JAHIS

ＪＡＨＩＳ標準 24－xxx

Japanese Association of Healthcare Information Systems Industry

# ＪＡＨＩＳ
# 「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書」ガイド
# Ver.5.0

２０２４年＊月

一般社団法人 保健医療福祉情報システム工業会

医療情報システム部会　セキュリティ委員会

開示説明書 WG

# JAHIS「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書」ガイド

## Ver.5.0

# ま　え　が　き

近年の情報技術の進歩は目覚しく、社会的にも情報化の要請は一層高まりつつあります。医療情報においても、医療情報システムの導入及びそれに伴う外部保存を行う場合の取扱いに関し、個人情報保護法や e-文書法への適切な対応の総合的な指針として、厚生労働省から「医療情報システムの安全管理に関するガイドライン」（以下、安全管理ガイドラインと略す）が発行されています。

本開示書が公開される前は、各製造業者の医療情報システムのセキュリティ機能に関する説明には標準的記載方法の定めがなく、その記載レベルもさまざまである状況でした。このことは、医療機関等内のトータルシステムの構築を担う担当組織においては、各システム間の整合性を取る際の支障であり、各医療機関等で独自に策定した書式にその都度、製造業者が対応することもまた、業務の効率化を妨げることにもなります。

そこで、一般社団法人保健医療福祉情報システム工業会（JAHIS）医療システム部会セキュリティ委員会及び一般社団法人日本画像医療システム工業会（JIRA）医用画像システム部会セキュリティ委員会は、製造業者による製品のセキュリティに関する説明を、日本での標準書式とすることを想定して「製造業者による医療情報セキュリティ開示書（略称：MDS）」の書式を作成しました。Ver.4.0 でサービス事業者が提供する医療情報サービスを対象とした医療情報セキュリティ開示書（略称：SDS）を追加するため、JAHIS/JIRA に加えて一般社団法人電子情報技術産業協会（JEITA）、一般社団法人日本クラウド産業協会（ASPIC）にも参画していただきました。

この標準的な書式を用いることにより、製造業者/サービス事業者と医療機関等の双方にとって効率的なシステム構築が進むことを目的としています。

本書の意図は、医療機関等が医療情報システムによって保存、伝送される医療情報に関するリスクアセスメントを行うとき、それを支援できる重要な情報を提供することにあります。製造業者/サービス事業者は、標準化された書式を使用することにより、自らが製造する医療情報システムのセキュリティ関連機能に関して、医療機関等から情報提供を要求されたとき迅速に答えることができます。一方、医療機関等は、標準化された書式の記載により、製造業者によって提供されるセキュリティ関連情報のレビューを行い易くなります。

本書は、安全管理ガイドライン第 6.0 版（2023.5 発行）に基づく開示書書式と、この書式の記入方法と解説からなっています。また、読者の知識としては、安全管理ガイドラインの理解を前提にしています。Q&A 集も発行されていますので合わせてご参照ください。

202＊年＊月　一般社団法人保健医療福祉情報システム工業会
医療システム部会セキュリティ委員会
一般社団法人日本画像医療システム工業会医用画像システム部会セキュリティ委員会
JAHIS-JIRA 合同開示説明書 WG

**<<　告知事項　>>**

**本ガイドは関連団体の所属の有無に関わらず、ガイドの引用を明示することで自由に使用することができるものとします。ただし一部の改変を伴う場合は個々の責任において行い、本ガイドに準拠する旨を表現することは厳禁するものとします。**

**本ガイドならびに本ガイドに基づいたシステムの導入・運用についてのあらゆる障害や損害について、本ガイド作成者は何らの責任を負わないものとします。ただし、関連団体所属の正規の資格者は本ガイドについての疑義を作成者に申し入れることができ、作成者はこれに誠意をもって協議するものとします。**

# 目　　次


**1. 適用範囲** ..... 1

**2. 引用文献・参考文献** ..... 2

**3. 用語の定義** ..... 3

**4. 記号及び略語** ..... 4

**5. チェックリストの書き方** ..... 5

**6. チェックリスト（製造業者編）** ..... 7

「製造業者による医療情報セキュリティ開示書」チェックリスト ..... 7

**7. チェックリストの解説（製造業者編）** ..... 11

医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践 ..... 11
物理的安全対策 ..... 11
技術的安全対策 ..... 11
情報及び情報機器の持ち出しについて ..... 13
災害、サイバー攻撃等の非常時の対応 ..... 14
外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理 ..... 14
法令で定められた記名・押印を電子署名で行うことについて ..... 16
真正性の確保について ..... 17
見読性の確保について ..... 20
保存性の確保について ..... 20
診療録等をスキャナ等により電子化して保存する場合について ..... 22

**8. チェックリスト（サービス事業者編）** ..... 24

「サービス事業者による医療情報セキュリティ開示書」チェックリスト ..... 24

診療録及び診療諸記録等の医療情報の取り扱いを外部に委託する際の基準 ..... 34
医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践 ..... 36
組織的安全管理対策（体制、運用管理規程） ..... 36
物理的安全対策 ..... 37
技術的安全対策 ..... 38
人的安全対策 ..... 41
情報の破棄 ..... 43
医療情報システムの改造と保守 ..... 44
情報及び情報機器の持ち出し並びに外部利用について ..... 46
災害、サイバー攻撃等の非常時の対応 ..... 49
外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理 ..... 51
法令で定められた記名・押印を電子署名で行うことについて ..... 55
真正性の確保について ..... 57
見読性の確保について ..... 61

保存性の確保について ..... 62
診療録等をスキャナ等により電子化して保存する場合について ..... 64
**付録．作成者名簿** ..... 65
**改訂履歴** ..... 66

# 1. 適用範囲

本書にて規定する書式の記載内容は、製品説明の一部として製造業者/サービス事業者によって作成され、セキュリティマネジメントを実施する医療機関等を支援するため、以下の用途に用いられることを想定しています。

（1）製造業者が提供する医療情報システム、又はサービス事業者が提供する医療情報システムを用いたサービス（以下、「対象とするシステム/サービス」とする。）のセキュリティに関して、安全管理ガイドラインへの適合性を示すことにより、医療機関等側において必要な運用的対策の理解を容易にすること。

（2）安全管理ガイドラインを遵守しなければならない医療機関等にとって有用な情報を提供すること。当該システム/サービス導入医療機関等においてセキュリティマネジメントを実施するにあたって、製造業者/サービス事業者により提供される情報がリスクアセスメントの材料となること。

（3）各製造業者/サービス事業者にとって、安全管理ガイドラインへの適合性の自己評価手段として利用すること。

（4）医療機関等が製造業者/サービス事業者にセキュリティに関する説明を求める際の、要求のベースとして利用すること。

本書式での記載対象の単位は、製造業者の製品として提供される医療情報システム、又はサービス事業者による医療情報システムを用いたサービスです。例えば、ある型式製品/サービス名とそのオプションとして一まとまりに提供される機能の一式です。その中に他社の製品（例えばOSやミドルウェア）/サービスを含むならば、それによって実現される機能も記載対象に含めます。

なお、MDS/SDSにおけるオプションとは、自社で動作確認ができており、保守問い合わせ等の一時窓口なれる製品、またはサービスを指します。

さらに、本書の書式は、個々の医療情報システムにおける技術的セキュリティ関連、また医療情報サービスの技術的・運用的セキュリティ関連の具体的内容の記載を可能としています。

チェックリスト（製造業者編）は次のような構成になっています。

| | |
|---|---|
| １　～　１２ | 個人情報を含むデータを扱うすべての医療機関等で参照されるべき内容です。 |
| １３　～　２９ | 保存義務のある診療録等を電子的に保存する場合の内容です。 |
| ３０　～　３１ | 診療録等をスキャナ等により電子化して保存する場合の内容です。 |

チェックリスト（サービス事業者編）は次のような構成になっています。

| | |
|---|---|
| １ | 医療機関等とサービス事業者の契約に関する内容です。 |
| ２　～　７６ | 個人情報を含むデータを扱うすべての医療機関等で参照されるべき内容です。 |
| ７７　～　１０４ | 保存義務のある診療録等を電子的に保存する場合の内容です。 |
| １０５　～　１０６ | 診療録等をスキャナ等により電子化して保存する場合の内容です。 |

本書式の使用は強制されるものではありませんが、全ての製造業者/サービス事業者が本書式を使用し、多くの医療機関等で利用されて標準となることを期待しています。

本書式を作成したJAHIS/JIRAは、製品設計・設置・保守等の認証・試験・検査等は行っていません。また、特定の医療機関等における特定の目的・ニーズを満たすこと、あるいは個々の製品またはサービスの性能を保証するものではありません。この書式への記入内容は、記入した製造業者/サービス事業者が全責任を負います。

本書式の使用は、安全管理ガイドライン、本編及びQ&A集を理解していることを前提としています。

# 2. 引用文献・参考文献

(1) 厚生労働省・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

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

(2) 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（HISPRO）・「支払基金等へのレセプトオンライン請求用IPsec＋IKE サービス」チェックリスト項目集

http://www.hispro.or.jp/open/pdf/200909OnRece koumoku.pdf

(3) 独立行政法人情報処理推進機構セキュリティセンター（IPA）・TLS暗号設定ガイドラインVer.3.0.1

https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-3.0.1.pdf

(4) ANSI/NEMA NH1-2019 American National Standard— Manufacturer Disclosure Statement for Medical Device Security

https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx#download

和訳版（JIRA 作成）
http://www.jira-net.or.jp/commission/system/files/MDS2-2019_ja.pdf

# 3. 用語の定義

| 用語 | 説明 |
|---|---|
| e-文書法 | 「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」の通称 |
| 生体認証 | 人間の身体的特徴の情報を用いて個人の認証を行う行為のことを言う。バイオメトリクス（biometrics）認証 とも呼ばれる。 |
| 管理区域 | 情報資産を守るために、医療機関等によって定められた特別な管理を必要とされる区域 |
| 経路制御 | ルーティングとも呼び、ネットワーク上で IP パケットを目的地に転送するための、パケットの通り道（経路）についての情報を管理し、最適な経路を選択する仕組み。 |
| プロトコル制御 | 標準規格などで定められた通信手順などの各種プロトコル（ネットワークを介してコンピュータ同士が通信を行う上で、相互に決められた約束事の集合）を実装した機器やソフトウェアにおいて、プロトコルに従った処理手順を適切に実行できるようにするために組み込まれた仕組みのこと。 |
| 認定認証局 | 電子署名法にて定められている特定認証業務のうち認定認証業務を行う事業者により運用される電子認証局。 |
| 真正性 | 正当な権限において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である。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。（安全管理ガイドラインより引用） |
| クリアスクリーン | 個人端末のセキュリティ管理に関する概念。機密漏えいの防止、情報等に対する不正操作の防止を目的とした対策で、離席時に端末の表示を見られないようにログオフ等をすること。 |
| オブジェクト・セキュリティ | 情報資産に対する安全対策のこと。例えばファイルの暗号化や改ざん検知のための電子署名付与などの対策を指す。 |
| チャネル・セキュリティ | 通信経路に対する安全対策のこと。VPN などの対策を指す。 |
| 外部委託 | SDS において、サービス事業者が行う「委託」は医療機関から見た外部への委託となるため本ドキュメントでは「外部委託」とする。 |

# 4. 記号及び略語

本書では、次の記号及び略語・表記を用います。

| | |
|---|---|
| MDS | Manufacturer Disclosure Statement for Medical Information Security |
| SDS | Service Provider Disclosure Statement for Medical Information Security |
| CAdES | CMS Advanced Electronic Signatures |
| HPKI | Healthcare Public Key Infrastructure |
| IPsec | Security Architecture for Internet Protocol |
| JAHIS | Japanese Association of Healthcare Information Systems Industry |
| JIRA | Japan Medical Imaging and Radiological Systems Industries Association |
| JEITA | Japan Electronics and Information Technology Industries Association |
| ASPIC | ASP-SaaS-AI-IoT Cloud Industry Association (Japan Cloud Industry Association) |
| OSI | Open Systems Interconnection |
| S/MIME | Secure Multipurpose Internet Mail Extensions |
| SSL | Secure Socket Layer |
| TLS | Transport Layer Security |
| VPN | Virtual Private Network |
| XAdES | XML Advanced Electronic Signatures |

# 5. チェックリストの書き方

チェックリストは製造業者用/サービス事業者用それぞれ二部構成となっています。それぞれ最初のパートはチェックリストそのものであり、もう一つのパートは、チェックリストの補足事項を記載する備考記載欄です。チェックリストは質問に対する回答を選択する形式、備考記載欄は自由記載形式になっています。

チェックリストの項目は以下の通りです。

（1）基本情報

| | |
|---|---|
| 製造業者/サービス事業者 | ：対象とするシステムを提供する製造業者/対象とするサービスを提供する事業者の名称を記入します。 |
| 製品/サービス名称 | ：対象とするシステム/サービスの名称・型名を記入します。 |
| バージョン | ：対象とするシステム/サービスのバージョン（版番号）を記入します。 |
| 作成日 | ：チェックリストの記載日を記入します。 |

（2）質問項目

質問項目の括弧内に記載されている番号は、安全管理ガイドライン各章番号に対応するものです。

質問によっては主従形式になっており、主質問の回答によって従属質問への回答が必要になる場合は従属質問にも回答してください。

階層の主質問等で、製品/システム/サービスの機能(/運用)を問う場合の回答は、「該当」「非該当」とします。

セキュリティ機能(/運用)を問う場合の回答は、「はい」「いいえ」「対象外」とします。

※別添のExcel版チェックリストでは回答不要な従属質問はグレーアウトされます。

| | |
|---|---|
| 該当 | ：質問に該当する場合に選択します。 |
| 非該当 | ：質問に該当しない場合に選択します。 |
| はい | ：質問に対応している場合に選択します。質問によっては詳細説明を備考に記載する必要があります。また、オプション（＊）で対応可能な場合は備考にその旨を必ず記載しなければなりません。 |
| いいえ | ：質問に対応していない場合に選択します。基本的に備考に記載が必要となります。 |
| 対象外 | ：対象とするシステム/サービスの対応する機能でない場合に選択します。 |
| 備考 | ：「備考記載欄」に対応する番号を左欄に記入します。実際の内容は「備考記載欄」の右欄に記載します。 |

＊ MDS/SDSにおけるオプションとは、自社で動作確認ができており、保守問い合わせ等の一時窓口なれる製品、またはサービスを指します。

（3）備考記載欄

左欄に「備考」にて記した番号を記入し、右欄に機能の補足説明や「はい」「いいえ」「対象外」では説明しきれない内容等を自由に記載してください。

対象とするシステム/サービスがオプションにより「はい」となる場合は、具体的にオプションを記載してください。「いいえ」となる場合は医療機関等における運用での代替手段等の記載が必要です。「対象外」となる場合は、必要に応じてその理由等を記載してください。

安全管理ガイドラインの改訂などにより、本書式が最新の安全管理ガイドラインに対応していない場合、JAHIS/JIRA が本書式の改訂を行うまでの間、不整合箇所について「備考記載欄」にて記載することにより対応を行うこととしてください。

※別添のExcel版チェックリストでは、予め左欄に番号が記入されています。

# 6. チェックリスト（製造業者編）

## 「製造業者による医療情報セキュリティ開示書」チェックリスト

（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 版対応）

| | |
|---|---|
| 製造業者　： | 作成日　： |
| 製品名称　： | バージョン　： |
| | |
| **医療機関等における情報セキュリティマネジメントシステムの実践** | |
| １　扱う情報のリストを医療機関等に提示できるか？(概 4.5、経 2.2、企 6②、③) | はい　いいえ　対象外　備考____ |
| **物理的安全対策** | |
| ２　個人情報が入力・参照できる端末の覗き見防止の機能があるか？(シ 12.3.2、シ 12⑥) | はい　いいえ　対象外　備考____ |
| **技術的安全対策** | |
| ３　離席時の不正入力防止の機能があるか？(シ 12⑥) | はい　いいえ　対象外　備考____ |
| ４　アクセス管理の機能があるか？(シ 14①) | はい　いいえ　対象外　備考____ |
| ４．１　利用者の認証方式は？(シ 14⑤)<br>・記憶（ID・パスワード等）<br>・生体認証（指紋等）<br>・物理媒体（IC カード等）<br>・上記のうちの二要素を組み合わせた認証<br>（具体的な組み合わせを備考に記入してください）<br>・その他（具体的な認証方式を備考に記入してください） | <br>はい　いいえ　対象外　備考____<br>はい　いいえ　対象外　備考____<br>はい　いいえ　対象外　備考____<br>はい　いいえ　対象外　備考____<br><br>はい　いいえ　対象外　備考____ |
| ４．１．１　パスワードを利用者認証手段として利用している場合、パスワード管理は可能か？(シ 14⑥) | はい　いいえ　対象外　備考____ |
| ４．１．２　セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？(シ 14③) | はい　いいえ　対象外　備考____ |
| ４．２　利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？(経 4.2、シ 14.2) | はい　いいえ　対象外　備考____ |
| ４．３　アクセス記録（アクセスログ）機能があるか？(シ 17①) | はい　いいえ　対象外　備考____ |
| ４．３．１　アクセスログを利用者が確認する機能があるか？(経 4.2、企 5③、シ 17①) | はい　いいえ　対象外　備考____ |
| ４．３．２　アクセスログへのアクセス制限機能があるか？(企 5②、シ 17②) | はい　いいえ　対象外　備考____ |
| ５　時刻情報の正確性を担保する機能があるか？(シ 17③) | はい　いいえ　対象外　備考____ |
| ６　不正ソフトウェア対策機能を有しているか？(シ 8①、②) | はい　いいえ　対象外　備考____ |
| ７　無線 LAN を利用する場合のセキュリティ対策機能はあるか？(シ 13⑬) | はい　いいえ　対象外　備考____ |
| **情報及び情報機器の持ち出しについて** | |
| ８　ソフトウェアのインストールを制限する機能があるか？(企 8⑤、シ 7⑥) | はい　いいえ　対象外　備考____ |
| ９　外部入出力装置の機能を無効にすることができるか？(企 8⑤、シ 7⑥) | はい　いいえ　対象外　備考____ |
| １０　管理区域外への持ち出しの際、起動パスワード等のアクセス制限機能または暗号化機能があるか？(シ 7③) | はい　いいえ　対象外　備考____ |
| **災害、サイバー攻撃等の非常時の対応** | |
| １１　非常時アカウント又は、非常時機能を持っているか？(企 11、シ 11①) | はい　いいえ　対象外　備考____ |
| **外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理** | |
| １２　「外部と個人情報を含む医療情報を通信する機能」や「リモートメンテナンス機能」を有するか？ | 該当　非該当　　備考____ |
| １２．１　なりすましの対策（認証）機能を有するか？(シ 13②、④、⑪) | はい　いいえ　対象外　備考____ |
| １２．２　データの暗号化が可能か？(シ 13⑦) | はい　いいえ　対象外　備考____ |

| | |
|---|---|
| １２．３　ネットワークの経路制御・プロトコル制御に関わる機能を有しているか？(シ 13⑤) | はい　いいえ　対象外　備考____ |
| １２．３．１　ネットワークの経路制御・プロトコル制御に関わる機能について、安全性を確認できるようなセキュリティ対策が規定された文書を示すことができるか？(企 15⑦、シ 13⑤、⑥) | はい　いいえ　対象外　備考____ |
| １２．３．１．１　対応している通信方式はいずれか？(企 15⑦、シ 13④、⑤、⑥)<br>・専用線<br>・公衆網<br>・IP-VPN<br>・IPsec-VPN<br>・TLS1.2 以上 高セキュリティ型、クライアント認証 | <br>該当　非該当　備考____<br>該当　非該当　備考____<br>該当　非該当　備考____<br>該当　非該当　備考____<br>該当　非該当　備考____ |
| １２．３．２　ネットワークの経路制御・プロトコル制御に関わる機能の適正さ（回り込み対策を含む）を証明できる文書があるか？(企 15⑦、シ 13⑤、⑥) | はい　いいえ　対象外　備考____ |
| １２．４　リモートメンテナンス機能を有するか？ | 該当　非該当　備考____ |
| １２．４．１　リモートメンテナンスサービスに関し、不必要なリモートログインを制限する機能があるか？(シ 7⑫、シ 10.1、シ 18.1) | はい　いいえ　対象外　備考____ |
| **法令で定められた記名・押印を電子署名で行うことについて** | |
| １３　記名・押印が義務付けられた文書を扱っているか？ | 該当　非該当　備考____ |
| １３．１　HPKI 認証局、認定認証局、又は公的個人認証サービスが発行する証明書対応の署名機能があるか？(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| １３．２　HPKI 認証局、認定認証局、又は公的個人認証サービスが発行する証明書対応の検証機能があるか？(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| １３．３　総務省の「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が付与可能か？(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| １３．４　総務省の「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が検証可能か？(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| １３．５　保存期間中の文書の真正性を担保する仕組みがあるか？(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| **真正性の確保について** | |
| １４　入力者及び確定者を正しく識別し、認証を行う機能があるか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| １４．１　区分管理を行っている対象情報ごとに、権限管理（アクセスコントロール）の機能があるか？(企 15⑬、シ 14④) | はい　いいえ　対象外　備考____ |
| １４．２　権限のある利用者以外による作成、追記、変更を防止する機能があるか？(企 15⑬) | はい　いいえ　対象外　備考____ |
| １５　システムが端末を管理することによって、権限を持たない者からのアクセスを防止する機能があるか？(企 15⑬) | はい　いいえ　対象外　備考____ |
| １６　システムは記録を確定する機能があるか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| １６．１　確定情報には、入力者及び確定者の識別情報、信頼できる時刻源を用いた作成日時が含まれているか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| １６．２　「記録の確定」を行うにあたり、内容の確認をする機能があるか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| １６．３　確定された記録に対して、故意による虚偽入力、書換え、消去及び混同を防止する機能があるか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| １７　装置が確定機能を持っていない場合、記録が作成される際に、当該装置の管理責任者や操作者の識別情報、作成日時を含めて記録する機能があるか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |

