラウドサービスの評価の取得」。 併せて、gの「プライバシーマーク認定、ISMS認証のいずれも取得していない場合」を「プライバシーマーク認定、ISMS認証、民間事業者による医療情報に係るクラウドサービスの評価のいずれも取得していない場合」とする。もしくは、「fのいずれも取得していない場合」と簡略化して記載。 その上でgの「民間事業者による医療情報に係るクラウドサービスの評価」（一般社団法人保健医療福祉情報安全管理適合性評価協会）を削除。 [理由] 　一般社団法人保健医療福祉情報安全管理適合性評価協会（以下、HISPRO）は、日本医師会、日本歯科医師会、日本薬剤師会、日本医療情報学会を社員団体として構成し、利用者・現場の視点から、事業者が提供するシステムの安全管理に対する適合性を本ガイドラインに基づいて評価する団体として、2009年から活動をしている団体である。医療情報の外部保存（クラウド利用）における評価についても、上記の通り実施している。 その評価項目は、PマークやISMS認証と同等の評価を実施しており、(6)の外部保存委託先事業者を選定するに当たり、前記2者と比較しても、より医療現場の利用者視点での評価を行うことができるため、f項に同列でHISPRO評価の取得を位置付けてもらいたい。なお、総務省、経済産業省の2省ガイドラインにおいては、HISPRO評価を取得することが明記されている。	ご指摘の箇所は、事業者に関する認証、サービスに関する認証、それらの例外などで整理しております。原案の通りとさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
70	企画管理編	7	遵守事項６　(丸付き)g 【・「民間事業者による医療情報に係るクラウドサービスの評価」（一般社団法人保健医療福祉情報安全管理適合性評価協会）】は資格ではないため、下記の表現にしてはどうか？ ＜修文案＞ 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果”もしくは第三者による評価結果”により、上記と同等の能力の有無を確認すること	ご指摘の修正案を踏まえて修正しました。
71	企画管理編	7	ISMSやISMAP等のセキュリティ認証等を用いる外部保存の委託先事業者の選定基準について、「外部保存」を目的としないクラウドサービス（医療画像等のAI解析サービス、その他文書の生成AIサービス等や、クラウド型VPN等のネットワークサービスなど）を利用・委託する場合の適用要否を明確化し、ガイドライン本文又は解説に明記していただきたいです。 システム運用編において脆弱性対策として推奨されている「クラウド型VPN」や、昨今医療現場で急速に利用が拡大している「クラウド上のAI解析サービス」は、医療情報の長期的な「保存」を主目的としない（一時的な処理や通信の通過のみを行う）場合がありますが、しかし、これらのサービスは機微な医療情報がネットワークを介して事業者の国外サーバに送信・処理（FFRCT等）されたり、院内ネットワークの重要な経路上に位置したりするため、情報セキュリティの観点では「外部保存」と同等以上の高いセキュリティ管理能力が事業者側に求められるべきです。 現在のガイドラインにおける「外部保存の委託先事業者を選定する際は」という限定的な表現のままでは、データ保存を主目的としないAIサービスやクラウド型VPN等の導入時に、医療機関側がISMAP等の基準を適用して事業者を選定する義務があるのかどうか、医療現場やシステム関連事業者との間で解釈が分かれ、セキュリティ水準の低下を招く懸念があります。 もしこれらの一時的な処理や通信中継等もガイドライン上は「外部保存」の定義に内包されるという解釈であれば、その旨を読者に誤解のないよう解説部分に明記してください。	ご指摘の箇所については、「⑥ 外部保存等の委託先事業者を選定する際は」とし、外部保存事業者以外も想定するようにいたしました。
72	企画管理編	7	医療情報システムの安全管理に関するガイドライン第6.1版企画管理編「７．安全管理のための人的管理」遵守事項５等における「保存された情報を格納する情報機器等が、国内法の適用及び執行の及ぶ範囲にあることを確実にすること。」にかかる修正については、実質的な内容の改正ではなくて趣旨の明確化等の意であるとの理解でよいか。 また、本規定は、その文言に従えば、国外に物理的に存在するサーバー等への情報の保存を一般的・網羅的にに禁止したものではないという理解であるが、様々なサービスが広がる中で、保存先や保存方法自体がサービスにより異なる中で、医療機関の予見可能性向上の観点からは、どのような条件下でどのような対応が許容可能か、具体的に明らかにしていくべきと考える。例えば、文科省の教育情報セキュリティーポリシーのP165（https://www.mext.go.jp/content/20250325-mxt_jogai01-100003157_1.pdf）においては、この部分だけでも判断要素を各種示しており、同様の対応を行うことも選択肢として考慮いただきたい。	医療情報の保存場所については引き続き検討を進める予定ですので、今回の改定では原案の通りとさせていただきます。
73	企画管理編	7	スタイルの振りがあります。 「ⓖ」で箇条書きのインデントを揃える（このガイドラインはWordで編集していると思いますので、a～i を直接入力するのではなく「新しい番号形式の定義」から「a, b, c, …」を選択すると揃うようになります。）	ご指摘の修正案を踏まえて修正しました。
74	企画管理編	7	【次回以降の改訂用のコメント】 「システム監査技術者」は経済産業省が2026年度を最後に廃止する方針を発表しています。方針が確定したら後継の「プロフェッショナルデジタルスキル(マネジメント)」(2027年度から)や「論述試験」(2028年度から)を含めるか、あるいは含めないかを明示的に読み取れるような記載に変更してください。 参考： "情報処理技術者試験における試験区分体系などの見直し（案）について　(METI/経済産業省）" https://www.meti.go.jp/press/2025/03/20260331003/20260331003.html "情報処理技術者試験及び情報処理安全確保支援士試験の見直しの検討状況について	試験情報	IPA 独立行政法人 情報処理推進機構" https://www.ipa.go.jp/shiken/syllabus/henkou/2025/20260331.html (左記参照)	ご意見として参考にさせていただきます。
75	企画管理編	7	■ISMAPの扱いに関して 係守委託機関編 P.5 「外部保存の委託先事業者選定」におけるISMAPの位置づけは「Q15001(プライバシ？マーク)、JISQ27001(ISMS)又はこれと同等の規格の認証を受 ているシステム関連事業者を選定すること。」とAND条件に読み取れる。 他方、企画管理編P.26,27「７．安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約）」におけるf,gでは下記のようにOR条件に読み取れる f　プライバシーマーク認定又は ISMS 認証の取得 g　プライバシーマーク認定、ISMS 認証のいずれも取得していない場合は(中略) 　　適切な外部保存に求められる技術及び運用管理能力の有無 　　・政府情報システムのためのセキュリティ評価制度（ISMAP） 上記2か所の相違が誤解を生むリスクがあるので、どちらかと言うと、企画管理編の記述に統一すべきであると思う。	ご指摘の修正案を踏まえて修正しました。
76	企画管理編	7	「f　プライバシーマーク認定又はISMS認証の取得」に以下を追記 | 「f　プライバシーマーク認定又はISMS認証の取得又は一般社団法人保健医療福祉情報安全管理適合性評価協会の民間事業者による医療情報に係るクラウドサービス評価の取得」。 併せて、gの「プライバシーマーク認定、ISMS認証のいずれも取得していない場合」を「プライバシーマーク認定、ISMS認証、民間事業者による医療情報に係るクラウドサービス評価のいずれも取得していない場合」とする。もしくは、「fのいずれも取得していない場合」と簡略化して記載。 その上で『・「民間事業者による医療情報に係るクラウドサービスの評価」（一般社団法人保健医療福祉情報安全管理適合性評価協会）』を削除。 【理由】 一般社団法人保健医療福祉情報安全管理適合性評価協会（以下、HISPRO）は、日本医師会、日本歯科医師会、日本薬剤師会、日本医療情報学会を社員団体として構成し、利用者・現場の視点から、事業者が提供するシステムの安全管理に対する適合性を本ガイドラインに基づいて評価する団体として、2009年から活動をしている団体である。医療情報の外部保存（クラウド利用）における評価についても、上記の通り実施している。 その評価項目は、PマークやISMS認証と同等の評価を実施しており、(6)の外部保存委託先事業者を選定するに当たり、前記2者と比しても、より医療現場の利用者視点での評価を行うことができるため、f項に同列でHISPRO評価の取得を位置付けてもらいたい。なお、総務省、経済産業省の2省ガイドラインにおいては、HISPRO評価を取得することが明記されている。 【意見内容2】 意見内容1が難しい場合、g の記載について、以下のように認識齟齬があるため修正を願いたい。 「上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力の有無を確認すること」（P.27の上から7行目） | 「上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果もしくは第三者による評価結果により、上記と同等の運用管理能力の有無を確認すること」 【理由】 HISPROによる評価は、有資格者による外部監査ではなく、HISPROが実施する第三者による評価となる。長らく当該記載になっていたものを指摘できていなかったが、今回「第三者による評価結果」を追記して、正しい表現に訂正をお願いしたい。 ただし、HISPROの位置付けに鑑みて、「意見内容1」を優先して考慮を願いたい。	ご指摘の修正案を踏まえて修正しました。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
77	企画管理編	7	遵守事項⑤について 【現状と課題】 現状の案では、保存された情報を格納する情報機器等の「管理または運用主体」に対し、「国内法が適用されかつその執行が及ぶ範囲にあること」を確実にすることが遵守事項として求められています。この規定は実運用上、以下の課題を生じさせます。 ・グローバル先進サービスの導入障壁： 世界共通のインフラで提供される最先端の診断支援AIやSaaS型医療機器プログラム（SaMD）は、スケールメリットを活かした24時間365日のグローバルSOC監視や即時パッチ適用を前提としています。運用の実体（海外本社等）に対して直接的な国内法の執行を求める解釈がなされると、日本独自の個別基盤構築が必要となり、コスト増大や提供遅延、最悪の場合は日本市場への導入断念を招きます。 ・物理的設置場所への過度な依存：「執行が及ぶ」ことを担保するために物理的な国内設置が事実上強制されると、災害復旧（DR）や負荷分散の観点からグローバルに分散配置された高度なクラウド基盤の恩恵を受けられなくなります。これはガイドラインが掲げる「可用性（医療継続性）」の維持に逆行する恐れがあります。 ・外資系企業の責任構造との乖離：外資系企業の日本法人は、国内でのサポートや責任を一手に引き受けますが、基盤の運用実体は海外の親会社にあることが一般的です。運用の実体そのものに直接の法執行を求める現規定は、日本法人が責任主体として機能する実態を反映できていません。 【修正案（解決策）】 企画管理編 7.5 遵守事項に以下の但し書き、または解釈の追記を提案します。 「保存された情報を格納する情報機器等の管理または運用主体に対し、国内法が適用されかつその執行が及ぶ範囲にあることを確実にすること。ただし、医療機関等と直接契約を締結する事業者（国内責任主体）が日本国内に拠点を有し、本ガイドラインに基づく全責任（データの真正性、見読性、保存性の維持等）を負うことを契約上担保した上で、海外の運用主体に対して実効的な管理監督を行っている場合は、本要件を満たしているものとみなす。」 【妥当性（理由）】 ・ガバナンスによる「執行力」の代替： 情報セキュリティマネジメントの基本は「責任の所在（Accountability）」です。物理的なサーバの場所や運用の実体がどこにあろうとも、日本の司法・行政権が及ぶ**「国内責任主体（元請け）」が、契約上の全責任を負う唯一の窓口となる**ことで、インシデント時の損害賠償や行政命令の履行は実効的に担保されます。これはISMS（ISO27001）における委託先管理の考え方とも整合します。 ・個人情報保護法との整合性： 個人情報保護法（第28条）では、外国にある第三者への提供において「相当措置（国内と同等の保護レベルを担保する体制）」を講じている場合には、国内と同等の取り扱いを認めています。ガイドラインにおいても、場所の制限ではなく、「国内法人が監督責任を負う」というガバナンス構造の構築によって法執行の目的は十分に達成可能です。 ・「サービス仕様適合開示書」による透明性の確保： サービス仕様適合開示書を活用し、外国法の適用リスク（例：米CLOUD法等）を透明化した上で、国内責任主体がそれをどうリスクヘッジ（暗号化の鍵管理を国内で行う等）しているかを医療機関に説明し合意を得るフローの方が、形式的な国内設置よりも実効的なセキュリティ向上に寄与します。 ・セキュリティの「動的」な維持： 現代の脅威は国境を超えて発生します。グローバルな運用主体が最新の脅威インテリジェンスに基づき一斉に防御策を講じ、それを国内法人が日本の基準で監視・評価する体制は、日本国民が最新かつ安全な医療サービスを享受するために合理的で現実的な構成です。	医療情報の保存場所については引き続き検討を進める予定ですので、今回の改定では原案の通りとさせていただきます。
78	企画管理編	7．3	「企画管理者は、職員に対する教育・訓練を定期的に行うことが必要である。また、就業時間内に実施すること。」 職員に対する情報セキュリティの教育・訓練（研修）の実施主体について、本ガイドラインでは実務を担う「企画管理者」とされている一方で、診療報酬の施設基準等では「医療情報システム安全管理責任者」とされており、記載の整合性が取れていません。現場での混乱を避けるため、両者の役割分担（計画・実務の主体と統括・責任の主体）を明確にするよう、記載の整理又は解釈の提示をお願いいたします。 例えば、「企画管理者は、医療情報システム安全管理責任者の指示・承認のもと、職員に対する教育・訓練の計画策定や実務を行うこと」といった、実務と責任の切り分けがわかる記載への修正を提案します。またこのような記載にする場合は、施設基準を満たすという解釈であることを、関連Q&Aや事務連絡等で明確にお示しください。	QAで医療情報システム安全管理責任者と、企画管理者の業務または役割分担を明確にさせていただきます。
79	企画管理編	7．3	本文書では「資格」が「試験」を含めるものと想定して以下コメントします。 ①「情報処理技術者資格」は「情報処理技術者試験」の誤りです。（補足：IPA系試験のうち国家資格に関連するものは情報処理安全確保支援士だけで、残りは全て国家試験です。） ②注釈9の参照元は『「情報処理安全確保支援士」、「情報セキュリティマネジメント試験」等の資格取得』となっているのに対し、注釈9は『情報処理安全確保支援士以外にも』となっているのは不揃いです。 ③「情報処理技術者資格等」の「等」について、この書き方では「等」は不要です。（補足：IPA系試験は情報処理技術者試験と情報処理安全確保支援士の2種類に区別されます。関連：情報処理の推進に関する法律） ④民間資格については並列されている資格からCISSP等を想定していると考えられるので、「医療情報の取り扱いに関する」または「情報セキュリティに関する」は「情報セキュリティまたは、これに関連する技術分野の」誤植だと思います。（補足：セキュリティそのものではないがこれに関連する民間資格（例：CCNA）を含める意図で記載しているのであれば、案2のほうが好ましいと思います。） (案1)独立行政法人情報処理推進機構（IPA）の実施する「情報処理安全確保支援士」等の資格取得[9]、演習・訓練への参加等を推進することが望ましい。 [9]資格については情報処理安全確保支援士以外にも、独立行政法人情報処理推進機構による情報処理技術者試験や民間事業者が認定する情報セキュリティの取扱いに関する資格が含まれる。 (案2)独立行政法人情報処理推進機構（IPA）の実施する「情報処理安全確保支援士」等の資格取得[9]、演習・訓練への参加等を推進することが望ましい。 [9]資格については情報処理安全確保支援士以外にも、独立行政法人情報処理推進機構による情報処理技術者試験や民間事業者が認定する情報セキュリティまたはそれに関連する技術分野の資格が含まれる。	ご指摘の修正案を踏まえて修正しました。
80	企画管理編	8．1．2	図8-1の「廃棄」内の「■廃棄」はメディアの物理的な廃棄、「■消去」はメディアの機能を維持した状態でデータだけ削除することを意図していると思いますので、「■廃棄」で列挙する記憶媒体は他に種類があることを読み取れる方が良いと思います。 （補足：企画管理編で他に「紙やフィルム」と記載している箇所がありますが、それらは電子化に関連するものなので横展開は不要です。） (案1)保存期間を過ぎた紙カルテ、フィルム、またはHDD等の記憶媒体の物理的廃棄 (案2)保存期間を過ぎた紙カルテ、フィルム、またはデータが格納されているHDD等の記憶媒体の物理的廃棄	次回の改定時に検討いたします。
81	企画管理編	8．1．2	図8-1の「暗号化消去」について、実運用としてはこれを許容しても良いかもしれませんが、本ガイドラインのように規範となるセキュリティとりまとめる文書においてはHNDL攻撃を想定して、この手法は推奨しないほうが良いと思います。 （補足：HNDL攻撃とは未来技術による計算速度向上や未来に発見される脆弱性を期待して、攻撃者が現時点で暗号データを取得・保管しておき、未来の技術を使って復号する攻撃のことを指します。例えば、量子コンピュータの登場で、現在の暗号技術はこの点で脆弱になることが想定されます。） （削除）	次回の改定時に検討いたします。
82	企画管理編	8．2．4	患者だけでなく、家族が参照する可能性があるため、下記の表現にしてはどうか？ ＜修文案＞ 患者”等”が、自宅等から”患者”の情報にアクセスする場合	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。
83	企画管理編	8．2．6	持ち出しの状況が限定されるか否かに関わらず、レビューは必要であるため、下記の表現にしてはどうか？ ＜修文案＞ ”（削除）”不正な持ち出し等が生じないように、定期的に持ち出し状況のレビューを行う必要がある。	原案は制限されていることを受けての不正持ち出しに対する対応を示す趣旨ですので、原案の通りとさせていただきます。
84	企画管理編	8．2．6	「医療情報が外部へ持ち出される状況は限定されており」は日本語が不自然なので（一般的にそうであるという事実を記載してあるように読めるので）他の表現に置き換えたほうが良いと思います。 医療情報の外部へ持ち出しは必要最小限にし、不正な持ち出し等が生じないように、定期的に持ち出し状況のレビューを行う必要がある。	ご指摘の修正案を踏まえて修正しました。
85	企画管理編	9	【遵守事項】④ サプライチェーンリスクの「確認・整理」に関して、事業者に対して求める文書および証跡の範囲が不明確である。 サプライヤー情報の開示、リスク登録簿、SBOM等との関係を含め、具体的な確認項目を明確に示されたい。	原案において「医療情報システムに係る委託先や機器に関するサプライチェーン関係を整理し、リスクアセスメントや対策の整備」の重要性を示しておりますので、原案の通りとさせていただきます。
86	企画管理編	12	表記揺れがあります。 ⑨サイバーセキュリティインシデントによる非常時としての対応が生じた場合には	ご指摘の修正案を踏まえて修正しました。
87	経営管理編	12．3	経営管理編に、サイバー攻撃を受けた又はその疑いがある場合について記載があるため、企画管理編にも下記の文章を追記してはどうか？ ＜修文案＞ ” 被害の拡大を防ぐために、連絡手段として、早急に状況を厚生労働省、社会保険診療報酬支払基金、都道府県警察、その他所管官庁等に報告することを含めること。”	ご指摘の修正案を踏まえて修正しました。
88	企画管理編	13	【遵守事項】⑤ 「管理者権限」の対象範囲について、OSの管理者権限に限定されるのか、クラウドサービスにおけるテナント管理者やアプリケーション管理者を含むのかが不明確である。 最小権限の原則が適用される対象範囲について、明確に示されたい。	例示である旨を示しました。
89	企画管理編	13	脚注10 デジタルアイデンティティガイドラインにおけるIALの適用主体について、患者以外の外部利用者（例：薬剤師等）に対する適用範囲が不明確である。 ガイドライン上の位置づけおよび参照方法について、明確に示されたい。	ご意見として参考にさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
90	企画管理編	１３．１．２	➢登録されたIDを利用する際の当人認証についても、厳格な認証方法が求められており、多要素認証やこれに準じた方法によること等を要する。 「厳格な認証方法」について、具体的な要件が読み取りにくく、解釈に幅が生じる可能性があると考えます。 また、本章では「多要素認証」という表現が用いられていますが、システム運用編の認証に関する記載では「二要素認証」という用語が使用されており、用語および要求水準の整合性について確認が必要ではないでしょうか。 ガイドライン全体の一貫性および現場での解釈の統一の観点から、表現の明確化、あるいは用語の統一をするべきと考えます。	「厳格な認証」につきましては、同ページ内脚注５にて記載をしております。また、他文書の引用を除き、本ガイドラインにおいては「二要素認証」に記載を統一しました。
91	企画管理編	１４．１	文章がおかしくなっているため、下記の表現にしてはどうか。 <修文案> システム更新や検証システムの互換性等の観点からも、”標準技術等を用いて適切に保存すること。”例えば、前”項”の標準技術を用い、～	ご意見として参考にさせていただきます。
92	企画管理編	１４．２	タイムスタンプが、一般財団法人日本データ通信協会が認定した時刻認証事業者のものとの記載のみで国際的にスタンダードな認証のものがない、WebTrust for CA - Time-Stamping, ETSI EN 319 422, eIDAS Qualified Time Stamp の３つを追加すべきである。 なお、法令保存期間等がない文書については、「タイムビジネスに係る指針ーネットワークの安心な利用と電子デ ータの安全な長期保存のためにー」等で示されている時刻認証業務の基準に準拠し、一般財団法人日本デー タ通信協会が認定した時刻認証事業者のものを使用することも可能である。 ↓ なお、法令保存期間等がない文書については、「タイムビジネスに係る指針ーネットワークの安心な利用と電子データの安全な長期保存のためにー」等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者のものを使用することも可能である。 他にも国際的な認証である、WebTrust for CA - Time-Stamping, ETSI EN 319 422, eIDAS Qualified Time Stampのいづれかを取得したタイムスタンプ局を使用することも可能である。	ご指摘の修正案を踏まえて修正しました。
93	企画管理編	１４．２	一般財団法人日本データ通信協会が認定した時刻認証事業者のもの自体が、既に存在せず、総務大臣認定による認定制度のものに置き換えられているため、下記の表現にしてはどうか。 <修文案> なお、法令保存期間等がない文書について”も、「時刻認証業務の認定に関する規程」に基づき認定された事業者が提供するタイムスタンプを利用することが望ましい。”	ご指摘の修正案を踏まえて修正しました。
94	企画管理編	１５．１	一方で、医療情報システムにおける技術的対応については、専門的な知見が必要であり、これを有する担当者に委ねることが想定される。この場合、技術的な対応のうち、基本的なルールを規程や規則などで定め、具体的な運用管理は担当者に権限移譲することとなる。また、運用管理は事業者に委託することも想定される。特に、アップデートについては可能な限り、事業者の保守範囲に含めることが望ましい。保守範囲とならない場合は、医療機関等の責任でアップデートが必要となる。 クラウドサービス利用は責任共有モデルが前提となる。「特に、アップデートについては可能な限り、事業者の保守範囲に含めることが望ましい。保守範囲とならない場合は、医療機関等の責任でアップデートが必要となる。」となると、後述3.4にもある責任分界において一方的に事業者側の負担を強いるものになる。 以下のように修正してはどうか。 「特に、アップデートについては、医療機関等と事業者において対応範囲を明確にして、双方において管理範囲の機器類に責任をもってアップデートを行う必要がある。」保守委託機関編P3注釈2も同様。	ご指摘の内容は具体的な契約内容に依存する部分も多いため、原案の通りとさせていただきます。
95	企画管理編	１５．１	保守を行うシステム関連事業者と契約やSLA等により管理項目(ISやソフトウェアのアップデート、パッチ適用に関する役割分担)について取り決めを行うこと、と記載されているが15.1にあるように事業者の保守範囲に含めること記載があり、事業者側責任としてアップデートを行う事を期待していると捉えるべきでしょうか。	専門性の観点から事業者の対応に委ねるべきとする趣旨であり、費用に関して無償とする趣旨ではないので、原案の通りとさせていただきます。
96	企画管理編	１５．１	事業者側責任においてアップデートを行うという事は、アップデートを行った結果不幸にも不具合が発生した場合は、ベンダー責任範疇において対処する事を期待するものでしょうか。	専門性の観点から事業者の対応に委ねるべきとする趣旨であり、費用に関して無償とする趣旨ではないので、原案の通りとさせていただきます。
97	企画管理編	１５．１	ソフトウェアの動作に問題が発生したり、OSがストールするような事例も極まれに発生する事が考えられますが、セキュリティアップデートへ対応を行う事が最優先課題であると捉えるべきでしょうか。	システム運用編11.1において「OSのセキュリティ・パッチ適用後やマルウェア対策ソフトのパターンファイル最新化後の稼働確認、あるいはバックアップファイルの復旧テストなどを実施することが求められる。」と記載しております。
98	企画管理編	１５．１	アップデートの結果、動作異常が発生し機能停止が発生した場合、SLA内のシステム稼働率の計算対象になるでしょうか。環境要因に対するリスクをベンダーが担保する場合、保守契約料としてユーザー様へご負担を頂く事も想定されますが、ご容赦頂けますでしょうか。	ご意見の内容は個別事案の内容かと存じますので、原案の通りとさせていただきます。