| | |
|---|---|
| １８　確定された診療録等が更新された場合、更新履歴を保存し、更新前後の内容を参照する機能があるか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| １８．１　同じ診療録等に対して更新が複数回行われた場合、更新の順序性を識別できる機能があるか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| １９　代行入力の承認機能があるか？(企 13⑧、企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| １９．１　代行入力が行われた場合、誰の代行がいつ誰によって行われたかの管理情報を、その代行入力の都度、記録する機能があるか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| １９．２　代行入力により記録された診療録等に対し、確定者による「確定操作（承認）」を行う機能があるか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| **見読性の確保について** | |
| ２０　目的に応じて速やかな検索結果の出力機能があるか？(企 15⑬、シ 9④) | はい　いいえ　対象外　備考____ |
| ２１　システム障害に備えた冗長化手段や代替的な見読化手段はあるか？(企 15⑬、シ 11①、シ 11.1) | はい　いいえ　対象外　備考____ |
| ２１．１　冗長化手段があるか？(企 11.2、企 15⑬、シ 11.1) | はい　いいえ　対象外　備考____ |
| ２１．２　システム障害に備えた代替的な見読化手段があるか？(企 15⑬、シ 11①) | はい　いいえ　対象外　備考____ |
| **保存性の確保について** | |
| ２２　不正ソフトウェアによる情報の破壊、混同等が起こらないようにするための防護機能があるか？(経 3.4、企 15⑥、⑬、シ 7④、シ 8③、シ 8.1) | はい　いいえ　対象外　備考____ |
| ２３　記録媒体及び記録機器の保管及び取扱いについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？(企15③、④) | はい　いいえ　対象外　備考____ |
| ２４　情報の保存やバックアップについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？(企 15④、企 15.1) | はい　いいえ　対象外　備考____ |
| ２５　システムが保存する情報へのアクセスについて、履歴を残す機能があるか？(経 4.2、企 5①、④、シ 17①) | はい　いいえ　対象外　備考____ |
| ２５．１　システムが保存する情報へのアクセスについてその履歴を管理するための機能があるか？(経 4.2、企 5②、シ 17①) | はい　いいえ　対象外　備考____ |
| ２６　システムが保存する情報がき損した時に、バックアップされたデータを用いて、き損前の状態に戻すための機能があるか？(経 3.4.1、シ 11①、シ 18①、シ 18.1) | はい　いいえ　対象外　備考____ |
| ２７　記録媒体が劣化する前に情報を新たな記録媒体又は、記録機器に複写する機能があるか？(企 15⑬、シ 12⑤、シ 12.2) | はい　いいえ　対象外　備考____ |
| ２８　システムの移行の際に診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能があるか？(企 15⑬、シ 5①) | はい　いいえ　対象外　備考____ |
| ２９　マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えているか？(企 15⑬、シ 5②) | はい　いいえ　対象外　備考____ |
| **診療録等をスキャナ等により電子化して保存する場合について** | |
| ３０　診療録などをスキャナなどにより電子化して原本として保存する機能があるか？ | 該当　非該当　　備考____ |
| ３０．１　光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いているか？(企 16①、シ 16①) | はい　いいえ　対象外　備考____ |
| ３０．２　電子署名を行える機能があるか？(経 4.1、企 16③、⑦、シ 1①、シ 15①) | はい　いいえ　対象外　備考____ |
| ３１　診療録などをスキャナなどにより電子化して参照情報として保存する機能があるか？ | 該当　非該当　　備考____ |
| ３１．１　光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いているか？(企 16①、⑧、シ 16①) | はい　いいえ　対象外　備考____ |

| 備考記載欄 | |
|---|---|
| | |

# 7. チェックリストの解説（製造業者編）

## 医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践

### 「1　扱う情報のリストを医療機関等に提示できるか？(概 4.5、経 2.2、企 6②、③)」

本項目は、安全管理ガイドライン企画管理編「6. リスクマネージメント（リスク管理)」の考え方に基づいてシステムにおけるリスク分析を行うため、扱う情報をすべてリストアップしているかを確認するものです。

医療情報システムで扱う情報をすべてリストアップしている場合は「はい」、そうでない場合は「いいえ」としてください。リストが一部不足している等、補足説明が必要な場合は備考に記載してください。

## 物理的安全対策

### 「2　個人情報が入力・参照できる端末の覗き見防止の機能があるか？(シ 12.3.2、シ 12⑥)」

本項目は、安全管理ガイドライン　システム運用編「12.3.2　端末・サーバ装置等の不適切な利用等に関する対策」の考え方に基づいて覗き見防止機能の有無を確認するものです。

覗き見防止の機能を有している場合は「はい」、そうでない場合は「いいえ」、対象機器が本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

## 技術的安全対策

### 「3　離席時の不正入力防止の機能があるか？(シ 12⑥)」

医療情報を入力・参照する機能を有する端末では、正当な利用者以外の者による入力・参照を防止する必要があります。本項目は、長時間離籍の際に不正入力のおそれがある場合に、権限を持たない者による不正入力を防止する対策の有無を確認するものです。

クリアスクリーンやパスワード付きスクリーンセーバー等の対策を有する場合は「はい」、有していない場合は「いいえ」、対象機器が本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

### 「4　アクセス管理の機能があるか？(シ 14①)」

医療情報システムは、システムへのアクセスを正当な利用者のみに限定するために、利用者の識別・認証を行う機能が必要です。本項目は、このアクセス管理機能の有無を確認するものです。

医療情報システムの利用者の識別・認証の機能を有している場合は「はい」、有していない場合は「いいえ」としてください。アクセス管理を機能的な面から必要としない場合は 「対象外」としてください。

なお、本項目は、安全管理ガイドライン システム運用編「14. 認証・認可に関する安全管理措置」をよく理解した上で回答してください。

### 「4．1　利用者の認証方式は？(シ 14⑤)」

本項目は、利用者の認証方式として、「記憶（ID・パスワード等)」、「生体認証（指紋等)」、「物理媒体（IC カード等)」のいずれが利用できるのか、また、二要素認証が利用できるかを確認するものです。

「記憶（ID・パスワード等)」、「生体認証（指紋等)」、「物理媒体（IC カード等)」は、それぞれについて、利用できる場合は「はい」、利用できない場合は「対象外」としてください。

「上記のうちの二要素を組み合わせた認証」は、二要素認証が利用できる場合は「はい」、利用できない場合は「いいえ」とし、「はい」の場合は、記憶、生体認証、物理媒体の 3 要素の中から可能な組み合わせを備考に記入してください。

「その他」は、記憶、生体認証、物理媒体の 3 要素のいずれに該当するか判断できない認証方式で、利用できるものがある場合は「はい」、そのようなものがない場合は「対象外」とし、「はい」の場合は具体的な方式を備考に記入してください。

### 「４．１．１　パスワードを利用者認証手段として利用している場合、パスワード管理は可能か？(シ 14⑥)」

本項目は、パスワードを利用者認証手段として利用している場合、パスワード管理ができるかを確認するものです。

パスワードが管理可能である場合は「はい」、できない場合は「いいえ」としてください。本項目に記載されているパスワード管理においては、パスワードが暗号化（不可逆変換によること）されていることと、容易に類推されないための手段の両方を有する必要があります。

参考情報：米国国立標準技術研究所（「SP 800-63-4（Digital Identity Guidelines（デジタルアイデンティに関するガイドライン））第 4 版」

### 「４．１．２　セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？(シ 14③)」

本人の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合は、例えば、そのデバイスである IC カードの破損や所持忘れなどで、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意する必要があります。本項目は、その代替手段の有無を確認するものです。

技術的な代替手段を用意してある場合は「はい」、運用により行うことを求める場合は「いいえ」とし、推奨される運用があれば備考に記入ください。

### 「４．２　利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？(経 4.2、シ 14.2)」

医療情報システムは、利用者に応じてアクセスできる情報の範囲や、作業の内容（参照のみ、作成権限あり、更新権限あり等）に関する権限が付与されます。権限の付与は、基本的には医療機関等の内部の人事で定めた権限規程や、医療従事者の資格などに応じて設定されます。本項目は、利用者の職種・担当業務別の情報区分ごとのアクセス管理機能の有無を確認するものです。

その機能を有している場合は「はい」、有していない場合は「いいえ」としてください。

### 「４．３　アクセス記録（アクセスログ）機能があるか？(シ 17①)」

医療情報システムを利用するに当たっては、医療機関等は利用者のアクセスを監視するためのアクセスログ管理が必要です。本項目は、アクセスログ機能の有無を確認するものです。アクセスログには、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録できる必要があります。

アクセスログ機能を有する場合は「はい」、有していない場合は「いいえ」としてください。

### 「４．３．１　アクセスログを利用者が確認する機能があるか？(経 4.2、企 5③、シ 17①)」

医療情報システムの運用担当者は、特に個人情報を含む資源については、定期的にアクセスログの内容をチェックして不正利用がないことを確認することが求められています。本項目は、利用者がアクセスログを確認する機能の有無を確認するものです。

機能を有する場合は「はい」、有していない場合は「いいえ」としてください。

### 「４．３．２　アクセスログへのアクセス制限機能があるか？(企5②、シ17②)」

アクセスログは、それ自体に個人情報が含まれている可能性があること、情報セキュリティインシデントが発生した際の調査に非常に有効な情報であることから、不当な削除／改ざん／追加等を防止する対策が必要です。本項目は、アクセスログの保護機能の有無を確認するものです。

アクセスログに対して、アクセスする操作者の制限、改ざん防止措置等により、不当な削除／改ざん／追加等を防止する機能を有する場合は「はい」、有してない場合は「いいえ」としてください。

### 「５　時刻情報の正確性を担保する機能があるか？(シ17③)」

アクセスログの正確性のため、記録する時刻の精度は重要であり、管理対象の全てのシステムで時刻同期が取られている必要があります。本項目は、時刻情報の正確性を担保する機能の有無を確認するものです。

医療情報システムが、アクセス記録に使用される時刻情報に対して、標準時刻と時刻同期させる機能を有する場合は「はい」、有してない場合は「いいえ」としてください。

### 「６　不正ソフトウェア対策機能を有しているか？(シ8①、②)」

本項目は、不正ソフトウェア対策機能の有無を確認するものです。

不正ソフトウェア対策機能（例えばコンピュータウイルスの検出機能と駆除機能）を有する場合は「はい」、有してない場合は「いいえ」としてください。コンピュータウイルス対策ソフトがパターン定義ファイルを使用する場合、定期的にパターン定義ファイルの更新が必要になります。具体的な対策や制約等がある場合は備考に記載してください。

### 「７　無線 LAN を利用する場合のセキュリティ対策機能はあるか？(シ13⑬)」

医療情報システムにおいて無線 LAN を利用する際は、不正利用や盗聴などのほか、可用性などにも配慮した対策を講じることが求められます。本項目は、システム運用編「13. ネットワークに関する安全管理措置」の遵守事項⑬の要件を満たすセキュリティ対策機能の有無を確認するものです。

以下の３つのセキュリティ対策機能を全て有する場合は「はい」、いずれか１つでも満たさない場合は「いいえ」として、対策できていない内容について備考に記載してください。なお、無線 LAN の使用を認めていない場合（システムとしてサポート外）は「対象外」としてください。

・適切な利用者以外に無線 LAN を利用されないために、例えば、ANY 接続拒否等の機能を有すること。
・不正アクセス対策を実施するために、例えば MAC アドレスによるアクセス制限 機能を有すること。
・不正な情報の取得を防止するために、WPA2 AES、WPA2 TKIP 等により通信を暗号化する機能を有すること。

※　総務省発行の「一般利用者が安心して無線LANを利用するために」や「企業等が安心して無線LANを導入・運用するために」を参考に記載してください。

## 情報及び情報機器の持ち出しについて

### 「８　ソフトウェアのインストールを制限する機能があるか？(企8⑤、シ7⑥)」

本項目は、システムとしてソフトウェアのインストールを制限する機能の有無を確認するものです。例えば、ファイル交換ソフト（Winny 等）のような不適切な設定がされた外部ソフトウェアにより情報が漏えいする可能性があるため、外部から持ち込まれたソフトウェアのインストールを制限する等の情報漏えい対策が必要となります。

システム側で、ソフトウェアのインストールを制限する機能がある場合は「はい」、制限する機能が無い場合は「いいえ」、ソフトウェアのインストール自体ができない場合は「対象外」としてください。

### 「９　外部入出力装置の機能を無効にすることができるか？(企 8⑤、シ 7⑥)」

本項目は、外部入出力装置（DVD ドライブ、USB メモリー等）の機能を無効にすることができることを確認するものです。外部入出力装置の機能を無効にすることで、コンピュータウイルスなどの侵入防止や情報漏えい防止等の情報の持ち出しを制限することが可能となります。

外部入出力装置の機能を無効にすることができる場合は「はい」、できない場合は「いいえ」としてください。外部入出力装置を持たない場合は「対象外」としてください。

### 「１０　管理区域外への持ち出しの際、起動パスワード等のアクセス制限機能または暗号化機能があるか？(シ 7③)」

本項目は、ノートパソコンのような情報端末や心電計のようなポータブル機器等の情報記録可搬媒体を管理区域外へ持ち出す際に、起動パスワード等のアクセス制限の設定で使用制限が可能かを確認するものです。情報端末やポータブル機器の場合には、盗難、紛失、置忘れ等のリスクが存在するため、これらのリスクに対応した情報漏えい対策が必要となります。

情報端末やポータブル機器等に、起動時パスワード等のアクセス制限を設定できる機能または暗号化機能を有する場合は「はい」、有していない場合は「いいえ」、物理的に管理区域外へ持ち出しができない場合や情報を保有していない場合は「対象外」としてください。

## 災害、サイバー攻撃等の非常時の対応

### 「１１　非常時アカウント又は、非常時機能を持っているか？(企 11、シ 11①)」

本項目は、自然災害や IT 障害等の非常時に、システムとして医療サービスを提供できる機能を有するかを確認するものです。非常時には、システムとして正常なユーザ認証が不可能な場合の対応（非常時アカウントによる患者データへのアクセス機能）や、災害時の受付での患者登録を経ないような非常時の運用に対応した機能等が求められます。

上記のような非常時機能又は非常時アカウントを有する場合は「はい」、有していない場合は「いいえ」、システムとして該当しない場合（アカウント管理機能等が無い場合）は「対象外」としてください。

## 外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理

### 「１２　「外部と個人情報を含む医療情報を通信する機能」や「リモートメンテナンス機能」を有するか？」

本項目は標準機能、オプション機能を問わず、外部のシステムと個人情報を含む医療情報を通信する機能あるいはリモートメンテナンス機能の有無を確認するものです。１方向のみの場合も含まれます。「外部のシステムと個人情報を含む医療情報を通信」とは、医療機関、薬局、検査会社等間での診療情報の交換、医療機関等の従事者がモバイル型端末で外部から医療機関内の情報システムに接続、患者等による外部からのアクセスなどのケースを指します。

上記のような通信機能を有する場合は「該当」、機能を有していない場合は「非該当」としてください。

### 「１２．１　なりすましの対策（認証）機能を有するか？(シ 13②、④、⑪)」

外部との情報交換の際に、機密性保持のために送信元及び送信先が正しいことが担保されなくてはなりません。本項目は、送信元及び送信先を偽装するなりすましの対策として、認証機能の有無を確認するものです。

認証機能を有する場合は「はい」、有していない場合は「いいえ」としてください。補足説明が必要な場合は、どのような仕様の認証機能かを備考に記載してください。

### 「１２．２　データの暗号化が可能か？(シ 13⑦)」

本項目は、外部との情報交換の際に、機密性保持のためにデータ自体の暗号化（オブジェクト・セキュリティ）機能の有無を確認するものです。

データの暗号化機能を有する場合は「はい」、有していない場合は「いいえ」としてください。使用している暗号の仕様等の補足説明が必要な場合は、備考に記載してください。

例えば、S/MIME の利用、ファイルに対する暗号化、IPsec(ESP プロトコルを使用している場合等)又は TLS1.2 若しくは TLS1.3 は、暗号化するため、「はい」となります。

### 「１２．３　ネットワークの経路制御・プロトコル制御に関わる機能を有しているか？(シ 13⑤)」

本項目は、ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、異なる施設間を結ぶVPN の間で医療施設のルータを経由して送受信ができないように経路設定されていることを確認するものです。

「ネットワークの経路制御・プロトコル制御」とはネットワーク機器（ルータ、スイッチ、ファイアウォールなど)、又はそれと同等の機能を持つことを指しています。特に情報セキュリティリスクを極小化するために接続経路を限定したり、回り込みを禁止したりすることを指します。

機能を有する場合は「はい」、有していない場合は「いいえ」としてください。有する場合は、従属質問に回答してください。

### 「１２．３．１　ネットワークの経路制御・プロトコル制御に関わる機能は、安全管理ガイドラインを満たす設定が可能か？(企 15⑦、シ 13⑤、⑥)」

可能な場合は「はい」、設定できない場合は「いいえ」としてください。

安全性を確認できるようなセキュリティ対策が規定された文書を示すことができることが望ましいです。

### 「１２．３．１．１　対応している通信方式はいずれか？(企 15⑦、シ 13④、⑤、⑥)」

本項目は安全管理ガイドラインにおいて許容されている通信方式のそれぞれについて対応しているかを確認するものです。自社サービスで対応している場合は「該当」、他社が提供するネットワークサービスを契約する必要がある場合は「非該当」として備考に動作保証しているサービス等を記載してください。

＜「TLS1.2 以上」の場合（いわゆる SSL-VPN ではない）＞

- チャネル・セキュリティとして TLS を利用する場合は、相手の確認の手段が「TLS 暗号設定ガイドライン」の「高セキュリティ型」によって規定されるため、規定された内容に従って設定している場合は「はい」としてください。
- チャネル・セキュリティとして TLS を利用する場合、利用する端末にセッション間の回り込み等による攻撃を受ける可能性があるため、攻撃への防護対策について実施している場合は「はい」とし、備考へ詳細の記載を行ってください。

※SSL-VPN は利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれます。SSL-VPN を利用する場合は備考に適切であることの根拠、必要な対策があればその内容を記載してください。

### 「１２．３．２　ネットワークの経路制御・プロトコル制御に関わる機能の適正さ（回り込み対策を含む）を証明できる文書があるか？(企 15⑦、シ 13⑤、⑥)」

本項目は、外部との情報交換用のネットワーク機器に対し、安全管理ガイドラインの要求事項に適合していることを確認できる文書を添付しているかを確認するものです。例えば、ISO15408 で規定されるセキュリティターゲット、又はそれに類するセキュリティ対策が規定された文書のことを指します。

添付している場合は「はい」、していない場合は「いいえ」としてください。

### 「１２．４　リモートメンテナンス機能を有するか？」

本項目は、装置に対し保守事業者によるリモートメンテナンスサービスを提供しているかを確認するものです。提供している場合、従属質問にも回答してください。

機能を提供している場合は「該当」、機能を提供していない場合は「非該当」としてください。

### 「１２．４．１　リモートメンテナンスサービスに関し、不必要なリモートログインを制限する機能があるか？(シ 7⑫、シ 10.1、シ 18.1)」

本項目は、リモートメンテナンスサービスにおいて、利用者側がアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なリモートログインを防止する機能の有無を確認するものです。

有する場合は「はい」、有していない場合は「いいえ」としてください。

## 法令で定められた記名・押印を電子署名で行うことについて

### 「１３　記名・押印が義務付けられた文書を扱っているか？」

本項目は、当該ソフトウェアが記名・押印を義務付けられた文書の作成、参照、保存などを行っているかどうかを確認するものです。記名・押印を義務付けられた文書の例としては、診断書、紹介状、放射線照射録などが挙げられます。義務付けられた文書を取り扱っている場合は「該当」としてください。取り扱っていない場合は「非該当」としてください。「該当」の場合は、従属質問に回答してください。これらを電子的に作成する場合には電子署名法に適合する電子署名が必要です。また、電子署名、タイムスタンプが付された文書を参照する場合には、電子署名、タイムスタンプの検証が必要になる場合があります。さらに電子文書をタイムスタンプの有効期限（一般的には 10 年程度）を超えて長期保存する場合には、真正性の確保のための長期署名技術、又はそれに準ずる措置を行う必要があります。

### 「１３．１　HPKI 認証局、認定認証局、又は公的個人認証サービスが発行する証明書対応の署名機能があるか？(企 14①、シ 15①)」

本項目は、記名・押印を義務付けられた文書の署名機能の有無を確認するものです。安全管理ガイドラインにおいて HPKI 認証局、認定認証局、又は公的個人認証サービスが発行する証明書を用いることが求められており、電子署名を付与するために必須の機能です。署名機能を有する場合は「はい」、有していない場合は「いいえ」としてください。

「はい」の場合は備考に対応している証明書の種類（HPKI、認定認証局、公的個人認証サービス~~等~~）を記入してください。また、「いいえ」の場合は、電子署名を付与するための別の手段を提供する必要があり、備考に署名機能の提供方法を記載してください。記名・押印を義務付けられた文書の作成機能がない場合は「対象外」としてください。

### 「１３．２　HPKI 認証局、認定認証局、又は公的個人認証サービスが発行する証明書対応の検証機能があるか？(企 14①、シ 15①)」

本項目は、記名・押印を義務付けられた文書の検証機能の有無を確認するものです。安全管理ガイドラインにおいて HPKI 認証局、又は認定認証局もしくは公的個人認証サービスが発行する証明書の検証が求められており、電子署名付き文書を参照するために必須の機能です。署名検証機能を有する場合は「はい」としてください。有していない場合は「いいえ」としてください。

「はい」の場合は、対応している証明書を備考に記入してください。また、「いいえ」の場合は、電子署名を検証するための別の手段を提供する必要があり、備考に署名検証機能の提供方法を記載してください。記名・押印を義務付けられた文書の参照機能がない場合は「対象外」としてください。

### 「１３．３　総務省の「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が付与可能か？(企 14①、シ 15①)」

本項目は、タイムスタンプの付与が可能かを確認するものです。電子文書作成においては、電子署名を行った後、タイムスタンプを付与する必要があります。安全管理ガイドラインにおいてタイムスタンプは、総務省の「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ものを使用することが求められています。付与可能な場合は「はい」としてください。そうでない場合は「いいえ」としてください。

「はい」の場合は対応するタイムスタンプサービスを記入してください。また、「いいえ」の場合は、タイムスタンプを付与するための別の手段を提供する必要があり、備考にタイムスタンプの付与方法を記載してください。記名・押印を義務付けられた文書の作成機能がない場合は「対象外」としてください。

### 「１３．４　総務省の「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が検証可能か？(企 14①、シ 15①)」

本項目は、タイムスタンプの検証が可能かを確認するものです。電子文書作成においては、電子署名を行った後、タイムスタンプを付与する必要があります。参照時にはタイムスタンプの検証が必要になります。検証可能な場合は「はい」としてください。そうでない場合は「いいえ」としてください。

「はい」の場合は対応するタイムスタンプサービスを記入してください。また、「いいえ」の場合は、タイムスタンプを検証するための別の手段を提供する必要があり、備考にタイムスタンプの検証方法を記載してください。記名・押印を義務付けられた文書の参照機能がない場合は「対象外」としてください。

### 「１３．５　保存期間中の文書の真正性を担保する仕組みがあるか？(企 14①、シ 15①)」

本項目は記名・押印を義務付けられた文書の保存機能を確認するものです。法定保存期間が 10 年を超えるものや、法定保存期間を越えて 10 年以上保存するものについてはタイムスタンプ単独では真正性を確保できません。タイムスタンプの有効期限を越えた際に長期保存するための ISO 規格である CAdES、XAdES、PAdES などの機能、又はそれと同等の真正性を確保する機能があるかどうかの確認を行います。仕組みを有する場合は「はい」としてください。そうでない場合は「いいえ」としてください。

「はい」の場合は備考に具体的な実現方式を記載してください。「いいえ」の場合は、真正性を確保するための別の手段を提供する必要があり、備考に真正性確保手段を記載してください。記名・押印を義務付けられた文書の保存機能がない場合は「対象外」としてください。

## 真正性の確保について

### 「１４　入力者及び確定者を正しく識別し、認証を行う機能があるか？(企 15⑬、シ 14⑧)」

本項目は、人による確定操作が必要な場合（電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合）を対象としています。そうでない場合（臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合）は「対象外」としてください。入力者及び確定者を識別し、認証する機能を有して入れば「はい」、有していなければ「いいえ」としてください。

「はい」ならば、従属質問に回答してください。

### 「１４．１　区分管理を行っている対象情報ごとに、権限管理（アクセスコントロール）の機能があるか？(企 15⑬、シ 14④)」

真正性を担保するためには、故意または過失による追記、修正および削除ならびに混同を防止することが必要です。そのために、本項目は、操作者の権限に応じてアクセスできる情報を区分単位で制限する機能の有無を確認するものです。

アクセス者の権限に基づき各区分において操作内容に制限を加えることが可能ならば「はい」、そうでない場合

は「いいえ」としてください。システムにより記録が作成される場合など本機能が不要な場合は「対象外」とし、理由を備考に記載してください。

### 「１４．２　権限のある利用者以外による作成、追記、変更を防止する機能があるか？(企 15⑬)」

本項目は、一般利用者に対して権限管理の機能の有無を確認するものです。
権限管理の機能を有していれば「はい」としてください。有していない場合は「いいえ」としてください。システムにより記録が作成される場合など本機能が不要な場合は「対象外」とし、理由を備考に記載してください。

### 「１５　システムが端末を管理することによって、権限を持たない者からのアクセスを防止する機能があるか？(企 15⑬)」

本項目は、システムとして利用者を認証する機能がない場合等に、業務アプリケーション等がアクセスできる端末を制限する機能を有するかを確認するものです。
システムが端末を管理する機能を有する場合は「はい」、そうでない場合は「いいえ」としてください。利用者を認証する機能があるなど本機能が不要ならば「対象外」とし、理由を備考に記載してください。

### 「１６　システムは記録を確定する機能があるか？(企 15⑬、シ 14⑧)」

本項目は、確定機能の有無を確認するものです。
安全管理ガイドラインで求められている記録の確定機能を有している場合は「はい」、有していない場合は「いいえ」としてください。確定が必要な情報を管理していない場合は、「対象外」を選択してください。「はい」ならば、従属質問に回答してください。

### 「１６．１　確定情報には、入力者及び確定者の識別情報、信頼できる時刻源を用いた作成日時が含まれているか？(企 15⑬、シ 14⑧)」

本項目は、記録の確定の必須要件である、記録が・いつ・誰によって作成されたかを明確にするための機能の有無を確認するものです。
入力者及び確定者の識別情報と信頼できる時刻源に基づく作成日時が記録される場合は「はい」としてください。そうでない場合（例えば運用で管理し「メモ」で記録するなどの場合）は「いいえ」としてください。

### 「１６．２　「記録の確定」を行うにあたり、内容の確認をする機能があるか？(企 15⑬、シ 14⑧)」

本項目は、記録の確定の際には確定者による内容の確認が必須要件であるため、その機能を有するかを確認するものです。
記録を確定するにあたり、内容を確認する機能を有している場合は「はい」、そうでない場合は「いいえ」としてください。

### 「１６．３　確定された記録に対して、故意による虚偽入力、書換え、消去及び混同を防止する機能があるか？(企 15⑬、シ 14⑧)」

真正性の確保のためには、確定後のデータに対し、正当な権限に基づかないいかなる追記、修正および削除も行われていないことを保証しなければなりません。本項目は、そのための機能の有無を確認するものです。
確定後のデータに対して権限者以外の追記、修正および削除ができないようになっている場合は「はい」、そうでない場合は「いいえ」としてください。

### 「１７　装置が確定機能を持っていない場合、記録が作成される際に、当該装置の管理責任者や操作者の識別情報、作成日時を含めて記録する機能があるか？(企 15⑬、シ 14⑧)」

本項目は、臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合に関する質問です。運用でそれを実現しようとする際に、装置が記録自体に作成責任者の識別情報や作成日時を含めて記録する機能の有無を確認するものです。

装置からのデータに識別情報（作成責任者の氏名あるいは識別情報）、作成日時が含まれ記録される場合は「はい」としてください。記録されない場合は「いいえ」としてください。

### 「１８　確定された診療録等が更新された場合、更新履歴を保存し、更新前後の内容を参照する機能があるか？(企 15⑬、シ 14⑧)」

確定済みの診療録等に追記や修正などの更新が行われた場合、それが正当な行為なのか、不正な行為なのかを判別するために、記録の更新内容、更新日時、更新者の識別情報が関連付けて保存され、必要な時に参照できなければなりません。本項目は、そのための機能の有無を確認するものです。

確定情報への更新内容、更新日時を記録するとともに、更新前と更新後の内容を参照する機能を有している場合は「はい」、有していない場合は「いいえ」、対象機器が本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

### 「１８．１　同じ診療録等に対して更新が複数回行われた場合、更新の順序性を識別できる機能があるか？(企 15⑬、シ 14⑧)」

同じ診療録等に対して複数回更新が行われた場合、それぞれの更新がどの順序で行われたかが重要になる場合があり、そのため更新の順序性を識別できるようにする機能が求められます。例えば更新時刻を分単位で記録している場合でも、同じ時刻の更新記録の順序が分かるようにしなければなりません。

更新の順序を識別できる機能を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

### 「１９　代行入力の承認機能があるか？(企 13⑧、企 15⑬、シ 14⑧)」

情報入力は診療行為の実施者自らが行うことが原則ですが、代行者による入力が必要になる場合があります。本項目は、そのような代行入力において、作成責任者による代行入力の実施に関する承認機能（確定時の承認とは別）を有するかを確認するものです。対象システムの権限としてあらかじめ代行権限が付与されているものも承認の中に含みます。

承認機能を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。「はい」ならば、従属質問に回答してください。

### 「１９．１　代行入力が行われた場合、誰の代行がいつ誰によって行われたかの管理情報を、その代行入力の都度、記録する機能があるか？(企 15⑬、シ 14⑧)」

代行入力での運用が行われる場合、例えば医師の入力の代行を医師事務作業補助者が行う場合に、誰の代行がいつ誰によって行われたかを記録することが必要です。本項目は、そのような管理情報を、その代行操作の都度記録する機能の有無を確認するものです。

機能を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

### 「１９．２　代行入力により記録された診療録等に対し、確定者による「確定操作（承認）」を行う機能があるか？(企 15⑬、シ 14⑧)」

代行入力での運用が行われる場合、代行入力によって入力された診療録等の情報を、できるだけ速やかに作成責

任者による「確定操作（承認）」が行われることが必要です。本項目は、そのような「確定操作（承認）」機能の有無を確認するものです。

機能を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

## 見読性の確保について

### 「２０　目的に応じて速やかに検索結果を出力する機能があるか？(企 15⑬、シ 9④)」

見読性とは、保存された情報を目的に対して支障のないレスポンスやスループットと操作性で、肉眼で見読可能な状態にできることです。本項目は、見読性の確保を確認するためのものです。『速やかに』とは、権限保有者からの「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応じて、それぞれの目的に対し支障のないレスポンスやスループット、操作方法で提供できることを示します。

機能を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

### 「２１　システム障害に備えた冗長化手段や代替的な見読化手段はあるか？(企 15⑬、シ 11①、 シ 11.1)」

本項目は、見読化手段の耐障害性を向上させるための冗長構成又は代替手段の有無を確認するものです。

システム障害に備えた冗長化手段や代替的な見読化手段を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。

### 「２１．１　冗長化手段があるか？(企 11.2、企 15⑬、シ 11.1)」

本項目は、冗長化の具体的な内容について確認するものです。サーバ又はディスク、ネットワークI/F、回線などにおいて冗長化手段を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。「はい」の場合は、具体的な内容を備考に記載してください。

### 「２１．２　システム障害に備えた代替的な見読化手段があるか？(企 15⑬、シ 11①)」

本項目は、代替的な見読化手段の具体的な内容について確認するものです。代替的な見読化手段には、①一般的な記録形式（例えばPDF、XML、JPEGなどのファイルフォーマット）で記録しておくことによって、標準的な見読化装置で見読可能とする方法と、②別の専用の代替的な見読化手段を用意する方法があります。いずれかの方法を有している場合は「はい」、有していない場合は「いいえ」としてください。代替的な手段の具体的な内容を備考に記載してください。

## 保存性の確保について

### 「２２　不正ソフトウェアによる情報の破壊、混同等が起こらないようにするための防護機能があるか？(経 3.4、企 15⑥、⑬、シ 7④、シ 8③、シ 8.1)」

本項目は、保存性を確保するために、不正ソフトウェアによる情報の破壊、混同等を防ぐための機能の有無を確認するものです。

機能を有している場合は「はい」、有していない場合は「いいえ」としてください。

### 「２３　記録媒体及び記録機器の保管及び取扱いについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？(企 15③、④)」

保存性の確保のために、医療機関等には、記録媒体及び記録機器の保管及び取扱いについての運用管理規程の作

成と、関係者への教育が求められます。本項目は、その運用管理規程作成のために、機器における記録媒体や記録機器の保管や取り扱い（例えば、記録媒体の品質保証期間、保存場所の推奨環境等）について、取扱説明書等の文書として提供されているかを確認するものです。

提供されている場合は「はい」、そうでない場合は「いいえ」、対象となる製品が記憶媒体や記録機器を有さない場合は「対象外」としてください。

### 「２４　情報の保存やバックアップについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？(企 15④、企 15.1)」

保存性の確保のために、医療機関等には、情報を保存する場所や、その場所ごとの保存可能容量、期間、リスク、レスポンス、バックアップ頻度、バックアップ方法等を運用管理規程にまとめ、関係者に周知することが求められます。本項目は、その運用管理規程作成のために、機器における情報の保存方式やバックアップ手順について、取扱説明書等の文書として提供されているかを確認するものです。

提供されている場合は「はい」、そうでない場合は「いいえ」、対象となる製品が記憶媒体や記録機器を有していない場合は「対象外」としてください。

### 「２５　システムが保存する情報へのアクセスについて、履歴を残す機能があるか？(経 4.2、企５①、④、シ 17①)」

本項目は、保存性確保のために機器に求められる、情報に対するアクセス履歴を保存する機能の有無を確認するものです。ここでのアクセス履歴とは、医療情報システムの動作に関するアプリケーションログだけではなく、保存された情報に対する通常の操作以外でのアクセス（例：データベースへの直接ブラウズ等）にも対応するものです。

そのような機能を有している場合は「はい」、有していない場合は「いいえ」、対象となる製品が情報を保持しない場合は「対象外」としてください。「はい」ならば、従属質問に回答してください。

### 「２５．１　システムが保存する情報へのアクセスについてその履歴を管理するための機能があるか？(経 4.2、企 5②、シ 17①)」

本項目は、アクセス履歴を管理するための機能（例えば、アクセスログの表示、時系列表示、フィルタ機能、検索機能等）の有無を確認するものです。

そのような機能を有している場合は「はい」、有していない場合は「いいえ」、対象となる製品が情報を保持しない場合は「対象外」としてください。

### 「２６　システムが保存する情報がき損した時に、バックアップされたデータを用いて、き損前の状態に戻すための機能があるか？(経 3.4.1、シ 11①、シ 18①、シ 18.1)」

本項目は、システムが保存する情報がき損した場合に、事前に作成したバックアップデータを用いるなどして、き損前の状態に回復させる機能の有無を確認するものです。もし、戻せない場合は損なわれた範囲が容易に分かるようにする必要があります。

このような機能を有している場合は「はい」、有していない場合は「いいえ」、対象となる製品が情報を保存しない場合は「対象外」としてください。

き損前と同一状態に戻せても、バックアップからの復元であることが判ることが望ましいです。

### 「２７　記録媒体が劣化する前に情報を新たな記録媒体又は、記録機器に複写する機能があるか？(企 15⑤、シ 12⑤、シ 12.2)」

本項目は、バックアップを含む記録媒体について、記録媒体の劣化による情報の読み取り不能や不完全な読み取りを防止するために、記録媒体が劣化する前に記録されている情報を他の媒体に複写する機能の有無を確認する

ものです。
機能を有している場合は「はい」、有していない場合は「いいえ」、対象となる製品が情報を保存しない場合は「対象外」としてください。

### 「２８　システムの移行の際に診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能があるか？(企15⑬、シ5①)」

標準形式とは「厚生労働省標準規格」を始めとする業界標準や国際標準等で定められた形式のことです。変換が容易なデータ形式とはCSV、XML等のような、特定のアプリケーションに依存しないデータ形式のことです。本項目は、システム更新時の移行が迅速に行えるように、上記のようなデータ形式で診療録等のデータを出力及び入力できる機能の有無を確認するものです。
機能を有している場合は「はい」、有していない場合は「いいえ」、対象となるシステムが情報を保存しない場合は「対象外」としてください。

### 「２９　マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えているか？(企15⑬、シ5②)」

本項目は、過去の記録については当時のマスタを参照して表示するなど、機能で対応できるかを問うています。
マスタデータベースの変更の際に、過去の診療記録等の情報に対する内容の変更が起こらないような機能を有している場合は「はい」、有していない場合は「いいえ」、対象となるシステムが情報を保存しない場合は「対象外」としてください。

## 診療録等をスキャナ等により電子化して保存する場合について

### 「３０　診療録などをスキャナなどにより電子化して原本として保存する機能があるか？」

スキャナなどによる電子化により法令等で作成又は保存を義務付けられている診療録等の情報を原本として電子保存する機能を有している場合は「該当」、機能を有していない場合は「非該当」としてください。「該当」ならば、従属質問にも回答してください。

### 「３０．１　光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いているか？(企16①、シ16①)」

スキャナ等による電子化においては、医療に関する業務等に支障が生じないように、スキャンによる情報量低下を防ぎ、保存義務を満たす情報として必要な情報量を確保することが求められます。本項目は、安全管理ガイドラインに例示されているユースケース毎に個別に定められた規格・基準を満たす形でスキャナを使用しているかを確認するものです。
使用している場合は「はい」、そうでない場合は「いいえ」、製造業者から医療機関等にスキャナを提供しない場合は「対象外」としてください。どのユースケースに適合するシステムかを備考に記載してください。

### 「３０．２　電子署名を行える機能があるか？(経4.1、企16③、⑦、シ1①、シ15①)」

本項目は、改ざん防止のために、スキャンした電子情報に対して安全管理ガイドラインに適合する電子署名を行う機能の有無を確認するものです。
機能を有している場合は「はい」、有していない場合は「いいえ」としてください。オプションではない他のシステムと組み合わせて機能を実現する場合は「対象外」とし、その実現方式を備考に記載してください。

### 「３１　診療録などをスキャナなどにより電子化して参照情報として保存する機能があるか？」

スキャナなどによる電子化により法令等で作成又は保存を義務付けられている診療録等の情報を参照情報として電子保存する機能を有している場合は「該当」、有していない場合は「非該当」としてください。「該当」ならば、従属質問にも回答してください。

### 「３１．１　光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いているか？(企 16①、⑧、シ 16①)」

スキャナ等による電子化においては、医療に関する業務等に支障が生じないように、スキャンによる情報量低下を防ぎ、保存義務を満たす情報として必要な情報量を確保することが求められます。本項目は、安全管理ガイドラインに例示されているユースケース毎に個別に定められた規格・基準を満たす形でスキャナを使用しているかを確認するものです。

使用している場合は「はい」、そうでない場合は「いいえ」、製造業者から医療機関等にスキャナを提供しない場合は「対象外」としてください。どのユースケースに適合するシステムかを備考に記載してください。