99	企画管理編	１５．１	非インターネット環境下でセキュリティアップデートを行う為には、アップデータを手動で収集し、院内への持値込みを行う必要があり実現は非常に困難となります。現実的な対応としては適切な通信先設定を施したFierWallが必要と考えますが、これらの環境はベンダーの責務で準備するべきでしょうか。	アップデートの方法は個々のシステムや構成により異なるため、原案の通りとさせていただきます。
100	企画管理編	１５．１	アップデートを利用者が少ない時間帯で実施する場合、夜間、深夜、休日での対応となる事が考えられますが、有人監視を伴わない自動実行する事は許容されるでしょうか。 適用結果確認もベンダーの責務に含む場合は有人対応が必要となりますが、労働人口の減少と労務時間管理の関係上、対応は困難と考えております。通常稼働時間内でのシステム停止に対して、お客様へ協力を頂く事も必要になると考えておりますが、ガイドラインの中であるいはQ&Aの中で、全体方針についてお示し頂けないでしょうか。	アップデートの方法は個々のシステムや構成により異なるほか、現在の記載はリアルタイムでの臨席を求めるものではないため、原案の通りとさせていただきます。
101	企画管理編	１６	【遵守事項】②③④ 紙媒体の医療情報を電子化する際に求められている、情報作成管理者の配置（②）および電子署名の遅滞ない付与（③）等について、一律に厳格適用した場合、大規模薬局等の実務運用との乖離が生じるおそれがある。 特に、多数の処方箋を取り扱う現場においては、スキャンごとの個別確認や即時の電子署名は現実的に困難であり、運用の形骸化を招く懸念がある。 このため、真正性の担保手段については人的確認のみに限定せず、ログ管理や改ざん検知等の技術的統制や、一定条件下での後追い確認等を含めた柔軟な要件とされたい。	原案は従来からの変更はありません。原案の通りとさせていただきます。
102	システム運用編	全体	医療情報システムの定義には、医療情報を扱う医療機器も当然として含まれます。しかし、医療機器といってもさまざまなものがあり、OSのないもの、キーボードのないものなど、その特性はさまざまなものが存在しています。また、組込みを意識したEmbeddedと呼ばれるOSは、廉価である半面、End Userにその機能がアクセスできないようにすることが望まれていて、それに適した構成をとります。基本的には、本ガイドラインの主旨を考慮した上で適切な対応が望まれるのかと思います。しかし、医療機器ならではの考慮も必要かと思っています。医療機器を特性に応じてグループわけした上で適切な解釈が可能なガイドラインなどを医療機器の業界とともに作成、開示することが良いのではないかと考えます。	ご意見として参考にさせていただきます。
103	システム運用編	全体	2. 全体に対する概要 ガイドライン（案）システム運用編について フィッシングメールやなりすましメールは増加傾向にあり、国内のフィッシング報告件数は直近5年間で約25倍に増加しています。医療機関を装った不正メールによる情報漏えいやマルウェア感染のリスクも高まっており、電子メールを起点としたサイバー攻撃対策の重要性は一層高まっています。 本ガイドライン（案）の項目にある「通信の暗号化・盗聴等の防止」「サイバーセキュリティ対応」「第三者提供（メール送信）の責任分界」に関連して、サイバー攻撃の侵入経路として電子メールが想定されますが、送信側ドメインのなりすまし対策についての具体的な言及が無いため、アンチウイルスやEDR等のエンドポイントセキュリティ対策と組み合わせた多層防御の一環として、送信ドメイン認証技術を用いたなりすまし対策を盛り込むことを提案します。 なお政府においては、内閣官房国家サイバー統括室が公表する「政府機関等のサイバーセキュリティ対策のための統一基準群」に含まれる「政府機関等の対策基準策定のためのガイドライン（令和7年度版）」において、DMARCの導入・活用が基本対策事項として示されています。 DMARCは国際的に広く利用されている仕組みであり、総務省においても事業者・団体に対して導入や段階的なポリシー強化が周知・推奨されています。医療分野においても、監視から隔離、拒否へと段階的に対応を進める形で記載することで、現場負担を抑えつつ、なりすましメールによる被害低減につながると考えます。 本ガイドラインにDMARCを明示的に位置付けることは、医療機関から送信される電子メールの信頼性向上及び関係者全体のセキュリティ確保の観点から有益であると考えます。	ご意見として参考にさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
104	システム運用編	３．４	サービス類型による責任分界点を例示されていますが、オンプレミス型でも複雑な責任分界点が発生します。 例えば、病院情報システムの稼働基盤として、仮想化基盤を選択された場合、仮想化基盤のベンダー、 ハードウェア調達のベンダー、OS調達キッティングのベンダー等が必要になりますが、 動作条件やセキュリティ等に関しては相互に影響を及ぼすため、明確な境界設定が困難になる事例が存在します。 サーバーへの二要素認証がOSレベルでの実装となるため、OSに付随する機能として基盤ベンダー側が提供するべきか、アプリケーションを動作させるベンダーが提供するべきかは、ガイドライン中で明記頂く方が混乱は生じないと考えます。	ご意見の内容は個別事案の内容かと存じますので、原案の通りとさせていただきます。
105	システム運用編	３．５	医療機関等が、管理する医療情報を第三者に提供する場合に、医療機関等と提供先との間で責任分界を取り決めることになる。第三者提供を実施する方法としては、下記などが想定される。 ・メール等による情報の送信 ・サーバやクラウドサービス等への提供 ・アプリケーションが連携する際のデータの提供 ➢ 提供方法に応じたデータの送受信に係る責任分界など技術的対策に関する内容を定める必要がある。例えば、 メール送信の場合、医療機関等が利用するメールサーバまでは、医療機関等が責任を有する等が考えられる。 ➢ システム運用担当者は、企画管理者が取り決めた第三者提供における責任分界と整合性をとれる責任範囲を 設定し、企画管理者に報告すること。 意見（修正案） ３．５ 第三者提供における責任分界 医療機関等が、管理する医療情報を第三者に提供する場合に、医療機関等と提供先との間で責任分界を取り決めることになる。第三者提供を実施する方法としては、下記などが想定される。 ・メール等による情報の送信および受信 ・サーバやクラウドサービス等への提供 ・アプリケーションが連携する際のデータの提供 ➢ 提供方法に応じたデータの送受信に係る責任分界など技術的対策に関する内容を定める必要がある。例えば、 メール送信の場合、医療機関等が利用するメールサービスまでは、医療機関等が責任を有する等が考えられる。 ➢ システム運用担当者は、企画管理者が取り決めた第三者提供における責任分界と整合性をとれる責任範囲を 設定し、企画管理者に報告すること。 （追記事項） メールサービスを利用した第三者提供を行う場合、メールの送受信に対して、なりすまし対策（送信ドメイン認証技術の導入）を実施すること、不正な利用やなりすましが行われていないかを送信ドメイン認証技術を利用して監視するなどが考えられる。 理由： 「メール等による情報の送信および受信」と受信を追加する必要があると考えます。また、クラウド環境も踏まえて「メールサーバ」→「メールサービス」と表記するのが一般的と考えます。外部攻撃の代表的入口であるメールに対し、技術的対策例としてDMARC等を例示すると、現場の導入判断がしやすくなるため。本件、「１８．１ サイバーセキュリティ対応」「１３．３ 通信の暗号化・盗聴等の防止」と関連付けての記述としても有効です。	ご指摘の修正案を踏まえて「メール等による情報の送信および受信」に修正いたしました。「（追記事項）」においてご指摘いただいた内容については、クラウドサービスを利用する場合以外にも想定されることから、原案のままといたします。
106	システム運用編	4	【意見5】PDCAサイクルを定着させるための「簡易ツール」の提供 該当箇所：第2編（経営管理編）及び第4編（システム運用編） 意見の要旨： 安全管理対策の継続的改善（PDCA）を実効性のあるものとするためには、運用負荷の軽減が重要である。特に小規模な医療機関においても実施可能なよう、 ·①自己点検用の簡易チェックシート ·②外部監査を活用する際の留意点 ·③改善活動の記録様式（標準フォーマット） 等を付録として提示することが望ましい。これにより、専門人材が限られる現場においても、自律的な安全管理水準の維持・向上に資するものと考えられる。	ご意見の内容は今後の対応の参考にさせていただきます。
107	システム運用編	5	この記載では脆弱性が発見され安全でなくなった暗号通信(例:SSL3.0)や、そもそも現時点で平文通信が行われているプロトコルを廃止できなくなります。これはセキュリティ的に危険であるため、何かしら追記が必要です。通信に互換性を求めるのではなく、システム全体で見た機能に互換性を求める記載にしてはいかがでしょうか？	ご指摘を踏まえ、危殆化したプロトコルに関して追記しました。
108	システム運用編	5	相互運用性確保のために標準規格の利用を推奨されております。 他方、近年医療技術発展のために、多数のレジストリデータ収集が行なわれておりますが、毎年多くの改訂が入り収集項目の追加のみならず、カテゴライズの変更、基準の変更等が発生し、標準化出来ていないデーターも多数発生する状況にあります。 研究目的のデータ収集を事前に正規化することは困難ではありますが、大規模データ収集を行う場合には、レジストラー側にもご協力いただき相互運用性確保を目指す事が必要と考えますので、レジストリデータについても、互換性に配慮し相互運用に配慮することが望ましいと記載整理することは出来ないでしょうか。	ご意見の内容は個別事案の内容かと存じますので、原案の通りとさせていただきます。
109	システム運用編	7	■ 該当箇所 システム運用編 （「7 IoT機器を利用する場合…」の項、および「必要に応じて速やかに脆弱性対策を講じる必要があるが…」に続く「検査装置等に付属するシステム・機器についても同様である」の記載箇所） ■ 意見の要旨 「検査装置等に付属するシステム・機器についても同様である」という限定的な表現を改め、「医療機器」を対象としていることが明確に伝わる表現への修正を求めます。 ■ 修正案 【現行案】「検査装置等に付属するシステム・機器についても同様である。」 l 【修正案】「医療機器およびそれらに付属するシステム・機器についても同様である。」 （いずれの箇所も同様の文章） ■ 理由 ガイドライン案では、IoT機器と同様の対策（リスク分析、脆弱性対策、不正接続防止等）を求める対象として、医療機器のなかでも「検査装置等」という特定の機器が特出しされて記載されています。 しかし、現場の視点で見ると、現在の院内ネットワークには、放射線装置、内視鏡システム、ダヴィンチ等の手術支援ロボット、そして生体情報モニターのシステムなど、多種多様な医療機器が接続されています。サイバーセキュリティの脅威に晒されているのは決して検査装置のみではなく、検査装置のリスクが他より高い根拠も示されていません。 とりわけ、今年2月に発生した事例においては、検査装置ではなくナースコールおよび医療機器の保守回線からサイバー攻撃を受けたと報道されています。あらゆる医療機器およびそれらに付属するシステム・機器が攻撃の起点となり得る現状において、厚労省のガイドラインで「検査装置等」と特定の機器群のみを例示することは、現場の医療従事者やシステム管理者に「検査装置以外の機器は対象外、あるいは対策の優先度が低い」というセキュリティ上の死角（誤認識）を生じさせる強い懸念があります。 サイバー攻撃から病院機能を確実に守り抜くためには、一部の装置に限定するような表現を避け、すべての医療機器が網羅的にサイバーセキュリティ管理の対象となるよう、文言の適正化を強く要望いたします。	ご指摘の修正案を踏まえて修正しました。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
110	システム運用編	7	【遵守事項】⑬利用者による外部からのアクセスを許可する場合は、盗聴、なりすまし防止及びアクセス管理を実現したVPN技術により安全性を確保した上で、仮想デスクトップ等を利用する運用の要件を設定すること。 【遵守事項】⑬において、利用者による外部からのアクセスを許可する場合の対策として、VPN 技術により安全性を確保した上で「仮想デスクトップ等を利用する運用の要件を設定すること」と記載されている点について意見を述べます。当該記載は、医療情報が利用端末側に残存しない運用を求める趣旨として、適切な方向性を示しているものと理解しております。 一方で、「仮想デスクトップ」が例示として明記されていることにより、それ以外の技術的選択肢が分かりづらく、医療機関が自施設の規模や運用体制に応じた方式を選択しにくくなる可能性があると考えます。特に医療分野においては、ガイドラインにおいて例示された手法が事実上の必須要件として受け取られる傾向が強く、記載されていない方式については、同等の安全性を有していたとしても採用判断が難しくなるケースが見受けられます。実務上は、仮想デスクトップ方式に加え、セキュアブラウザ、コンテナ方式による業務領域分離、アプリケーション仮想化等、端末側に医療情報や業務データを残さないことを目的とした各種手法が存在します。これらはいずれも、適切な利用者認証およびアクセス管理と組み合わせることで、同様の安全管理水準を実現可能な方式と考えられます。 総務省が所管する各種ガイドラインにおいては、特定の実装方式に限定せず、複数の技術的手段を例示する形で記載されていることから、同様の公共性を有する医療分野のガイドラインにおいても、技術中立性の観点から、仮想デスクトップ以外の方式についても例示、もしくは包含的な表現とすることが望ましいと考えます。 つきましては、【遵守事項】⑬の記載について、仮想デスクトップ方式に限定されない形で、「管理下の環境にのみアクセスさせる方式」等の表現を用いる、あるいは複数の実現手法を例示するなどの修正を求めます。	原案においてもデスクトップ等としており、必ずしもこれに限定する記載ではないため、原案通りとさせていただきます。
111	システム運用編	7	・ 医療機関等の管理が及ばない私物のPC や、不特定多数の人間が使用するPCの場合、医療機関等の想定と異なる環境で使用され、安全管理上の支障が生じる可能性がある。したがって、職員による外部からのアクセスを行う場合は、盗聴、なりすまし防止及びアクセス管理を実現したVPN技術等により安全性を確保した上で、仮想デスクトップを利用する等の運用要件を設定すること。ここでいう仮想デスクトップ等とは、利用する端末の作業環境内に、ユーザ認証を経た後で、医療機関等に設置した機器の画面を表示する仕組みである。その他、ユーザ権限を厳格に管理した専用端末の貸与等も考えられる。 医療機関等の管理が及ばない私物端末や不特定多数が使用する端末からのアクセスに関する考え方について、VPN 技術等を用いて安全性を確保した上で、「仮想デスクトップを利用する等の運用要件を設定すること」とされている点について意見を述べます。当該記載は、医療情報が端末側に残存しない環境を実現するという点において、適切な方向性を示しているものと理解しております。 一方で、「仮想デスクトップ」が単独で例示されていることにより、それ以外の技術的手法の選択肢が分かりづらく、医療機関において導入方式の検討が行いにくくなる可能性があると考えます。 特に医療分野においては、ガイドラインに例示された手法が事実上の標準要件として受け取られる傾向が強く、記載されていない方式については、技術的に同等のセキュリティ水準を満たしていたとしても、採用に慎重にならざるを得ないケースが少なくありません。実務上は、仮想デスクトップ方式に加えて、セキュアブラウザ、コンテナ方式による業務領域分離、アプリケーション仮想化等、同様に端末側への医療情報の残存を防止し、利用者認証およびアクセス制御を適切に行う手法が存在します。 総務省が所管する分野のガイドラインにおいては、特定の実装方式に限定せず、複数の技術的手段を例示する形で記載されていることから、同様に公共性の高い医療分野のガイドラインにおいても、これらの方式を含む表現とすることで、技術中立性の確保および医療機関における適切な方式選択を促進できると考えます。 つきましては、当該記載において仮想デスクトップ以外の手法についても例示する、または「管理された環境にのみ画面表示または業務領域を限定する方式」等のより包括的な表現に修正いただくことを求めます。	原案で、「仮想デスクトップ等」としておりご指摘の内容に対応できることを想定しております。原案の通りとさせていただきます。
112	システム運用編	7	医療情報システムに接続されるIoT機器（ネットワークカメラ、各種センサー、ウェアラブル端末等）の安全な選定基準として、経済産業省等が推進する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の認証取得を要件化、あるいは推奨とする方向での検討がなされているか伺いたいです。 また、検討されているのであれば、本ガイドライン又は解説書等にその旨を追記・明示していただきたいです。	セキュリティ要件適合評価及びラベリング制度（JC-STAR）」に関しては、その性格等を検討した結果ですので、原案の通りとさせていただきます。なお、IoT機器が同制度に対応すること自体は妨げるものではありません。
113	システム運用編	7．1	「設定」が曖昧なので、「認証機能の有効化」の方が良いと思います。 例えば端末の起動パスワード等の認証機能の有効化は必須であり、このパスワード等は認証ルールに沿った内容であることが求められる。	ご指摘の内容では、パスワードルールの設定などが読み取れないことから、原案の通りとさせていただきます。
114	システム運用編	8	BYODは「個人端末を持ち込むこと」を表す言葉なので、ここでは「BYOD端末」が適切です。 (案1)⑪BYOD端末であっても、医療機関等が管理する情報機器等と同等の対策が講じられるよう、手順を作成すること。 (案2)⑪BYODデバイスであっても、医療機関等が管理する情報機器等と同等の対策が講じられるよう、手順を作成すること。	ご指摘の修正案を踏まえて修正しました。
115	システム運用編	8．1	「パッチの適用」はソフトウェアの更新方法の一部を指すので、より広い表現の方が良いと思います。 (案1)報告されているソフトウェアのアップデート (案2)報告されているソフトウェアの更新	ご指摘の箇所については、医療機関等における対応を示す趣旨ですので、原案の通りとさせていただきます。
116	システム運用編	8．1	①「通信ポート」をファイアウォール等でブロックすることを「非活性化」と呼ばないので、別の表現に置き換えたほうが良いと思います。 ②ポートを塞ぐだけでなく、利用するポートについても宛先を制限することでセキュリティの向上できることから、それを読み取れる記載のほうが良いと思います。 ③特に理由がなければ、サービスの非活性化はサービスの停止に置き換えたほうが良いと思います。（ただし、何かしら停止できないサービスを想定して記載しているのであれば、そのままのほうが良い。） 利用していないサービスの停止、通信のフィルタや遮断	ご指摘を踏まえ、記載を「対策としてはセキュリティ・ホール（脆弱性）が報告されているソフトウェアへのパッチ適用、利用していないサービスや通信ポートの閉鎖、ネットワークの構成分割やネットワーク間のアクセス制御、マクロ等の利用停止、メールやファイルの無害化がある。」に修正しました。
117	システム運用編	8．1	システム運用編　p.16 「＞　対策としてはマルウェアのスキャン用ソフトウェア」で始まる項目について 【現状と課題】 本項目を元に、医療機関指定のマルウェア対策ソフトウェアを医療機器（有体物）へ導入することを強く求められることがありますが、製造販売業者が検証していないマルウェア対策ソフトをインストールすることができません。 医療機器（有体物）にはホワイトリスト型のマルウェア対策を行っている製品が多々ありますが、マルウェアの感染を防止するための対策の事例としてホワイトリスト型のマルウェア対策が記載されていないため、医療機関にホワイトリスト型がマルウェア対策として有効であると認識されないことがあります。 【修正案（解決策）】 以下のように修正し、スキャン用ソフトウェア以外にも効果的なマルウェア対策があると表すことを提案します。 ▼----------▼ 対策としてはマルウェアのスキャン用ソフトウェアの導入等のマルウェア対策が効果的である。 ▲----------▲ さらに、Q&Aに以下の内容を追記することを提案します。 ▼----------▼ Q-nn ガイドライン（システム運用編 8.1）に記載されている「マルウェア対策」には、ホワイトリスト型のマルウェア対策も含まれるか。 A はい、含まれます。ホワイトリスト型マルウェア対策は、マルウェアの感染を防止するための有効な対策の一つです。特に医療機器のように、実行されるプログラムが固定されているシステムにおいては、許可されたプログラムのみの実行を許容するホワイトリスト型対策は非常に有効です。一般的な「ブラックリスト型（シグネチャ型）」のマルウェア対策ソフトは、頻繁な定義ファイルの更新が必要であり、ネットワーク隔離環境にある機器や、動作リソースに制約がある医療機器には適さない場合があります。システムの特性や運用環境に応じ、ホワイトリスト型対策を含めた最適な手法を選択することが推奨されます。 ▲----------▲ 【妥当性（理由）】 医療機器の品質保証と製造販売業者による保守責任を継続することで機器を動作継続し患者安全を保つと共に、効果的なマルウェア対策を行うことができます。	ご指摘の修正案を踏まえて修正しました。また後段のご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
118	システム運用編	８．１	システム運用編　p.16 「➢　対策としてはマルウェアのスキャン用ソフトウェア」で始まる項目について 【現状と課題】 本項目を元に、医療機関指定のマルウェア対策ソフトウェアを医療機器（有体物）へ導入することを強く求められることがありますが、製造販売業者が検証していないマルウェア対策ソフトウェアを医療機器にインストールすることができません。 未検証ソフトウェアの導入は、機器の動作不良を招く患者安全上のリスクに加え、薬機法上の改造に該当する可能性があり、製造販売業者による品質保証や保守責任の継続が不可能となるため、未検証のマルウェア対策ソフトをインストールすることができない理由を製造販売業者から医療機関へ説明いたしますが、医療機関にご納得いただくまで多大な時間を要することがあります。 【修正案（解決策）】 Q&Aに以下の内容を追記することを提案します。 --- Q-nn　医療情報システムに接続する医療機器に対して、医療機関が独自に指定するマルウェア対策ソフトをインストールして稼働させるよう、製造販売業者に求めることは適切か。 A　医療機器（有体物）に対して、製造販売業者が許可していないソフトウェアを導入することは、薬機法上の改造に該当する可能性があり、適切ではありません。医療機器は、特定のハードウェアとソフトウェアの組み合わせで薬事承認・認証を受けており、未検証のソフトウェアの導入は機器の動作不良を招くなど、患者安全上のリスクとなります。また、製造販売業者による品質保証や保守責任の継続が不可能となる恐れもあります。 医療機器におけるマルウェア対策については、まずMDS2等を確認し、当該機器の特性に応じた適切な対策（ホワイトリスト型対策の採用、又は特定の対策ソフトの指定等）を製造販売業者に確認することが必要です。 --- 【妥当性（理由）】 医療機器の品質保証と製造販売業者による保守責任を継続することで機器を動作継続し患者安全を保つと共に、効果的なマルウェア対策を行うことができます。	医療情報システムが医療機器である場合に、薬機法などに則った適切な対応を行うことは所与のことですので、原案の通りとさせていただきます。
119	システム運用編	８．２	編集ミス？ 利用するソフトウェアについて、SBOM（Software Bill of Materials：ソフトウェア部品表）が事業者から提供されることもある。	ご指摘の修正案を踏まえて修正しました。
120	システム運用編	８．２	SBOMの提供について「適宜」との記載では運用解釈にばらつきが生じるおそれがある。 提供形式、更新頻度、更新契機等について、最低限の指針を具体的に示されたい。 また、一般的な薬局や小規模医療機関においては、SBOMを解析し脆弱性を評価・管理できる専門人材が限られており、SBOMの提供のみを前提とした運用では実効性の確保が困難となるおそれがある。 このため、SBOMの提供に加え、事業者側における脆弱性管理および対応状況の整理・説明を求めるなど、役割分担を明確にした運用とされたい。 また、OSSやライブラリの管理方針や脆弱性対応プロセス等の提供を通じて、医療機関側が妥当性を評価できる形を認めるなど、実務に即した対応が可能となるよう配慮されたい。	SBOMの現状の運用状況等を勘案し、原案の通りとさせていただきます。
121	システム運用編	８．２	システム運用編　p.17「➢　検査装置等に付属する」で始まる項目について 【現状と課題】 本項目の「また医療機器がEOSを迎えた場合」以降の説明は、この6.1版で追加されています。 本項目より四つ上の項目で、EOSの対象となった情報機器が起点となったサイバー攻撃について触れており、それを受けて医療機器がEOSを迎えた場合の対応について本項で指針を示していると思いますが、医療機器のEOS以降、使用継続することで発生し得るリスクなどの重要な説明が「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」で述べられています。そのため、医療機器のEOSに際しての説明を本項で行うのであれば、手引書を確認していただいたうえで、医療機器を管理する部署の担当者と連携していただくことが重要であると考えます。 また、現行の安全管理ガイドラインには用語集が準備されていますが、現行の用語集にもEOS（End of Support）の定義・説明がない ので、正しい理解のためにも追加するべきではないかと考えます。 【修正案】 「➢　検査装置等に付属する」で始まる項目について以下のような追記・修正することを提案します。 --- ➢　検査装置等に付属するシステム・機器についても同様である。また医療機器がEOSを迎えた場合の対応等については、「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」を事前に確認しておき、医療機器安全管理責任者等の医療機器を管理する部署の担当者と医療情報システム安全管理責任者等のシステム担当者が十分に連携を取りながら管理すること。 --- さらに、6.1版の用語集にEOS（End of Support）の定義・説明をお願いいたします。 【妥当性】 医療機器については先述の通り、手引書で重要な説明が行われているため、医療情報システム安全管理責任者等のシステム担当者においても手引書に対して理解いただいておくことが必要と考えます。	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。