# 8. チェックリスト（サービス事業者編）

## 「サービス事業者による医療情報セキュリティ開示書」チェックリスト

（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 版対応）

| | |
|---|---|
| サービス事業者　： | 作成日　： |
| サービス名称　： | バージョン　： |
| | |
| **診療録及び診療諸記録等の医療情報の取扱いを受託する際の基準** | |
| 1　診療録及び診療諸記録等の外部保存を受託するか？ | 該当　非該当　　備考____ |
| 1．1　保存場所が「病院、診療所、医療法人等が適切に管理する場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？(経 5、企 7③、④、⑤、⑥、⑦、⑧、⑨) | はい　いいえ　対象外　備考____ |
| 1．2　保存場所が「医療機関等が外部の事業者との契約に基づいて確保した安全な場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？(経 5、企 7③、④、⑤、⑥、⑦、⑧、⑨) | はい　いいえ　対象外　備考____ |
| **医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践** | |
| 2　扱う情報のリストを医療機関等に提示できるか？(概 4.5、経 2.2. 企 6②、③) | はい　いいえ　対象外　備考____ |
| **組織的安全管理対策（体制、運用管理規程）** | |
| 3　医療情報システムを運用する際に、医療情報システムの企画管理者を設置しているか？(経 3.1.2、企 3①、③) | はい　いいえ　対象外　備考____ |
| 4　医療情報システムを運用する際に、技術担当者を指定しているか？(経 3.1.2、企 3①、③) | はい　いいえ　対象外　備考____ |
| 5　個人情報が参照可能な場所に対しては、入退管理のルールを定めているか？(経 3.2、企 8③、企 15②) | はい　いいえ　対象外　備考____ |
| 6　情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成しているか？(概 4.4、経 3.2、企 13①) | はい　いいえ　対象外　備考____ |
| 7　医療機関等との契約に安全管理に関する条項を含めているか？(概 4.4、経 3.2、企 7④、⑤、⑦、⑧、⑨) | はい　いいえ　対象外　備考____ |
| 8　個人情報を含む医療情報システムの業務をサービス事業者が外部委託する場合、その外部委託先との契約に再委託先を含めた安全管理に関する条項を含めているか？(概 4.4、経 5.2.2、企 1②) | はい　いいえ　対象外　備考____ |
| 9　運用管理規程等において組織的安全管理対策に関する事項等を定めているか？(概 4.4、経 3.1、経 3.2、企 4) | はい　いいえ　対象外　備考____ |
| **物理的安全対策** | |
| 10　個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠しているか？(企 8③、シ 12.1) | はい　いいえ　対象外　備考____ |
| 11　個人情報を入力・参照できる端末が設置されている区画は、許可されたもの以外立ち入ることができないように対策されているか？(企 15②) | はい　いいえ　対象外　備考____ |
| 12　個人情報が保存されている機器が設置されている区画への入退管理を実施しているか？(企 15②) | はい　いいえ　対象外　備考____ |
| 12．1　入退出の事実を記録しているか？(企 15②) | はい　いいえ　対象外　備考____ |
| 12．2　入退者の記録を定期的にチェックし、妥当性を確認しているか？(企 15②) | はい　いいえ　対象外　備考____ |
| 13　個人情報が保存されている機器等の重要な機器に盗難防止策を講じているか？(企 8③、シ 12③) | はい　いいえ　対象外　備考____ |

| | |
|---|---|
| １４　個人情報が入力･参照できる端末に覗き見防止の機能があるか？(シ12⑥､シ12.3.2) | はい　いいえ　対象外　備考____ |
| １５　サービス事業者の管理端末に覗き見防止対策が取られているか？(シ 12⑥、シ12.3.2) | はい　いいえ　対象外　備考____ |
| **技術的安全対策** | |
| １６　権限を持たない者による不正入力を防止する対策が行われているか？(シ12⑥) | はい　いいえ　対象外　備考____ |
| １７　アクセス管理の機能があるか？(シ14①) | はい　いいえ　対象外　備考____ |
| １７．１　利用者の認証方式は？(シ14⑤)<br>・記憶（ID・パスワード等）<br>・生体認証（指紋等）<br>・物理媒体（IC カード等）<br>・上記のうちの二要素を組み合わせた認証<br>（具体的な組み合わせを備考に記入してください）<br>・その他（具体的な方法を備考に記入してください） | <br>はい　いいえ　対象外　備考____<br>はい　いいえ　対象外　備考____<br>はい　いいえ　対象外　備考____<br>はい　いいえ　対象外　備考____<br><br>はい　いいえ　対象外　備考____ |
| １７．１．１　パスワードを利用者認証手段として利用しているか？ | はい　いいえ　対象外　備考____ |
| １７．１．１．１　他の手段と併用した際のパスワードの運用方法を運用管理規程に定めているか？(シ14②) | はい　いいえ　対象外　備考____ |
| １７．１．１．２　本人確認の実施の際、本人確認方法を台帳に記載しているか？(シ 14⑥) | はい　いいえ　対象外　備考____ |
| １７．１．１．３　パスワードの有効期限が管理できるか？(シ14⑥) | はい　いいえ　対象外　備考____ |
| １７．１．１．４　文字列制限をチェックすることができるか？(シ14⑥) | はい　いいえ　対象外　備考____ |
| １７．１．１．５　類推しやすいパスワードをチェックすることができるか？(シ14⑥) | はい　いいえ　対象外　備考____ |
| １７．１．１．６　パスワード変更の際に類似性のチェックをすることができるか？(シ14⑥) | はい　いいえ　対象外　備考____ |
| １７．１．１．７　ID とパスワードの組み合わせが本人しか知りえないよう保たれているか？(シ14②、⑥) | はい　いいえ　対象外　備考____ |
| １７．１．２　運用管理規程にセキュリティ・デバイスの代替手段が規定されているか？(シ14③) | はい　いいえ　対象外　備考____ |
| １７．２　利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？(経4.2、シ14.2) | はい　いいえ　対象外　備考____ |
| １７．３　アクセス記録（アクセスログ）機能があるか？(企5③、シ17①) | はい　いいえ　対象外　備考____ |
| １７．３．１　アクセスログを利用者が確認する機能があるか？(経4.2、企5①、③) | はい　いいえ　対象外　備考____ |
| １７．３．２　アクセスログへのアクセス制限ができるか？(企5②、シ17②) | はい　いいえ　対象外　備考____ |
| １７．３．３　アクセスログへのアクセス制限機能がない場合、不当な削除/改ざん/追加等を防止する運用的対策を講じているか？(企5②、シ17②) | はい　いいえ　対象外　備考____ |
| １７．４　アクセス記録（アクセスログ）機能が無い場合、利用者が監査できる形でサービス事業者が業務日誌等に操作の記録を行っているか？(企5①、シ17①) | はい　いいえ　対象外　備考____ |
| １８　時刻情報の正確性を担保する仕組みがあるか？(シ17③) | はい　いいえ　対象外　備考____ |
| １９　不正なソフトウェアが混入していないか確認しているか？(企15⑥、シ8①、②) | はい　いいえ　対象外　備考____ |
| ２０　システムにメールの送受信機能がある場合、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理等が行われているか？(シ8④) | はい　いいえ　対象外　備考____ |
| ２１　システムでファイル交換機能を使用する場合、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理等が行われているか？(シ8④) | はい　いいえ　対象外　備考____ |
| ２２　無線 LAN を利用する場合のセキュリティ対策機能はあるか？(シ13⑬) | はい　いいえ　対象外　備考____ |

| | |
|---|---|
| ２３　IoT 機器を使用するか? | 該当　非該当　　備考____ |
| ２３．１　IoT 機器を使用する場合、IoT 機器により患者情報を取り扱うことに関する運用管理規程を定めた上で、医療機関等に開示できるか?(シ 8⑥) | はい　いいえ　対象外　備考____ |
| ２３．２　ウェアラブル端末や在宅設置の IoT 機器を利用する場合、患者のリスク等に関する説明資料を提供できるか?(シ 7⑧) | はい　いいえ　対象外　備考____ |
| ２３．３　IoT 機器のセキュリティアップデートを必要なタイミングで適切に実施できるか?(シ 8⑥) | はい　いいえ　対象外　備考____ |
| ２３．４　使用が終了または停止した IoT 機器の接続を遮断できるか?(シ 8⑥) | はい　いいえ　対象外　備考____ |
| **人的安全対策** | |
| ２４　従業者との間で、雇用時または契約時に守秘義務契約を結んでいるか?(経 3.1.2、企 7①) | はい　いいえ　対象外　備考____ |
| ２５　従業者に対し、定期的に個人情報管理に関する教育訓練を行っているか?(経 3.2.2①、企 7②) | はい　いいえ　対象外　備考____ |
| ２６　従業者の退職後または契約終了後における個人情報保護に関する規程が従業者との契約に含まれているか?(企 7①) | はい　いいえ　対象外　備考____ |
| ２７　就業規則等には守秘義務違反に対する包括的な罰則規定が含まれているか?(企 7.1) | はい　いいえ　対象外　備考____ |
| ２８　保守作業等で医療情報システムに直接アクセスする作業を行う際には、作業者・作業内容・作業結果を医療機関等に報告できるようになっているか?(シ 10①、③、④) | はい　いいえ　対象外　備考____ |
| ２９　清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行っているか?(企 1②) | はい　いいえ　対象外　備考____ |
| ３０　業務の一部を外部委託する場合に、外部委託先に対し、自らに課しているのと同等の個人情報保護に関する対策を施す義務を、契約によって担保しているか?（企 1②、企 7③、④) | はい　いいえ　対象外　備考____ |
| ３１　やむを得ない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行っているか?(企 1②、企 7③、④) | はい　いいえ　対象外　備考____ |
| **情報の破棄** | |
| ３２　ユーザに提示できる情報種別ごとの破棄の手順があるか?(企 8①、シ 7⑨) | はい　いいえ　対象外　備考____ |
| ３２．１　手順には破棄を行う条件を含めているか?(企 8⑪、シ 7⑨) | はい　いいえ　対象外　備考____ |
| ３２．２　手順には破棄を行うことができる従業者の特定を含めているか?(企 8⑪、シ 7⑨) | はい　いいえ　対象外　備考____ |
| ３２．３　手順には破棄の具体的な方法を含めているか?(企 8⑪、シ 7⑨) | はい　いいえ　対象外　備考____ |
| ３３　情報処理機器自体を破棄する場合、必ず専門的な知識を有する者が行うこととし、残存し、読み出し可能な情報がないことを報告できるか?(シ 7⑨、⑩) | はい　　いえ　対象外　備考____ |
| ３４　破棄を外部委託した場合、外部委託業者の監督及び守秘義務契約に準じた監督責任の下、情報の破棄を確認しているか?(企 8⑫、シ 7⑪) | はい　いいえ　対象外　備考____ |
| ３５　不要になった個人情報を含む媒体の破棄を、運用管理規程に定めているか?(企 8①、⑪) | はい　いいえ　対象外　備考____ |
| **医療情報システムの改造と保守** | |
| ３６　改造や保守に関する動作確認で個人情報を含むデータを使用する場合、作業員と守秘義務契約を交わしているか?(企 7①、③、④) | はい　いいえ　対象外　備考____ |
| ３７　作業員はサービス事業者自身が定めた運用管理規程に従い、改造や保守に関する業務を行っているか?(企 8①、⑫、シ 7①、⑨) | はい　いいえ　対象外　備考____ |
| ３８　運用管理規程には作業終了後に動作確認で使用した個人情報を含むデータを消去することに関する規定が含まれているか?(企 15⑨、シ 10①) | はい　いいえ　対象外　備考____ |

| | |
|---|---|
| ３９　改造や保守に用いるアカウントは、作業員個人の専用アカウントを使用しているか?(シ10③) | はい　いいえ　対象外　備考____ |
| ４０　改造や保守に関する作業の記録として、個人情報へのアクセス有無、及びアクセスした対象を特定できる情報を医療機関等に提供できるか?(シ10③) | はい　いいえ　対象外　備考____ |
| ４１　作業員のアカウントにおけるアクセス権限とアクセス状況を管理しているか?(企13⑤、シ10③、④) | はい　いいえ　対象外　備考____ |
| ４２　作業員の離職や担当替え等に対して速やかに保守用アカウントを削除しているか?(企13⑤、⑦) | はい　いいえ　対象外　備考____ |
| ４３　改造や保守を外部委託している場合、保守要員の離職や担当替え等の際に報告を義務付けているか?(企13⑤、⑦) | はい　いいえ　対象外　備考____ |
| ４３．１　報告に応じてアカウントを削除する管理体制ができているか?(企13⑤、⑦) | はい　いいえ　対象外　備考____ |
| ４４　メンテナンスを実施する場合は、事前に医療機関等に作業申請を提出できるか?(シ10.1) | はい　いいえ　対象外　備考____ |
| ４５　メンテナンス終了時に、速やかに医療機関等に作業報告書を提出できるか?(シ10.1) | はい　いいえ　対象外　備考____ |
| ４６　保守を外部委託する場合、保守事業者と守秘義務契約を締結しているか?(企7③、④) | はい　いいえ　対象外　備考____ |
| ４７　システムの改造や保守で個人情報を含むデータを組織外に持ち出す際に、医療機関等の責任者の承認を得ることが運用管理規程に定められているか?(企8①、⑤、シ7①、②) | はい　いいえ　対象外　備考____ |
| ４８　リモートメンテナンスによる改造・保守を行う場合は、アクセスログを収集するか?(シ10④) | はい　いいえ　対象外　備考____ |
| ４９　リモートメンテナンスにおいて、医療機関等へ送付等を行うファイルは、送信側で無害化処理が行われているか?(シ10⑤) | はい　いいえ　対象外　備考____ |
| ５０　保守業務を外部委託している場合、外部委託事業者にも自らと同等な義務を求め、契約しているか?(企1②) | はい　いいえ　対象外　備考____ |
| **情報及び情報機器の持ち出し並びに外部利用について** | |
| ５１　持出機器を提供しているか? | 該当　非該当　備考____ |
| ５１．１　持出機器においてソフトウェアのインストールを制限する機能があるか?(企8⑤、シ7⑥) | はい　いいえ　対象外　備考____ |
| ５１．２　持出機器において外部入出力装置の機能を無効にすることができるか?(企8⑤、シ7⑥) | はい　いいえ　対象外　備考____ |
| ５１．３　外へ持ち出す際、情報に対して暗号化等の対策を行うことができるか?(シ7③) | はい　いいえ　対象外　備考____ |
| ５１．４　持ち出した情報機器を外部のネットワークや他の外部媒体に接続する場合、情報漏えいや改ざんの対策を実施しているか?(シ7④) | はい　いいえ　対象外　備考____ |
| ５２　提供するサービスに係わる情報及び情報機器の持ち出しについて、リスク分析を実施しているか?(企9.2、シ7.1) | はい　いいえ　対象外　備考____ |
| ５３　サービス事業者が情報及び情報機器を持出する場合があるか? | 該当　非該当　備考____ |
| ５３．１　リスク分析の結果を受けて、情報及び情報機器の持ち出しに関する方針を運用管理規程に定めているか?(企8①、⑤、⑦、⑧、⑪、⑫、シ7①、⑦、⑨、⑮) | はい　いいえ　対象外　備考____ |
| ５３．２　持ち出した情報及び情報機器の管理方法を定めているか?(企8⑤) | はい　いいえ　対象外　備考____ |
| ５３．３　情報を格納した媒体及び情報機器の盗難、紛失時の適切な対応を自社方針・規則等に定めているか?(企8⑦、シ7⑮) | はい　いいえ　対象外　備考____ |
| ５３．４　自社方針・規則等で定めた盗難、紛失時の対応を従業員等に対して周知徹底し、教育を行っているか?(企7②、企7.1) | はい　いいえ　対象外　備考____ |
| ５３．５　情報機器について、起動パスワード等を設定しているか?(シ7③、シ8⑤) | はい　いいえ　対象外　備考____ |

| | |
|---|---|
| ５３．６　パスワード設定においては、適切なパスワード管理措置を行っているか？(企 13②、シ 8⑤) | はい　いいえ　対象外　備考____ |
| ５３．７　サービス事業者が外へ持ち出す際、情報に対して暗号化等の対策を行っているか？(シ 7③) | はい　いいえ　対象外　備考____ |
| ５３．８　医療機関等または医療機関等に委託されたサービス事業者が、持ち出した情報機器を外部のネットワークや他の外部媒体に接続する場合、情報漏えいや改ざんの対策を実施しているか？(企 8⑤、⑥、シ 7④、⑤、⑥) | はい　いいえ　対象外　備考____ |
| ５４　情報の管理者は情報機器・媒体の所在について台帳を用いる等して管理しているか？(企 9①、②、③、シ 7⑦) | はい　いいえ　対象外　備考____ |
| ５５　個人保有の情報機器の利用を禁止しているか？(企 9⑥、シ 8.5) | はい　いいえ　対象外　備考____ |
| **災害、サイバー攻撃等の非常時の対応** | |
| ５６　医療機関等に提供可能なサービス事業者の BCP 手順書が用意されているか？(経 3.4.1、企 11) | はい　いいえ　対象外　備考____ |
| ５７　非常時アカウント又は、非常時にも医療サービスを継続して提供できる機能を持っているか？（企 11、シ 11①) | はい　いいえ　対象外　備考____ |
| ５７．１　「非常時のユーザアカウントや非常時用機能」の管理手順を提供できるか？(企 11①、④、⑤、⑥、シ 11①) | はい　いいえ　対象外　備考____ |
| ５７．２　非常時機能を有している場合、非常時機能が定常時に不適切に利用されることがないよう適切に管理及び監査できる情報を提供できるか？(シ 11①) | はい　いいえ　対象外　備考____ |
| ５７．３　非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更できるか？(シ 11①) | はい　いいえ　対象外　備考____ |
| ５７．４　標的型メール攻撃等により医療情報システムに不正ソフトウェアが混入した場合、関係先への連絡手段を準備しているか？(企 11④、⑤、⑨、企 12⑦、シ 11①) | はい　いいえ　対象外　備考____ |
| ５８　重要なファイルをバックアップしているか？(経 3.4.1、企 7⑥、企 11④、⑤、シ 11①、シ 12.2) | はい　いいえ　対象外　備考____ |
| ５８．１　バックアップは数世代、複数の方式で実施しているか？(企 11④、⑤、シ 11①、シ 12.2、シ 18①) | はい　いいえ　対象外　備考____ |
| ５８．２　数世代、複数方式のバックアップの一部は不正ソフトウェアの混入による影響が波及しないように管理されているか？(企 11④、⑤、シ 11①、シ 12.2、シ 18①) | はい　いいえ　対象外　備考____ |
| ５８．３　バックアップからの復元手段が整備されているか？(企 11④、⑤、シ 11①、シ 12.2) | はい　いいえ　対象外　備考____ |
| **外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理** | |
| ５９～６３の質問は、提供するサービスで利用している通信方式について確認するものです。通信方式によって対策すべき項目が異なりますので、対応している通信方式それぞれに対して確認が必要です。対応する通信方式に「該当」とし、対応していない通信方式を「非該当」としてください。 | |
| ５９　通信方式として専用線に対応しているか？ | 該当　非該当　　備考____ |
| ５９．１　提供事業者に閉域性の範囲を確認しているか？(シ 13⑨) | はい　いいえ　対象外　備考____ |
| ５９．２　採用する認証手段が定められているか？(企 15⑦、シ 13④) | はい　いいえ　対象外　備考____ |
| ６０　通信方式として公衆網に対応しているか？ | 該当　非該当　　備考____ |
| ６０．１　提供事業者に閉域性の範囲を確認しているか？(シ 13⑨) | はい　いいえ　対象外　備考____ |
| ６０．２　採用する認証手段が定められているか？(企 15⑦、シ 13④) | はい　いいえ　対象外　備考____ |
| ６１　通信方式として IP-VPN に対応しているか？ | 該当　非該当　　備考____ |
| ６１．１　提供事業者に閉域性の範囲を確認しているか？(シ 13⑨) | はい　いいえ　対象外　備考____ |
| ６１．２　採用する認証手段が定められているか？(企 15⑦、シ 13④) | はい　いいえ　対象外　備考____ |

| | |
|---|---|
| ６２　通信方式としてIPsec-VPN ＋IKEに対応しているか? | 該当　非該当　　備考____ |
| ６２．１　セッション間の回り込み等の攻撃への適切な対策をしているか?(企 15⑦、シ 13⑥) | はい　いいえ　対象外　備考____ |
| ６２．２　採用する認証手段が定められているか?(企 15⑦、シ 13④) | はい　いいえ　対象外　備考____ |
| ６３　チャネル・セキュリティとして TLS1.2 以上のクライアント認証に対応しているか? | 該当　非該当　　備考____ |
| ６３．１　サーバ/クライアントともに「TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行っているか?(企 15⑦、シ 13⑥) | はい　いいえ　対象外　備考____ |
| ６３．２　セッション間の回り込み等による攻撃への適切な対策を実施しているか?(企 15⑦、シ 13⑥) | はい　いいえ　対象外　備考____ |
| ６４　ネットワーク上において、改ざん及び中間者攻撃等を防止する対策を行っているか?(シ 13⑨) | はい　いいえ　対象外　備考____ |
| ６５　施設間の経路上において、盗聴を防止する対策を行っているか?(シ 13⑩) | はい　いいえ　対象外　備考____ |
| ６６　ネットワーク上において、なりすましへの対策を行っているか?(シ 13②、⑪) | はい　いいえ　対象外　備考____ |
| ６７　データ送信元と送信先において、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行っているか?(シ 13④) | はい　いいえ　対象外　備考____ |
| ６８　ネットワークの経路制御･プロトコル制御を行える機器または機能を有するか?(シ 13⑤) | はい　いいえ　対象外　備考____ |
| ６９　ネットワークの経路制御・プロトコル制御に関わる機器または機能は、安全性を確認できるようなセキュリティ対策が規定された文書を示すことができるか?(企 15⑦、シ 13⑤) | はい　いいえ　対象外　備考____ |
| ７０　医療機関等との通信経路について回り込みが行われないように経路設定を行っているか?(企 15⑦、シ 13⑤、⑥) | はい　いいえ　対象外　備考____ |
| ７１　送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施しているか?(シ 13⑦) | はい　いいえ　対象外　備考____ |
| ７１．１　暗号化を利用する場合、暗号化の鍵について電子政府推奨暗号のものを使用しているか?(企 14①) | はい　いいえ　対象外　備考____ |
| ７２　脅威に対する管理責任の範囲について、医療機関等に明確に示し、その事項を示す文書等を提示できるか?(経 1.3.2①、経 5.2.1①、経 5.3、企 2①、④、⑤、シ 3②、シ 13①) | はい　いいえ　対象外　備考____ |
| ７３　医療機関等から委託をされた範囲において、脅威に対する管理責任の範囲を医療機関等に明確に示し、その事項を示す文書等を提示できるか?(企 2①、④、⑤、シ 13①) | はい　いいえ　対象外　備考____ |
| ７４　リモートメンテナンスサービスを有しているか? | 該当　非該当　　備考____ |
| ７４．１　リモートメンテナンスサービスに関し、不必要なリモートログインを制限する仕組みを有しているか?(シ 7⑫、シ 10.1、シ 18.1) | はい　いいえ　対象外　備考____ |
| ７５　回線の可用性等の品質に関して問題がないことを確認し、明確に文書等の証跡を残し、医療機関等に提示できるか?(企 15⑩) | はい　いいえ　対象外　備考____ |
| ７６　患者が情報を閲覧する機能があるか? | 該当　非該当　　備考____ |
| ７６．１　情報の閲覧のために公開しているサービスにおいて、医療機関等の内部システムに不正な侵入等が起こらないように対策を実施しているか?(企 8⑧、シ 7⑭) | はい　いいえ　対象外　備考____ |
| ７６．２　医療機関等が患者等へ情報セキュリティに関するリスクや情報提供目的について説明を行うために必要となる情報を資料として提示できるか?(企 8⑨) | はい　いいえ　対象外　備考____ |
| ７６．３　説明資料では、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にしているか?(企 8⑨、シ 7⑭) | はい　いいえ　対象外　備考____ |

| 法令で定められた記名・押印を電子署名で行うことについて | |
|---|---|
| ７７　記名・押印が義務付けられた文書を扱っているか?(経 4、企 14、シ 15①) | 該当　非該当　　備考____ |
| ７７．１　HPKI 対応、又は認定認証局もしくは公的個人認証サービスが発行する証明書対応の署名機能があるか?(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| ７７．２　HPKI 対応、又は認定認証局もしくは公的個人認証サービスが発行する証明書対応の検証機能があるか?(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| ７７．２．１　特定の国家資格の確認を行う必要がある場合に、電子的に検証できる機能があるか?(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| ７７．３　総務省の「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が付与可能か?(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| ７７．４　総務省の「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が検証可能か?(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| ７７．５　保存期間中の文書の真正性を担保する仕組みがあるか?(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| ７８　上記タイムスタンプを付与する時点で有効な電子証明書を用いているか?(企 14①、シ 15①) | はい　いいえ　対象外　備考____ |
| ７９　電子署名に用いる秘密鍵の管理が、認証局が定める「認証書ポリシー」（CP）等で定める鍵の管理の要件を満たして行われるよう管理しているか？（企 14②、シ 15①） | はい　いいえ　対象外　備考____ |
| **真正性の確保について** | |
| ８０　記録の確定操作が必要な情報を扱っているか? | 該当　非該当　　備考____ |
| ８０．１　入力者及び確定者を正しく識別し、認証を行う機能があるか?(企 15⑬、シ 14④) | はい　いいえ　対象外　備考____ |
| ８０．２　区分管理を行っている対象情報ごとに、権限管理（アクセスコントロール）の機能があるか?(企 15⑬、シ 14④) | はい　いいえ　対象外　備考____ |
| ８０．３　権限のある利用者以外による作成、追記、変更を防止する機能があるか?(企 15⑬) | はい　いいえ　対象外　備考____ |
| ８０．４　サービス事業者内の利用者の権限管理の機能があるか?(企 15⑬) | はい　いいえ　対象外　備考____ |
| ８０．５　サービス事業者内の利用者が作成、追記、変更を防止する機能があるか?(企 15⑬) | はい　いいえ　対象外　備考____ |
| ８０．６　システムが端末を管理することによって、権限を持たない者からのアクセスを防止する機能があるか?(企 15⑬) | はい　いいえ　対象外　備考____ |
| ８０．７　システムがサービス事業者の保守等端末を管理することによって、権限を持たない者からのアクセスを防止する機能があるか?(企 15⑬) | はい　いいえ　対象外　備考____ |
| ８１　システムは記録を確定する機能があるか?(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| ８１．１　確定情報には、入力者及び確定者の識別情報、信頼できる時刻源を用いた作成日時が含まれているか?(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| ８１．２　「記録の確定」を行うにあたり、内容の確認をする機能があるか?(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| ８１．３　確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止する機能があるか?(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| ８２　装置が確定機能を持っていない場合、記録が作成される際に、当該装置の管理責任者や操作者の識別情報、作成日時を含めて記録する機能があるか？（企 15⑬、シ 14⑧） | はい　いいえ　対象外　備考____ |
| ８３　確定された診療録等が更新された場合、更新履歴を保存し、更新前後の内容を参照する機能があるか?(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| ８３．１　同じ診療録等に対して複数回更新が行われた場合、更新の順序性を識別できる機能があるか?(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |

| | |
|---|---|
| ８４　代行入力の承認機能があるか？(企 13⑧、企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| ８４．１　代行入力が行われた場合、誰の代行がいつ誰によって行われたかの管理情報を、その代行入力の都度、記録する機能があるか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| ８４．２　代行入力により記録された診療録等に対し、確定者による「確定操作（承認）」を行う機能があるか？(企 15⑬、シ 14⑧) | はい　いいえ　対象外　備考____ |
| ８５　システムがどのような機器・ソフトウェアで構成され、どのような場面、用途で利用されるのか明確にしているか？(企 15⑬、シ 9①) | はい　いいえ　対象外　備考____ |
| ８６　機器・ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスが規定されているか？(企 15⑬、シ 9②) | はい　いいえ　対象外　備考____ |
| ８７　機器・ソフトウェアの品質管理に関する作業内容をルールに定めて、策定したルールに基づいて従業者等への教育を実施しているか？(企 15⑪、⑬) | はい　いいえ　対象外　備考____ |
| ８８　システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施しているか？(経 1.2.1、経 3.3.2、企 15⑫、⑬) | はい　いいえ　対象外　備考____ |
| ８９　通信の相手先が正当であることを確認するための相互認証を実施しているか？(シ 13⑫) | はい　いいえ　対象外　備考____ |
| ９０　ネットワークの転送中に改ざんされていないことを保証する機能を有しているか？(企 15⑦、シ 13⑧、⑨、⑪) | はい　いいえ　対象外　備考____ |
| ９１　サービス事業者の機器・システムはリモートログインの機能を制限しているか？(企 15⑬、シ 7⑫) | はい　いいえ　対象外　備考____ |
| **見読性の確保について** | |
| ９２　患者ごとの全ての情報の所在が日常的に管理されているか？(企 8④、企 15⑬、シ 4①) | はい　いいえ　対象外　備考____ |
| ９３　電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理し、また、見読化手段である機器・ソフトウェア・関連情報等は常に整備された状態になっているか？(企 15⑬、シ 5④) | はい　いいえ　対象外　備考____ |
| ９４　目的に応じて速やかに検索結果を出力する機能又はサービスがあるか？(企 15⑬、シ 9④) | はい　いいえ　対象外　備考____ |
| ９５　システム障害に備えた冗長化手段や代替的な見読化手段はあるか？(企 11.2、企 15⑬、シ 11①、シ 11.1) | はい　いいえ　対象外　備考____ |
| ９５．１　冗長化手段があるか？(企 11.2、企 15⑬、シ 11①) | はい　いいえ　対象外　備考____ |
| ９５．２　システム障害に備えた代替的な見読化手段があるか？(企 15⑬、シ 11①) | はい　いいえ　対象外　備考____ |
| **保存性の確保について** | |
| ９６　不正ソフトウェアによる情報の破壊、混同等が起こらないように、システムで利用するソフトウェア、機器及び媒体の管理を行っているか？(経 3.4、企 15⑥、⑬、シ 7④、シ 8③、シ 8.1) | はい　いいえ　対象外　備考____ |
| ９７　記録媒体及び記録機器の院内での保管及び取扱いについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？また、クラウドサービスを提供する場合において、サービス事業者による記録媒体及び記録機器の保管及び取扱いについてSLA等の文書に含めて医療機関等に提供されているか？(企 15③、④、⑬、シ 12.2) | はい　いいえ　対象外　備考____ |
| ９８　情報の保存やバックアップについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？(企 15③、④、⑬、企 15.1、シ 12.2) | はい　いいえ　対象外　備考____ |
| ９９　システムが保存する情報へのアクセスについて、履歴を残しているか？(経 4.2、企 5①、④、企 15⑬、シ 17①) | はい　いいえ　対象外　備考____ |

| | |
|---|---|
| ９９．１　システムが保存する情報へのアクセスについてその履歴を管理しているか？(経 4.2、企 5②、企 15⑬、シ 17①) | はい　いいえ　対象外　備考____ |
| １００　システムが保存する情報がき損した時に、バックアップされたデータ等を用いて、き損前の状態に戻せるか、又はもし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしているか？(経 3.4.1、企 15⑬、シ 11①、シ 18①、シ 18.1) | はい　いいえ　対象外　備考____ |
| １０１　システムの移行の際に診療録等のデータを、標準形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式にて出力及び入力できる機能があるか？(企 15⑬、シ 5①、シ 5.2) | はい　いいえ　対象外　備考____ |
| １０２　マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能またはサービスを備えているか？(企 15⑬、シ 5②) | はい　いいえ　対象外　備考____ |
| １０３　外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持できるか？(シ 5③) | はい　いいえ　対象外　備考____ |
| １０４　SLA 等に医療機関等に対して設備の条件を提示して、回線や設備が劣化した場合は SLA 等の要件を満たすように更新できるか？(企 15⑤、シ 12⑤、シ 12.2) | はい　いいえ　対象外　備考____ |
| **診療録等をスキャナ等により電子化して保存する場合について** | |
| １０５　診療録などをスキャナなどにより電子化して原本として保存する機能があるか？ | 該当　非該当　　備考____ |
| １０５．１　光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いているか？(企 16①、シ 16①) | はい　いいえ　対象外　備考____ |
| １０５．２　電子署名等を付与する機能があるか？(経 4.1 企 16③、⑦、シ 1①、シ 15①) | はい　いいえ　対象外　備考____ |
| １０６　診療録などをスキャナなどにより電子化して参照情報として保存する機能があるか？ | 該当　非該当　　備考____ |
| １０６．１　光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いているか？(企 16①、シ 16①) | はい　いいえ　対象外　備考____ |

| 備考記載欄 | |
|---|---|
| | |

# 9. チェックリストの解説（サービス事業者編）

## 診療録及び診療諸記録等の医療情報の取り扱いを受託する際の基準

### 「1　診療録及び診療諸記録等の外部保存を受託するか？」

外部保存を受託する場合は「該当」、そうでない場合は「非該当」としてください。
本質問の回答が「該当」の場合は、従属質問のいずれかを「はい」としてください。
注：本1項は1.1、1.2に分かれているが、これは安全管理ガイドライン第5.2版対応のチェックリストとの互換性の為であり、第6版ではこの区別が無いため、要求内容は同一である。解説は区別をしない。1.2の解説を参照してください。

### 「1．1　保存場所が「病院、診療所、医療法人等が適切に管理する場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？(経5、企7③、④、⑤、⑥、⑦、⑧、⑨)」

1.2の解説を参照してください。

### 「1．2　保存場所が「医療機関等が外部の事業者との契約に基づいて確保した安全な場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？(経5、企7③、④、⑤、⑥、⑦、⑧、⑨)」

以下の①～⑩の各事項は、サービスを利用する医療機関等にとってサービス事業者選定に当たっての必須条件ですので、事業者においては肯定的に応えることが求められています。
以下の項目について法的根拠なしに、要件に条件を付ける場合は「いいえ」として下さい。
また、その理由を「備考」に記載してください。

「安全管理ガイドラインで示された選定基準と情報の取扱い要件とは以下の全てを含みます。(経5、企7③、④、⑤、⑥、⑦、⑧、⑨)
① ②は④の説明です。⑩はサービス事業者名が院内において開示されることを示しています。

① 医療情報を取り扱う者を職員として採用するに当たっては、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含める等の安全管理対策を実施すること。
② 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。
③ 医療機関等の事務、運用等を外部の事業者に委託する場合は、委託契約の契約書に守秘・非開示に関する内容を含めること。
④ ③の委託契約の際に、当該委託先事業者の就業規則等に①及び②の対応を含めるよう求めること。
⑤ 外部の事業者との契約に基づいて医療情報を外部保存する場合、以下の対応を行うこと。重要度の高い委託の場合は、経営層に丁寧に報告し、承認を得ること。
- 保存した医療情報の取扱いに関して監督できるようにするため、外部保存の委託先事業者及びその管理者、電子保存作業従事者等に対する守秘義務に関連する事項やその事項に違反した場合のペナルティを契約書等で定めること。
- 医療機関等と外部保存の委託先事業者を結ぶネットワークインフラに関しては、委託先事業者にも本ガイドラインを遵守させること。
- 総務省・経済産業省の定めた「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」を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等して遵守状況を確認すること。
- 外部保存の委託先事業者の選定に当たっては、システム関連事業者の情報セキュリティ対策状況を示した資料を確認すること。（例えば、「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」における「サービス仕様適合開示書」の提供を求めて確認することなどが挙げられ

る。）

－　外部保存の委託先事業者に、契約書等で合意した保守作業に必要な情報以外の情報を閲覧させないこと。

－　保存した情報（Cookie、匿名加工情報等、個人を特定しない情報を含む。本項において以下同じ。）を独断で分析、解析等を実施してはならないことを契約書等に明記し、外部保存の委託先事業者に遵守させること。

－　保存した情報を外部保存の委託先事業者が独自に提供しないよう、契約書等で情報提供のルールについて定めること。外部保存の委託先事業者に情報の提供に係るアクセス権を設定する場合は、適切な権限を設定させ、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないよう求めること。

－　保存された情報を格納する情報機器等が、国内法の適用を受けることを確認すること。

⑥　外部保存の委託先事業者を選定する際は、少なくとも次に掲げる事項について確認すること。

a 医療情報等の安全管理に係る基本方針・取扱規程等の整備状況

b 医療情報等の安全管理に係る実施体制の整備状況

c 不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況

d 実績等に基づく個人データ安全管理に関する信用度

e 財務諸表等に基づく経営の健全性

f プライバシーマーク認定又はISMS認証の取得

g 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、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）

・JASAクラウドセキュリティ推進協議会CSゴールドマーク

・米国FedRAMP

・AICPA SOC2（日本公認会計士協会IT7号）

・AICPA SOC3（SysTrust/WebTrust）（日本公認会計士協会IT2号）

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

・システム監査技術者

・Certified Information Systems Auditor ISACA認定

H 医療情報を保存する情報機器が設置されている場所(地域、国)

I 委託先事業者に対する国外法の適用可能性

⑦　医療情報の外部保存の委託先事業者との契約には、以下の内容を含めること。

－　委託元の医療機関等、患者等の許可なく保存を受託した医療情報を分析等の目的で取り扱わないこと。

－　保存を受託した医療情報の分析等は正当な目的の場合に限り許可されること。

－　匿名化した情報であっても、匿名化の妥当性の検証を行う、及び院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱うこと。

－　保存を委託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存の委託先事業者に適切な利用者権限や閲覧の範囲を設定し、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮すること。

－　情報の提供は、原則、患者が受診している医療機関等と患者との間での同意に基づいて実施すること。

⑧　委託先事業者が契約に基づいて必要な対応を行っていることを定期的に確認するため、委託先事業者に報告を求めること。当該報告の結果、改善が必要である場合にはその旨を求めること。また委託先事業者からの報告内容については、経営層に報告し、承認を得ること。

⑨　委託契約終了に際し、医療情報の返却とその方法など、委託先事業者が行うべき内容についてあらかじめ契約により取り決めておくこと。

⑩　外部保存の委託に当たり、あらかじめ患者に対して、必要に応じて個人情報が特定の外部の施設に送付・保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得ること。

## 医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践

### 「2　扱う情報のリストを医療機関等に提示できるか？(概 4.5、経 2.2、企 6②、③)」

本項目は、安全管理ガイドライン企画管理編「6. リスクマネージメント（リスク管理）」の考え方に基づいてシステムにおけるリスク分析を行うため、扱う情報をすべてリストアップしているかを確認するものです。

情報システムで扱う情報をすべてリストアップしている場合は「はい」、そうでない場合は「いいえ」としてください。リストが一部不足している等、補足説明が必要な場合は、備考に記載してください。

## 組織的安全管理対策（体制、運用管理規程）

### 「3　医療情報システムを運用する際に、医療情報システムの企画管理者を設置しているか？(経 3.1.2、企 3①、③)」

本項目は、サービス事業者が受託しているサービスを運用する際に使用する情報システムに対し、企画管理を行うために必要な運用管理である企画管理者の設置を問うものです。運用管理には組織的対応と技術的対応を含みます。設置している場合は「はい」、設置していない場合は「いいえ」としてください。

### 「4　医療情報システムを運用する際に、技術的担当者を指定しているか？(経 3.1.2、企 3①、③)」

本項目はサービス事業者が受託しているサービスを運用する際に使用する情報システムに対し、安全管理の内特に技術的担当者を指定しているか問うものです。指定している場合は「はい」、指定していない場合は「いいえ」としてください。

### 「5　個人情報が参照可能な場所に対しては、入退管理のルールを定めているか？(経 3.2、企 8③、企 15②)」

サービスを提供している情報システムにおいて個人情報が取り扱われる場合、個人情報が閲覧可能なエリアに対する入退管理は重要な項目になります。運用管理規程等にて入退管理を定めている場合は「はい」、定めていない場合は「いいえ」としてください。

### 「6　情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成しているか？(概 4.4、経 3.2、企 13①)」

提供しているサービスに対するアクセス管理及び、情報システムに関するアクセス管理規程を作成している場合は「はい」、作成していない場合は「いいえ」としてください。

### 「7　医療機関等との契約に安全管理に関する条項を含めているか？(概 4.4、経 3.2、企 7④、⑤、⑦、⑧、⑨)」

契約に安全管理に関する条項を含めている場合は「はい」、そうでない場合は「いいえ」としてください。安全管理に関する条項とは安全管理ガイドラインに適合する運用を実施するということである。

### 「8　個人情報を含む医療情報システムの業務を受託する場合、委託元である医療機関等との契約に再委託先を含めた安全管理に関する条項を含めているか？(概 4.4、経 5.2.2、企 1②)」

個人情報を含む医療情報システムの業務をサービス事業者が受託し、契約に安全管理に関する条項を含めている場合は「はい」、そうでない場合は「いいえ」としてください。サービス事業者がさらに再委託している場合はその安全管理も含めて回答してください。個人情報を含む医療情報システムの業務をサービス事業者が外部委託していない場合は「対象外」としてください。

### 「９　運用管理規程等において組織的安全管理対策に関する事項等を定めているか？(概 4.4、経 3.1、経 3.2、企 4)」

組織的安全管理対策に関する事項とは、「体制」、「契約書・マニュアル等の文書の管理方法」、「リスクに対する予防措置、発生時の対応の方法」、「機器を用いる場合は機器の管理方法」、「個人情報の記録媒体の管理（保管・授受等）の方法」、「患者等への説明と同意を得る方法」、「監査」、「苦情・質問の受付窓口」等です。

サービス事業者が受託しているサービスの運用管理規程等において、上記全てを定めている場合は「はい」、そうでない場合は「いいえ」としてください。規程が一部不足している場合は、その旨を備考に記載してください。

## 物理的安全対策

### 「１０　個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠しているか？(企 8③、シ 12.1)」

個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠している場合は「はい」、そうでない場合は「いいえ」、個人情報を保存していない場合は「対象外」としてください。

### 「１１　個人情報を入力・参照できる端末が設置されている区画は、許可されたもの以外立ち入ることができないように対策されているか？(企 15②)」

個人情報を入力、参照できる端末が設置されている区画は、許可されたもの以外立ち入ることができないように対策されている場合は「はい」、そうでない場合は「いいえ」、個人情報を保存していない場合は「対象外」としてください。他の取り得る手段を用いる場合は備考に記載してください。

### 「１２　個人情報が保存されている機器が設置されている区画への入退管理を実施しているか？(企 15②)」

個人情報の物理的保存を行っている区画への入退管理を実施している場合は「はい」、そうでない場合は「いいえ」、個人情報の物理的保存を行っていない場合は「対象外」としてください。

### 「１２．１　入退出の事実を記録しているか？(企 15②)」

入退出の事実を記録している場合は「はい」、そうでない場合は「いいえ」としてください。

### 「１２．２　入退者の記録を定期的にチェックし、妥当性を確認しているか？(企 15②)」

入退者の記録を定期的にチェックし、妥当性を確認している場合は「はい」、そうでない場合は「いいえ」としてください。

### 「１３　個人情報が保存されている機器等の重要な機器に盗難防止策を講じているか？(企 8③、シ 12③)」

個人情報が存在する PC 等の重要な機器に盗難防止策（例えば　チェーン設置）を講じている場合は「はい」、そうでない場合は「いいえ」としてください。他の取り得る手段を用いる場合は、備考に記載してください。

### 「１４　個人情報が入力・参照できる端末に覗き見防止の機能があるか？(シ 12⑥、シ 12.3.2)」

本項目は、安全管理ガイドライン　システム運用編「12.3.2　端末・サーバ装置等の不適切な利用等に関する対策」の考え方に基づいて覗き見防止機能を有するかを確認するものです。

覗き見防止の機能を有している場合は「はい」、そうでない場合は「いいえ」、対象機器が本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