122	システム運用編	８．２	【該当箇所】 第 6.1 版 システム運用編 ８．２「情報機器等の脆弱性への対策」 【意見の内容】 SBOMの活用に関する記述において、経済産業省「ソフトウェア管理に向けた SBOM導入に関する手引2.0」との整合性を図り、VEX（Vulnerability Exploitability eXchange）等を用いた「悪用可能性評価」の重要性を明記することを要望します。 【理由・根拠】 現行案の記述では、SBOMの作成・入手のみが強調され、あたかも「SBOMから検知された脆弱性すべて」が対応対象であるかのような誤解を与える懸念があります。 【実務上の懸念】 SBOMによりコンポーネントが可視化されると、製品の実際の動作環境では悪用不可能な脆弱性（False Positive）も多数検知されます。悪用可能性評価を欠いた形式的な運用がなされた場合、医療機関およびメーカー双方において、優先度の低い脆弱性対応に過大なリソースが割かれ、真に深刻なリスクへの対応が遅れる恐れがあります。 【他省庁ガイドラインとの整合性】 経済産業省の「ソフトウェア管理に向けた SBOM導入に関する手引 ver2.0」では、SBOMは脆弱性管理の「出発点」であり、VEX等を用いて「当該製品での悪用可能性」を評価し、対応の要否を判断する運用の重要性が明示されています。 https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html 【要望事項】 医療情報システムにおける脆弱性管理の実効性を高めるため、以下の趣旨をガイドライン本文または注釈に含めることを検討いただきたいです。・SBOMは脆弱性特定のための基盤情報であること。・特定された脆弱性に対し、VEX等を活用して「自組織の環境や製品仕様における悪用可能性」を評価し、リスクに基づいた合理的な対応判断を行うことが推奨されること。これにより、医療現場とメーカにおける過度な運用負荷を軽減しつつ、リスクに基づいた実効性の高いセキュリティ対策が促進されるものと考えます。	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。
123	システム運用編	８．２．６	４番の項番がなくなっています。	ご指摘を踏まえて修正しました。
124	システム運用編	８．３	医療機器製造販売業者の視点でのコメントになりますが、IDの変更(例えば、Windowsログオン)IDの変更)を義務付けると事前にセットアップしたものを納品することができなくなるため、医療機関に設置する際の作業や、運用時の保守におけるコミュニケーションの増加が想定されます。本ガイドラインでは利用者に初期パスワードの変更等を求めているため、IDは攻撃者にとって既知でも問題ないはずで、この部分は削除しても問題ないと思います。 --もしくは、何かしら技術的背景によって(例えば、リバースブルートフォース攻撃の対策として)IDを隠すことを推奨している場合は、その旨をガイドラインに明確にし、IDをパスワードと同種の取り扱いにすることを記載しておかなければ、機密性を維持できないと考えられます。 また製品出荷時にパスワード等が設定されているものは、必ず製品出荷時から変更すること。	改定案ではIDの変更を求めているわけではありませんので、原案の通りとさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
125	システム運用編	８．３	２段落目 （p.18） ①何の「ID」であるかを明確に。 ②本改訂でIDの変更まで求めるようになっていますが、一般的な概念としてIDは知られても問題ありません。 ③サーバで管理者権限を持つIDに限定するのは、優先度としては理解できますが、特に区別する必要はありません。 ＜現行版(第6.0版)＞ また製品出荷時にパスワード等が設定されているものについては、必ず製品出荷時のものから変更することが重要である。サーバで利用するソフトウェアの管理者権限を有する ID 等においても同様である。 ＜修正前＞ また製品出荷時にパスワード等が設定されているものは、必ず製品出荷時から変更すること。サーバで利用するソフトウェアの管理者権限を有する ID 等においても同様である。 ＜修正後＞ また製品出荷時にパスワード等が設定されているものは、必ず製品出荷時から変更すること。製品出荷時から設定されているアカウント ID については使用予定がないものは削除または無効化すること。	ご指摘の修正案を踏まえて修正しました。
126	システム運用編	９	スタイルに誤りがあります。(色) (「③」と「医療情報システム」の間の灰色を削除)	ご指摘の修正案を踏まえて修正しました。
127	システム運用編	９．１	システム運用編　p.19「➢　システム運用担当者は、医療情報システムで」で始まる項目について 【現状と課題】 医療機器においては、システム構成やソフトウェバージョン、その組み合わせ等は製造販売業許可や修理業許可のもと業者が管理することが要求されます。本項目において「医療情報システムを構成するソフトウェアのバージョンや組み合わせ等の直接管理」という説明がありますが、「直接管理」という言葉からはシステム運用担当者が第三者に委ねず自ら手を下す必要があると解釈されてしまうリスクがあります。その場合、医療機器関連法規と逸脱した運用を招きかねないと存じます。 【修正案】 「➢　システム運用担当者は、医療情報システムで」で始まる項目について、以下のように修正することを提案します。 --- （修正前）医療情報システムを構成するソフトウェアのバージョンや組み合わせ等の直接管理することが求められる。 （修正後）医療情報システムを構成するソフトウェアのバージョンや組み合わせ等を適切に管理nすることが求められる。 （標外に追加） n 医療機器の場合は関連法規に則った運用を要する --- 【妥当性】 設置型医療機器（CT、MRI等）および診断支援用SaMD等の医療機器は、複数のソフトウェアおよびハードウェアが高度に統合された複雑な構成を持っており、その構成変更やバージョン管理は、通常、製造販売業者または保守事業者が実施することを前提とした運用が行われているため、上記修正案は妥当であると考えます。	ご指摘の修正案を踏まえて修正しました。
128	システム運用編	９．１	句点による文の接続が不自然です。 構成管理に関する計画を策定し、実施されていることを確認することが重要である。 クラウドサービスの場合は特に、このような構成管理を直接、医療機関等が行うことは困難であり、同様に手順や計画の整備状況し、実施状況の確認を行うこと。	ご意見として参考にさせていただきます。
129	システム運用編	１０． １２．	１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置 １２．物理的安全管理措置 スタイルに誤りがあります。(インデントの不揃い) (それぞれ、④～⑦、③～⑥のインデントの不揃いの解消)	ご指摘の修正案を踏まえて修正しました。
130	システム運用編	１０	個人情報保護法を念頭に置いた項目だと思いますが、その視点で言えば第17条の「利用目的の特定」をここに記載したほうが良いと思います。 https://laws.e-gov.go.jp/law/415AC0000000057#Mp-Ch_4-Se_2-At_17 ①動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、利用目的を明らかにし、保守終了後に確実にデータを消去することを求め、その結果の報告を求めること。	ご指摘の点は、動作確認等の保守作業目的であることを示しておりますので、原案の通りとさせていただきます。
131	システム運用編	１０	【遵守事項】④ リモートメンテナンスに関する記載 および 表10-1、ならびに 第14章 認証・認可に関する安全管理措置 【遵守事項】④において、リモートメンテナンス実施時の外部接続に関するリスク低減措置について記載されていますが、本文中では具体的な認証手段として二要素認証の実施が明記されておりません。 一方で、表10-1においては、リモートアクセス時に OS の二要素認証を採用することを前提とした整理がなされており、また、第14章「認証・認可に関する安全管理措置」では、【遵守事項】および本文の双方において二要素認証の必要性が明確に記載されています。 これらを踏まえると、リモートメンテナンスが外部からの侵入リスクおよび影響度の高い行為である点を考慮し、 【遵守事項】④の本文においても、リモートアクセス時には二要素認証等の強固な認証方式を実施する旨を明記することで、ガイドライン全体としての記載の統一性および意図の明確化につながると考えます。 つきましては、【遵守事項】④において、リモートメンテナンス時の対策例の一つとして、 OS レベルを含む二要素認証の採用について補足的に記載いただくべきと考えます。	表10-1において14.1.1の参照を促しておりますので、原案の通りとさせていただきます。
132	システム運用編	１０	OSのアカウント管理を、事業者側とシステム管理者側で並行して行う事は可能ですが、安全上はシステム管理者側に一本化された方がよろしいかと思います。但し、その場合ベンダー側保守要員の増減に伴う作業はシステム管理者側にお願いする事となり業務負荷が非常に重いと思われます。	ご意見として参考にさせていただきます。
133	システム運用編	１０	システム運用編　p.20「➢　また保守を行う際には、サーバ上のOS」で始まる項目について 【現状と課題】 対象となる医療情報システムが医療機器である場合、保守業務を行うにあたっては修理業許可を受けた事業者による対応が求められています。本項目は一般的な医療情報システムの保守を想定したものとは思いますが、医療機器においては薬機法など関連法規に基づいた対応が必要である旨の記載を追記すべきと思います。 【修正案】 「➢　また保守を行う際には、サーバ上のOS」で始まる項目の文末に以下を追記することを提案します。 --- なお、医療機器の場合は、薬機法などの関連法規を遵守した対応を図ること。 --- 【妥当性】 本記載を追加することで、対象となる医療情報システムが医療機器である場合に、薬機法などに則った適切な対応が実施されるため、妥当であると考えます。	医療情報システムが医療機器である場合に、薬機法などに則った適切な対応を行うことは所与のことですので、原案の通りとさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
134	システム運用編	１０．１	システム運用編 p.21 表１０－１について 【現状のパブコメ案で生ずる実運用上の具体的課題】 p.21 表１０－１でリモートメンテナンスにおいて実施すべき事項として、特権ID権限の厳格管理（管理者共通アカウントの禁止等）が記載されておりますが、「管理者共通アカウントの禁止」が一律に適用された場合、以下のような課題が発生すると考えます。 ・リモートサービスのサービス対象システムやサービス範囲にも依りますが、以下のような管理者権限を要する作業も多く、多数の要員がリモート保守に従事します。リモートサービスの対象医療機関の医療情報システムは数百システムの場合も多く、管理者共通アカウントを禁止した場合、要員一人ひとりの個別アカウントの管理は対象システム数および要員数に伴って非常に煩雑化してしまいます。そのため、多数の管理者アカウントの管理は管理ミスを誘発し、不正アクセスや情報漏えいのリスクを高めてしまうと考えられます。 ・業務上、（Windowsの場合）サービスやイベントログ、ディスクアレイ管理などの情報を確認するために、管理者権限が必要となります 【解決策としての修正文案】 該当項目を以下のように修正することを提案します。 ―― ・特権ID権限の厳格管理（管理者共通アカウントの禁止を原則とするが、以下の措置も許容する） 　－ リモート接続において二要素認証を導入し、接続者の特定を確実に行うこと ―― 【解決策が妥当である理由】 10.1　保守時の安全管理対策として、「保守した者が特定できるようにすること」を求めており、その目的の観点からも上記解決策は妥当と考えます。	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。
135	システム運用編	１０．１	システム運用編 10.医療情報システム・サービス事業者による保守対応等に対する安全管理措置 保守作業の為にサーバに事業者の保守要員がアクセスする場合、専用アカウントを使用すると明記されていますが、病院のシステム管理者はサーバにアクセスしない前提での記載でしょうか。 10.1ではシステム運用担当者側がアクセス権管理を行うように記載されていますので、システム管理者側にも同様に専用アカウントが必要にならないでしょうか。	ご指摘の内容は、現行の内容でも読み取れると判断しましたので、原案の通りとさせていただきます。
136	システム運用編	１０．１	1システムで使用するシステムサービス用アカウントは、多くても数種類と思われますが、保守作業時に制限されたアクセス権でアクセスした場合でも、必要に応じてシステムサービスアカウントを使用する必要が発生します。こららのサービスアカウント情報は、一時的な作業時キャッシュ情報として残る危険性があります。ブラウザなどに記憶情報としての残存、あるいはメモ情報として制限されたユーザプロファイル上にシステムアカウントが残存するような場合です。運用でこれらを完全に回避するのは困難ですので、システムサービスアカウントの操作が必要な場合には管理者アカウントでのログインを許容する方が合理的ではないでしょうか。専用のアカウントという文言を削除し、管理者権限を有しないアカウントを大量にサーバー上で管理するのは危険性も踏まえ、管理者権限を有しない保守要員用のアカウントを使用させという表現に改めることは出来ないでしょうか。	ご指摘の点は個々のシステムに依存するところもありますので、原案のとおりとさせて頂きます。
137	システム運用編	１０．１	システム運用編 p.21 表１０－１について 【現状と課題】 表１０－１「通信経路・接続方式に起因するリスク」の「実施すべき事項」において、暗号化（SSH、VPN による安全なプロトコルの採用、RDP・VNC などを直接インターネットに開放しない利用等）が記載されているが、暗号化には例示されているもの以外にも、「１３．ネットワークに関する安全管理措置」に示されているプロトコル／ツールがある。SSHやVPNに限定されてしまうと、他のプロトコルの暗号化が医療機関から否定されてしまうリスクがある。 【修正案（解決策）】 以下のように修正することを提案します。 ―――――――――――――――――――――――――――――――― ・「１３．ネットワークに関する安全管理措置」を参照 【妥当性（理由）】「１３．ネットワークに関する安全管理措置」で暗号化に限らず遵守事項が定められているため、参照させるのが妥当であると考えます。	ご指摘の修正案を踏まえて「表１０―１ リモートメンテナンスにおいて実施すべき事項」を修正しました。
138	システム運用編	１０．１ １４．１．１	医療情報システムの安全管理に関するガイドライン第6.1版 システム運用編（案） １０．１ 保守時の安全管理対策 該当文：「サーバ上の OS や DBMS などで製品出荷時に設定されている管理者 ID（例えば Administrator）などは使わず、各保守担当者の ID を設けて、管理者権限を付与する等、保守した者が特定できるようにすることも求められる。 １４．１．１ 利用者の識別・認証 該当文：「サーバについては OS のログイン時に二要素認証を実装すること。 サーバのOSログインに対する二要素認証の導入や、不要アカウントの削除等が求められていますが、実際の医療現場では、システム保守事業者（ベンダー）が「社内規定」や「担当SEがその都度変わる」ことを理由に1つの共通アカウント（特権ID）を使い回している実態が多々あります。このベンダー側の運用実態が二要素認証導入の大きな阻害要因となっているため、ベンダー側に対する指導の強化や、実効性のある技術的代替策（踏み台サーバや特権ID管理ツールの活用条件など）をガイドライン及び関連Q&Aで明確にしていただきたいです。 本ガイドラインや毎年の医療法立入検査における「サイバーセキュリティ対策チェックリスト」において、「職種・業務別のアクセス権限設定」や「不要アカウントの削除」等の厳格なアカウント管理が求められ、本改定ではサーバOSへの二要素認証の導入も明記されています。 しかしながら、多くの医療機関において、サーバの保守を担うベンダー側からは「全国の顧客に対して、夜間休日を含めその時の事案でどのSEが保守対応するか分からないため、SE個人のアカウント管理は不可能である」「社内規定で1つの保守用共通アカウントで実施する決まりになっている」と主張されるケースが後を絶ちません。さらには、これを理由としてチェックリストの事業者用回答において「対象外」と回答して済ませようとするベンダーも多く存在します。 複数の人間が1つのアカウントを共有する運用では、誰が操作したのかという「責任の所在（証跡）」が追えなくなるだけでなく、二要素認証（多要素認証）における「所持情報」や「生体情報」を個々のSEに紐づけることが技術的・運用的に困難となり、サーバOSへの二要素認証導入が実質的に不可能となってしまいます。 医療機関側が安全管理措置を講じようとしても、ベンダー側が「共通アカウント運用」を譲らない限り、システム改修が進まないというジレンマに直面しています。 上記の懸念を踏まえ、以下の対応を提案いたします。 ・ベンダー側の「対象外」回答の禁止と指導強化 「担当SEが特定できない」といったベンダー側の都合を理由として、共通アカウントの使い回しを正当化し、二要素認証やアカウント管理の要件を「対象外」とすることを認めない旨を、医療機関向けのみならず「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（2省ガイドライン）」とも連携して明確に示し、事業者への指導を強化してください。 ・実務に即した技術的代替策の明記 ベンダーの組織体制上、どうしても個々のサーバに全SEの個別アカウントを発行することが困難な場合を想定し、「別ドメインに設置された踏み台端末」や「特権ID管理ツール（一時的なパスワードの払い出しや操作録画を行うシステム）」等を活用し、「誰が、いつ、共通アカウントを利用したか」を厳密に統制・追跡できる仕組みが担保されていれば要件を満たすとするなど、医療機関とベンダーが現実的に実装可能な管理手法を例示してください。	ご指摘の点については、各医療機関等の運用方法に依存すると考えられますので、原案の通りとさせていただきます。
139	システム運用編	１０．２	【遵守事項】④、本文 リモートメンテナンスの対象となる作業範囲について、具体的な境界が不明確である。 リモートデスクトップ等を用いた保守作業（証明書更新等）が対象に含まれるかを含め、明確に示されたい。	リモートメンテナンスの作業範囲は、具体的なシステムや対象により多様であることなどを踏まえて、原案の通りとさせていただきます。
140	システム運用編	１０．２	正確には「リモートサービス」と「セキュリティガイドライン」の間にスペースが入ります。 リモートサービス セキュリティガイドライン	ご指摘の修正案を踏まえて修正しました。
141	システム運用編	１０．２	表１０－１ リモートメンテナンスにおいて実施すべき事項に関して、VPNの脆弱性に対応できない内容となっており、VPNの脆弱性があっても攻撃の対象とならなような対策が必要である。特にVPNはアクセス元、アクセス先を攻撃者に見つからないようにすることが重要である。 通信経路・接続方式に起因するリスク　に以下を追加。 ・VPN、SSHなどのリモート接続元をリモートメンテナンス元のみに制限 ・VPNの接続先を対象機器のみに制限 ・接続をIPv6のみもしくは携帯電話閉域網のみに限定を推奨	ご指摘事項につきましては、原案のままで読み取れると判断し、本改定ではご意見として頂戴しました。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
142	システム運用編	１０．２	システム運用編　p.35 「➢　このため、サーバ OS については」で始まる項目について 【現状と課題】 ガイドラインの記述がRDPまたはSSHを想定した対策が記載されており、RDPまたはSSH以外のプロトコルや仕組みを利用するリモートメンテナンスでは技術的に実施できない対策となっております。このため、RDPまたはSSHを利用するリモートメンテナンスでのサーバOSについての要件であることを明記するのはいかがでしょうか。 【修正案（解決策）】 「このため、サーバOSについては」で始まる項目の２行を修正することを提案します。 --- ➢　このため、RDPやSSHを利用する場合のサーバOSについては、以下①②いずれか、またはそれと同等以上の措置が施されていれば、二要素認証を実装できているものとみなす。 （末尾までは修正なし） --- 【妥当性（理由）】 ・元々の記載内容がRDPとSSHに限定されており、他が排除されてしまうリスクを考慮して、RDP・SSHを利用する場合と明記することが妥当と考えます。	原案ではRDP、SSH等としており、それ外のプロトコルや仕組みを認めない趣旨ではありません。原案の通りとさせていただきます。
143	システム運用編	１０．２	システム運用編　p.35 「➢　このため、サーバ OS については」で始まる項目関連について 【現状と課題】 RDPまたはSSH以外のプロトコルや仕組みを利用するリモートメンテナンスでは、院内のネットワークやシステムの再構築を必要とせずとも、リモートメンテナンスの仕組みの中に二要素認証を導入できることが多々あります。このため、RDPまたはSSH以外のプロトコルや仕組みを利用するリモートメンテナンスについては、リモートメンテナンスの仕組みの中に二要素認証が導入されていれば良いことを明記するのはいかがでしょうか。 【修正案（解決策）】 以下の項目を「このため、サーバOSについては」で始まる項目の下に追記することを提案します。 --- ➢　また、RDPまたはSSH以外のプロトコルや仕組みを利用するリモートメンテナンスでは、リモートメンテナンスの仕組みの中に二要素認証を実装していれば、サーバOSにて二要素認証を実装できているものとみなす。 --- 【妥当性（理由）】 外部からの攻撃が実施される状況としてリモートメンテナンスが想定されております。リモートメンテナンスの仕組みに二要素認証を実装していることを確実にすることで、攻撃が実施されるリスクを有意に低減できると考えられます。	二要素認証について示している内容は、ネットワーク機器の二要素認証だけで代替することを認めておりませんので、原案の通りとさせていただきます。
144	システム運用編	１１	①「／」が「または」なのか「かつ」なのかを明確にしたほうが良いと思います。 ②ここでは「分離」の方が良いと思います。構成分割は分離の手段であること、このコンテキストにおいては分離の方が一般的に使われる表現であるためです。 (5)サイバー攻撃による被害拡大の防止の観点から、論理的または物理的に分離されたネットワークを整備すること。	①については「本ガイドラインにおける『論理的／物理的』は、論理分離又は物理分離のいずれかもしくはその両方を満たすことを意味しており、「／」を用いる方が意図が伝わりやすいと考えるため、原案のとおりとさせていただきます。」 ②についてはご指摘の修正案を踏まえて修正しました。
145	システム運用編	１１．１	医療情報システムの安全管理に関するガイドライン第6．1版システム運用編（案） １１．１ 通常時における運用対策 表１１－１ 通常時に対応すべき技術的対応例 ランサムウェア対応のバックアップにおいては、３種類あり ・一定期間追記不能型のWORM機能ストレージ ・追記不能型のデータバックアップのWORM記録媒体 ・オフラインバックアップ これらのいずれかの対応で良いことからこの３種類を含む表記に変更したほうが良い。WORMは製品種類のキーワードなので検索性を高めるために入れたほうが良い。 ・追記不能型のデータバックアップの記録媒体の整備 | ・追記不能型のデータバックアップのWORM記録媒体、一定期間追記不能型のWORM機能ストレージもしくはオフラインバックアップの整備	ご指摘の修正案を踏まえて修正しました。
146	システム運用編	１１．１	「繰り返す、」の部分が編集ミスと思われます。 特にサイバー攻撃の場合、バックアップデータには既にマルウェアの混入による影響が及んでいる可能性も高く、不用意にバックアップデータから復旧により被害を繰り返すことで、被害を拡大する等のリスクもある。	ご指摘の修正案を踏まえて修正しました。
147	システム運用編	１１．２	システム運用編　p.23「➢　非常時における対応の一つとして」で始まる項目とその次の項目について 【現状と課題】 これら２項目では、非常時における対応として非常時用ユーザアカウントの運用が挙げられており、非常時用アカウントの利用に関するリスクに言及していますが、非常時アカウントの作成／利用に限られていると思います。他には、非常時の運用に関する事前の準備不足・周知不足がある場合、たとえば医療機器においてアカウントロックを発生させてしまうことで、医療機器の利用が阻害されてしまうリスクも考えられます。 【修正案】 「➢　非常時は、通常時とは」で始まる項目の文末に以下を追記することを提案します。 --- なお、非常時の運用に関する事前の準備・周知不足は、医療情報システム／医療機器の利用が阻害されてしまうリスクも考えられるため、システム運用責任者及び関係者間で慎重に管理すること。 --- 【妥当性】 非常時の対策に起因するセキュリティリスクだけでなく、非常時の対策の徹底が不十分だった場合のリスクについて理解し、事前の準備、システム／機器を利用する可能性がある関係者への周知を徹底することは不可欠と考えられるため、上記修正は妥当と考えます。	ご指摘の修正案を踏まえて修正しました。
148	システム運用編	１２．１	バックアップの取り方についての記載が分散しているので、12.1に集約した方が良いと思います。 （関連：11、12.1、18.1）	ご意見として参考にさせていただきます。
149	システム運用編	１２．１	空行になっている「▸」があります。 （中身のない箇条書きを削除）	ご指摘の修正案を踏まえて修正しました。
150	システム運用編	１２．３	【意見3】インシデント発生時における「行動指針」の具体化 該当箇所：第4編（システム運用編）「インシデント対応」 意見の要旨： サイバー攻撃発生時には、現場の混乱により初動対応が遅れるリスクがあることから、より実践的な対応指針の提示が有用と考えられる。 現行案の基本的な考え方に加え、以下の事項についてフローチャートやアクションカード形式で補足することが望ましい。 ① タイムラインの例示： 検知からネットワーク隔離、証拠保全、復旧判断に至るまでの時系列に沿った対応手順。 ② 外部報告の整理： 厚生労働省、警察、IPA、JPCERT/CC等への報告ルート及び優先順位の整理。 ③ 診療継続性の確保： システム停止時における代替手段（紙カルテ運用等）への切替判断の考え方。	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。
151	システム運用編	１３	遵守事項６ (丸付き) TLSを用いたSSL-VPNが⑥の遵守事項で対策を行うように見えるため、下記の表現 にしてはどうか？ <修文案> ～IPsecによるVPN等を利用せず”プロトコルを限定したTLS接続をする場合 （HTTPS、FTPS等）”、TLSのプロトコルバージョンを～	ご指摘の修正案を踏まえて修正しました。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
152	システム運用編	１３	医療情報システムの安全管理に関するガイドライン第6．1版システム運用編（案） １３．ネットワークに関する安全管理措置 【遵守事項】⑤ ルータ等のネットワーク機器は管理インターフェイスやログイン画面が露出していることが侵害される原因になっているので、これらを露出させない必要があります。 以下の文章を追加。 機器の管理インターフェイスやログインページ、管理ポートを外部からアクセスできないようにすること。	ご指摘の修正案を踏まえて修正しました。
153	システム運用編	１３	医療情報システムの安全管理に関するガイドライン第6．1版システム運用編（案） １３．ネットワークに関する安全管理措置 【遵守事項】⑦ VPNの種類が前世代のもののみになっています。AWSが採用しているOpenVPNやWireGaurdも採用すべきVPN方式です。IPSec+IKEはセキュリティ上の理由で強く非推奨となっているプロトコルです、IPsec+IKEv2に移行すべきなので残してはいけません。 (https://datatracker.ietf.org/doc/html/rfc9395) 原則としてIP-VPNかIPsec＋IKEによること。 ↓ 原則としてIP-VPNかIPsec＋IKEv2(PSK認証を除く)、OpenVPN，WireGuardによること。	ご意見を踏まえて修正、追記しました。
154	システム運用編	１３	【遵守事項】⑥ TLSクライアント認証に代わる「同等以上の安全性を有する措置」について、具体的な技術的構成が不明確である。 ZTNAやトークンベース認証等を含め、許容されるアーキテクチャおよび判断基準を明確に示されたい。	原案では、適切な通信の暗号化と接続先相互での信頼性の確保を求めることを想定しておりますが、個々の技術を示すことは困難なので、原案の通りとさせていただきます。 必要に応じてQAでの反映を検討します。
155	システム運用編	１３	システム運用編にあった「境界防御的な対応を原則とする」という記載が無くなったことについて。 「境界防御では不十分」だとする記載との整合性が取れていなかった点が改善し、「原則をまずやるべきで他は優先度が低い」と誤って受け止められることが減ると期待されるため、望ましい変更であると思います。	ご意見として参考にさせていただきます。
156	システム運用編	１３	「採用する」はまとめられます。 必要な単位で、互いに確認し、採用する通信方式や認証手段を決めること。	ご指摘の修正案を踏まえて修正しました。
157	システム運用編	１３	ネットワーク機器の脆弱性についての記載がないので、追加した方が良いと思います。 直近の関連ニュース： "一部ネットワーク商品における複数の脆弱性とその対処方法（JVN#83788689）	バッファロー" https://www.buffalo.jp/news/detail/20260323-01.html "NV26-001: セキュリティ情報	NEC" https://jpn.nec.com/security-info/secinfo/nv26-001.html ⑮運用中のネットワーク機器の脆弱性情報を定期的に収集すること。脆弱性が報告されている場合は脆弱性が修正されたバージョンのファームウェアに更新するか、もしくは補完的措置を講じること。EOSを迎えたネットワーク機器は使用を停止し、サポートされている機器に置き換えること。	8.2における記載の中で対応しておりますので、原案の通りとさせていただきます。
158	システム運用編	１３	11番の項番がなくなっています。	ご指摘を踏まえて修正しました。
159	システム運用編	１３	１３．１ ネットワークに対する安全管理 ⑩ ネットワーク経路でのメッセージ挿入、マルウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。 ↓ 意見（修正案） ⑩ ネットワーク経路でのメッセージ挿入、マルウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。特に電子メールにおける送信ドメイン認証技術（SPF/DKIM/DMARC）導入による受信メールの認証、送信時に受け取り手が認証できるように送信メールに対しても同様に導入すること。 理由： ネットワーク経路における改ざんや中間者攻撃への対策としては、通信の暗号化等に加え、電子メールを悪用したなりすましやマルウェア配布への対策が重要となっています。電子メールは日常的に利用される通信手段であり、送信元を詐称した攻撃が多発していることから、ネットワークに対する安全管理の一環として位置付ける必要があります。	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。
160	システム運用編	１３．１	図番号および参照している文章で、下記の修正をするべき。 <修文案> ・”図12-1” →”図13-1” ・”図12-2” →”図13-2”	ご指摘の修正案を踏まえて修正しました。
161	システム運用編	１３．１	昨今では、回線事業者による回線サービスとして、携帯電話網を利用することも増加 しているため、下記の表現を追加してはどうか？ <修文案> 回線事業者による回線サービス（ex. Flets、ISDN”、携帯電話網”）	ご指摘の修正案を踏まえて修正しました。
162	システム運用編	１３．１	図12-1で示されている回線事業者による回線サービスが、接続先が限定され経路が管理されている回線として、セキュアなネットワークとしての「公衆網」もしくは「回線事業者による回線サービス」として定義される記載されるべきところ、図12-2では表現されていない。 医療機関と接続先（外部保存先、関係機関等）を結ぶ線として、公衆網を、専用線とIKE＋Ipsec接続の間に配置すべき。	ご意見として参考にさせていただきます。
163	システム運用編	１３．１．１	ネットワークの論理的または物理的な構成分割、接続機器の制御、通信するデータの制御等のセキュリティ対策を実施する旨が記載されている点について意見を述べます。 当該記載は、医療情報システムにおけるネットワークセキュリティ確保の基本的な考え方を示すものとして、適切な方向性であると理解しております。一方で、「ネットワークの論理的な構成分割」について、どのような考え方や実現手法を想定しているのかが本文からは読み取りにくく、医療機関やシステム構築担当者において解釈に差が生じる可能性があると考えます。実務上、ネットワークの論理的構成分割には、VLAN 等によるセグメンテーションや仮想ネットワークによる分離といったネットワークレイヤでの分割に加え、セキュアブラウザやコンテナ方式による業務領域の分離など、端末上の利用環境を論理的に分離する手法も広く用いられています。これらの手法はいずれも、医療情報や業務データを管理下にない利用環境から隔離するという点で、論理的な構成分割の一つの実現形態と考えられます。 このように、「論理的な構成分割」はネットワーク機器構成のみに限られるものではなく、利用端末やアプリケーションレイヤにおける分離方式を含めた多様な実装方法が存在します。代表的な考え方や例示を補足的に記載いただくことで、医療機関が自施設の規模や運用体制に応じて適切なセキュリティ対策を検討・選択しやすくなり、ガイドラインの実効性向上につながると考えます。 つきましては、本項において、ネットワークの論理的構成分割に関する考え方について、複数の実現手法を包含する形で補足説明または例示を追加することが必要するべきと考えます。	本ガイドラインではクラウドサービスの実装形態までを示すことを目的としていないので、原案の通りとさせていただきます。
164	システム運用編	１３．１．２	495250498000000005_医療情報システムの安全管理に関するガイドライン_署名URL.pdf（mTLSに関する代替措置対応に関する図資料による要望）	ご意見として参考にさせていただきます。
165	システム運用編	１３．１．２	表13-1においては、オンプレミス環境を前提としたネットワーク構成に軸足が置かれた記載となっているが、近年はクラウドファーストの進展により、フルクラウドで運用される医療情報システムも増加している。 クラウド基盤上における閉域的な通信制御やアクセス管理等により、実質的に高い安全性を確保している構成も存在するが、これらに関する言及がないため、現行の記載のみでは実務との乖離が生じるおそれがある。 このため、クラウド前提のネットワーク構成についても、ガイドライン適合性の考え方および評価観点を明確に示されたい。	該当記載は「オンプレミス環境を前提としたネットワーク構成に軸足が置かれた記載」を想定するものではないこと、TLS接続に関する要件を示しているのはクラウド環境も想定していることから、原案の通りとさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
166	システム運用編	１３．１．２	自治体において総務省が「自治体情報セキュリティ対策の抜本的強化」として具体的なネットワーク分離モデル（三層分離のαモデル、βモデル等）を提唱しているのと同様に、医療機関においても、現代のクラウド利用やゼロトラスト思考を前提とした具体的な「医療機関向けネットワークアーキテクチャモデル（推奨構成モデル）」をガイドライン本文又は別冊等で明示すべきではないでしょうか。 医療機関においては、これまでも長らく「電子カルテネットワークとインターネットの分離」という事実上のネットワーク分離（境界防御）が行われてきました。 しかし近年、オンライン資格確認の導入、クラウド型電子カルテや各種SaaSの利用拡大、さらには保守ベンダーごとのVPN回線の乱立により、医療機関のネットワークは複雑なツギハギ状態となっており、従来の単純なネットワーク分離では境界が曖昧になっています。結果として、放置されたVPN装置等の脆弱性を突かれ、ランサムウェア等の被害に遭う医療機関が後を絶ちません。 本ガイドライン案においても、「ゼロトラスト思考の導入（システム運用編13.2）」や「論理的／物理的なネットワークの構成分割（システム運用編11.遵守事項）」、「外部接続点（保守回線等）の集約（企画管理編3.2.2）」など、ネットワークの安全性確保に向けた概念や方針は示されています。 しかし、これらを具現化するための「標準的な構成モデル」が国から提示されていないため、各医療機関やシステムベンダーが独自にネットワークを設計・構築せざるを得ず、セキュリティレベルに大きなばらつきが生じています。 上記の背景を踏まえ、以下の対応を提案いたします。 ・推奨ネットワークモデルの提示 ガイドラインにおいて、医療機関の規模やクラウド利用の度合いに応じた具体的な「推奨ネットワークモデル（構成図のパターン）」を提示してください。 （例：インターネット接続系、医療情報システム（電子カルテ）系、外部機関連携系（オンライン資格確認等）の安全な分離と、各層間の安全なデータ連携・通信手法を示したモデルなど） ・ベンダーへの標準化の提示 ネットワークモデルを国が提示することで、システム関連事業者に対しても「医療機関に導入するシステムは、このネットワークモデルに準拠した通信仕様（API連携やセキュアなゲートウェイの利用等）とすること」という明確なメッセージ（要件）として発信してください。	今回の改正では、医療機関等向けの推奨構成モデルを示すことは目的としていないので、原案の通りとさせていただきます。
167	システム運用編	１３．１．２	システム運用編 p.29「１３．１．２　選択すべきネットワークのセキュリティ」において、「 IP-VPN は、インターネットを用いず、通信事業者が提供するものである。」 という説明があるが、以下のような課題があるため、修正を提案します。 【現状のパブコメ案で生ずる実運用上の具体的課題】 通信は、通信事業者が管理するIP-VPN（閉域IP網）内で行われ、インターネットとは論理的に分離されていると思いますが、IP-VPNを提供している通信事業者のサービスでは、インターネット回線を敷設する場合と同様に光回線を敷設し、インターネット向けのアクセス回線・設備を共有する場合が多いと存じます。そのため、「インターネットを用いず」との表現は、誤解を招きかねません（物理的に分離されているわけではない）。 【解決策としての修正案】 該当項目を以下のように修正することを提案します。 --- ➢ IP-VPNは、通信事業者が管理する閉域ネットワークを利用するため、通信事業者以外の侵入のリスクは小さい。但し専用線ほどではないものの、利用コストは高いものとなる。 --- 【解決策が妥当である理由】 IP-VPNは、通信事業者が使用するインターネット回線設備と物理的に分離されているわけではなく、通信事業者があくまでも論理的に分離して閉域性を担保するものであるため、上記の修正案は妥当と考えます。	ご指摘の修正案を踏まえて修正しました。
168	システム運用編	１３．１．２	■ 意見の要旨 本ガイドライン案はネットワークセキュリティに関して境界防御（ペリメータ）モデルを前提としている。国際的にはゼロトラストへの移行が進み、VPN機器の脆弱性を起点とした医療機関へのサイバー攻撃が多発している現状を踏まえ、以下の見直しを提案する。 ■ 意見1：ペリメータモデルからゼロトラストモデルへの移行 【問題】ガイドラインはネットワークを「セキュア」と「オープン」に二分し、原則「セキュアなネットワーク」利用としている（13.1節）。一方、13.2節ではゼロトラスト思考を紹介しており、遵守事項がペリメータモデルに留まることと乖離がある。 【国際動向】米国：NIST SP 800-207策定、大統領令14028・OMB M-22-09で連邦政府にゼロトラスト移行を義務化。EU：NIS2指令でリスクベースアプローチ採用。英国：NCSCがVPNを「過渡期の技術」と位置づけ。 【提案】ペリメータモデルからゼロトラストモデルへ段階的に移行し、すべての通信に認証・認可・暗号化・監視を求める枠組みへ転換すべきである。 ■ 意見2：VPN推奨記述がもたらす誤解とリスク 【問題】表13-1ではVPN関連方式が「適合」として上位に列挙され、VPN利用が最も望ましいという印象を与える。しかし近年VPN脆弱性を悪用した重大攻撃が相次いでいる。 ・2021年 つるぎ町立半田病院（Fortinet VPN未パッチ） ・2022年 大阪急性期・総合医療センター（委託業者VPN経由侵入） ・2023年 名古屋港コンテナターミナル（Fortinet VPN脆弱性） ガイドライン自身も13.2節でVPN通信による被害拡大を指摘しながら、表13-1がVPN推奨に見えることは矛盾である。 【提案】表13-1でVPN方式とTLS方式を並列記載しVPN上位の印象を排除。VPN機器のファームウェア管理・脆弱性対応の困難さを具体的リスクとして明記。VPN利用時の追加対策（パッチ管理、EDR導入、ネットワーク分割等）を遵守事項として明確化すること。 ■ 意見3：オープンなネットワークを前提とした安全性確立への移行 【問題】現行遵守事項は「セキュアなネットワーク」利用を原則とし、オープン経由を例外的に認める構成だが、クラウド普及・テレワーク・地域医療連携等でオープン経由の場面は今後さらに増加する。 【提案】オープンなネットワーク上の安全な通信を標準として位置づけ、以下を遵守事項の中心に据えるべき。 TLS 1.3以上による通信暗号化 多要素認証（MFA）の必須化（令和9年度義務化方針を支持） デバイスポスチャの導入（意見4参照） 通信の異常検知・ログ分析の義務化 WAF、APIゲートウェイ等の導入推奨 これによりネットワーク種類に依存せず通信ごとに安全性を確保できる。 ■ 意見4：端末管理における新しい方式への移行 【問題】遵守事項6はオープン経由接続時に「クライアント証明書によるTLSクライアント認証、または同等以上の端末識別・認証」を求めている。クライアント証明書は端末の「身元」を静的に証明するが、セキュリティ状態（OSパッチ、マルウェア対策、ディスク暗号化等）は検証できない。国際的には端末の「健康状態」を継続検証する「デバイスポスチャ」が標準となっている。 比較（クライアント証明書ーデバイスポスチャ）：端末身元は両方対応可。OSパッチ適用状況・EDR稼働・ディスク暗号化・接続中の継続検証はいずれも証明書では不可、ポスチャでは対応可。 【提案】デバイスポスチャを「同等以上の安全性」の具体例として明示。FIDO2/パスキーをクライアント証明書の代替として明示的に認める。端末管理を「静的な身元証明」から「動的な状態検証」に拡張すること。 ■ 意見5：DX・利便性とセキュリティのバランスを基本原則に 【問題】セキュリティ要件が高すぎると医療DX推進が阻害され、以下の問題が生じる。 ・可用性低下：VPN設置が必要なため地域医療連携展開が遅延 ・シャドーIT：正規システムが使いにくく非公式手段（個人メール、LINE等）で医療情報がやり取りされる ・中小医療機関の対応困難：高コストなVPN機器+PKI導入が過大な負担 情報セキュリティの三要素「機密性・完全性・可用性」のうち、可用性もセキュリティの重要な構成要素である。 【提案】基本原則として以下を明記すべき。 1. セキュリティと利便性は両立を目指すべきものであること 2. 医療DX推進を阻害しないよう実装容易さ・コスト・運用負荷を考慮した要件設定を行うこと 3. 医療機関の規模に応じた段階的対応を認め、最新技術（クラウドネイティブセキュリティ、パスキー認証等）で低コスト高セキュリティな実装を可能とすること 4. 過度な制約による可用性毀損はそれ自体がセキュリティリスクであること	ご意見として参考にさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
169	システム運用編	１３．２	1.背景 〇今回の「医療情報システムの安全管理に関するガイドライン」の第6.1版への改定において、巧妙化するサイバー攻撃等の脅威から医療情報を保護するための対策を強化するという趣旨には、医療機関等へシステムやサービスを提供する医療機器・診断薬メーカーとして賛同する。 〇 一方で、グローバルに事業を展開し、世界共通のシステム基盤やクラウドサービスを日本の医療機関にも提供している外資系企業にとって、日本固有の規制や要件が設けられることは、最新の医療技術や高度な情報システム（リモートサポートサービス等）の迅速な導入のハードルとなる可能性がある。 〇より安全で優れた医療情報システムを継続的に提供するため、グローバルスタンダードに則った柔軟な制度設計を要望するものである。 2.現状＆課題 〇特に外資系企業にとってシステム提供・運用上の高いハードルとなるのは、以下の4点です。 ➢Pマーク（プライバシーマーク）等、国内固有の認証取得に関する点 ✧当該ガイドライン案の経営管理編では、委託先事業者を選定する基準として「JIS Q 15001（プライバシーマーク制度）」や「JIS Q 27001（ISMS）」等の認証を取得しているシステム関連事業者を選定するよう指示することが定められている。 ✧企画管理編において、これらを取得していない場合はISMAP等の代替認証等で確認すると記載されているが、外資系企業はGDPR準拠など、グローバルスタンダードな個人情報保護・セキュリティ基準を満たしていることは、一般的である。 ✧一方で、日本独自のPマーク取得が事実上の「遵守要件」として医療機関側に求められると、外資系企業がグローバル統一のシステムを提供する上での障壁となる。 ➢国内法の適用・執行が及ぶ範囲でのクラウドサーバー構築の点 ✧ガイドライン案の企画管理編では、外部保存の委託先事業者との契約において「保存された情報を格納する情報機器等が、国内法の適用及び執行の及ぶ範囲にあることを確実にすること」と規定されており、事業者の選定の際にも情報機器が設置されている場所（地域、国）を確認することとされている。 ✧外資系企業は、スケールメリットや高度なセキュリティ監視（脅威インテリジェンス）を実現するため、海外のデータセンターを利用したグローバル共通のクラウド基盤でサービスを展開しているケースが多い。 ✧物理的なサーバー設置場所を日本国内に限定されるような解釈がなされると、グローバル共通運用される最先端の医療ソリューションの導入遅延を招き、最新の医療を受ける日本国民の権利を阻害する恐れがある 。本ガイドラインが目指すべきは「実効的な安全」であり、形式的な場所の制限ではなく、有事における責任の所在とデータ保全の担保に重点を置くことであると考える。 ➢セキュリティとしての二要素認証の義務化の点 ✧ガイドライン案では、令和9年度（令和9年4月1日時点）で稼働しているシステムに対し、新規導入又は更新時に「二要素認証を採用、又はこれに相当する対応を行うこと」が求められており、クライアント端末のアプリケーションログイン時およびサーバーのOSログイン時の双方に実装が求められている。 ✧しかし、グローバル展開しているシステム基盤において、特定の国の規制に合わせて一斉にシステム構造を改修（二要素認証の組み込み）することは、膨大な開発リソースとテスト期間を要する。 ✧「技術的な理由等により対応が困難な場合は、直近の次期システムの更新までを期限とする」という猶予規定はありますが、グローバルシステムのライフサイクルと合致しない場合、期限内の対応が極めて困難になるケースが想定される。 ➢リモート接続手法における技術限定的な記述 ✧システム運用編13.2で言及されている通り、現在は境界防御に依存しない「ゼロトラスト」の考え方が主流となっており、ゼロトラストをベースとしたID認識型のリモートアクセス手法等を用いれば、VPNや閉域網といったネットワーク境界に依存した接続制限は必ずしも重要ではなくなる。I ✧しかし、現状のガイドライン案の具体要件（14.1.1等）では、「VPNを経由し、踏み台端末へのRDP、SSH等による接続に限定する」といった従来型の境界防御を前提とした記述が中心となっており、ガイドライン全体でゼロトラストの思想と乖離が生じている。 ✧このような特定の古い手法をベースとした記述のままでは、ベンダーや医療機関がゼロトラストに即した新しくよりセキュアな技術を導入しようとした際に、「ガイドラインが想定するVPNやRDPでないため適合しないのではないか」という不要な議論や解釈の滞曲を生み、結果として企業側の対応の難しさやコスト増、先進的なセキュリティ対策の導入阻害を招くものである。	ISMS認証は、ISO27001への適合性も含まれること、またISMAPについては米国 FedRAMPなども含めている等、国外の認証等についても対応しておりますので、この部分は原案の通りとさせていただきます。 医療情報の保存場所や医療機器の二要素認証については引き続き検討を進める予定ですので、今回の改定では原案の通りとさせていただきます。
170	システム運用編	１３．２	3.論点 〇グローバル認証との同等性評価の明確化 ➢Pマーク等の国内認証は、情報機器等の管理および運用主体が日本法人でなく委託先である同社の海外法人の場合であっても必要とされるかの基準が不明確である点。 〇クラウドサーバーの設置場所と法適用の解釈 ➢「国内法の適用及び執行が及ぶ範囲」という要件が、地理的に日本国内クラウドサーバー（データセンター）の利用（データの国内保存）を必須とするものか、あるいは日本国内の責任主体（日本法人等）が法的窓口として機能することで実質的な法執行力を担保すれば足りるのかどうか、の解釈が分かれる点。 〇二要素認証実装の現実的な移行期間と代替措置 ➢グローバルシステムの改修サイクルを考慮した現実的な猶予期間のあり方と、「二要素認証に相当する対応」の柔軟な解釈の必要性。 〇ゼロトラストアーキテクチャを前提としたリモート接続手法の包括と技術中立性の確保 ➢リモートメンテナンスや外部接続に関する要件が、VPNやRDP/SSHといった特定の従来型技術に限定（例示）されることで、ゼロトラストに基づくモダンなアクセス技術の導入が阻害される可能性がある点。 ➢時代に沿った新しい手法の存在を認識し、手段を狭めない柔軟な記述としていただく必要性。 4.整理の方向性 〇上記の論点を踏まえ、以下の通りガイドラインの記載内容の整理・明確化を要望する。 〇Pマーク取得等の要件について ➢経営管理編等の記述において、JIS Q 15001（Pマーク）や JIS Q 27001（ISMS）の認証取得については、委託している海外法人先が認定取得しているのであれば、日本法人は省略してもよいと解釈できれば好ましいと考えるが如何か。 〇国内法適用の範囲および適合条件の明確化について ➢「国内法の適用及び執行の及ぶ範囲」について、物理的なクラウドサーバー（データセンター）の設置場所を地理的に日本国内に限定するものではないという解釈が好ましいがその解釈でよいか。 ➢上記を踏まえて、物理的な設置場所を問わずのであれば、日本国内の法人（日本支社等）が契約主体となり、日本の法令に基づく情報の取り扱いを保証するとともに、規制当局からの要請に対して当該日本法人が責任を持って情報開示や説明責任を果たせる体制が構築されている場合には、当該要件を満たすものと整理できると好ましいと考えるが如何か。 ➢さらに、これにより、セキュリティレベルの高いグローバルクラウドの活用と、国内法の実効性確保の両立が可能と整理される方が好ましいと思料するが如何か。 ➢これらについて、法的ガバナンスが担保されていれば海外のクラウドサーバー（データセンター）の利用も許容される旨を、Q&A等を含めて明示的に記載していただけると好ましいが如何か。 〇二要素認証の義務化について ➢令和9年度という期限について、グローバルシステムの改修の難易度を考慮し、さらなる猶予期間の設定、またはシステム更新サイクルの実態に即した柔軟な期限設定を認めていただきたいと考える。 ➢また、多層防御やゼロトラストアーキテクチャの採用等、システム全体のセキュリティ対策によってリスクが十分に低減されている場合には、厳密な各レイヤーでの二要素認証の実装がなくても「二要素認証に相当する対応」として許容される代替措置（「入室制限がある区画への入場時と端末利用時で計2要素以上の認証がなされる等の物理的保護策や、米国HIPAAで認められているリスク分析に基づく合理的・技術的な代替策」）の条件を、より具体的に明記していただけると好ましいと考えるが如何か。 〇リモート接続要件の技術中立化について ➢システム運用編「１０．２ リモートメンテナンスにおける安全管理対策」および「１４．１．１ 利用者の識別・認証（二要素認証の代替措置）」など、外部接続に関する要件全般について、特定の技術（VPN、踏み台経由のRDP・SSH等）に限定する記述を見直すことが好ましいと考えるが如何か。 ➢ゼロトラストアーキテクチャに基づくモダンなリモートアクセス技術（ZTNA等）も要件を満たす手法として包含されるよう、技術中立的な表現に改めるか、新技術の利用を許容する旨を明記することが好ましいと考えるが如何か。 ※本意見における専門用語の補足： ✧VPN：インターネット上に仮想のトンネルを設け、通信を暗号化する「従来型」のネットワーク技術（境界防御）。 ✧ZTNA（Zero Trust Network Access）：「ネットワークの内外に関わらず誰も信頼しない（ゼロトラスト）」という前提に基づき、ネットワークの境界ではなく、アクセス要求ごとにユーザーや端末の安全性を厳格に認証・認可する「最新型」のアクセス技術。 ✧RDP / SSH：いずれも離れた場所にあるサーバーやパソコンの画面やシステムを、遠隔操作するための通信規格。 ✧踏み台端末：外部から内部システムへ遠隔操作（RDP等）を行う際、直接接続させないために、一時的な中継地点として設置されるパソコンやサーバーのこと。"	ISMS認証は、ISO27001への適合性も含まれること、またISMAPについては米国 FedRAMPなども含めている等、国外の認証等についても対応しておりますので、この部分は原案の通りとさせていただきます。 医療情報の保存場所や医療機器の二要素認証については引き続き検討を進める予定ですので、今回の改定では原案の通りとさせていただきます。