### 「１５　サービス事業者の管理端末に覗き見防止対策が取られているか？(シ 12⑥、シ 12.3.2)」

サービス事業者の管理端末に覗き見防止の対策がされている場合は「はい」、そうでない場合は「いいえ」、対象機器が本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

## 技術的安全対策

### 「１６　離席時に権限を持たない者による不正入力を防止する対策が行われているか？(シ 12⑥)」

本項目は、離席時に権限を持たない者による不正入力を防止する対策を有するかを確認するものです。

クリアスクリーン等の対策がされている場合は「はい」、そうでない場合は「いいえ」、対象サービスが本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

### 「１７　アクセス管理の機能があるか？(シ 14①)」

医療情報システムの利用者の識別・認証の機能を有している場合は「はい」、有していない場合は「いいえ」としてください。アクセス管理を必要としない場合は 「対象外」としてください。
なお、本項目は、安全管理ガイドライン システム運用編「14. 認証・認可に関する安全管理措置」をよく理解した上で回答してください。

### 「１７．１　利用者の認証方式は？(シ 14⑤)」

利用者の認証方式として、「記憶（ID・パスワード等)」、「生体認証（指紋等)」、「物理媒体（IC カード等)」の 3 要素それぞれについて、利用可能な場合は「はい」、利用できない場合は「対象外」でお答えください。
二要素を組み合わせた認証は、利用できる場合は「はい」、利用できない場合は「いいえ」とし、「はい」の場合は、記憶、生体認証、物理媒体の 3 要素の中から可能な組み合わせを備考に記入してください。
その他の認証に対応している場合は、具体的な認証方式を備考に記入してください。

### 「１７．１．１　パスワードを利用者認証手段として利用しているか？」

パスワードを利用者認証手段として利用している場合は「該当」、そうでない場合は「非該当」としてください。
本項目に記載されているパスワード管理においては、パスワードが暗号化（不可逆変換によること）されていることと、容易に推定されないための手段の両方を有する必要があります。（１７．１．１．４～１７．１．１．７に相当）
参考情報：米国国立標準技術研究所（「SP 800-63-4（Digital Identity Guidelines（デジタルアイデンティに関するガイドライン)）第 4 版」

### 「１７．１．１．１　他の手段と併用した際のパスワードの運用方法を運用管理規程に定めているか？(シ 14②)」

IC カード等他の手段と併用してパスワードを運用するにあたり、運用方法を運用管理規程に定めている場合は「はい」、定めていない場合は「いいえ」としてください。他の手段と併用したパスワードの運用を行っていない場合は「対象外」としてください。

### 「１７．１．１．２　本人確認の実施の際、本人確認方法を台帳に記載しているか？(シ 14⑥)」

システム管理者がパスワードを変更する場合において、本人確認を実施した際に本人確認方法を台帳に記載している場合は「はい」、記載していない場合は「いいえ」としてください。システム管理者がパスワードを変更しない場合は「対象外」としてください。

### 「１７．１．１．３　パスワードの有効期限が管理できるか？(シ 14⑥)」

サービスにおいてパスワードの有効期限の管理ができている場合は「はい」、できていない場合は「いいえ」としてください。

### 「１７．１．１．４　文字列制限をチェックすることができるか？(シ 14⑥)」

パスワードの文字列が規定を満たしていることをチェックできる場合は「はい」、できない場合は「いいえ」としてください。

### 「１７．１．１．５　類推しやすいパスワードをチェックすることができるか？(シ 14⑥)」

類推しやすいパスワード（利用者の氏名もしくは、生年月日、または「12345678」、もしくは、「administrator」、「password」、その他辞書に記載されている単語等）をチェックすることができる場合は「はい」、できない場合は「いいえ」としてください。

### 「１７．１．１．６　パスワード変更の際に類似性のチェックをすることができるか？(シ 14⑥)」

2 つのパスワードを繰り返して利用するなど、パスワード変更の際に過去のパスワードを再利用することなどに対するチェックが行える場合は「はい」、行えない場合は「いいえ」としてください。

### 「１７．１．１．７　ID とパスワードの組み合わせが本人しか知りえないよう保たれているか？(シ 14②、⑥)」

パスワードを不可逆変換による暗号化（ハッシュ化等）し、管理者にも分からないような仕組みで管理されている場合は「はい」、そうでない場合は「いいえ」としてください。

### 「１７．１．２　運用管理規程にセキュリティ・デバイスが利用できない場合の代替手段が規定されているか？(シ 14③)」

セキュリティ・デバイスを利用者認証手段として用いている場合において、セキュリティ・デバイスの破損等により利用できない緊急時の代替手段およびその運用方法について運用管理規程に規定されている場合は「はい」、そうでない場合は「いいえ」としてください。セキュリティ・デバイスを利用者認証手段として用いていない場合は、対象外としてください。

### 「１７．２　利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？(経 4.2、シ 14.2)」

利用者の職種・担当業務別の情報区分ごとのアクセス管理機能がある場合は「はい」、そうでない場合は「いいえ」としてください。

### 「１７．３　アクセス記録（アクセスログ）機能があるか？(企 5③、シ 17①)」

アクセスログ機能がある場合は「はい」、ない場合は「いいえ」としてください。

### 「１７．３．１　アクセスログを利用者が確認する機能があるか？(経 4.2、企 5①、③)」

アクセスログを利用者が確認する機能がある場合は「はい」、そうでない場合は「いいえ」としてください。

### 「１７．３．２　アクセスログへのアクセス制限機能があるか？(企 5②、シ 17②)」

アクセスログへのアクセス制限機能がある場合は「はい」、そうでない場合は「いいえ」としてください。

### 「１７．３．３　アクセスログへのアクセス制限機能がない場合、不当な削除/改ざん/追加等を防止する運用的対策を講じているか？(企 5②、シ 17②)」

システムにアクセスログへのアクセス制限機能がない場合において、運用的対策を行っている場合は「はい」、そうでない場合は「いいえ」としてください。アクセス制限機能がある場合は、「対象外」としてください。

### 「１７．４　アクセス記録（アクセスログ）機能が無い場合、利用者が監査できる形でサービス事業者が業務日誌等に操作の記録を行っているか？(企 5①、シ 17①)」

システムにアクセス記録機能が無い場合、利用者が監査できる形でサービス事業者が業務日誌等に操作の記録を行っている場合は「はい」、そうでない場合は「いいえ」としてください。アクセス記録機能がある場合は「対象外」としてください。

### 「１８　時刻情報の正確性を担保する仕組みがあるか？(シ 17③)」

医療情報システムが、アクセス記録に使用される時刻情報に対して、標準時刻と時刻同期手段を有している場合は「はい」、そうでない場合は「いいえ」としてください。

### 「１９　不正なソフトウェアが混入していないか確認しているか？(企 15⑥、シ 8①、②)」

システムの構築時や外部ファイルの受領時などにシステムに不正なソフトウェアが混入していないか確認を行っている場合は「はい」、そうでない場合は「いいえ」としてください。

### 「２０　システムにメールの送受信機能がある場合、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理等が行われているか？(シ 8④)」

この質問は、不正ソフトウェアの対策の一環として要求されているものです。不正ソフトウェアが実行されることによる被害が増えていることから、メールにあたっては、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又は実行プログラムの起動を阻止する対策、テキスト化等の無害化処理等が取られているかが必要になります。対策がある場合は「はい」、無い場合は「いいえ」を選択してください。メールの送受信機能が無い場合は「対象外」を選択します。

### 「２１　システムでファイル交換機能を使用する場合、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理等が行われているか？(シ 8④)」

この質問は、不正ソフトウェアの対策の一環として要求されているものです。不正ソフトウェアが実行されることによる被害が増えていることから、ファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又は実行プログラムの起動を阻止する対策、無害化処理等が取られているかが必要になります。対策がある場合は「はい」、無い場合は「いいえ」を選択してください。ファイル交換機能が無い場合は「対象外」を選択します。

ファイル無害化とは、ファイルの構造を分析・分解し、ポリシーに従って「マルウェアの可能性のある部分」を取り除いて、安全なファイルに再構築する技術です。

### 「２２　無線 LAN を利用する場合のセキュリティ対策機能はあるか？(シ 13⑬)」

無線 LAN を使用している場合において、以下のセキュリティ対策を全て満たす場合は「はい」とし、いずれか 1 つでも満たさない場合は「いいえ」として、対策できていない内容について備考に記載してください。なお、無線 LAN の使用を認めていない、又は保証されていない場合は「対象外」としてください。

・適切な利用者以外に無線 LAN を利用されないようにすること。例えば、ANY 接続拒否等の対策を実施すること。

・不正アクセス対策を実施すること。例えば MAC アドレスによるアクセス制限を実施すること。

・不正な情報の取得を防止するため、WPA2 AES、WPA2 TKIP 等により通信を暗号化すること。

・利用する無線 LAN の電波特性を勘案して、通信を阻害しないものを利用すること 。

※ 総務省発行の「一般利用者が安心して無線 LAN を利用するために」や「企業等が安心して無線LANを導入・運用するために」を参考に記載してください。

### 「２３　IoT 機器を使用するか？」

IoT 機器を使用する場合は「該当」、使用しない場合は「非該当」としてください。

### 「２３．１　IoT 機器を使用する場合、IoT 機器により患者情報を取り扱うことに関するサービス事業者の運用管理規程を定めた上で、医療機関等に開示できるか？(シ 8⑥)」

IoT 機器を使用する場合、IoT 機器により患者情報を取り扱うことに関する運用管理規程を定めた上で、医療機関等に開示できるときは「はい」、そうでないときは「いいえ」としてください。IoT 機器を使用しない場合は「対象外」としてください。

### 「２３．２　ウェアラブル端末や在宅設置の IoT 機器を利用する場合、患者のリスク等に関する説明資料を提供できるか？(シ 7⑧)」

ウェアラブル端末や在宅設置の IoT 機器を利用する場合、患者のリスク等に関する説明資料を提供できるときは「はい」、そうでないときは「いいえ」としてください。ウェアラブル端末や在宅設置の IoT 機器を利用しない場合は「対象外」としてください。

### 「２３．３　IoT 機器のセキュリティアップデートを必要なタイミングで適切に実施できるか？(シ 8⑥)」

アップデートの必要が生じた際には、IoT 機器ベンダーと連携して、動作確認の上、アップデートモジュールを可及的速やかに適用することができる場合は「はい」、そうでない場合は「いいえ」としてください。アップデート適用にあたり、特別な対応が必要となるような場合は、その内容を備考に記載してください。

### 「２３．４　使用が終了または停止した IoT 機器の接続を遮断できるか？(シ 8⑥)」

使用が終了または停止した IoT 機器を悪用されないように、サービス事業者側で接続を遮断できる場合は「はい」、できない場合は「いいえ」としてください。

## 人的安全対策

### 「２４　従業者との間で、雇用時または契約時に守秘義務契約を結んでいるか？(企 7①)」

従業者との間で守秘義務契約を結んでいる場合は「はい」、結んでいない場合は「いいえ」としてください。

**「２５　従業者に対し、定期的に個人情報管理に関する教育訓練を行っているか？(経 3.2.2①、企７②)」**

定期的に個人情報管理に関する教育訓練を行っていれば「はい」、行っていなければ「いいえ」としてください。

**「２６　従業者の退職後または契約終了後における個人情報保護に関する規程が従業者との契約に含まれているか？(企 7①)」**

従業者の退職後や契約終了後も個人情報保護は継続する必要があります。従業者との契約の中に契約終了後の個人情報保護に関する規程が含まれていれば「はい」、含まれていなければ「いいえ」としてください。

**「２７　就業規則等には守秘義務違反に対する包括的な罰則規定が含まれているか？(企 7①、企 7.1)」**

就業規則等に守秘義務違反に対する包括的な罰則規定が含まれていれば「はい」、含まれていなければ「いいえ」としてください。「包括的」とは一部の守秘義務違反ではなく、すべての（あらゆる）守秘義務違反を対象とするという意味です。

**「２８　保守作業等で医療情報システムに直接アクセスする作業を行う際には、作業者・作業内容・作業結果を医療機関等に報告できるようになっているか？(シ 10①、③、④)」**

医療情報システムに直接アクセスする作業について、医療機関等にその作業について報告できるようになっていれば「はい」、なっていなければ「いいえ」としてください。報告内容には作業者、作業内容、作業結果が含まれます。

**「２９　清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行っているか？(企 1②、企 7③、④)」**

医療情報システムに直接アクセスしない作業についてもチェックを行い、医療機関等に作業状況を報告できるようになっていれば「はい」、なっていなければ「いいえ」としてください。

**「３０　業務の一部を外部委託する場合に、外部委託先に対し、自らに課しているのと同等の個人情報保護に関する対策を施す義務を、契約によって担保しているか？(企 1②、企 7③、④)」**

業務の一部を外部委託し、外部委託契約の中で、自らに課している「個人情報保護に関する対策を施す義務」と同等の義務を外部委託先にも課している場合は「はい」、課していない場合は「いいえ」としてください。外部委託していない場合は「対象外」としてください。

**「３１　やむを得ない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行っているか？(経 3.2、企 1②、企７③、④)」**

外部の保守要員が診療録等の個人情報にアクセスすることがある場合に、その保守要員に対しても守秘義務を課すことを契約で担保している場合は「はい」、担保していない場合は「いいえ」としてください。その際、外部の保守要員に守秘義務を確実に守らせるために、罰則のある就業規則などによる裏付けが必要です。

## 情報の破棄

### 「３２　ユーザに提示できる情報種別ごとの破棄の手順があるか？(企 8①、シ 7⑨)」

ユーザに提示できる情報種別ごとの破棄の手順がある場合は「はい」、そうでない場合は「いいえ」としてください。

### 「３２．１　手順には破棄を行う条件を含めているか？(企 8⑪、シ 7⑨)」

本項目は、前述の手順に情報の破棄を行う条件を含めているかを確認します。条件を含めている場合は「はい」、含めていない場合は「いいえ」としてください。

### 「３２．２　手順には破棄を行うことができる従業者の特定を含めているか？(企 8⑪、シ 7⑨)」

本項目は、前述の手順において情報の破棄を行うことができる従業者を特定していることを確認します。従業者を特定している場合は「はい」、特定していない場合は「いいえ」としてください。

### 「３２．３　手順には破棄の具体的な方法を含めているか？(企 8⑪、シ 7⑨)」

本項目は、前述の手順において情報の破棄の具体的な方法を定めていることを確認します。当手順の中で具体的な破棄方法を定めている場合は「はい」、定めていない場合は「いいえ」としてください。

### 「３３　情報処理機器自体を破棄する場合、必ず専門的な知識を有する者が行うこととし、残存し、読み出し可能な情報がないことを報告できるか？(シ 7⑨、⑩)」

本項目は、情報処理機器自体を破棄する場合、専門的な知識を有する者が行うこと、及び、読み出し可能な情報が無いことを報告できることを確認します。情報処理機器自体を破棄しない場合は「対象外」、専門的な知識を有する者が破棄し、かつ読み出し可能な情報が無いことを報告できる場合は「はい」、それ以外の場合は「いいえ」としてください。

### 「３４　破棄を外部委託した場合、外部委託業者の監督及び守秘義務契約に準じた監督責任の下、情報の破棄を確認しているか？(企 8⑫、シ 7⑪)」

本項目は、サービス事業者が情報の破棄を外部委託した場合、外部委託業者の監督及び守秘義務契約に準じた監督責任の下、情報の破棄を確認していることを問うものです。サービス事業者が情報の破棄を外部委託しない場合は「対象外」、サービス事業者が委託業者の監督及び情報の破棄を確認している場合は「はい」、それ以外の場合は「いいえ」としてください。

### 「３５　不要になった個人情報を含む媒体の破棄を、運用管理規程に定めているか？(企 8①、⑪)」

本項目は、不要になった個人情報を含む媒体の破棄を、サービス事業者の運用管理規程に定めていることを確認します。定めている場合は「はい」、定めていない場合は「いいえ」としてください。

## 医療情報システムの改造と保守

### 「３６　改造や保守に関する動作確認で個人情報を含むデータを使用する場合、作業員と守秘義務契約を交わしているか？(企 7①、③、④、)」

改造と保守に関する動作確認で個人情報を含むデータを使用し、作業員および外部委託先との守秘義務契約を交わしている場合は「はい」、そうでない場合は「いいえ」としてください。改造と保守に関する動作確認で個人情報を含むデータを使用しない場合は「対象外」としてください。

### 「３７　作業員はサービス事業者自身が定めた運用管理規程に従い、改造や保守に関する業務を行っているか？(（企 8①、⑫、シ 7①、⑨)」

外部委託を含む作業員はサービス事業者自身が定めた情報の持ち出しと破棄に関する手順を含む運用管理規程を踏まえて改造や保守の業務を行っている場合は「はい」、そうでない場合は「いいえ」としてください。作業を外部委託（再委託）している場合、外部委託先にサービス事業者自身が定めた運用管理規程を遵守させる必要があります。改造や保守の業務を行っていない場合は「対象外」としてください。

### 「３８　運用管理規程には作業終了後に動作確認で使用した個人情報を含むデータを消去することに関する規定が含まれているか？(企 15⑨、シ 10①」

運用管理規程に目的完了後の個人情報を含むデータ消去に関する規定を含んでいる場合は「はい」、そうでない場合は「いいえ」としてください。なお、「はい」と回答するには、データ消去に関する規定としてデータを消去したことを報告する内容が含まれている必要があります。

### 「３９　改造や保守に用いるアカウントは、作業員個人の専用アカウントを使用しているか？(シ 10③)」

本項目は、メンテナンス時に作業員が直接個人情報に触れる可能性があるため、作業員個人の専用アカウントを使用し、かつ、作業記録に個人情報へのアクセス有無、及びアクセスした対象を特定できる情報を残すことを運用管理規程に定め、適切に運用されていることを問うものです。

作業員個人のアカウントを使用してシステムにアクセスする場合は「はい」、そうでない場合は「いいえ」としてください。「いいえ」の場合は、備考にその理由を記載してください。

### 「４０　改造や保守に関する作業の記録として、個人情報へのアクセス有無、及びアクセスした対象を特定できる情報を医療機関等に提供できるか？(シ 10③)」

改造や保守に関する作業時に記録した個人情報へのアクセス有無、及びアクセスした対象を特定できる情報を医療機関等に提供できる場合は「はい」、そうでない場合は「いいえ」としてください。「いいえ」の場合は、備考にその理由を記載してください。

### 「４１　作業員のアカウントにおけるアクセス権限とアクセス状況を管理しているか？(企 13⑤、シ 10③、④)」

本項目は、作業員のアカウントにおけるアクセス権限とアクセス状況が適切に管理されていることを問うものです。なお、アクセス権限が適切に管理されていることとは、医療情報システムの利用用途とアクセス範囲、アクセス権限等の必要に応じて ID やアクセス権限が付与されていることを意味します。また、アクセス状況が適切に管理されていることとは、施設内のサーバに作業員（保守要員）がアクセスする際には専用アカウントを使用し、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報及び作業内容を記録すること、および、リモートメンテナンス（保守）によるシステムの改造・保守作業が行われる場合には、アクセスログを収集し、保守に関する作業計画書と照合するなどにより確認することを意味します。

管理している場合は「はい」、そうでない場合は「いいえ」としてください。「いいえ」の場合は、備考にその理由を記載してください。

### 「４２　作業員の離職や担当替え等に対して速やかに保守用アカウントを削除しているか？企 13⑤、⑦)」

本項目は、作業員の離職や担当替え等により、メンテナンス時に使用する作業員個人の専用アカウントの削除について運用管理規程で定める等、適切に運用されている場合は「はい」、そうでない場合は「いいえ」としてください。

### 「４３　改造や保守を外部委託している場合、保守要員の離職や担当替え等の際に報告を義務付けているか？(企 13⑤、⑦)」

改造や保守を外部委託し、保守要員の離職や担当替え等の際に外部委託元への報告を義務付けている場合は「はい」、そうでない場合は「いいえ」としてください。改造や保守を外部委託していない場合は「対象外」としてください。

### 「４３．１　報告に応じてアカウントを削除する管理体制ができているか？(企 13⑤、⑦)」

運用管理規程に記載する等、報告に応じてアカウントを削除する管理体制ができている場合は「はい」、そうでない場合は「いいえ」としてください。

### 「４４　メンテナンスを実施する場合は、事前に医療機関等に作業申請を提出できるか？(シ 10.1) 」

本項目は、メンテナンスを実施する際、医療機関等に対して事前に作業申請を提出できるかを問うものです。SLA 若しくは保守契約書、又は運用管理規程において事前提出を明記していることが必要です。本件は紙文書の提出を義務付けるものではなく、契約等で作業開始前にメール等で通知することで医療機関等と合意を取る方法もあります。

医療機関等に対して事前に作業申請を提出する場合は「はい」、そうでない場合は「いいえ」としてください。「いいえ」の場合は、備考にその理由を記載してください。メンテナンスを実施しない場合は「対象外」としてください。