171	システム運用編	１３．２	ゼロトラスト思想の取り込みについて記載がありますが、本ガイドライン全体において、攻撃者の侵入ポイントはリモートアクセスルーターに限定され、それが適切に設定されているにも関わらず、突破される前提で防御策をお示しいただいているように感じられます。 適切な設計と管理を行われてもなお、未知の脆弱性による侵入は想定されますが、ならば侵入経路不明で電子カルテ端末に侵入されている前提での防御策も必要に思います。 この場合、二要素認証の実装は防御策としては機能せず、OSやアプリケーションが抱える脆弱性なり単純にパスワードクラッキング耐性の方が重要になりますので、パスワード長を長くし対クラック性能を向上させることを優先とした方が安全ではないでしょうか。	「攻撃者の侵入ポイントはリモートアクセスルーターに限定され、それが適切に設定されているにも関わらず、突破される前提で防御策をお示しいただいている」との意図ではございませんので、原案のままとさせていただきます。
172	システム運用編	１３．３．１	脚注9 サーバ証明書をクライアント証明書に利用することは推奨されない。下記に修正しては どうか？ ＜修文案＞ 公的認証局から発行されたサーバ証明書をクライアント証明書”に利用してはならな い。サーバ証明書をクライアント証明書にも利用すると”セキュリティ上のリスクを有する ことから、大手ブラウザ事業者において、2026年6月15日以降、「正当な端末」と認 識されなくなるとされる。	ご指摘の修正案を踏まえて修正しました。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
173	システム運用編	１３．３．３	ネットワークを利用して医療情報を外部と交換する場合、送信先に確実に情報を送り届ける必要がある。システム運用担当者は下記脅威に対して適切な措置を講じることが求められる。 ・ 盗聴 ・ 改ざん ・ なりすまし ・ マルウェアの混入等や中間者攻撃 措置としては、ネットワークや機器、サービス等の監視、通信の相手先との相互認証などが想定される。 ↓ （修正案） １３．３．３ 盗聴およびなりすまし防止等 ネットワークを利用して医療情報を外部と交換する場合、送信先に確実に情報を送り届ける必要がある。システム運用担当者は下記脅威に対して適切な措置を講じることが求められる。 ・ 盗聴 ・ 改ざん ・ なりすまし ・ マルウェアの混入等や中間者攻撃 措置としては、ネットワークや機器、サービス等の監視、通信の相手先との相互認証などが想定される。 メール送受信時においては送信ドメイン認証技術(SPF/DKIM/DMARC)による送信元のなりすまし対策、送信メールに対してなりすまされないための送信ドメイン認証技術、特にDMARCにおけるより強いポリシー(quarantine, reject)を段階的に設定すること、DMARCレポートを活用し、なりすましメールの状況把握に努めることが想定される。 これらは他の対策（利用者への注意喚起、メール無害化、アクセス監視等）と組み合わせ、多層的に実施することが望ましい。 理由：第13章では「盗聴・改ざん・なりすまし」等の脅威への対策が求められていますが、攻撃経路として日常的に頻発している電子メールのなりすましについて、具体的な例示があると実効性が高まると考えられます。このため、通信におけるなりすまし対策の具体例として、メールの送信元真正性を検証する代表的な手法である送信ドメイン認証技術（DMARC等）を例示することが有効と考えます。	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。
174	システム運用編	１３．４	無線LAN特有のリスクとして、不正利用、盗聴、マルウェア混入、ならびに可用性への配慮の必要性が整理されており、また、暗号化方式として WPA2-PSK 等の事前共有鍵方式については鍵漏えいリスクが高いことから利用を避けるべき旨が記載されている点について、全体として適切な整理であると理解しております。一方で、無線LAN 利用時の利用者および端末の真正性確保について、本文中では具体的な認証方式や設計上の考え方が明示されておらず、医療機関やシステム運用担当者が、より安全な方式を選択する際の判断材料が読み取りにくいと感じます。近年の無線LAN 環境においては、事前共有鍵方式を用いない方式として、電子証明書を用いた利用者・端末認証を行う方式など、より高い安全性を確保できる手法が広く用いられています。これらの方式は、暗号鍵の安全な管理に加え、なりすまし防止や端末単位での認証・無効化を可能とする点で、医療情報を取り扱う無線LAN 環境において有効な対策と考えられます。つきましては、本項において、無線LAN通信の暗号化および利用者認証に関する考え方として、事前共有鍵方式を避ける理由に加え、電子証明書を用いた認証方式等、より強固な認証・鍵管理を実現する手法が存在する旨を補足的に記載いただくべきと考えます。	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。
175	システム運用編	１４	該当箇所⑤において、二要素認証の実装箇所として、クライアント端末については「アプリケーションのログイン時」、サーバについては「OSログイン時」と明記されている点について意見を述べます。 厚生労働省より令和7年5月に公表された「令和7年度版医療機関におけるサイバーセキュリティ対策チェックリスト」においては、二要素認証の対象を医療情報システム全般とした上で、サーバ、端末PC、ネットワーク機器への認証技術実装を含むものとして整理されています。また、二要素認証の採用例として示されている方式は、端末OSログイン時の認証を想定した運用とも整合する内容となっています。このような背景から、既に端末ログイン時に二要素認証を実装する対応を進めている医療機関も存在している状況と認識しております。 一方で、今回の改定案の記載は、クライアント端末における二要素認証の実装箇所がアプリケーションログイン時に限定されているように読み取れるため、従来のガイドラインやチェックリストとの考え方との間に一定の齟齬が生じる可能性があります。二要素認証は、実装箇所や方式の違いによりセキュリティ強度や運用特性が異なることから、アプリケーションログイン時に限らず、端末OSログイン時に二要素認証を実装する方式についても、同等に許容される選択肢として位置付けられるべきです。 アプリケーションログイン時に二要素認証をする場合、医療従事者はシステムを起動・利用するたびに二要素認証を求められることになります。一分一秒を争う医療現場において、この運用は業務効率を著しく低下させます。また、過度な認証要求は「MFA疲労」を引き起こし、現場スタッフが「ログインしたまま端末を放置する」「利便性のためにパスワードを共有する」といった運用回避（シャドーIT）に走る原因となり、結果としてセキュリティが形骸化する恐れもあります。 つきましては、本項の記載について、クライアント端末における二要素認証の実装箇所を限定せず、アプリケーションログイン時および端末ログイン時のいずれも運用や環境に応じた選択肢として包含する表現とする必要があると考えます。	チェックリストについては今後改定を検討しているので、原案の通りとさせていただきます。
176	システム運用編	１４	表14-1 医療情報システムにおける二要素認証の要否 表14-1において、二要素認証の実装箇所として、サーバについては OS ログイン時に二要素認証が「要」とされている一方、クライアント端末については、アプリケーションのログイン時における二要素認証のみが要件として示され、端末 OS ログイン時の二要素認証については想定されていないように読み取れます。しかしながら、近年発生している医療機関を含む各種サイバー攻撃の事例では、VPN 等の外部接続経路の脆弱性を起点としてネットワーク内に侵入した後、侵入者が端末を乗っ取り、院内ネットワーク内を横断的に移動する、いわゆる内部活動（ラテラルムーブメント）を行う傾向が見受けられます。このような攻撃手法を踏まえると、端末単位で利用者本人を厳格に識別する対策の重要性は高まっているものと考えます。端末の OS ログイン時に二要素認証を実装する方式は、たとえ認証情報の一部（パスワード等）が漏えいした場合であっても、追加の要素（IC カードや生体情報等）がなければ端末へのログインそのものが困難となるため、端末乗っ取りや内部ネットワーク内での不正な活動を抑止する観点からも、有効な対策と考えられます。一方、クライアント端末においてアプリケーション単位で二要素認証を実装する方式の場合、すべての医療情報システムが当該認証方式に対応しているとは限らず、未対応のアプリケーションや認証が実装されていない経路が存在した場合には、そこを起点とした攻撃リスクが残る可能性も否定できません。さらに、OSログインが単一要素（パスワードのみ）で突破可能であれば、電子カルテ等のアプリケーションに入れなくとも、端末のOS内に侵入が可能です。これにより、ローカルやファイルサーバ上に保存された患者データ（ExcelやPDF等）の窃取が可能となります。また、既存システムへのアプリケーションレベルでの二要素認証対応には、一定の改修期間やベンダー対応を要することも想定されます。これらを踏まえると、クライアント端末においては、アプリケーションログイン時に限定せず、端末 OS ログイン時に二要素認証を実装し、その認証結果を後続の医療情報システム利用に紐付ける運用を含め、より現実的かつ実効性の高い方式を選択できる余地を残すことが望ましいと考えます。つきましては、表14-1の記載および注記について、クライアント端末における二要素認証の実装箇所をアプリケーションに限定して解釈されることのないよう、端末 OS ログイン時の二要素認証についても、要件を満たす方式として適切に包含される表現への修正を求めます。	ご意見として参考にさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
177	システム運用編	１４	（システム運用編） 現在、ランサムウェア被害発生後の再接続判断にあたっては、「医療情報システムの安全管理に関するガイドライン 第6.0版」に明示された以下の5項目を満たしたことをもって、安全性が回復されたと判断しています。 【現行（6.0版）の復旧確認5項目】 ・バックドアを残さない ・無効にされたセキュリティ機能を復旧する ・同じ脆弱性を突かれて侵入されない ・他の脆弱性を突かれない ・不正に作成されたり、盗まれたりしたID・パスワード等を使われないようにする このうち、後半3項目は特に重要であり、「侵入が成立した原因の除去」および「侵入後に悪用された手段が再利用されない状態の確保」までを明確に射程に含む、実務的かつ結果重視の要件となっていました。 具体的には、 ・「同じ脆弱性を突かれて侵入されない」 → 今回利用された侵入経路・脆弱性が再利用不能であること ・「他の脆弱性を突かれない」 → 少なくとも同種・同階層・同影響範囲の脆弱性については再侵入に耐えうる状態であること ・「ID・パスワード等を使われないようにする」 → 侵入後に窃取・生成された認証情報が、将来の攻撃に用いられない状態になっていること を意味しており、対応すべき範囲は「侵入成功に直結する実効性のあるリスク」に限定されていました。 ところが、第6.1版（案）では、これらが以下のように変更されています。システム運用編P42 【第6.1版（案）の記載】 ・利用された脆弱性に対処する ・他にリスクとなる脆弱性がないか十分に検証、対応する ・不正に作成されたり、盗まれたりしたID・パスワード等を無効化する この変更により、対応対象となる範囲と確認責任の性質が、本質的に変化していると認識しております。 1)脆弱性対応範囲の変質について 従来記載は、「再侵入を防げる状態にあるか」という結果基準であったのに対し、第6.1版（案）では、「十分な検証を行ったか」「他にリスクが存在しないか」 という、範囲無限定・努力義務型・過程重視の要件に変質しています。 しかしながら、「他にリスクとなる脆弱性がないこと」を証明することは、技術的にも、現実の運用上も不可能であり、結果として復旧判断が事実上できなくなることが想定されます。 2) 認証情報（ID・パスワード）の扱いの変質について 従来の「使われないようにする」という表現は、再利用リスクの遮断（パスワード変更、特権ID再発行、認証経路変更等）という複数の実務的手段を包含する柔軟な結果基準でした。 一方で「無効化する」という表現は、 ・どの範囲のIDを ・どの期間について ・システム外を含めどこまで 無効化すれば足りるのかが不明確であり、かえって現場判断を困難にしています。	「将来の不正アクセスに利用されない状態」のような将来に向かっての不存在の証明を医療機関等に求めるのは難しいなど観点から、原案の通りとさせていただきます。
178	システム運用編	１４	3)実務への影響 この記載を復旧判断基準とした場合、 ・医療機関が要件充足を「証明」できない ・判断主体ごとに解釈が分かれる ・オンライン資格確認の再開が不必要に遅延する という事態が現実に発生し、医療機関の診療継続および財政に深刻な影響を与えることが強く懸念されます。 以上を踏まえ、復旧判断要件については、少なくとも次のように 「対応範囲」「達成基準」「復旧判断可能性」が明確になる表現へ修正すべきと考えます。 【修正案（例）】 ・利用された脆弱性に対処する ー同じ脆弱性を用いた再侵入が発生しない状態であること ・他にリスクとなる脆弱性がないか十分に検証、対応する ー同種または同等の影響を及ぼす脆弱性について、再侵入を防止できる対策が講じられていること ・不正に作成されたり、盗まれたりしたID・パスワード等を無効化する ー不正に作成・取得されたID・パスワード等が、将来の不正アクセスに利用されない状態が確認されていること （※ 少なくとも第6.0版と同等の明確性を確保すること） 以上、ご検討のほどよろしくお願い致します。	「将来の不正アクセスに利用されない状態」のような将来に向かっての不存在の証明を医療機関等に求めるのは難しいなど観点から、原案の通りとさせていただきます。
179	システム運用編	１４	【遵守事項】 ５番の二要素認証の項目について 質問（１） 端末系について「クライアント端末とサーバーのいずれも二要素認証を実装する」とされておりますが、その通りの対応をすると、数千万の投資が必要となるような要件となっている認識です。例えば、ドメインコントローラーに登録するユーザーとパスワードだけでなく、登録された端末からしかログインできないような制限をかけておくことで、疑似的な二要素認証を実現する形でも問題がないか、Q&Aで例示していただけないでしょうか。 質問（２） サーバー系について「サーバーについては、OSのログイン時に二要素認証を実装すること。」とされておりますが、これはクラウドサービスに限定した要件と解釈してもよいのでしょうか。　大手クラウドサービスでは、クラウド基盤として二要素認証が整備されておりますが、部門システム等で多いオンプレミスのシステムでは、実現することがかなり困難ではないかと考えられます。　具体的にオンプレミスのシステムでどのように実現することができる要件として記載されているのか、Q&Aでオンプレミス型での実現方法を例示いただければ幸いです。	ご意見として参考にさせていただきます。
180	システム運用編	１４	【遵守事項】⑤ 「二要素認証に相当する対応」の範囲について、物理的入退室管理やネットワーク境界の統制のみをもって該当すると解釈可能か、また利用者の論理的認証に限定されるのかが不明確である。 判断基準および具体例を明確に示されたい。 また、アプリケーションごとに異なる認証方式が求められる場合、医療機関の運用負荷が過大となるおそれがあるため、統一的な方針についても併せて示されたい。	物理的入退室管理やネットワーク境界の統制のみをもって該当するとはしておりません。
181	システム運用編	１４	【遵守事項】⑤ 二要素認証の導入期限として令和9年4月1日が明記されているが、電子カルテ事業の遅延、医療機関の準備状況、ベンダーの開発期間等を踏まえると、現実的な対応が困難となるおそれがある。 したがって、十分な移行期間を確保した記載とするべきである。 また、経過措置としての「更新」の範囲について、クラウド型医療情報システムにおける事業者側のリリースおよび医療機関側の設定変更のいずれを指すのかが不明確であるため、具体例を含め明確に示されたい。 さらに、運用切替には一定期間を要することから、期限については令和10年3月末時点とすることが望ましい。	ご指摘の修正案を踏まえて修正しました。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
182	システム運用編	１４	【遵守事項】⑥ ログイン試行制限における「一定回数」および「一定時間」について定量的な基準が示されていない。 医療機関が適切に設定可能となるよう、推奨値または考え方を明確に示されたい。	システムの性格や構成、業務上のリスク検討結果などに依存するため、原案の通りとさせていただきます。
183	システム運用編	１４	【遵守事項】⑤ ・クライアント端末の二要素認証について、アプリケーションレベルでログイン保護しても、OSレベルで保護されていなければアプリケーション情報に不当アクセスされるリスクがあると考えられます。 ・そのことから、OSレベルのログインン二要素認証の方が広域かつ強固に保護されると考え、” OSレベルで二要素認証を実装することで本遵守事項を満たせている” という理解でよろしいでしょうか。 ・この理解でよろしければ、弊社としては"OSレベルの二要素認証の実現"を検討していきたいと考えております。 ・また、その旨、注記等への追記を検討いただけますと幸いです。	一般利用者においては、クライアント端末のOSログインだけでは、アプリケーション利用の真正性は担保できないため、原案の通りとさせていただきます。
184	システム運用編	１４	【遵守事項】⑥ 異なる医療情報システム間におけるパスワード使い回し禁止について、統合認証基盤（IDaaS等）を利用する場合の適用範囲が不明確である。 また、過去履歴の再利用制限の範囲を含むのかについても、明確に示されたい。	一般論として、異なるシステムでPWの使い回しは妥当ではないという判断の上、個々の対応は適切な管理方法を採用することを想定しています。原案の通りとさせていただきます。
185	システム運用編	１４	【遵守事項】⑥ ・「(6)一定数回数、認証に失敗し場合には、以降一定時間ログイン施行が不能になる仕組みを講じること」 について、一定回数、および一定時間の推奨値をご教示いただきたいです。 ガイドライン推奨値を加味したシステム初期値の設定、およびユーザにご説明して理解・納得いただくための情報としたく伺いました。 ・また、本遵守事項を実現検討するための猶予期間として、「１４．認証・認可に関する安全管理措置【遵守事項】⑤」と同様に下記の追記をお願いしたく存じます。 『令和９年度（令和 9 年 4 月 1 日時点）時点で稼働していることが想定される医療情報システムを今後、新規導入又は更新するに際しては(略) ・・・・。 なお技術的な理由等により令和９年度までの対応が困難な場合には、令和９年度以降、直近の次期の医療情報システムの更新までを期限とする』	システムの性格や構成、業務上のリスク検討結果などに依存するため、原案の通りとさせていただきます。
186	システム運用編	１４	１．入場時の利用者確認を二要素から除かれる件 下記一文（P56）が削除されていますが、現実的には令和9年4月以降に更新、新規導入するシステムに入場者管理を除く二要素認証を導入することは困難と思われる。下記一文の削除を取り消すか、期限を延期していただきたい。 ― 医療情報システムに二要素認証が実装されていないとしても、例えば放射線管理区域や薬局の調剤室など、指定された者以外の者の入室が法令等により制限されるような区画の中に端末が設置されている医療情報システムであって、当該区画への入場に当たって利用者の識別・認証が適切に実施されており、入場時と端末利用時を含め二要素以上（記憶・生体計測・物理媒体のいずれか2つ以上）の認証がなされている場合には、二要素認証に相当すると考えてよい。 ― ２．医療情報システムの更新の定義 医療情報システムの更新は、診療報酬改定に伴うプログラムの更新、OSのアップデート、ハードウェアの更新、システム全体の一新など、いくつかの状況が考えられるので、更新の定義を明確にしていただきたい。 ３．サーバOSログイン時の二要素認証 サーバとクライアントが同居しているオンプレミス型の医療情報システムにおいては、クライアントの2要素認証とサーバOSの2要素認証は同じものを認めていただきたい。	一つ目の点は、令和３年よりお示ししているところであり、原案の通りとさせていただきます。 二つ目の点はご指摘の内容を踏まえて修正いたしました。 三つ目の点はQAで対応させていただく予定です。
187	システム運用編	１４	【遵守事項】⑤ (1)遵守事項は二要素認証を実施することのようなシンプルな表現にして、令和9年などの表現は、14.1の記載に追記したほうがわかりやすいと思います。 (2)後半の3つの箇条書きは、あるシステム(クライアント、サーバ構成で、サーバにデータを保存、OSがあり、そこに複数のユーザがＯＳにログインでき、その上で任意のアプリが動作するシステム)の場合は、その通りかもしれませんが、例えば、1つの筐体で動作する医療機器や、ＯＳとただ1人のユーザとアプリしか動作しないkioskモード端末などには適さない表現。本来、セキュリティを確保するためのkiosk端末などが否定された記載にも読めてしまう。遵守事項ではなく、下記の説明で、想定するシステム構成とともに理由を含めて明記すべきかと思います。 (3)” ログイン”は、技術が特定されすぎている。ログインなしに使用可能なシステムも存在するし、認証でログインの処理を経由しないものもある。テクニカルニュートラルで記載するか、あくまである想定のシステムでの要求にすべきではないかと考えます。 <修正前>⑤令和９年度（令和9年4月1日時点）時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新するに際しては、二要素認証を採用、又はこれに相当する対応を行うこと。なお技術的な理由等により令和９年度までの対応が困難な場合には、令和９年度以降、直近の次期の医療情報システムの更新までを期限とする。 ・ クライアント端末とサーバのいずれも二要素認証の実装を要する。 ・ クライアント端末では電子カルテ等のアプリケーションのログイン時に二要素認証を実装すること。 ・ サーバについてはOSのログイン時に二要素認証を実装すること。 <修正後> 【遵守事項】 ⑤医療情報にアクセスするために2要素以上の認証、又はこれに相当する対応を行うこと。	ご指摘の修正案を踏まえて、以下の通り修正しました。 「サーバについてはOSのログイン時に二要素認証を実装すること。」を「OSでの二要素認証を実装すること」に修正
188	システム運用編	１４	リモートメンテナンスにおける安全管理対策についてです。 クライアント端末にOSでの二要素認証を必須とすべきです。 クライアント端末において、有資格者のみアクセス可能とするアプリケーションで二要素認証を実施しているからといって、OSにおける二要素認証を不要とする理由にはなりません。 医療機関によっては、クライアント端末が一般人でも触れる場所に配置されており（物理的対策ができない場合）、悪意を持つ人に操作される可能性が考えられます。そのため、クライアント端末OSに二要素認証を適用する必要があると考えます。 サーバーのメンテナンスは、基本的に管理者権限を要する作業が多いため、サーバーに対する二要素認証というよりも、特権ID管理が中心となると思われます。特権ID管理においては、二要素認証を導入することも可能です。	一般利用者においては、クライアント端末のOSログインだけでは、アプリケーション利用の真正性は担保できないため、原案の通りとさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
189	システム運用編	１４	今回の改定案は、医療機関の実態を正しく把握した上で、6.0版では各編に分散して言及されていた業務委託の考え方及び今後増加していく可能性が高いクラウドサービスを利用する際の考え方を保守委託機関編として切り出し、詳細化・具体化したことは高く評価できる。特にAI自身がサイバー攻撃を仕掛けてくる現状を踏まえて、境界防護型セキュリティやゼロトラスト型セキュリティに代表される完全防御をめざすのではなく、万一サイバー攻撃を受けた場合にでも医療機関の本分である医療の継続的な提供を狙ったIT-BCPの具備やサイバーレジリエンスの４つの目標（予測→耐える→回復→適応）の定着を狙って、サイバー攻撃を受けた際の非常時対応を具体化した内容になっている。また、保守委託機関と医療機関の間の責任分界点の明確化が重要であり、「業務委託を前提とした医療現場がどの様にセキュリティ対策を担保するか」を具体化した改定であり、特に契約・責任分界・非常時の対応・バックアップ・管理証跡について具体化している。 特に保守委託機関編は、IT人財が不足している中小医療機関にとって有用な内容となっており、この層の医療機関に内容を深く理解してもらい、医療現場に適用し、順守してもらうためには下記5項目について例示を含めてより具体的な内容にすることが重要と考える。 １）外部接続制御基盤の例示を追加する 　医療機関が、SaaSに代表される複数のクラウドサービスやCT・MRI・内視鏡などに代表される医療機器、及び、電子カルテ・PACSなどに代表される医療ＩＴシステムが保守の目的で複数の事業者と個別に接続する場合、認証・接続制御・ログ取得・責任分界の明確化を行う統制点として、ゲートウェイ、踏み台、接続制御装置等の具体的な活用を例示していただきたい。 ２）リモート保守のアクセスは“院内ネットワークへ直接入れない構成”推奨すべく具体例を追加する 　リモート保守は、院内ネットワークへ直接到達させず、踏み台・中継基盤経由で認証、時間制御、ログ取得を行うなどの具体的な構成を有効例として明記していただきたい。 ３）外部ネットワークとの接続点の集約やログ情報の集約の事例を補足説明として追加する 外部接続されているサービス毎に管理を分散させるのではなく、接続先制御・監査ログ集約・責任分界整理を一元管理する考え方の方が現実的であり、かつ、サイバー攻撃の可視化がやりやすいため、補足説明を追加していただきたい。 ４）ネットワーク分割の段階的な導入を追記する 　ネットワークの全面更改は、医療機関の負担も大きいため、外部クラウド接続や保守ネットワーク接続から優先的に分離・統制する段階な導入のプロセスを有効例として示していただきたい。 ５）セキュリティアセスメントやシステムセキュリティ監査の重要性について言及する サイバーレジリエンスの考え方に則って、医療機関のセキュリティ対策の現状を定点観測するための、セキュリティアセスメントの重要性やシステムセキュリティ監査（内部・外部）の重要性について、具体的に記載をお願いしたい。特に、セキュリティ対策は、優先順位付けによる継続的な実施が必須と考えられるため、セキュリティ対策の重要性を医療機関全体で意識づけを行うためにも、毎年のセキュリティ対策の進化をトレースすることが重要だと考える。システムセキュリティ監査については、外部監査を毎年受ける事は費用面や対応工数の面から厳しいとは考えるが、内部監査であれば、毎年テーマを決めて部分的に実施をすることが可能であり、医療機関全体で認知度の向上させ、医療従事者全員に意識づけを行うためにも継続的な実施が重要である。	ご指摘の３）につきましては、「なお、例えば外部ネットワークとの接続点の集約に際しては、外部に接続されているサービス毎にログ管理等を分散させるのではなく、接続先制御・監査ログ集約・責任分界整理を一元管理することが負担軽減のために有効である。 」と追記いたしました。 そのほかのご指摘事項につきましては、QAにて記載いたします。
190	システム運用編	１４	システム運用編　p.35 「➢　クライアント端末のアプリケーションログイン時」で始まる項目と次の項目について 【前提】p.33 遵守事項⑤において、クライアントに二要素認証（2FAと略）を実装することと、医療情報を格納するサーバはOSのログイン時に2FAを実装することが要求されています。医療機器においては単一のハードウェアでクライアント／サーバの両方の要素も併せ持つ場合も多く、この場合OSとアプリのそれぞれで2FAの実装が求められると考えています。 p.35 表１４－１より下の説明では、リモートメンテナンスを想定した対策も規定されており、サーバOSに2FAを実装しない場合の代替措置として、①と②のいずれか、またはそれと同等以上の措置の実装を要求しています。①と②は踏み台端末を必要とするため、医療機器のリモート環境としては大規模な構成となってしまうのと、医療機器のアラートや医療情報を保持しないログをリモートサービスセンター（RSCと略）側で収集して医療機器のダウンタイムを最小化する、といったサービスにおいては、踏み台端末は大きな障壁となってしまうため、リモート接続も考慮した措置について具体的な例示が必要であると考えます。 【実運用上の課題】医療機器のサーバOS（例：Windows）に2FAを実装して、ベンダーのRSCのPCから医療機関の医療機器OSにリモートログイン（RDP等）する場合、一般に以下のようなリモート構成でなければ、RSCから医療機器のOSにリモートログインできないという大きな制限が生じると認識しています。 ・サーバOSの2FA：　知識認証 ＋ 所持認証（スマートカード（一部のUSBトークン（スマートカードとして振る舞うデバイス）を含む）） ・RSCのPCからのリモートログイン：　Windows標準のRDP ※ コスト面で大きな弊害とはならないWindows標準のRDPでも、スマートカード以外の認証情報（生体認証やOTP認証）をRSCから医療機器OSへリダイレクトできないため、リモート接続を考慮すると、サーバOSの2FAはスマートカード認証（一部のUSBトークンを含む）に限定されてしまうと考えます。 【解決策としての修正案】p.35 中央 「➢　このため、サーバOSについては」で始まる項目の最下行に以下を追加。 --- なお、サーバOSへのリモートログインについては、以下のような措置が実施されていれば二要素認証を実装できているものとみなす。 ・医療機関等の外部からのリモート接続において二要素認証を実施すると共に、「１３．ネットワークに関する安全管理措置」の遵守事項を元に安全な通信経路を経由すること ・医療機関等の外部からのリモート接続において接続ログを記録すること。接続ログには少なくともリモート接続者やその接続ツール、接続開始時刻、接続終了時刻、接続先システムが含まれること ・「１０．２　リモートメンテナンスにおける安全管理対策」の表１０-１を参照し、各リスクに応じた対策を講じること 【解決策が妥当である理由】昨年意見募集（本年施行予定）された米国のHIPAA Security Rule（90 FR 898, www.govinfo.gov/content/pkg/FR-2025-01-06/pdf/2024-30983.pdf）では、リスク分析の上ePHIへのアクセスに多要素認証を要求していますが、OS／アプリといったレイヤー別の多要素認証は求めていません。国際整合の観点からも修正案のように、医療機関等の外部からリモート接続する際に二要素認証を行った上で、サーバOSへ単一認証でリモートログインすることを許容するのは妥当であると考えます。	二要素認証について示している内容は、ネットワーク機器の二要素認証だけで代替することを認めておりませんので、原案の通りとさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
191	システム運用編	１４	システム運用編　p.34～35において、6.0版にあった「入室制限による二要素認証相当」の説明が削除された件について ・今回の6.1版（案）のまま発行された場合、令和9年4月以降に稼働／導入する医療情報システムは技術的に二要素認証を実装していることが求められます。従来、医療機関等において入室制限を適切に行っていれば、その区画にある単一認証の医療情報システムでも二要素認証に相当すると考えてよい（併せて経過措置ではない）という認識でいたため、現在、製造販売を行っている医療情報システムへの二要素認証の実装を行っておりませんでした。 ・今回の6.1版（案）でサーバOSに対する二要素認証を初めて必須化しており、6.0版まではまったく求められておりませんでした。踏み台端末による代替措置も提示されていますが、医療情報システム、特に医療機器においては、機器のアラート（例：温度異常）や医療情報を含まないログ（リモート保守で活用）を製販業者のリモートサービスセンター側へ送信する仕組みが実装されているケースが多く、単純に踏み台端末による代替措置を適用できません。このような状況下で、令和9年3月末までに対応を完了（二要素認証を実装した新たな医療機器の販売開始）することは非常に困難であり、現行の医療機器の多くが本セクションの要求を満たすことは事実上不可能と考えられます。このため、医療機関は、本セクションを完全に遵守する医療機器を選定し、導入することは現実的に難しい状況にあると言えます。 【解決策としての修正案】 14.1.1の最後に以下の項目を追加。 －－ ➢　医療情報システムに二要素認証が実装されていないとしても、例えば放射線管理区域や薬局の調剤室など、指定された者以外の者の入室が法令等により制限されるような区画の中に端末が設置されている医療情報システムであって、当該区画への入場に当たって利用者の識別・認証が適切に実施されており、入場時と端末利用時を含め二要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証がなされている場合には、 二要素認証に相当すると考えてよい 。 －－ 【解決策が妥当である理由】 米国で昨年意見募集（本年施行予定）されたHIPAA Security Rule（90 FR 898, www.govinfo.gov/content/pkg/FR-2025-01-06/pdf/2024-30983.pdf）では、技術的に多要素認証を利用できない場合、リスク分析に基づいて合理的かつ適切な代替措置を導入することを求めており、その中の一つとして、上記のような物理的保護策を例示しております（特に経過措置ではありません）。国際整合の観点から、6.0版まで記載されていた二要素認証相当の要件は今後も継続する必要があると考えます。	ご意見認証の要請は、我が国におけるサイバー攻撃の実情等を勘案してもものなので、原案の通りとさせていただきます。
192	システム運用編	１４．１．１	前記１４の遵守事項⑤に対する指摘の対応案 ＜修正前＞本ガイドラインでは令和３年度より二要素認証技術の実装を促してきたが、令和9年度時点（令和9年4月1日時点）で稼働していることが想定される医療情報システムを、今後、導入又は更新する場合、原則として二要素認証を採用すること。 ＜修正後＞令和９年度（令和9年4月1日時点）時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新するに際しては、二要素認証を採用、又はこれに相当する対応を行うこと。なお技術的な理由等により令和９年度までの対応が困難な場合には、令和９年度以降、直近の次期の医療情報システムの更新までを期限とする。	ご指摘の修正案を踏まえて、14.1.1の５つ目の箇条書きにて、以下の通り修正しました。 「本ガイドラインでは令和３年度より二要素認証技術の実装を促してきた。令和9 年度時点（令和9年4月1日時点）で稼働していることが想定される医療情報システムを、今後、導入又は更新する場合、原則として二要素認証を採用すること。」
193	システム運用編	１４．１．１	前記１４の遵守事項⑤に対する指摘の対応案 ＜修正前＞また、医療情報を格納するサーバのOSについても、原則として二要素認証の実装を目指すこと。サーバでは例えばアプリケーションを介さずにデータベースにアクセス可能であることから、OSのログイン時に二要素認証を実施することが合理的である。ただし、運用対応等の技術的な理由で対応が間に合わない場合には、令和９年度以降、直近のシステムの更改、新規導入までの間を経過措置とする。 ＜修正後＞前記、修正前の文の前に下記を挿入して、それ以降を1段、段落を落とす ＞例えば、クライアントとサーバとにより構成され、データがサーバに保存され、それぞれにOSがあり、それぞれでログインでき、クライアントからサーバに接続する際にログインを要求されない構成の場合、 ・ クライアント端末とサーバのいずれも2要素以上の認証の実装を要する。 (クライアントだけの2要素認証の場合、サーバに直接ログインされる可能性があるため) ・ クライアント端末では電子カルテ等のアプリケーションのログイン時に2要素以上の認証を実装すること。 (クライアント端末のアプリケーションから医療情報にアクセスできるため) ・ サーバについてはOSのログイン時に2要素以上の認証を実装すること。 (クライアント端末からだけのアクセス以外にサーバOSに直接ログインされ医療情報にアクセスできてしまうため) 本記載はあくまで一例であり、実際の運用環境や規制要件に応じて、より強固な認証や追加の対策が求められる場合があります。内容の解釈にあたっては、不必要に範囲を緩めることなく、求められる要件を過不足なく適切にご理解いただくようお願いいたします。 (詳細説明) ・また、医療情報を格納するサーバのOSについても、原則として二要素認証の実装を目指すこと。サーバでは例えばアプリケーションを介さずにデータベースにアクセス可能であることから、OSのログイン時に二要素認証を実施することが合理的である。ただし、運用対応等の技術的な理由で対応が間に合わない場合には、令和９年度以降、直近のシステムの更改、新規導入までの間を経過措置とする。	個別のケースの説明になりますので、原案の通りとさせていただきます。
194	システム運用編	１４．１．１	今回、下記の文書が削除されている。 「医療情報システムに二要素認証が実装されていないとしても、例えば放射線管理区域や薬局の調剤室など、指定された者以外の者の入室が法令等により制限されるような区画の中に端末が設置されている医療情報システムであって、当該区画への入場に当たって利用者の識別・認証が適切に実施されており、入場時と端末利用時を含め二要素以上（記憶・生体計測・物理媒体のいずれか2つ以上）の認証がなされている場合には、二要素認証に相当すると考えてよい。」 NIST SP800-63-4(最新)でも、多要素認証として1つのデバイス・認証器の中で2種類の異なる要素を組合せて認証を行う、Multi-Factor Authenticatorのほかに、複数の独立した認証器を組み合わせて、多要素認証を実施するTwo Single-Factor Authenticatorsも定義されている。Two Single-Factor Authenticatorsを排除すべきではない。あくまで情報にアクセスするために2つ以上の要素の認証が必要。端末がどこにあるかだけでもない。また、昨年意見募集された米国のHIPAA Security Rule（90 FR 898, www.govinfo.gov/content/pkg/FR-2025-01-06/pdf/2024-30983.pdf）では、リスク分析に基づき多要素認証を求める一方で、技術的に対応できない場合には合理的かつ適切な代替措置の検討が認められる旨が示されているため、上述の物理的保護策を削除するのは妥当ではないと考える。 さらに、本記載が必要以上に拡大解釈されないような記載も必要であると考える。 (修正後)下記文書を追加。 医療情報システム自体に二要素認証が実装されていないとしても、医療情報にアクセスするために2要素以上の認証が必要である。 例えば、 (1)医療情報にアクセスする端末にID,パスワードの認証しかない医療情報システムの場合、その端末が放射線管理区域や薬局の調剤室など、指定された者以外の者の入室が法令等により制限されるような区画の中に設置され、当該区画への入場に当たって利用者の識別・認証が適切に実施されている場合、医療情報システムの認証と組み合わせて、2要素認証になる。 (2)医療情報にアクセスする端末にID,パスワードの認証しかない医療情報システムの場合、携帯SMSへのコード送信や、ハードウェアOTPトークンなどの医療情報システム自体以外の機器を組み合わせた認証でも、2要素認証になる。 本記載はあくまで例示であり、実際の運用環境や規制要件に応じては、さらなる認証強化や対策が必要となる場合があります。必要以上の拡大解釈とならないようご留意ください。	NIST SP800-63-4では、ご意見におけるFactorには、入退出管理は含まれないと解せられますので、原案の通りとさせていただきます。
195	システム運用編	１４．１	システム運用編において、二要素認証の実装については、医療情報システムだけでなく、医療機関で使用される医療機器にも接続されて運用される医療情報システムもあるかと思います。つきましては、「医療情報や患者情報を扱う医療機器においても二要素認証の実装されることが望ましい」というような文面を含めていただくことは可能でしょうか。	医療機器における認証については引き続き検討を進める予定ですので、今回の改定では原案の通りとさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
196	システム運用編	１４．１．１	国際整合性（International Harmonization）の観点からの懸念について 1. 対象箇所 本ガイドライン案において示されている、医療機器へのログイン時における2要素認証（多要素認証）を原則として求める方向性について。 _____ 2. 意見（結論） 医療機器のサイバーセキュリティ強化の重要性については強く賛同する一方で、本ガイドライン案におけるログイン時の2要素認証を事実上必須とする整理については、国際的な医療機器規制との整合性（International Harmonization）の観点から懸念があると考える。 _____ 3. 理由 （1）国際的な主要規制・ガイダンスでは認証方式を特定していない 米国における医療情報セキュリティ規制である HIPAA Security Rule では、 電子的保護対象保健情報（ePHI）へのアクセスに際し、アクセス主体が本人又は正当な主体であることを確認する手続きを実装することを求めているが、2要素認証や多要素認証といった特定の認証方式を明示的に要求していない。 HIPAAは公式に「技術中立（technology-neutral）」な規制であることを明言しており、 認証強度や実装方式は、対象システムのリスク評価、利用環境、運用形態に応じて各組織が決定する枠組みとなっている。 このため、OSレベルあるいはアプリケーションレベルで一律に2要素認証を要求する考え方は、少なくともHIPAAの現行規制の整理とは一致していない。 [mhlw.go.jp]. [accountablehq.com] .[Summary of the HIPAA Security Rule	HHS.gov] _____ （2）IMDRFおよびIEC規格の考え方との関係 本ガイドライン案が参照している IMDRFガイダンス や IEC 81001-5-1 においても、 サイバーセキュリティ対策は リスクベースアプローチ に基づくことが基本原則とされており、 ・各脅威の発生可能性 ・患者安全への影響 ・医療現場での可用性・即応性 等を総合的に評価した上で、適切な管理策を選択することが求められている。 これらの国際文書においても、ログイン時に2要素認証を必須とする旨は明示されておらず、あくまで「有効な対策の一例」として位置付けられているにとどまる。 そのため、国内ガイドラインにおいて特定の認証方式を強く要求する記載とした場合、国際的な規制・規格との実質的な乖離が生じる可能性がある。 _____ （3）グローバル製品開発・供給への影響 多くの医療機器はグローバルに同一設計・同一ソフトウェアを前提として開発されており、 国・地域ごとに認証方式（例：日本のみ2要素認証を必須）を分けて実装することは、現段階では以下の点で課題がある。 ・ソフトウェア構成の複雑化による安全性・品質管理リスクの増加 ・認証方式差異に起因する開発・検証・許認可・保守コストの増大 ・結果として医療機器の安定供給や迅速な改良への影響 これらは、医療機器規制が本来目指す 患者安全の確保および安定供給 という目的の観点からも、慎重な検討が必要である。 _____ 4. 要望 以上を踏まえ、以下の点について検討いただきたい。 1.2要素認証を原則・必須と断定する表現ではなく、リスク評価に基づき選択可能な対策例の一つとして位置付けること 2.国際的な規制・ガイダンス（HIPAA、IMDRF、IEC等）との 整合性についての考え方をガイドライン内で明確化すること 3.医療現場の可用性・緊急対応（患者安全）とのバランスを考慮した運用上の柔軟性を確保すること 4.日本国において先行し、2要素認証を原則・必須と断定する表現で確定となる場合においては、国内・外医療機器供給側への開発及び適応期間（薬機法への適応・変更等を含む）の現実的な期間確保をすること _____ 5. まとめ サイバーセキュリティ強化の方向性自体については賛同するものである。一方で、特定の認証方式を一律に求める枠組みとすることについては、国際的な整合性や製品の安全性、安定供給の観点から、慎重な整理が必要であると考える。 仮に本件を進める場合、医療情報を取り扱う小規模機器を含む多様な医療機器に対し一律の変更を求めることとなるが、その際には決定通知後に相応の準備期間を設ける必要がある。また、対応に伴う費用増加や、本来の医療目的における有効性・効率性の低下が生じる可能性についても懸念される。 さらに、医療機器本体内部での実装対応、あるいは外部システムとのインテグレーションによる対応など、いずれの場合においても開発段階からの設計変更が求められるものであることについて、十分に認識されたい。_____	医療機器における認証については引き続き検討を進める予定ですので、今回の改定では原案の通りとさせていただきます。
197	システム運用編	１４．１．１	本文、【遵守事項】⑤ クラウド環境において医療情報を格納するサーバが事業者管理下にある場合、医療機関および事業者それぞれの責任範囲において、どの接続およびどのOSログインが本遵守事項の対象となるのかが不明確である。 また、SaaSやPaaSを基盤としたクラウドネイティブな構成では、医療機関側がサーバOS層へ直接アクセスしない場合もあり、当該要件の適用範囲が不明確である。 このため、共有責任モデルに基づき、対象範囲を明確に示されたい。	表3-1などでクラウドに関する責任共有モデルを示しており、これを踏まえた対応は個々のシステム構成を踏まえて異なるので、原案の通りとさせていただきます。
198	システム運用編	１４．１．１	踏み台方式および「同等以上の措置」に該当する構成について、具体的な判断が困難である。 ゼロトラスト型アクセス、セキュアブラウザ、マネージドゲートウェイ等の代表的な構成例を示し、判断基準を明確に示されたい。	ご指摘を踏まえて、「同等以上の措置」について注釈を追記しました。
199	システム運用編	１４．１．１	パスワードの定期変更を不要とする記載について、院内規程や契約上の義務との優先関係が不明確である。 運用上の整理指針を明確に示されたい。 また、二要素認証未導入環境において一律に定期変更を不要とすることは、既存システムへの影響が大きいため、段階的な適用とすることが望ましい。 さらに、定期変更を不要とする運用の適用開始時期についても不明確であり、二要素認証の導入期限（令和9年4月1日）との関係を含め、具体的な適用時期を明確に示されたい。	原案では定期的変更は不要としていますが、定期的変更を禁止しているわけではありません。原案の通りとさせていただきます。
200	システム運用編	１４．１．１	踏み台端末の利用による二要素認証の実装事例が示されおりますが、踏み台端末にWindowsクライアントOS(Windows11等)を、複数ユーザー間で使用することは、ライセンス違反の可能性が高いと思われます。 複数人で使用する場合、WindowsServerOSが必要となり、利用者分に合わせたCALの追加も必要となります。 クライアントPCをサーバー同様に連続稼働させることは推奨さておりませんので、 お客様にもご協力いただき作業時に電源を投入頂く運用とするか、踏み台端末としてのサーバーハードウェアが 必要となり、導入コストとしてお客様にご負担いただく事は、ご容赦頂けると考えて良いでしょうか。	ご指摘のような趣旨では記載しておりませんので、原案の通りとさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
201	システム運用編	１４．１．１	踏み台端末にEDR機能を具備する事例をお示しされておりますが、EDR機能を有効化する為には、プロキシサーバーあるいは専用の外部通信用のルーターが必要になると考えます。 これらはネットワーク構成に合わせて適切に設計を行った後、設置、状態監視を行う必要があるはずですが院内内部から外部への通信設定、設計管理についての記載がないのは、別のリスクを発生させる要因とならないでしょうか。	ご指摘のような趣旨では記載しておりませんので、原案の通りとさせていただきます。
202	システム運用編	１４．１．１	二要素認証のみとすると、同等以上に安全な公開鍵ベースのパスキーが入らなくなるため、明示的に”二要素認証もしくはパスキー”とする必要があります。 本ガイドラインでは令和３年度より二要素認証技術の実装を促してきたが、令和9年度時点（令和9年4月1日時点）で稼働していることが想定される医療情報システムを、今後、導入又は更新する場合、原則として二要素認証を採用すること。 ↓ 本ガイドラインでは令和３年度より二要素認証技術の実装を促してきたが、令和9年度時点（令和9年4月1日時点）で稼働していることが想定される医療情報システムを、今後、導入又は更新する場合、原則として二要素認証もしくはパスキーを採用すること。	パスキーについては、二要素認証として排除しているわけではありません。原案の通りとさせていただきます。
203	システム運用編	１４．１．１	表１４－１ 医療情報システムにおける二要素認証の要否 オープンなネットワークからのVPN接続には二要素認証が必須です。そうでないと、VPNの認証情報漏洩によりLAN内への侵入を許します。 表１４－１に以下の行を追加 VPN　要　　－　　－	14-1ではVPNの認証を記載する目的ではないので、原案の通りとさせていただきます。
204	システム運用編	１４．１．１	ハッシュ関数の使用を念頭にした記載だと思いますが、ハッシュ値を取ることは一般に暗号化と呼びません。 (3)医療情報システム内のパスワードファイルはパスワードのハッシュ値を保存するなどして平文パスワードを復元できない状態にした上で、適切な手法で管理・運用すること。	ご指摘の修正案を踏まえて修正しました。
205	システム運用編	１４．１．１	【遵守事項】⑤ クライアント端末とサーバのいずれも二要素認証の実装を要する。 クライアント端末では電子カルテ等のアプリケーションのログイン時に二要素認証を実装すること。 サーバについては OS のログイン時に二要素認証を実装すること。 システム運用編P35 表14-1下部に「※認証した情報をアプリケーションの資格情報等と連携し、適切な権限付与が可能な場合はOSやミドルウェアでの二要素認証を許容する。ただし、OSで一要素、アプリケーションで一要素のような認証は許容されない。」という記載があるため、同じ文言を遵守事項5項に明記してはどうか。	ご意見として参考にさせていただきます。
206	システム運用編	１４．１．１	SaMDとしての医療機器をソフトウェアを動作する為のPC(ハードウェア)込みでご提供する場合、あるいはソフトウェアが統合された医療機器装置をご提供する場合、二要素認証が実装できる事例は非常に少ないとの認識ですが、これらの場合でも二要素認証は必須でしょうか。	二要素認証を対応は必要であると想定しています。