### 「４５　メンテナンス終了時に、速やかに医療機関等に作業報告書を提出できるか？(シ 10.1)」

本項目は、メンテナンスを実施する際、医療機関等に対して作業終了時に作業報告書を提出できるかを問うものです。SLA 若しくは保守契約書、又は運用管理規程において作業終了時の提出を明記していることが必要です。本件は紙文書の提出を義務付けるものではなく、契約等で作業終了時にメール等で通知することで医療機関等と合意を取る方法もあります。

医療機関等に対してメンテナンス終了時に、作業報告書を提出する場合は「はい」、そうでない場合は「いいえ」としてください。「いいえ」の場合は、備考にその理由を記載してください。メンテナンスを実施しない場合は「対象外」としてください。

### 「４６　保守を外部委託する場合、保守事業者と守秘義務契約を締結しているか？(企 7③、④)」

本項目は、保守作業を外部委託している場合、その保守事業者と守秘義務契約を締結していることを問うものです。

保守事業者と守秘義務契約を締結している場合は「はい」、そうでない場合は「いいえ」としてください。保守作業を外部委託していない場合は「対象外」としてください。

### 「４７　システムの改造や保守で個人情報を含むデータを組織外に持ち出す際に、医療機関等の責任者の承認を得ることが運用管理規程に定められているか？(企 8①、⑤、シ 7①、②)」

本項目は、例えば、障害対応時等での原因特定や解析等あるいは本番データを用いるためにやむを得ず個人情報を組織外に持ち出さなければならない場合、医療機関等の責任者の承認を得ることが運用管理規程に定められていることを問うものです。「組織」外とは、「医療機関等及びサービス事業者等（再委託事業者含む）」以外を指します。運用管理規程に定めている場合は「はい」、そうでない場合は「いいえ」としてください。

### 「４８　リモートメンテナンスによる改造・保守を行う場合は、アクセスログを収集するか？（シ 10④)」

本項目は、リモートメンテナンスによるシステムの改造や保守を行う場合にアクセスログを収集することを問うものです。

アクセスログを収集する場合は「はい」、そうでない場合は「いいえ」としてください。

### 「４９　リモートメンテナンスにおいて、医療機関等へ送付等を行うファイルは、送信側で無害化処理が行われているか？(シ 10⑤)」

本項目は、リモートメンテナンスによるファイル送信時の無害化処理について問うものです。

送信時に無害化処理を実施している場合は「はい」、そうでない場合は「いいえ」としてください。リモートメンテナンスを実施しない場合、又は、リモートメンテナンスでファイル送信がない場合は、「対象外」としてください。

ファイル無害化とは、ファイルの構造を分析・分解し、ポリシーに従って「マルウェアの可能性のある部分」を取り除いて、安全なファイルに再構築する技術です。

### 「５０　保守業務を外部委託している場合、外部委託事業者にも自らと同等な義務を求め、契約しているか？(企 1②)」

本項目は、保守業務を外部委託している場合、外部委託先業者との保守契約において、個人情報保護の徹底等、自らと同等な義務を含む内容で契約していることを問うものです。

外部委託先業者に対して自らの責任で同等の義務を含む契約を締結している場合は「はい」としてください。「いいえ」の場合は、備考にその理由を記載してください。外部委託を行っていない場合は「対象外」としてください。

## 情報及び情報機器の持ち出し並びに外部利用について

### 「５１　持出機器を提供しているか？」

本項目は、医療機関等に持出機器を提供しているかどうかを問うものです。

医療機関等に持出機器を提供している場合は「該当」、提供していない場合は「非該当」としてください。

### 「５１．１　持出機器においてソフトウェアのインストールを制限する機能があるか？(企 8⑤、シ 7⑥)」

本項目は、医療機関等に持出機器を提供している場合に、システムとしてソフトウェアのインストールを制限する機能を有するかを確認するものです。例えば、不適切な設定のされたファイル交換ソフト（Winny 等）のような外部ソフトウェアにより情報が漏えいする可能性があるため、外部から持ち込まれたソフトウェアのインストールを制限する等の情報漏えい対策が必要となります。例えば在宅診療や訪問看護で使用するタブレットを用いてクラウドサービスにアクセスする事例等がこれにあたります。

システム側で、ソフトウェアのインストールを制限する機能を有する場合は「はい」、有していない場合は「いいえ」としてください。「いいえ」の場合は、備考にその理由を記載してください。

医療機関等に持出機器を提供していない場合は「対象外」としてください。

### 「５１．２　持出機器において外部入出力装置の機能を無効にすることができるか？(企 8⑤、シ 7⑥)」

本項目は、外部入出力装置（DVD ドライブ、USB メモリー等）の機能を無効にすることができることを確認するものです。外部入出力装置の機能を無効にすることで、コンピュータウイルスなどの侵入防止や情報漏えい防止等の情報の持ち出しを制限することが可能となります。

外部入出力装置を無効にする機能を有している場合は「はい」、有していない場合は「いいえ」としてください。「いいえ」の場合は、備考にその理由を記載してください。

### 「５１．３　外へ持ち出す際、情報に対して暗号化等の対策を行うことができるか？(シ 7③)」

本項目は、管理区域外へ情報を持ち出す場合、媒体や情報機器の盗難、紛失等が発生しても直ちに情報漏えいとならないように、情報に対して暗号化等の情報漏えい対策を行っていることを確認するものです。情報漏えい対策を行っている場合は「はい」、行っていない場合は「いいえ」、医療機関等又は医療機関等の委託によりサービス事業者が管理区域外へ情報を持ち出すケースが無い場合は「対象外」としてください。「いいえ」の場合は、備考にその理由を記載してください。

### 「５１．４　持ち出した情報機器を外部のネットワークや他の外部媒体に接続する場合、情報漏えいや改ざんの対策を実施しているか？(シ 7④)」

本項目は、持ち出した情報機器を外部のネットワークや他の外部媒体に接続する場合、情報漏えいや改ざんの対策を実施していることを確認するものです。管理区域外のネットワーク（インターネットや公衆網等）に接続する場合には、ウイルス感染等を含む情報漏えいや改ざんの対策が必要です。情報漏えいや改ざんの対策を実施している場合は「はい」、実施していない場合は「いいえ」としてください。

### 「５２　提供するサービスに係わる情報及び情報機器の持ち出しについて、リスク分析を実施しているか？(企 9.2、シ 7.1)」

本項目は、医療機関等ならびにサービス事業者が情報及び情報機器の管理区域外への持ち出しを行うケースについて、サービス事業者がリスク分析を実施しているかを確認するものです。医療機関等が持ち出しを行うケース及びサービス事業者が持ち出しを行うケースの両方についてサービス事業者がリスク分析を実施している場合は「はい」、両方のケースにおいては実施していない場合は「いいえ」、情報及び情報機器の持ち出しを行うケースが無い場合は「対象外」としてください。

### 「５３　サービス事業者が情報及び情報機器を持出する場合があるか？」

本項目は、サービス事業者が情報及び情報機器の持ち出す場合があるかどうかを確認するものです。持ち出す場合がある場合は「該当」、ない場合は「非該当」としてください。

### 「５３．１　リスク分析の結果を受けて、情報及び情報機器の持ち出しに関する方針を運用管理規程に定めているか？(企 8①、⑤、⑦、⑧、⑪、⑫、シ 7①、⑦、⑨、⑮)」

本項目は、サービス事業者が情報及び情報機器を持出する場合にリスク分析の結果を受けて、サービス事業者が情報及び情報機器の持ち出しに関する方針を定めていることを確認するものです。当方針を定めている場合は「はい」、定めていない場合は「いいえ」としてください。「いいえ」の場合は、備考にその理由を記載してください。サービス事業者が情報及び情報機器を持ち出さない場合は「対象外」としてください。

### 「５３．２　持ち出した情報及び情報機器の管理方法を定めているか？(企 8⑤)」

本項目は、サービス事業者が持ち出した情報及び情報機器の管理方法を定めていることを確認するものです。管理方法を定めている場合は「はい」、定めていない場合は「いいえ」としてください。

### 「５３．３　情報を格納した媒体及び情報機器の盗難、紛失時の適切な対応を自社方針・規則等に定めているか？(企 8⑦、シ 7⑮)」

本項目は、情報を格納した媒体及び情報機器が盗難にあった場合や、紛失した場合の対応を自社方針・規則等に定めていることを確認するものです。自社方針・規則等に定めている場合は「はい」、それ以外の場合は「いいえ」としてください。

### 「５３．４　自社方針・規則等で定めた盗難、紛失時の対応を従業員等に対して周知徹底し、教育を行っているか？(企 7②、企 7.1)」

本項目は、サービス事業者の前記自社方針・規則等で定めた盗難、紛失時の対応を従業員等（派遣者を含む）に対して周知徹底し、教育を行っていることを確認するものです。当対応を周知徹底し、教育を行っている場合は「はい」、行っていない場合は「いいえ」としてください。

### 「５３．５　情報機器について、起動パスワード等を設定しているか？(シ 7③、シ 8⑤)」

本項目は、サービス事業者の情報機器について、アクセス権限を持たない者によるアクセスを禁止できるように、起動パスワード等（指紋等による生体認証を含む）を設定していることを確認するものです。設定している場合は「はい」、設定していない場合は「いいえ」としてください。

### 「５３．６　パスワード設定においては、適切なパスワード管理措置を行っているか？(企 13②、シ 8⑤)」

本項目は、サービス事業者の情報機器についてパスワード設定を行っている場合、適切なパスワード管理措置を行っていることを確認するものです。適切なパスワード管理措置とは、安全管理ガイドライン　システム運用編 14⑥　に記載のシステム内のパスワードの不可逆変換や再発行時の本人確認等を示します。適切なパスワード管理措置を行っている場合は「はい」、行っていない場合は「いいえ」、パスワード設定を用いていない場合は「対象外」としてください。

### 「５３．７　サービス事業者が外へ持ち出す際、情報に対して暗号化等の対策を行っているか？(シ 7③)」

本項目は、サービス事業者が、管理区域外へ情報を持ち出す場合、媒体や情報機器の盗難、置き忘れ等が発生しても直ちに情報漏えいとならないように、情報に対して暗号化等の対策を行っていることを確認するものです。対策を行っている場合は「はい」、行っていない場合は「いいえ」としてください。「いいえ」の場合は、備考にその理由を記載してください。

### 「５３．８　医療機関等または医療機関等に委託されたサービス事業者が、持ち出した情報機器を外部のネットワークや他の外部媒体に接続する場合、情報漏えいや改ざんの対策を実施しているか？(企 8⑤、⑥、シ 7④、⑤、⑥)」

本項目は、医療機関等または医療機関等に委託されたサービス事業者が、持ち出した情報機器を外部のネットワークや他の外部媒体に接続する場合、情報漏えいや改ざんの対策を実施していることを確認するものです。管

理区域外のネットワーク（インターネットや公衆網等）に接続する場合には、ウイルス感染等を含む情報漏えいや改ざんの対象にならないための対策が必要です。

なお、管理区域外のネットワーク（インターネットや公衆網等）に接続する場合、安全管理ガイドライン　システム運用編 「13.ネットワークに関する安全管理措置」に準じた設定を行う必要があります。また、公衆無線 LAN 等、安全管理ガイドライン　システム運用編 13⑬の基準を満たさないネットワークへの接続は禁止されています。

上記を踏まえて、情報漏えいや改ざんの対策を実施している場合は「はい」、実施していない場合は「いいえ」、医療機関等ならびにサービス事業者が情報機器を持ち出すケースが無い場合は「対象外」としてください。

### 「５４　情報の管理者は情報機器・媒体の所在について台帳を用いる等して管理しているか？(企 9①②、③、シ 7⑦)」

本項目は、サービス事業者の情報の管理者が、情報機器・媒体の所在について管理していることを確認するものです。サービス事業者の情報の管理者が台帳を用いる等で情報機器・媒体の所在管理をしている場合は「はい」、所在管理をしていない場合は「いいえ」としてください。

### 「５５　個人保有の情報機器の利用を禁止しているか？(企 9⑥、シ 8.5)」

本項目は、サービス事業者が業務を行う際に、個人保有の情報機器の利用を禁止していることを確認するものです。禁止していれば「はい」、禁止していなければ「いいえ」としてください。

## 災害、サイバー攻撃等の非常時の対応

### 「５６　医療機関等に提供可能なサービス事業者の BCP 手順書が用意されているか？(経 3.4.1、企 11)」

本項目は、委託された医療サービスに関する BCP 手順書を、医療機関等に対し提供可能かを確認するものです。BCP 手順書には、自然災害や IT 障害等が発生した際、医療機関等が「非常時である」と判断するために必要な「基準」、「手順」、実際に責任を持って判断を実施する「判断者」、ならびに正常に復帰したことを判断するための「正常復帰時の基準」、「正常復帰時の手順」について、それぞれ明記されていることが求められます。これら全ての要件を含む BCP 手順書を医療機関等に対して提供可能な場合は「はい」、そうでない場合は「いいえ」としてください。

### 「５７　非常時アカウント又は、非常時にも医療サービスを継続して提供できる機能を持っているか？(企 11、シ 11①)」

本項目は、自然災害や IT 障害等の非常時においても医療サービスを継続して提供できる機能を有するかを確認するものです。例えばバックアップからシステムを運用可能な状態に復旧するための機能、システムとして正常なユーザ認証が不可能な場合に対応する機能（非常時アカウントによる患者データへのアクセス機能等）が求められます。

上記のような非常時機能又は非常時アカウントがある場合は「はい」、無い場合は「いいえ」、システムとして該当しない場合（アカウント管理機能等が無い場合）は「対象外」としてください。

バックアップについては、ガイドライン 6.0 版本文の該当記載箇所、更に Q&A を参考にして、データ特性を考慮したバックアップ方式を定めること。

### 「５７．１　「非常時のユーザアカウントや非常時用機能」の管理手順を提供できるか？(企 11①、④、⑤、⑥、シ 11①)」

本項目は、「非常時のユーザアカウントや非常時用機能」の管理手順を提供できるかどうかを確認するものです。管理手順が記載された文書等が存在する場合は「はい」、そうでない場合は「いいえ」としてください。

### 「５７．２　非常時機能を有している場合、非常時機能が定常時に不適切に利用されることがないよう適切に管理及び監査できる情報を提供できるか？(シ 11①)」

本項目は、非常時機能を有する場合に、その適切な管理や監査できる情報を提供している場合は「はい」、そうでない場合は「いいえ」としてください。

### 「５７．３　非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更できるか？(シ 11①)」

本項目は、正常復帰後は継続使用ができないように変更する機能を有している場合は「はい」、そうでない場合は「いいえ」としてください。医療情報システムとして該当しない場合（非常時用ユーザアカウントが無い場合）は「対象外」としてください。

### 「５７．４　標的型メール攻撃等により医療情報システムに不正ソフトウェアが混入した場合、関係先への連絡手段を準備しているか？(企 11④、⑤、⑨、企 12⑦、シ 11①)」

標的型メール攻撃等により医療情報システムに不正ソフトウェアが混入した際、関係先への連絡手段を準備している場合は「はい」、そうでない場合は「いいえ」としてください。

### 「５８　重要なファイルをバックアップしているか？(経 3.4.1、企 7⑥、企 11④、⑤、シ 11①、シ 12.2)」

本項目は、重要なファイルについてバックアップ機能を有している場合は「はい」、そうでない場合は「いいえ」としてください。医療情報システムとして該当しない場合は「対象外」としてください。

### 「５８．１　バックアップは数世代、複数の方式で実施しているか？（企 11④、⑤、シ 11①、シ 12.2、シ 18①)」

本項目は、バックアップを数世代、複数の方式で実施している場合は「はい」、そうでない場合は「いいえ」としてください。

### 「５８．２　数世代、複数方式のバックアップの一部は不正ソフトウェアの混入による影響が波及しないように管理されているか？（企 11④、⑤、シ 11①、シ 12.2、シ 18①)」

本項目は、数世代、複数方式で取得したバックアップの一部が不正ソフトウェアの混入による影響が波及しないように管理されている場合は「はい」、そうでない場合は「いいえ」としてください。

混入による影響が波及しないような管理の例としては、取得したバックアップをオフライン状態で保存する、バックアップメディアを物理的に離れた場所に保管する等があります。

### 「５８．３　バックアップからの復元手段が整備されているか？(企 11④、⑤、シ 11①、シ 12.2)」

本項目は、バックアップからの復元手段が整備されている場合は「はい」、そうでない場合は「いいえ」としてください。

## 外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理

５９～６３の質問は、提供するサービスで対応している通信方式について確認するものです。通信方式によって対策すべき項目が異なりますので、対応している通信方式それぞれに対して確認が必要です。対応している通信方式に「該当」とし、対応していない通信方式を「非該当」としてください。

### 「５９　通信方式として専用線に対応しているか？」

本項目は、専用線による通信に対応している場合は「該当」、そうでない場合は「非該当」としてください。

### 「５９．１　提供事業者に閉域性の範囲を確認しているか？(シ 13⑨)」

範囲を確認している場合は「はい」、確認していない場合は「いいえ」としてください。「はい」の場合は、確認した内容を備考に記載してください。

### 「５９．２　採用する認証手段が定められているか？(企 15⑦、シ 13④)」

認証手段が定められている場合は「はい」、定められていない場合は「いいえ」としてください。

通信経路上で、送信元、送信先について相手の確認を行う必要があるため、認証の具体的手段について備考に記載してください。（認証手段の例：PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、の容易に解読されない方法）

### 「６０　通信方式として公衆網に対応しているか？」

本項目は、公衆網による通信に対応している場合は「該当」、そうでない場合は「非該当」としてください。

### 「６０．１　提供事業者に閉域性の範囲を確認しているか？(シ 13⑨)」

範囲を確認している場合は「はい」、確認していない場合は「いいえ」としてください。「はい」の場合は、確認した内容を備考に記載してください。

### 「６０．２　採用する認証手段が定められているか？(企 15⑦、シ 13④)」

認証手段が定められている場合は「はい」、定められていない場合は「いいえ」としてください。

通信経路上で、送信元、送信先について相手の確認を行う必要があるため、認証の具体的手段について備考に記載してください。（認証手段の例：PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法等）

### 「６１　通信方式として IP-VPN に対応しているか？」

本項目は、IP-VPN による通信に対応している場合は「該当」、そうでない場合は「非該当」としてください。

### 「６１．１　提供事業者に閉域性の範囲を確認しているか？(シ 13⑨)」

範囲を確認している場合は「はい」、確認していない場合は「いいえ」としてください。「はい」の場合は、確認した内容を備考に記載してください。

### 「６１．２　採用する認証手段が定められているか？(企 15⑦、シ 13④)」

認証手段が定められている場合は「はい」、定められていない場合は「いいえ」としてください。

通信経路上で、送信元、送信先について相手の確認を行う必要があるため、認証の具体的手段について備考に記載してください。(認証手段の例：PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、の容易に解読されない方法)

### 「６２　通信方式として IPsec-VPN＋IKE に対応しているか？」

本項目は、IPsec-VPN+IKE による通信に対応している場合は「該当」、そうでない場合は「非該当」としてください。

### 「６２．１　セッション間の回り込み等の攻撃への適切な対策をしているか？(企 15⑦、シ 13⑥)」

IPsec-VPN を利用する場合、オープンなネットワークでの接続を想定しているため、接続する各拠点においてセッション間の回り込みへの対策が必要となります。ルータ等のハードウェアの場合は機器において設定も含めた対策が必要となり、ソフトウェア型（ルータをソフトウェアで実装している場合等）の場合は、利用する端末での防護対策が必要となります。

対策している場合は「はい」、そうでない場合は「いいえ」としてください。

なお、IPsec-VPN を利用する場合の対策については、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(HISPRO）による「支払基金等へのレセプトオンライン請求用 IPsec＋IKE サービス」チェックリスト項目集が参考になります。

### 「６２．２　採用する認証手段が定められているか？(企 15⑦、シ 13④)」

認証手段が定められている場合は「はい」、定められていない場合は「いいえ」としてください。

通信経路上の送信元、送信先について相手の確認を行う必要があるため、認証の具体的手段について備考へ記載してください。(認証手段の例：PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、の容易に解読されない方法)

### 「６３　チャネル・セキュリティとして TLS1.2 以上のクライアント認証に対応しているか？」

本項目は、専用線、IP-VPN、IPsec-VPN を用いずにチャネル・セキュリティとして TLS1.2 以上（いわゆる SSL-VPN ではない）の証明書を用いたクライアント認証に対応している場合は「該当」、そうでない場合は「非該当」としてください。

※SSL-VPN は利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれます。SSL-VPN を利用する場合は備考に適切であることの根拠、必要な対策があればその内容を記載してください。

### 「６３．１　サーバ/クライアントともに「TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行っているか？(企 15⑦、シ 13⑥)」

TLS を利用する場合は、相手の確認の手段が「TLS 暗号設定ガイドライン」の「高セキュリティ型」によって規定されるため、規定された内容に従って設定している場合は「はい」、そうでない場合は「いいえ」としてください。

### 「６３．２　セッション間の回り込み等による攻撃への適切な対策を実施しているか？(企 15⑦、シ 13⑥)」

TLS を利用する場合、利用する端末にセッション間の回り込み等による攻撃を受ける可能性があるため、攻撃への防護対策について実施している場合は「はい」とし、詳細を備考に記載してください。そうでない場合は「いいえ」としてください。