207	システム運用編	１４．１．１	【前提】p.33 遵守事項⑤において、クライアントに二要素認証（以降、2FAと略）を実装することと、医療情報を格納するサーバはOSのログイン時に2FAを実装することが要求されています。医療機器においては単一のハードウェアでクライアント／サーバの両方の要素も併せ持つ場合も多く、この場合OSとアプリのそれぞれで2FAの実装が求められると考えています。 p.35 表１４－１より下の説明では、リモートメンテナンスを想定した対策も規定されており、サーバOSに2FAを実装しない場合の代替措置として、①と②のいずれか、またはそれと同等以上の措置の実装を要求しています。①と②は踏み台端末を必要とするため、医療機器のリモート環境としては大規模な構成となってしまうのと、医療機器のアラートや医療情報を保持しないログをリモートサービスセンター（以降、RSCと略）側で収集して医療機器のダウンタイムを最小化する、といったサービスにおいては、踏み台端末は大きな障壁となってしまうため、リモート接続も考慮した措置について具体的な例示が必要であると考えます。 【実運用上の課題】医療機器のサーバOS（例：Windows）に2FAを実装して、ベンダーのRSCのPCから医療機関の医療機器OSにリモートログイン（RDP等）する場合、一般に以下のようなリモート構成でなければ、RSCから医療機器のOSにリモートログインできないという大きな制限が生じると認識しています。 ・サーバOSの2FA：　知識認証 ＋ 所持認証（スマートカード（一部のUSBトークン（スマートカードとして振る舞うデバイス）を含む）） ・RSCのPCからのリモートログイン：　Windows標準のRDP ※ コスト面で大きな弊害とはならないWindows標準のRDPでも、スマートカード以外の認証情報（生体認証やOTP認証）をRSCから医療機器OSへリダイレクトできないため、リモート接続を考慮すると、サーバOSの2FAはスマートカード認証（一部のUSBトークンを含む）に限定されてしまうと考えます。 【解決策としての修正案】p.35 中央 「➢　このため、サーバOSについては」で始まる項目の最下行に以下を追加。 ―― なお、サーバOSへのリモートログインについては、以下のような措置が実施されていれば二要素認証を実装できているものとみなす。 ・医療機関等の外部からのリモート接続において二要素認証を実施すると共に、「１３．ネットワークに関する安全管理措置」の遵守事項を元に安全な通信経路を経由すること ・医療機関等の外部からのリモート接続において接続ログを記録すること。接続ログには少なくともリモート接続者やその接続ツール、接続開始時刻、接続終了時刻、接続先システムが含まれること ・「１０．２　リモートメンテナンスにおける安全管理対策」の表１０－１を参照し、各リスクに応じた対策を講じること 【解決策が妥当である理由】昨年意見募集された米国のHIPAA Security Rule（90 FR 898, www.govinfo.gov/content/pkg/FR-2025-01-06/pdf/2024-30983.pdf）では、リスク分析の上ePHIへのアクセスに多要素認証を要求していますが、OS／アプリといったレイヤー別の多要素認証は求めていません。国際整合の観点からも修正案のように、医療機関等の外部からリモート接続する際に二要素認証を行った上で、サーバOSへリモートログイン（例：記憶認証）することを許容するのは妥当であると考えます。	二要素認証について示している内容は、ネットワーク機器の二要素認証だけで代替することを認めておりませんので、原案の通りとさせていただきます。
208	システム運用編	１４．１．２	リモートメンテナンスにおいて、インターネット上の中継サーバーを提供するベンダーと、その機能を活用される病院側管理者が存在しております。 これらは主として普通にインターネットアクセスが可能な状況からの利用を前提として設計されているようで、外部認証サービスが利用する多数のアクセス先との通信が必要となり、リモートメンテナンス専用のFireWallへの通信制御が非常に煩雑となっているのが現状です。 本項で示されている通り、安全管理については注意深く対応する必要性があるはずですが、実際の管理状況は利用者である我々にはわかりません。二要素認証を実装する為に、別のリスクが増加しない事が確認してから利用する等の注記を明記するべきではないでしょうか。	「インターネット上の中継サーバーを提供するベンダー」を必ずしも所与としていない等、ご指摘のような趣旨では記載しておりませんので、原案の通りとさせていただきます。
209	システム運用編	１４．２	医療情報システムの範囲について、証明書配布ツール等の運用支援ソフトが含まれるかが不明確である。 対象範囲および経過措置適用の可否について、判断基準を明確に示されたい。	ご指摘の点については、配布ツール等についても医療情報システムを取り扱う場合には対象となることを想定しています。
210	システム運用編	１４．２	無条件での管理者権限での動作不可は、さまざまな機器を考慮すると困難であり、セキュリティを悪化される誘解を招く必要もあると考える。 (修正前)医療情報システムによっては、利用者がアプリケーション等を利用する際に、端末のOSの管理者権限を要するものがある。利用者に対する過度の権限を与えることになることから付与を避けるため、このような設計のアプリケーション等の選定は避けること。 (修正後)医療情報システムによっては、利用者がアプリケーション等を使用する際に、端末のOSの管理者権限が必要となる場合がある。このようなケースでは、利用者に端末に対する過度な権限を付与することになるため、原則としてそのような設計のアプリケーション等は選定を避けること。 一方、アカウント管理がなく唯一のユーザーが使う機器やキオスクモードで動作する機器は、特にリソースの限られた医療機器などの医療情報システムに多く見られる。こうした機器では細かな権限管理が難しい場合もあるが、あえて単純化した権限管理でセキュリティを確保している可能性もあり、慎重な運用が求められる。 ただし、現時点でやむを得ずこれらの環境を利用する場合には、適切な運用管理とリスク評価を十分に行ったうえで、利用を必要最小限に限定し許容するなどの対応が望ましいと考えられる。	KIOSK端末についてもMDM管理など、適切な管理方法の対応が想定できますので、原案の通りとさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
211	システム運用編	１４．３	電子保存の3原則における「真正性」と情報セキュリティの7要素における「真正性」は概念が異なることから、ここでは前者の説明をしていることを明確にした方が良いです。 案2は本ガイドラインにおいて後者の「真正性」が登場しない性質を使った説明になっています。 (案1)ここでいう真正性とは、正当な権限で作成された記録に対し、虚偽入力、書換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であることを指す。 (案2)本ガイドラインにおける真正性とは、正当な権限で作成された記録に対し、虚偽入力、書換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であることを指す。	ご意見として参考にさせていただきます。
212	システム運用編	１３	【遵守事項】⑭ 医療情報システムにおいて無線LAN を利用する場合、次に掲げる対策を実施すること。 (1) 適切な利用者のみに無線LAN の利用を制限すること。例えば、ANY 接続拒否等の対策を実施することが考えられる。 (2) 不正アクセス対策を実施すること。例えばIPアドレス等によるアクセス制限を実施すること。ただし、例えばMACアドレスについては、モバイル端末においてプライバシー保護の観点からMACアドレスランダム化が標準搭載されていることや、詐称可能であることから、MACアドレスによるアクセス制限の効果が限定的であることに留意する必要がある。 【遵守事項】⑭ (1) (2) において、無線LAN 利用時の対策例として「ANY 接続拒否」や「IP アドレス等によるアクセス制限」が挙げられている点は、基本的なネットワーク制御の観点から有効であると考えます。 一方で、これらの対策は主として通信経路や接続条件を制御するものであり、利用者および端末の真正性を直接的に確認する手法ではないことから、医療情報という高い機密性を有する情報を取り扱う環境においては、さらなる認証強化の余地があると考えます。 例えば、電子証明書を用いた無線LAN認証方式は、利用者および端末を一意に識別可能であり、なりすまし防止や端末紛失時のリスク低減、管理・失効の容易さ等の観点から、IP アドレスや MAC アドレスによる制限と比較して、より高い安全性を確保できる手法と考えられます。 特に、MAC アドレスランダム化や詐称の容易性が指摘されている現状を踏まえると、電子証明書を活用した認証方式は、無線LAN 利用における有効な対策の一つとして位置付けることが適切と考えます。 つきましては、現行記載の考え方を否定するものではありませんが、導入環境や医療機関の規模・運用体制に応じて、電子証明書を用いた無線LAN認証の活用も検討することが望ましい旨を、補足的・推奨事項として記載することが望ましいと考えます。	ご指摘を踏まえ電子証明書によるアクセス制限について追記しました。
213	システム運用編	１５．１	共通鍵および秘密鍵の格納に関し、クラウド事業者が提供するKMSやマネージドHSMが「格納する機器・媒体」に該当するかが不明確である。 実務上の解釈のばらつきを防ぐ観点から、具体的な取扱いおよび判断基準について明確に示されたい。	クラウド事業者が提供するKMSやマネージドHSMが「格納する機器・媒体」に該当します。
214	システム運用編	１５．１	医療情報システムの安全管理に関するガイドライン第6．1版システム運用編（案） １５．１ 電子署名、タイムスタンプが求められる場面での対策 「署名者の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名等を用いることなどが求められる。」とあるが、電子署名に用いる証明書と、国家資格の確認は切り離しても、署名の方法によって国家資格をと本人による電子署名をすることが可能であることと、デジタル国家資格に対応できるようにするために1は分離して確認できる形式に対応する必要がある。 署名者の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名等を用いることなどが求められる。 ↓ 署名者の国家資格が電子的に確認できる形式で電子署名を用いることが求められる。	原案は立会人型電子署名などを想定した際に、国家資格確認の方法を本人確認含めて別途行えることを示すものであり、それ以上の趣旨を示すものではありません。原案の通りとさせていただきます。
215	システム運用編	１５．１	医療情報システムの安全管理に関するガイドライン第6．1版システム運用編（案） １５．１ 電子署名、タイムスタンプが求められる場面での対策 タイムスタンプの記述がない。 ➢ 医療情報について、作成時刻又は変更時刻を証明する必要がある場合には、適切なタイムスタンプを付与し、保存義務のある期間中にその時刻及び真正性を検証できるよう、必要な技術的措置を講じること。 ➢ システム運用担当者は、タイムスタンプの付与対象、付与のタイミング、検証手順及び保存期間中の検証可能性の維持方法を定め、必要な情報及び検証手段を保全すること。	ご指摘の修正案を踏まえて修正しました。
216	システム運用編	１７	アクセスログの収集、照合について記載されておりますが、アクセスログには用途によって様々な粒度がありシステム管理者とベンダー間で認識のずれが発生する危険があると考えております。 OSレベルでのアクセスログ、アプリケーション単位での動作ログ、検査操作ログ、検査データへアタッチする事で発生する個人情報へのアクセスログなど様々なログがありますがお客様が容易に理解できるような形にする為には、データの再構成が必要になります。 監査時にベンダー立ち合いの下、データトレースを行う事は可能ですが、全てのベンダーが画一的なフォーマットで可読性の高いログを出力することは非常に困難と考えますので、特に個人情報を含む資源については部分を、個人情報を直接参照した場合のアクセスログを収集し、といった表現へ変更した方が現実的ではないでしょうか。	個人情報を参照せずに、ファイルを削除した場合などもトレースを行う必要がありますので、原案の通りとさせていただきます。
217	システム運用編	１７	システム運用担当者(お客様)は、全てのアクセスログを収集し、不正利用がないことを確認する必要があると記載されていますが、悪意をもったアクセスが発生した場合、正常利用と不正利用をログから判断する事は非常に困難と考えております。 また考えたくはないですが医療従事者自信による不正利用も考えられますが、こちらもログからは不正利用を疑う事は非常に困難で、極一部の明確な不正アクセスを監査する事が現実的な対応ではないでしょうか。	ご指摘を踏まえ、「この確認は、全てのログを目視確認することを指すのではなく、システムでの監視や、実際の運用に基づく適切な閾値を用いたスクリーニング後のログを確認することを想定する。」と追記しました。
218	システム運用編	１８．１	１９．１　サイバーセキュリティ対応　７段落目　(p.41-42) ７段落目に、複数方式のバックアップに関して４つの方式が例示されており、ここから２つ以上を選択することが想定とされている。本章で記載されているバックアップデータの保管に必要とされる対策および11意記載の遵守事項と本文記載事項に適合できる手段として、これら４つの方式に加えて磁気テープシステムの方式もあり、医療機関向けにも特に大容量のPACSなどの用途を中心に普及が進んでいる。そこで、「磁気テープシステム」もこれらの例示に追加していただきたい。 ＜修正前＞ ・HDD (Hard Disk Drive) ・RDX (Removable Disk Exchange system) ・NAS (Network Attached Storage) ・クラウドサービス ＜修正後＞ ・HDD (Hard Disk Drive) ・磁気テープシステム ・RDX (Removable Disk Exchange system) ・NAS (Network Attached Storage) ・クラウドサービス	ご指摘の修正案を踏まえて修正しました。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
219	システム運用編	１８．１	「システム運用編」中の「18.1 サイバーセキュリティ対応」7段落目にて、複数のバックアップ方式の例示として4点挙げられておりますが、以下の理由により「磁気テープシステム」の追加を希望いたします。 ①6段落目にて、ランサムウェア等の被害拡大を防ぐためにオフライン保管を推奨されていますが、磁気テープはドライブから抜き出しネットワークから切り離したオフライン保管に適しているため、最適なバックアップ方式であること。 ②同じく6段落目にて、バックアップデータへの感染リスクがあることが記載されており、実際の感染事例では感染から発症まで数か月を要する場合もございます。磁気テープは長期間のバックアップデータ保管が可能であり、感染前のデータを保持できるという重要な利点があります。 ③また、6.0版「システム運用編」QA集Q-69においては、オフラインバックアップ方式の例示として「磁気テープ、DVD、Blu-Ray等」が記載されており、お問い合わせが増加している状況です。6.1版の本文中の例示でこれらの記載が省略された場合、6.0版に基づき導入済みまたは検討中のユーザーに違和感を与えるおそれがあるためです。 〇修正前 例えば下記から2つ以上を選択することが想定される ・HDD（Hard Disk Drive） ・RDX（Removable Disk Exchange system） ・NAS（Network Attached Storage） ・クラウドサービス 〇修正後案 例えば下記から2つ以上を選択することが想定される ・HDD（Hard Disk Drive） ・RDX（Removable Disk Exchange system） ・磁気テープシステム ・NAS（Network Attached Storage） ・クラウドサービス	ご指摘の修正案を踏まえて修正しました。
220	システム運用編	１８．１	HDD・RDX・NAS・クラウドサービスから2つ以上を選択すること」が例示されており、また第12.2項では複数世代のバックアップ確保が求められています。しかしながら、クラウドネイティブなSaaSにおいては物理媒体（RDX等）の利用が構造上困難であり、現実的な選択肢はクラウドサービス内での対応に限定されます。別リージョン・別アカウントへのバックアップや、論理的な書き込み不可設定（S3 Object Lock等）といったクラウド環境における具体的な実装例を、本項の要件を満たす方式として明示いただくことを要望します。	原案では媒体の性格や方式を示すものであり、例示として媒体を示す趣旨ですので、原案の通りとさせていただきます。
221	システム運用編	１８．１	医療情報システムの安全管理に関するガイドライン第6．1版システム運用編（案） １８．１ サイバーセキュリティ対応 VPN機器の脆弱性が発見されてから攻撃が開始されるまでの時間は長くて数時間です、それまでに対応できない場合はクラウド型を推奨したい。自動アップデートに対応していても、自動アップデートの設定をしていないケースも多いため記述を追加したほうが良い。 十分な情報収集やシステム担当者自身によるVPN機器等のアップデートが困難と想定される場合には、クラウド 型VPNの採用や、自動アップデートに対応した製品を選定することが望ましい。 ↓ 十分な情報収集や脆弱性の発見されてからすぐにシステム担当者自身によるVPN機器等のアップデートが困難と想定される場合には、クラウド型VPNの採用や、自動アップデートに対応した製品を選定し自動アップデートを有効にすることが望ましい。	ご指摘の修正案を踏まえて、以下の通り修正しました。 「十分な情報収集やシステム担当者自身によるVPN機器等のアップデートが困難と想定される場合には、クラウド型VPNの採用や、自動アップデートに対応した製品を選定、活用することが望ましい。」
222	システム運用編	１８．１	医療情報システムの安全管理に関するガイドライン第6．1版システム運用編（案） １８．１ サイバーセキュリティ対応 ➢ なお、復旧するにあたっては、侵入継続と被害拡大を防ぐ観点から、 ・ 不正に作成されたり、盗まれたりしたID・パスワード等を無効化する は、盗まれる範囲を当事者やシステム担当者では想定し忘れることが多く具体的に入れておく必要があります。 ・ 不正に作成されたり、盗まれたりしたID・パスワード等を無効化する ↓ ・ 不正に作成されたり、侵害された可能性のある機器に保存されていたID・パスワード等を無効化する	ご指摘の修正案を踏まえて修正しました。
223	システム運用編	１８．１	医療情報システムの安全管理に関するガイドライン第6．1版システム運用編（案） １８．１ サイバーセキュリティ対応 ➢ なお、復旧するにあたっては、侵入継続と被害拡大を防ぐ観点から、 ・ 他にリスクとなる脆弱性がないか十分に検証、対応する は、システム担当者ではセキュリティ観点で十分に検証・対応することが難しく、不十分な多作になりやすいのでより確実な最新へのアップデートを推奨すべきである。 ・他にリスクとなる脆弱性がないか十分に検証、対応する ↓ ・ 他にリスクとなる既知の脆弱性がない状態にする。	ご指摘の修正案を踏まえて修正しました。
224	システム運用編	１８．１	（追記事項） 各種認証情報の摂取を目的としたフィッシング対策・なりすましメール対策の有効な手段の一つとして送信ドメイン認証（SPF/DKIM/DMARC等）の導入・運用を検討することが考えられる。DMARCを採用する場合は、レポートに基づく監視・是正や、段階的なポリシー強化 （例：none→quarantine→reject）を行う運用が考えられる。 理由：各種認証情報の摂取を目的とした外部攻撃の代表的入口であるメールに対し、技術的対策例としてDMARC等を例示すると、現場の導入判断がしやすくなるため。	ご指摘の内容はご指摘を踏まえ、別途Q&Aで考え方をお示しする予定です。
225	保守委託機関編	全体	保守委託機関編全ページ 全章 ページ番号の位置と形式 ページ番号の位置と形式を他の編と同様に下記としてはどうでしょうか 位置：　ページ下部中央 形式：　－番号－	ご意見として参考にさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
226	保守委託機関編	全体	【項番４】 【パブリックコメント対象個所】 保守委託機関編　全般 【意見内容】 「小規模医療機関向けの運用管理規定」やサービス事業者との「委託契約書」のひな型をガイドラインの別紙として提供する。 【理由】 小規模病院はシステム運用担当者が不在で経営管理と企画管理部門が分離されていなことで、セキュリティ確保作業に時間取れず、またセキュリティ知識が乏しいと考えられる。 サービス事業者のサービスが安全であることを前提にしているので、委託契約やシステム評価を厳しくする必要がある。	ご意見として参考にさせていただきます。
227	保守委託機関編	全体	1）新たに「保守委託機関編」を追加したことを評価したい。小規模医療機関では自らのネットワークセキュリティ対策を管理することが困難であり、構築や保守もほぼ丸投げしているのが現状だ。しかし委託業者も顧客要望や販売を前提に対応しているに過ぎず、公的なガイドラインに則ったセキュリティ対策を行っていない。 医療機関を狙い撃ちしたランサムウェア被害では、こうした業者が責任を持って保守管理していないため、政府・行政による業者向けのガイドラインの構築と責任臨界点明確化のアプローチは必須である。 2）一方で、保守委託機関等に上記のような義務を課すことで、保守契約に伴う費用が高額化することも懸念される。 加えて令和9年度中に実装が求められる二要素認証についても、OSやアプリケーションの対応となれば追加費用の発生が予想される。 さらに様々なセキュリティ規格に対応するためにも、これまで以上にコストが発生するが、医療界では圧倒的に診療報酬による経営で賄っているため、そうした対策に十分に対応できる診療報酬増額や補助金が求められる。	ご意見として参考にさせていただきます。
228	保守委託機関編	全体	【意見内容】 この分冊のタイトルを「システム委託小規模医療機関編」と変更する。 【理由】 　委託業務にはシステム運用、管理、保守があり、特に保守としてのパッチは大病院でもシステム提供者が行うことが多く、これをガイドラインの適用の区別とするのは、混乱のもとになると思います。	ご意見として参考にさせていただきます。
229	保守委託機関編	1	【項番２】 【パブリックコメント対象個所】 保守委託機関編　P2 下５行目 【意見内容】 「特に「システム運用編」における事項については、MDS/SDS を用いて機器、サービスのセキュリティ対応状況を確認することで、遵守事項に対応されたものとみなす。」 を以下に変更 「特に「経営管理編」および「システム運用編」における事項については、MDS/SDS を用いて本編の【別紙】 MDS/SDS におけるセキュリティ確認事項」の対応状況を確認することに加えて、本編「３. 保守委託機関における遵守項目」の確認及び運用管理規定の作成と遵守せることで、各編の遵守事項に対応されたものとみなす。 　この際、MDS/SDSの適合条項の「はい」に関して医療機関の運用等により達成するものをその旨の記述を義務付け、医療機関は運用規定に反映するものとする。また、対象外はその理由の記述を義務づける。 医療機関は委託先事業者と委託契約を締結し、特に非常時（システム障害、災害時、サイバー攻撃発生時）を含める。医療機関は運用管理規定を作成し、医療情報システム安全管理責任者と監査責任者を設置し運用管理規定を遵守させる。 【理由】 小規模病院で管理業務を楽にする為の特別編なので、できるだけ病院側の負担を軽くし、提供されたサービスがガイドライン順守であることを第三者も入れ客観的に確認し、セキュリティが確実に確保されやすい形にする為。	ご意見として参考にさせていただきます。
230	保守委託機関編	1	保守委託機関編P2 1．はじめに 第３段落　３行目 ・・・、運用は、医療情報システム提供事業者（以下「事業者」という）への・・・ 「医療情報システム・サービス事業者」に変更してはどうでしょうか ＞概説編とセットで読む場合は、医療情報システム・サービス事業者が使われています。 ＞「医療情報システム提供事業者」はここだけした出てきません。	ご指摘の修正案を踏まえて修正しました。
231	保守委託機関編	1	第４段落 SaaS（Software as a Service）を利用することでセキュリティアップデートを含めた保守管理を完全に事業者に委託することも可能となっている。 第６段落 ・セキュリティアップデートを含めたシステム保守を十分に事業者に委託している 「保守管理を全て事業者に委託」に統一してはいかがでしょうか ＞「十分に」がどの語句にかかるのかが不明 ＞語句を統一した方が読み手に易しい	ご指摘の箇所ですが、例示を目的とする趣旨ですので原案の通りとさせていただきます。
232	保守委託機関編	1	図1のフローチャートにおける 「1台以上のサーバのセキュリティアップデート責任が医療機関にある」という設問について 図1のフローチャートにおける 「1台以上のサーバのセキュリティアップデート責任が医療機関にある」という設問について、本文の対象定義（NOを選択した医療機関が対象）と論理的には整合しているものの、設問文およびYES／NOの方向性が直感的に理解しづらく、対象範囲を誤解する可能性があります。対象読者が小規模医療機関であることを踏まえ、設問文の表現の見直し、もしくは補足説明の追加をご検討ください。	ご意見として参考にさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
233	保守委託機関編	1	概説編の図も修正されているため、本文が修正されていないものと推察いたしました。 また、1章に記載の ・システム運用担当者が不在 ・小規模で、経営管理と企画管理の部門が区別されていない ・セキュリティアップデートを含めたシステム保守を十分に事業者に委託している （積極的なSaaSの活用や、保守契約による委託が想定される。） を対象としていること明確にするために、本文を下記に修正してはどうか？ ＜修文案＞ 保守委託機関編（以下、本編という）では、”システム運用担当者が不在かつ小規模で経営管理と企画管理の部門が区別されていない医療機関等で、”下図１のフローチャートにおいて、”「すべてのサーバのセキュリティアップデート責任を事業者に委託している」で「YES」”を選んだ医療機関等を対象とする。	ご指摘の修正案を踏まえて修正しました。
234	保守委託機関編	1	１行目 ■　保守委託機関編（以下、本編という）では、下図１のフローチャートにおいて、「１台以上のサーバのセキュ・・・ 文先頭の■を削除してはどうでしょうか ＞■が何を意味しているのか不明です ＞１章と同様な段落構成での記載が妥当です	ご指摘を踏まえて修正しました。
235	保守委託機関編	1	２行目 「１台以上のサーバのセキュリティアップデート責任が医療機関にある」で「NO」を選んだ医療機関等を対象とする。 フローチャートと説明が合っていませんので、修正をお願いします	ご指摘を踏まえて修正しました。
236	保守委託機関編	1	１１行目 （※）「医療情報システム・サービス事業者」とは、・・・ P2の１章の第３段落の下に移動してはどうでしょうか ＞意見番号２とセットの修正をおこなえば読みやすいと思います	医療情報システム・サービス事業者については削除しました。
237	保守委託機関編	2	保守委託期間編（案） 3．保守委託機関における遵守項目 9.医療情報システムの利用者に関する認証等及び権限 ④ クライアント端末のアプリケーションログイン時には、令和9年度までに二要素認証を採用すること。 本項はアプリケーション単位での二要素認証対応を求める記載となっているが、クライアント端末のOSログイン時に二要素認証を実施し、その認証を前提として同一または連携した認証情報によりアプリケーションを利用する構成についても、本要件を満たすものとして位置付ける旨を明確化すべきと考えます。その際、クラウドサービスの積極的な活用を前提とする保守委託機関においては、クラウド型の認証基盤を利用し、電子証明書等を用いた強固な認証方式を採用することも有効な対応策として位置付けることが考えられます。	ご指摘を踏まえて、以下の通り修正しました。 P16　3ポツ目に追記 「認証した情報をアプリケーションの資格情報等と連携し、適切な権限付与が可能な場合はOSやミドルウェアでの二要素認証を許容する。ただし、OSで一要素、アプリケーションで一要素のような認証は許容されない。」 ご指摘のうち後段については、個別性が高いためご意見として参考にさせていただきます。
238	保守委託機関編	2	番号に誤りがあります。 ③ 外部保存の委託先事業者選定の際は	ご指摘の修正案を踏まえて修正しました。
239	保守委託機関編	2	"JIS" が抜けています。 際は、JIS Q15001(プライバシーマーク)	ご指摘の修正案を踏まえて修正しました。
240	保守委託機関編	2	「許可なく分析等を行わないこと」については具体的に記載したほうが良いと思います。変更案は個人情報保護法第28条の表現をベースに作成しています。案1は障害調査等を目的とした事業者によるログの調査を含む全てのデータを対象としたー般的な表現です。案2は個人情報だけにフォーカスした表現です。 (案1)事業者がアクセス可能なデータについては、データの種別ごとに事業者の利用目的を明確にし、それ以外の用途では利用させないこと。 (案2)事業者が取り扱う個人情報については、事業者の利用目的を明確にし、それ以外の用途では利用させないこと。	ご指摘の修正案を踏まえて修正しました。
241	保守委託機関編	2	最近のマルウェアはフォレンジック調査を困難にすることを目的として自身を削除する処理を持つことがよくありますが、高度なフォレンジック調査においてはマルウェアの該当動作のトリガーとなるシステムのシャットダウンやネットワークの切断を意図的に行わない手法があります。（Note:ネットワーク切断の代わりに帯域を極端に絞る方法が使われます。）これらの手法をガイドラインが否定しないために、「など」を追加することで、必ずしもシャットダウン等を実施しなくても良いと読むこともできるようにします。 インシデント発生時は、ネットワーク切断、機器隔離、システム停止、バックアップからの復元（複数方式・数世代確保、オフライン管理等が重要）などを行うこと。	ご指摘の修正案を踏まえて修正しました。
242	保守委託機関編	2	「8.サイバーセキュリティ」ではインシデント発生時の遵守項目をまとめているので、情報漏洩に対する個人情報保護委員会への報告も追加すると良いと思います。 ④インシデント発生により情報漏えい等のおそれがある場合は、個人情報保護法に基づき速やか(概ね3～5日以内)に個人情報保護委員会に報告すること。	ご指摘の修正案を踏まえて、以下の通り修正しました。 P15　２ポツ目を追記 「個人情報の漏えい等（又はそのおそれ）が生じた場合には、個人情報保護法上の対応を図ること。」
243	保守委託機関編	2	「権限が最低限」か「人数が最小限」のどちらであるか明確な表現が良いと思います。 （類似する表現として、企画管理編→13の遵守事項の⑥には「最小限の対象者にのみ付与すること」という記載があります。） 特に、管理者権限を与えるアカウントは必要最小限のユーザとすること。	ご指摘の趣旨は他の箇所でも記載しておりますので、原案の通りとさせていただきます。
244	保守委託機関編	2	用語の誤りがあります。 OS (Operating System)	ご指摘の修正案を踏まえて修正しました。
245	保守委託機関編	2	現在医療機関で運用されている主要なサーバOSのそれぞれについて、現実的な話として、これは実施可能なのでしょうか。パスワード認証が脆弱という視点では、二要素認証以外の技術的手段も含めた方が良いと思います。	ご意見として参考にさせていただきます。
246	保守委託機関編	2	日本語が不自然です。 ⑥医療機関等で利用するIoT機器に対しても端末と同様にリスク評価のうえ、ファームウェアは脆弱性のないバージョンにアップデートすること。IoT機器の使用終了時は個人情報を削除し、接続解除をすること。	ご指摘の修正案を踏まえて修正しました。
247	保守委託機関編	2	「最新化」は日本語としてはあまり使わないので、別の表現の方が良いと思います。 ④全体構成図（ネットワーク・システム構成図）及び関係者一覧を作成し、変更が生じた際には速やかに反映すること。	ご指摘の修正案を踏まえて修正しました。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
248	保守委託機関編	2	【項番３】 【パブリックコメント対象個所】 保守委託機関編　P5 5.　安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約）（２） 【意見内容】 「外部保存の委託先事業者選定の際は、Q15001(プライバシ？マーク)、JIS、Q27001(ISMS)又はこれと同等の規格の認証を受けているシステム関連事業者を選定すること。」 を以下に変更する。 （２）は（３）と変更。冒頭の内容は企画管理編のP26 (6) f&gの表現をコピーする。そのあとに、さらに以下を追加する。 これら認証等の取得をもって、サービスそのもの安全管理水準を満たすわけではないことに留意する必要がある。システム等の安全管理の妥当性については、対象事業者内部の独立した監査部門や第三者機関が評価を行っていることを確認する必要がある。 【理由】 企画編と整合を取るため。安全管理に関するマネージメント評価と提供されるサービスそのものの安全性の評価があることの理解を深めるため。小規模医療機関用のサービスは少人数の開発者で開発しているため、社内でのシステム評価が甘くなるので、社内の監査部門や外部の第三者評価を義務化する（２省ガイドラインでは望ましいとなっているが）。医療機関側に知識が乏しい分、提供されるサービスが適正であることを前提としている為。第三者確認が必要。	ご指摘の修正案を踏まえて、Ｐ１２の表記について修正・加筆しました。 また、監査部門や第三者機関での評価につきましては、本保守委託機関編が比較的小さな医療機関等を想定しているため、原案のままとしております。
249	保守委託機関編	2	保守委託機関編のガイドラインの対象に関して 【意見の理由・内容】 現在、本ガイドラインの対象範囲は主に「電子カルテシステム」および「部門システム」と定義されています。しかし、一般医療機器である検体検査装置（血液分析装置等）において、リモートメンテナンスを実施するケースが増加しています。これらの医療機器が「保守委託機関編」の対象に含まれるのか、現行の定義では解釈が分かれる可能性があり、医療機関・メーカー双方でセキュリティ対策の基準にばらつきが生じる恐れがあります。 また、「リモートメンテナンス」の定義そのものも、技術の進展に伴い曖昧になっています。 例えば、従来のような「外部から機器本体へリモートデスクトップ等で直接アクセスし操作するもの」以外に、「機器の稼働状態やログのみをクラウドサーバへ送信し（個人情報は非識別化・暗号化済み）、メーカー側で状態を監視・診断するもの」も普及しています。 後者のような、医療機関内の機器に対して外部からの直接的な「侵入・操作」を伴わない形態が、本ガイドラインが規定する「リモートメンテナンス」の範囲に含まれるのかどうかが不明確です。	医療機器等における本ガイドラインの適用場面については示しておりますので、原案の通りとさせていただきます。
250	保守委託機関編	2	保守委託管理編　3. 保守委託機関における順守項目から1.2　医療機関などにおける責任において、まる1について、規程の列が空白ですが、個人情報保護教育等の職員への教育等、医療機関側の責任でしなければいけないことは必ず存在するため、医療情報システムの利用で医療機関側が運用管理規定を作らなくてよいことはあり得ないため、「要」の間違いではないでしょうか。	規程とすべき対象については見直しました
251	保守委託機関編	2	３．リスクマネジメント（リスク管理） ①医療情報システムで取り扱う情報及び関連する情報のリストを作成し、・・・・ 規程＝要　ではないでしょうか ＞本項目を説明するP11の最初の■で、「安全管理対策を施す対象を明確にするため、医療情報等のリストを作成する必要がある」と要求している	規程の対象となる項目については、見直して修正しました。
252	保守委託機関編	2	保守委託機関編P6 ３．保守委託機関における遵守項目 ７．医療情報システムに用いる情報機器等の資産管理 ①医療情報システムの資産管理を行うために必要な規程類を整備すること。 規程＝要　ではないでしょうか ＞②において「整備された規程に基づいて・・・」となっているので、①が整備されないと②は実行できまないと思われます	規程の対象となる項目については、見直して修正しました。
253	保守委託機関編	2	１０．技術的な 全管理対策の管理 ①サーバルーム等のセキュリティ境界への入退室管理（施錠、識別、記録）を行うこと。 規程＝ブランク　としてはどうか ＞ビルクリニックなど敷地面積が狭い診療所で、セキュリティエリアを区分することはできないと思われます もしくは、 規程＝要とするのであれば、本項の解説を行うP17の■群に、下記の説明文を追加してはどでしょうか ■複合ビル等内に開設した敷地面積が狭い診療所等において、セキュリティ境界を確保できない場合は、診療所の入口など外界との境界となる箇所の入退出管理を行うこと。	診療所等でセキュリティ区画が定義できな場合でも、原案では医療情報の記録媒体や医療情報システムが格納されるキャビネットやシステムラックなどは、施錠管理する旨を示しており、必要な対応を求めています。原案の通りとさせていただきます。
254	保守委託機関編	3	1.1　安全管理に関する法令の遵守 ７行目 ■　法令上求められる要件に必要な技術的対応、資料等は、委託先事業者に提出させることも十分想定される。MDS/SDS（Manufacture/Service、 rovider、Disclosure、Statement、for、Medical、Information、Security）の提出を事業者に求め、項目の適 性を確認すること。 MDS/SDSの説明を追記してはどうしょうか ＞P18の上から４つ目の■で、厚労省標準規格であることが記載されています。この記述を、MDS/SDSの解説が初めて出てくるＰ９に移動して説明行うのが良いと思われます	ご指摘の修正案を踏まえて修正しました。
255	保守委託機関編	3	欄外 SLA（Service　Level　Agreement）とは、事業者が提供するサービスの内容とレベルについて委託側と提供側が合意した文書・・・・ 下記の記述としてはどうでしょうか SLA（Service　Level　Agreement）とは、事業者が提供するサービスの品質水準を、委託側と提供側とで合意した文書・・・ ＞SLAはサービスを保障する最低ラインを明記した文書と理解しています。このためこのことを理解できる日本語に置き換えた方が良いと思います。	ご指摘の修正案を踏まえて修正しました。
256	保守委託機関編	3	８．サイバーセキュリティ １つ目行の■の３行目 ・・・、BCP に基づく対応を要する。警察や所管省庁等に報告を行うことも求められる。・・・ 下記の記述としてはどうでしょうか ・・・。警察や所管省庁等に報告を行うことも求められるので、直ちに報告できるように、報告先の名称及び連絡手段等をリスト化した緊急連絡網を作成することが望ましい。 ＞緊急時に連絡先の情報を探している余裕などないため	ご指摘の修正案を踏まえて修正しました。
257	保守委託機関編	3	1.2 医療機関等における責任 並列されているものの種別の不一致があります。 (案1)非常時（システム障害時、災害時、サイバー攻撃発生時）に (案2)非常時（システム障害、災害、サイバー攻撃の発生）に	ご指摘の修正案を踏まえて修正しました。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
258	保守委託機関編	3	2.　責任分界 注釈6でSLAの説明がありますが、本文書で初出は p.7 です。 (p.7 に移動)	ご指摘の修正案を踏まえて修正しました。
259	保守委託機関編	3	5. 安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約） 表記揺れです。（プライバシーマーク vs Pマーク） ③ 外部保存の委託先事業者選定の際は、プライバシーマーク[7]、ISMS[8]又はこれと同等の規格の認証を受 ているシステム関連事業者を選定すること。 また、安全管理方針、体制、バックアップ状況、信用度、認証（ISMAP[9]、JIS Q15001（プライバシーマーク）、JIS Q27001（ISMS）等）の取得状況、保存場所を確認し、情報機器等が、国内法の適用及び執行の及ぶ範囲にあることを確実にすること。	ご指摘の修正案を踏まえて修正しました。
260	保守委託機関編	3	5. 安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約） 注釈 7～9 は、それぞれ注釈 3～5と重複しています。 （削除）	ご指摘の修正案を踏まえて修正しました。
261	保守委託機関編	3	7. 医療情報システムに用いる情報機器等の資産管理 ①BYODは個人端末を「持ち込むこと」を指す言葉であり、持ち込んだ端末を指す言葉ではありません。端末を指す場合は「BYOD端末」と書きます。 ②BYODのスペルは初出の所で示したほうが良いです。 ⑤BYOD（Bring your own device、個人が所有する情報機器を持ち込むこと）端末の利用について、利用許諾条件や管理方法等を規程に含め、利用許諾状況も含めて台帳管理を行うこと。 職員の私物を利用するBYODも医療機関等が管理する機器と同等の管理が求められる。具体的には、BYOD端末の登録等に関する手順と設定、台帳管理を行うことや、医療機関等の所有する機器と同等の管理をするための手順を作成すること。	ご指摘の内容を反映しました。
262	保守委託機関編	3	7. 医療情報システムに用いる情報機器等の資産管理 「PCの計算能力の向上」が問題になるのは古い暗号技術の利用など、システムの作りが悪い場合に限定されます。ここでは読者にパスワード認証が脆弱である認識をもたせることを目的と思いますので、変更案のようにしてみてはいかがでしょうか。 また、昨今ではユーザ1人あたりが管理すべきパスワード数の増加や、人間の弱みを利用したサイバー攻撃の高度化により、パスワード単独による認証では十分な安全性を確保することが困難となってきている。	ご指摘の箇所はパスワードの脆弱性に関する背景の説明になりますので、原案の通りとさせていただきます。
263	保守委託機関編	3	１０．技術的な安全管理対策の管理 この段落の内容から推測すると、おそらく「クラウド型VPN」は消し忘れです。 ネットワーク機器については、自動アップデートを採用することが望ましい。	ご指摘を踏まえ、文章の意図を明確化し「ネットワーク機器についてはリスク低減のため、クラウド型VPN、自動アップデートを採用することが望ましい。」に修正しました。
264	保守委託機関編	3	１０．技術的な安全管理対策の管理 括弧が連続して読みにくいです。 可能な限りMDS/SDS[11]を事業者から入手すること。 11 書式は 「HS040「製造業者/サービス事業者による医療機関セキュリティ開示 」ガイド」を参照。厚生労働表標準規格については、https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html 参照。具体的な説明は、「「製造業者/サービス事業者による医療情報セキュリティ開示 」の概要」（厚生労働省）を参照。	ご指摘の修正案を踏まえて修正しました。
265	保守委託機関編	3	■保守委託機関編 P10 >VPN 機器をはじめとする外部ネットワークとの接続点となる情報機器については、脆脆弱性の管理が適切 に行われず、サイバー攻撃の起点となる事案が頻発している。脆弱性の管理等について保守契約 の範囲を明確にし、確実に管理可能な体制を整備すること。 →情報機器の管理を委託している医療機関については、保守契約の締結は必須にするべきと考えるが、これでは医療機関に伝わりにくい。よって修正案を提示する。 （修正案） VPN 機器をはじめとする外部ネットワークとの接続点となる情報機器については、脆弱性の管理が適切に行われない場合、サイバー攻撃の起点となる事案が頻発していることから、特に慎重な管理が求められる。 これらの情報機器の管理を委託先事業者に委ねている医療機関等においては、脆弱性対応やセキュリティアップデート等の安全管理措置が確実に実施されるよう、当該機器に関する保守契約を締結し、その契約範囲を明確にしておくことが不可欠である。 具体的には、脆弱性情報の継続的な把握、修正プログラムやファームウェアの更新対応、設定変更や緊急時対応等が保守契約の対象に含まれていることを確認し、医療機関等が自ら対応を行うことが困難な事項については、委託先事業者が責任をもって実施する体制を整備する必要がある。 なお、これらの内容が契約上明確に定められていない場合、脆弱性管理が実施されないまま放置されるおそれがあり、医療機関等における情報セキュリティリスクの増大につながることから、保守契約の締結または内容の見直しを行うことが強く望まれる。 P18 >医療機関等が用いる端 、ネットワーク機 については、不定期にセキュリティパッチや、マルウェア 対策ソフトのパ ーンファイルなどが公表され、その内容に従って更新することが求められる。上記のセ キュリティ対応について事業者に委託していない （特にPC 等の医療機関等が自ら購入したも の）には、医療機関等が自ら対応する必要がある。事業者に委託している には、委託する内 容や範囲を明確にし、対応の漏れがないようにすること。実際には、端 は OS の自動アップデート を適用することや、可能な限りセキュリティアップデートを保守契約に含めて事業者の責任範囲とす ることが考えられる。ネットワーク機 については、クラウド型 V N、自動アップデートを採用することが 望ましい。 →こちらも保守契約を締結せずに医療機関で実施するのは困難な内容であると考える。保守契約の締結を強く医療機関に促す内容に修正したほうが良い。以下の通り修正案を提示する。 （修正案） 医療機関等が用いる PC 等の端末やネットワーク機器については、セキュリティパッチやマルウェア対策ソフトのパターンファイル等が不定期に公表されており、それらの内容を適時に把握し、確実に更新することが求められる。 これらの対応について事業者に委託していない場合、とりわけ医療機関等が自ら購入・保有している PC 等の端末については、医療機関等が主体となって OS やソフトウェアの更新、マルウェア対策等を継続的に実施する必要がある。しかしながら、こうした作業を適切かつ継続的に実施するためには、専門的な知識や運用体制の確保が必要であり、医療機関等が単独で対応することは困難な場合が多い。 このため、PC 等の端末やネットワーク機器に関するセキュリティ対応については、可能な限り事業者との間で保守契約を締結し、セキュリティパッチの適用、マルウェア対策ソフトの更新、設定管理等を契約上の責任範囲として明確に位置付けることが強く望まれる。 事業者に業務を委託する場合には、委託内容および対応範囲を具体的に明確化し、PC 等の端末における OS の自動アップデートの適用状況や、セキュリティアップデート対応の実施責任について、対応の漏れが生じないよう管理することが重要である。あわせて、ネットワーク機器については、クラウド型 VPN や自動アップデート機能を備えた製品を採用するとともに、保守契約の下で継続的なセキュリティ管理が実施される体制を整備することが望ましい。	一つ目の点については、ご指摘の修正案を踏まえて、以下の通り修正しました。 「VPN機器をはじめとする外部ネットワークとの接続点となる機器については、脆弱性の管理が適切に行われず、サイバー攻撃の起点となる事案が頻発している。脆弱性の管理等について保守契約の範囲を明確にし、確実に管理可能な体制を整備すること。原則として、脆弱性対応を事業者の保守範囲として契約に含むことを想定する。昨今のサイバー攻撃事案では、事業者側が脆弱なパスワードや、他院と共通のパスワードを使い回すことで被害に遭った事案も発生している。例えば、事業者の設定するパスワードが本ガイドラインに適合していることや、電子証明書の利用によって認証することを契約書によって担保することが考えられる。」 二つ目の点については、保守委託機関編では、「すべてのサーバのセキュリティアップデート責任を事業者に委託している」医療機関等を対象としているため、原案の通りとさせていただきます。

「医療情報システムの安全管理に関するガイドライン第6.1版（案）」に関する御意見募集の結果について （別紙）

項番	対象	該当箇所	ご意見	回答
266	保守委託機関編	3	９．医療情報システムの利用者に関する認証等及び権限 ④クライアント端末 のアプリケーションログイン時には、令和９年度までに二要素認証を採用すること。対応が困難な場合には、令和９年度以降のシステム更新時に対応可能な事業者を選定すること。 システム運用編P35 表14-1下部に「※認証した情報をアプリケーションの資格情報等と連携し、適切な権限付与が可能な場合はOSやミドルウェアでの二要素認証を許容する。ただし、OSで一要素、アプリケーションで一要素のような認証は許容されない。」という記載があるため、同じ文言を注釈として記載してはどうか。	ご指摘の修正案を踏まえて修正しました。
267	保守委託機関編	3	３．リスクマネジメント（リスク管理） 一般的に、安全管理対策は、医療機関等がリスクを踏まえて行うことになる。しかし、リスクアセスメントやその管理については、専門的な分析などが必要となるため、本編では医療機関等において最低限実施すべきことを記載している。特にクラウドサービスを積極的に利用することにより、リスクや脅威への対応を事業者 に委ねることが可能となるため、これを推奨する。 2省ガイドラインでは事業者においてリスクベースアプローチにてリスクアセスメントを実施し、リスク対策の作成を求めている。 事業者が作成するリスク対策には、医療機関等にもリスク対策を求める記載がされる場合があり、且つ、契約書に2省ガイドラインの遵守への同意を盛り込むため、「事業者側から提示されたリスク対策について医療機関等も協力する必要がある。」という記載を追記してはどうか。	ご意見として参考にさせていただきます。
268	保守委託機関編	3	２． 責任分界 本項では、VPN機器等の外部ネットワークとの接続点における脆弱性管理および保守契約の範囲を明確にする重要性が示されていますが、外部からの侵入リスクを低減する観点では、当該接続点における認証方式の強度も重要な要素であると考えられます。特に、VPN接続に際しては、接続可能な端末や利用者を限定できるような認証方式を採用することが有効であり、例えば電子証明書の利用等により、端末および利用者の双方を適切に識別・制御する仕組みが考えられます。これらの観点も含め、VPN機器等の外部接続点における認証方式についても、保守契約の範囲や責任分界の整理対象として位置付ける旨を追記することが望ましいと考えます。	ご指摘を踏まえ、「原則として、脆弱性対応を事業者の保守範囲として契約に含むことを想定する。」と追記しました。
269	保守委託機関編	3	９．医療情報システムの利用者に関する認証等及び権限 本項では「クライアント端末のアプリケーションログイン時に二要素認証を採用すること」や、「クライアント端末上のアプリケーションおよびサーバOSについて二要素認証が可能なシステムを選定すること」が記載されていますが、文言上、アプリケーション単位での二要素認証対応を原則として求めているようにも読み取れます。実運用においては、クライアント端末のOSログイン時に二要素認証を実施し、当該認証を起点として同一または連携した認証基盤（SSO等）を介して各アプリケーションを利用する構成も一般的であり、すべてのアプリケーションが個別に二要素認証機能を有することが困難な場合も多いです。令和7年に示されたチェックリストにおける考え方との整合性の観点も踏まえ、認証の実現方法をアプリケーションログイン時に限定せず、OSログイン時や統合認証基盤においてニ要素認証が適切に実施されている構成についても、本要件を満たすものとして位置付ける旨を明確化するべきと考えます。	ご指摘を踏まえて、以下の通り修正しました。 P16 ３ポツ目に追記 「認証した情報をアプリケーションの資格情報等と連携し、適切な権限付与が可能な場合はOSやミドルウェアでの二要素認証を許容する。ただし、OSで一要素、アプリケーションで一要素のような認証は許容されない。」
270	保守委託機関編	4	【遵守事項】④ 受託した医療情報の分析等に関する規定について、品質維持や安全性向上を目的とした分析の必要性にも配慮した記載とすることが望ましい。 特に、精度検証や誤認識の修正等の分析は、医療システムの安全な運用に資する側面があるため、目的や安全管理措置を明示した上で、契約に基づき適切に実施可能とする運用が確保されることが望ましい。	受託した医療情報の分析については、患者への配慮を踏まえて医療機関等の判断によるため、原案の通りとさせていただきます。
	QA		【意見の背景と基本的立場】 医療分野におけるサイバーセキュリティ強化の趣旨に賛同いたします。一方で、病院情報システムと接続される医療機器（分析装置等）への本ガイドラインの適用範囲については、現場での解釈の齟齬を防ぐため、将来的な「3省2ガイドライン」を横断したQ&A等による整理を強く要望します。 【具体的な意見・要望事項】 1. 薬機法との整合性および適用範囲の明確化 医療機器は、薬機法に基づく基本要件基準第12条第3項等により、設計段階からリスクマネジメントおよびサイバーセキュリティ要件が課されており、電子カルテ等の一般的な情報システムとは制度的前提が異なります。本ガイドラインが、医療機器に固有の責任体系（製造販売業者等の責任）を代替・上書きするものではないことを明示してほしいです 2. 技術的制約を踏まえた代替策の許容 システム運用編で言及されている多要素認証（MFA）やEDR等の高度な対策について、医療機器においてはソフトウェアの変更管理や再バリデーションを伴い、医療安全や装置性能に予期せぬ影響を及ぼす実務上の制約があります。「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（令和5年3月31日 医政参発0331第1号）」に示されている設計原則に則り、ネットワーク分離や通信制御等の代替的なリスク低減策による「リスクベースのアプローチ」が許容される旨を、本ガイドライン内でも明確に言及することを求めます。 3. 責任分界の整理 企画管理編における責任分界と薬機法上の責任体系との関係を整理し、医療機器に関する本ガイドラインの適用範囲を、病院情報システムとの接続・データ連携、およびネットワーク境界部分の管理等に限定して補完的に適用する考え方を示してほしいです。（将来的な補足Q&Aでも構いません） 【期待される効果】 上記の内容がQ&Aや補足資料等で整理されることにより、医療機関と医療機器製造業双方の役割分担が明確化されます。結果として実務上の混乱が抑制され、ガイドラインの実効性がより向上することが期待されると考えます。	医療機器等における本ガイドラインの適用場面については示しておりますので、原案の通りとさせていただきます。