### 「６４　ネットワーク上において、改ざんを防止する対策を行っているか？(シ 13⑨)」

中間者攻撃等による改ざんを防止する対策を行っている場合は、「はい」とし、具体的内容を備考に記載してください。(脅威例：メッセージ挿入、不正ソフトウェアの混入等)　そうでない場合は「いいえ」としてください。

### 「６５　施設間の経路上において、盗聴を防止する対策を行っているか？(シ 13⑩)」

盗聴を防止する対策を行っている場合は、「はい」とし具体的内容を備考に記載してください。(脅威例：クラッカーによるパスワード盗聴、本文の盗聴)　そうでない場合は「いいえ」としてください。

### 「６６　ネットワーク上において、なりすましへの対策を行っているか？(シ 13②、⑪)」

なりすましへの対策を行っている場合は、「はい」とし、具体的内容を備考に記載してください。(脅威例：セッション乗っ取り、IP アドレス詐称等)　そうでない場合は「いいえ」としてください。

### 「６７　データ送信元と送信先において、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行っているか？(シ 13④)」

本項目は、データの送信元と送信先において、データが通る経路である拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じた必要な単位で相手の確認を行っているかを問う項目です。対策を行っている場合は、「はい」とし具体的内容を備考に記載してください。(例：PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法等) そうでない場合は「いいえ」としてください。

### 「６８　ネットワークの経路制御・プロトコル制御を行える機器または機能を有するか？(シ 13⑤)」

本項目は、ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、異なる施設間を結ぶ通信経路の間で医療施設のルータを経由して送受信ができないように経路設定されていることを確認するものです。

「ネットワークの経路制御・プロトコル制御」とはネットワーク機器（ルータ、スイッチ、ファイアウォールなど)、又はそれと同等の機能を持つことを指しています。特に情報セキュリティリスクを極小化するために接続経路を限定したり、回り込みを禁止したりすることを指します。

機能を有する場合は「はい」、有していない場合は「いいえ」としてください。

### 「６９　ネットワークの経路制御・プロトコル制御に関わる機器または機能は、安全性を確認できるようなセキュリティ対策が規定された文書を示すことができるか？(企 15⑦、シ 13⑤、⑥)」

文書を示すことができる場合は「はい」、示すことができない場合は「いいえ」としてください。

### 「７０　医療機関等との通信経路について回り込みが行われないように経路設定を行っているか？(企 15⑦、シ 13⑤、⑥)」

回り込みが行われないように経路設定を行っている場合は「はい」、そうでない場合は「いいえ」としてください。

### 「７１　送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施しているか？(シ 13⑦)」

本項目は、データの送信元と送信先において、データそのものに対して暗号化等のセキュリティ対策を実施しているかを問う項目です。対策を行っている場合は「はい」とし、具体的内容を備考に記載してください。行っていない場合は「いいえ」としてください。
（対策例： S/MIME の利用、ファイルに対する暗号化、IPsec（ESP プロトコルを使用している場合等）又は TLS1.2 若しくは TLS1.3 の利用等）

### 「７１．１　暗号化を利用する場合、暗号化の鍵について電子政府推奨暗号のものを使用しているか？(企 14①)」

本項目は、暗号化等のセキュリティ対策を行っている場合に、暗号化の鍵に対する基準として、電子政府推奨暗号のものを使用しているかを問う項目です。使用している場合は「はい」とし、具体的内容を備考に記載してください。使用していない場合は「いいえ」としてください。

### 「７２　脅威に対する管理責任の範囲について、医療機関等に明確に示し、その事項を示す文書等を提示できるか？(経 1.3.2①、経 5.2.1①、経 5.3①、企 2①、④、⑤、シ 3②、13①)」

脅威に対する管理責任の範囲について、医療機関等に明確に示し、その事項を示す文書等を提示できる場合は、「はい」、そうでない場合は「いいえ」としてください。なおこれに該当する項目が、例えば契約書や付帯する覚書、あるいは SLA などに明確に記載されていれば、それらが該当する文書になります。その文書名、作成日等を備考欄に記載してください。

### 「７３　医療機関等から委託をされた範囲において、脅威に対する管理責任の範囲を医療機関等に明確に示し、その事項を示す文書等を提示できるか？(企 2①、④、⑤、シ 13①)」

文書等を提示できる場合は「はい」、提示できない場合は「いいえ」としてください。
（責任範囲となる例：通信機器、暗号化装置、認証装置等の提供、ネットワーク利用に対する患者への説明、個人情報の取扱いに関する情報）

### 「７４　リモートメンテナンスサービスを有しているか？」

本項目はサービスに対してリモートメンテナンスサービスを実施しているかを確認するものです。
有している場合は「該当」、有していない場合は「非該当」としてください。

### 「７４．１　リモートメンテナンスサービスに関し、不必要なリモートログインを制限する仕組みを有しているか？(シ 7⑫、シ 10.1、シ 18.1)」

本項目は、リモートメンテナンスサービスにおいて、利用者側がアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なリモートログインを防止することが可能かを確認するものです。
有している場合は「はい」、有していない場合は「いいえ」としてください。

### 「７５　回線の可用性等の品質に関して問題がないことを確認し、明確に文書等の証跡を残し、医療機関等に提示できるか？(企 15⑩)」

本項目は回線の可用性等の品質が、サービスの提供に対して問題ないことを文書等で医療機関等に明確に示しているかを確認するものです。
文書等が提示できる場合は「はい」、提示できない場合は「いいえ」としてください。

### 「７６　患者が情報を閲覧する機能があるか？」

本項目は患者が情報を閲覧する機能の有無について問う項目です。閲覧する機能がある場合は「該当」としてください。機能が無い場合は「非該当」としてください。

### 「７６．１　情報の閲覧のために公開しているサービスにおいて、医療機関等の内部システムに不正な侵入等が起こらないように対策を実施しているか？(企 8⑧、シ 7⑭)」

本項目は、患者への情報閲覧のサービスや機能から、医療機関等の内部システムに不正な侵入が起こらないようにしているかを問う項目です。不正な侵入への対策を実施している場合は「はい」としてください。実施していない場合は「いいえ」としてください。
（対策例：、システムやアプリケーションを切り分けした上での、ファイアウォール、アクセス監視、通信の TLS 暗号化、PKI 認証等の技術を用いた対策の実施等）

### 「７６．２　医療機関等が患者等へ情報セキュリティに関するリスクや情報提供目的について説明を行うために必要となる情報を資料として提示できるか？(企 8⑨)」

情報を資料として提示できる場合は「はい」としてください。そうでない場合は「いいえ」としてください。

### 「７６．３　説明資料では、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にしているか？(企 8⑨、シ 7⑭)」

本項目は、IT に係る以外の法的根拠等も含めた幅広い対策をたて、責任を明確にしているかを問う項目です。責任を明確にしている場合は「はい」としてください。明確にしていない場合は「いいえ」としてください。

## 法令で定められた記名・押印を電子署名で行うことについて

### 「７７　記名・押印が義務付けられた文書を扱っているか？」

本項目は、当該サービスが記名・押印を義務付けられた文書の作成、参照、保存などを行っているかどうかを確認するものです。記名・押印を義務付けられた文書の例としては、診断書、紹介状、放射線照射録などが挙げられます。義務付けられた文書を取り扱っている場合は「該当」としてください。取り扱っていない場合は「非該当」としてください。「該当」の場合は、従属質問に回答してください。これらを電子的に作成する場合には電子署名法に適合する電子署名が必要です。また、電子署名、タイムスタンプが付された文書を参照する場合には、電子署名、タイムスタンプの検証が必要になる場合があります。さらに電子文書をタイムスタンプの有効期限（一般的には 10 年程度）を超えて長期保存する場合には、真正性の確保のための長期署名技術、又はそれに準ずる措置を行う必要があります。

### 「７７．１　HPKI 対応、又は認定認証局もしくは公的個人認証サービスが発行する証明書対応の署名機能があるか？(企 14①、シ 15①)」

本項目は、記名・押印を義務付けられた文書の署名機能を有するかを確認するものです。安全管理ガイドラインにおいて HPKI 証明書、又は認定認証局もしくは公的個人認証サービスが発行する証明書を用いることが求められており、電子署名を付与するために必須の機能です。署名機能を有している場合は「はい」、有していない場合は「いいえ」としてください。

「はい」の場合は、備考に対応している証明書の種類（HPKI、認定認証局、公的個人認証サービス等）を記入してください。また、「いいえ」の場合は、電子署名を付与するための別の手段を提供する必要があり、備考に署名機能の提供方法を記載してください。記名・押印を義務付けられた文書の作成機能がない場合は「対象外」としてください。

### 「７７．２　HPKI 対応、又は認定認証局もしくは公的個人認証サービスが発行する証明書対応の検証機能があるか？(企 14①、シ 15①)」

本項目は、記名・押印を義務付けられた文書の検証機能を有するかを確認するものです。安全管理ガイドラインにおいて HPKI 証明書、又は認定認証局もしくは公的個人認証サービスが発行する証明書の検証が求められており、電子署名付き文書を参照するために必須の機能です。署名検証機能を有している場合は「はい」、有していない場合は「いいえ」としてください。

「はい」の場合は、備考に対応している証明書を記入してください。また、「いいえ」の場合は、電子署名を検証するための別の手段を提供する必要があり、備考に署名検証機能の提供方法を記載してください。記名・押印を義務付けられた文書の参照機能がない場合は「対象外」としてください。

### 「７７．２．１　特定の国家資格の確認を行う必要がある場合に、電子的に検証できる機能があるか？(企 14①、シ 15①)」

本項目は、特定の国家資格（医師等に限らず国家資格を有する者）の確認を行う際、電子的に国家資格を検証できる機能を有するかを確認するものです。電子的に検証できる機能を有している場合は「はい」、有していない場合は「いいえ」としてください。また、「いいえ」の場合、電子的に検証するための別の手段を提供する必要があり、備考に電子的に検証する方法を記載してください。特定の国家資格の確認を行う必要が無い場合は「対象外」としてください 。

### 「７７．３　総務省の「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が付与可能か？(企 14①、シ 15①)」

本項目は、タイムスタンプの付与可能かを確認するものです。電子文書作成においては、電子署名を行った後、タイムスタンプを付与する必要があります。安全管理ガイドラインにおいてタイムスタンプは、総務省の「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ものを使用することが求められています。付与可能な場合は「はい」としてください。そうでない場合は「いいえ」としてください。

「はい」の場合は、対応するタイムスタンプサービスを記載してください。また、「いいえ」の場合は、タイムスタンプを付与するための別の手段を提供する必要があり、備考にタイムスタンプの付与方法を記載してください。記名・押印を義務付けられた文書の作成機能がない場合は「対象外」としてください。

### 「７７．４　総務省の「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が検証可能か？(企 14①、シ 15①)」

本項目は、タイムスタンプの検証可能かを確認するものです。電子文書作成においては、電子署名を行った後、タイムスタンプを付与する必要があります。安全管理ガイドラインにおいてタイムスタンプは、総務省の「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ものを使用することが求められています。検証可能な場合は「はい」としてください。そうでない場合は「いいえ」としてください。

「はい」の場合は対応するタイムスタンプサービスを記載してください。また、「いいえ」の場合は、タイムスタンプを検証するための別の手段を提供する必要があり、備考にタイムスタンプの検証方法を記載してください。記名・押印を義務付けられた文書の参照機能がない場合は「対象外」としてください。

### 「７７．５　保存期間中の文書の真正性を担保する仕組みがあるか？(企 14①、シ 15①)」

本項目は記名・押印を義務付けられた文書の保存機能を確認するものです。法定保存期間が 10 年を超えるものや、法定保存期間を越えて 10 年以上保存するものについてはタイムスタンプ単独では真正性を確保できません。タイムスタンプの有効期限を超えて長期保存するための ISO 規格である CAdES、XAdES、PAdES など

の機能、又はそれと同等の真正性を確保する機能があるかどうかの確認を行います。機能を有している場合は「はい」、有していない場合は「いいえ」としてください。

「はい」の場合は、備考に具体的な実現方式を記載してください。「いいえ」の場合は、真正性を確保するための別の手段を提供する必要があり、備考に真正性確保手段を記載してください。記名・押印を義務付けられた文書の保存機能がない場合は「対象外」としてください。

### 「７８　上記タイムスタンプを付与する時点で有効な電子証明書を用いているか？(企 14①、シ 15①)」

上記タイムスタンプを付与する時点で有効な電子証明書を用いている場合は「はい」としてください。そうでない場合は「いいえ」としてください。

### 「７９　電子署名に用いる秘密鍵の管理が、認証局が定める「証明書ポリシー」（CP）等で定める鍵の管理の要件を満たして行われるよう管理しているか？(企 14②、シ 15①)」

電子署名に用いる秘密鍵の管理を行っており、認証局が定める「証明書ポリシー」（CP）等で定める管理要件を満たして管理している場合は「はい」として、備考に管理要件である認証局が定める「証明書ポリシー」（CP）等を記載してください。そうでない場合は「いいえ」、秘密鍵の管理を行っていない場合は「対象外」としてください。

## 真正性の確保について

### 「８０　記録の確定操作が必要な情報を扱っているか？」

記録の確定操作が必要な情報を扱っている場合は「該当」、扱っていない場合は「非該当」としてください。

### 「８０．１　入力者及び確定者を正しく識別し、認証を行う機能があるか？(企 15⑬、シ 14④)」

本項目は、人による確定操作が必要な場合（電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合）を対象としています。そうでない場合（臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合）は「対象外」としてください。入力者及び確定者を識別し、認証する機能を有している場合は「はい」、有していない場合は「いいえ」としてください。

### 「８０．２　区分管理を行っている対象情報ごとに、権限管理（アクセスコントロール）の機能があるか？(企 15⑬、シ 14④)」

真正性を担保するためには、故意または過失による追記、修正および削除ならびに混同を防止することが必要です。そのために、本項目は、操作者の権限に応じてアクセスできる情報を区分単位で制限する機能を有するかを確認するものです。

アクセス者の権限に基づき各区分において操作内容に制限を加えることが可能な場合は「はい」、そうでない場合は「いいえ」としてください。システムにより記録が作成される場合など本機能が不要な場合は「対象外」とし、理由を備考に記載してください。

### 「８０．３　権限のある利用者以外による作成、追記、変更を防止する機能があるか？(企 15⑬)」

本項目は、一般利用者に対して権限管理の機能を有するかを確認するものです。

権限管理の機能がある場合は「はい」、そうでない場合は「いいえ」としてください。システムにより記録が作成される場合など本機能が不要な場合は「対象外」とし、理由を備考に記載してください。

### 「８０．４　サービス事業者内の利用者の権限管理の機能があるか？(企 15⑬)」

本項目は、一般利用者ではなく、サービス事業者内の利用者に対して権限管理の機能を有するかを確認するものです。権限管理の機能がある場合は「はい」としてください。そうでない場合は「いいえ」としてください。サービス事業者が権限管理機能を利用できない等の場合は「対象外」としてください。

### 「８０．５　サービス事業者内の利用者が作成、追記、変更を防止する機能があるか？(企 15⑬)」

本項目は、一般利用者ではなく、サービス事業者内の利用者に対して、権限管理の機能を有するかを確認するものです。権限を制限等する機能を有している場合は「はい」、有していない場合は「いいえ」としてください。サービス事業者が権限管理機能を利用できない等の場合は「対象外」としてください。

### 「８０．６　システムが端末を管理することによって、権限を持たない者からのアクセスを防止する機能があるか？(企 15⑬)」

本項目は、システムとして利用者を認証する機能がない場合等に、業務アプリケーション等がアクセスできる端末を制限する機能を有するかを確認するものです。

利用可能な端末を管理する機能を有している場合は「はい」、有していない場合は「いいえ」としてください。利用者を認証する機能があるなど本機能が不要な場合は「対象外」とし、理由を備考に記載してください。

### 「８０．７　システムがサービス事業者の保守等端末を管理することによって、権限を持たない者からのアクセスを防止する機能があるか？(企 15⑬)」

本項目は、システムとしてサービス事業者内の利用者を認証する機能がない場合等に、業務アプリケーション等がアクセスできる端末を制限する機能を有するか確認するものです。

システムが端末を管理する機能を有している場合は「はい」、有していない場合は「いいえ」としてください。サービス事業者内の利用者を認証する機能があるなど本機能が不要ならば「対象外」としてください。

### 「８１　システムは記録を確定する機能があるか？(企 15⑬、シ 14⑧)」

本項目は、確定機能を有するかを確認するものです。

安全管理ガイドラインで求められている記録の確定機能を有している場合は「はい」、有していない場合は「いいえ」としてください。確定が必要な情報を管理していない場合は、「対象外」としてください。「はい」ならば、従属質問に回答してください。

### 「８１．１　確定情報には、入力者及び確定者の識別情報、信頼できる時刻源を用いた作成日時が含まれているか？(企 15⑬、シ 14⑧)」

本項目は、記録の確定の必須要件である、記録がいつ・誰によって作成されたかを明確にするための仕組みを有するかを確認するものです。

入力者及び確定者の識別情報と信頼できる時刻源に基づく作成日時が記録される場合は「はい」、そうでない場合は、「いいえ」としてください。

### 「８１．２　「記録の確定」を行うにあたり、内容の確認をする機能があるか？(企 15⑬、シ 14⑧)」

本項目は、記録の確定の際には確定者による内容の確認が必須要件であるため、その機能を有するかを確認するものです。

記録を確定するにあたり、内容を確認する機能を有している場合は「はい」、有していない場合は「いいえ」としてください。

### 「８１．３　確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止する機能があるか？(企 15⑬、シ 14⑧)」

真正性の確保のためには、確定後のデータに対し、正当な権限に基づかないいかなる追記、修正および削除も行われていないことを保証しなければなりません。本項目は、そのための機能を有するかを確認するものです。

確定後のデータに対して権限者以外の追記、修正および削除ができないようになっている場合は「はい」、そうでない場合は「いいえ」としてください。

### 「８２　装置が確定機能を持っていない場合、記録が作成される際に、当該装置の管理責任者や操作者の識別情報、作成日時を含めて記録する機能があるか？（企 15⑬、シ 14⑧)」

本項目は、臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合に関しての質問です。運用でそれを実現しようとする際に、装置が記録自体に作成責任者の識別情報や作成日時を含めて記録する機能を有しているかを確認するものです。

装置からのデータに識別情報（作成責任者の氏名あるいは識別情報)、作成日時が含まれ記録される場合は「はい」、記録されない場合は「いいえ」としてください。

### 「８３　確定された診療録等が更新された場合、更新履歴を保存し、更新前後の内容を参照する機能があるか？(企 15⑬、シ 14⑧)」

確定済みの診療録等に追記や修正などの更新が行われた場合、それが正当な行為なのか、不正な行為なのかを判別するために、記録の更新内容、更新日時、更新者の識別情報が関連付けて保存され、必要な時に参照できなければなりません。本項目は、そのための機能を有しているかを確認するものです。

確定情報への更新内容、更新日時を記録するとともに、更新前と更新後の内容を参照する機能を有している場合は「はい」、有していない場合は「いいえ」、対象機器が本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

### 「８３．１　同じ診療録等に対して複数回更新が行われた場合、更新の順序性を識別できる機能があるか？(企 15⑬、シ 14⑧)」

同じ診療録等に対して複数回更新が行われた場合、それぞれの更新がどの順序で行われたかが重要になる場合があり、そのため更新の順序性を識別できるようにする機能が求められます。例えば更新時刻を分単位で記録している場合でも、同じ時刻の更新記録の記録された順序が分かるようにしなければなりません。

更新の順序を識別できる機能を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

### 「８４　代行入力の承認機能があるか？(企 13⑧、企 15⑬、シ 14⑧)」

情報入力は診療行為の実施者自らが行うことが原則ですが、代行者による入力が必要になる場合があります。本項目は、そのような代行入力において、作成責任者による代行入力の実施に関する承認機能（確定時の承認とは別）を有するかを確認するものです。対象システムの権限としてあらかじめ代行権限が付与されているものも承認の中に含みます。

承認機能を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。「はい」ならば、従属質問に回答してください。

### 「８４．１　代行入力が行われた場合、誰の代行がいつ誰によって行われたかの管理情報を、その代行入力の都度、記録する機能があるか？(企 15⑬、シ 14⑧)」

代行入力での運用が行われる場合、例えば医師の入力の代行を医師事務作業補助者が行う場合に、誰の代行がいつ誰によって行われたかを記録することが必要です。本項目は、そのような管理情報を、その代行操作の都度記録

する機能を有するかを確認するものです。

機能を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

### 「８４．２　代行入力により記録された診療録等に対し、確定者による「確定操作（承認）」を行う機能があるか？(企 15⑬、シ 14⑧)」

代行入力での運用が行われる場合、代行入力によって入力された診療録等の情報を、できるだけ速やかに作成責任者による「確定操作（承認）」が行われることが必要です。本項目は、そのような「確定操作（承認）」機能を有するかを確認するものです。

機能を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。補足事項がある場合は、備考に記載してください。

### 「８５　システムがどのような機器・ソフトウェアで構成され、どのような場面、用途で利用されるのか明確にしているか？(企 15⑬、シ 9①)」

本項目は、サービス事業者がサービスを提供するために使用する機器・ソフトウェア構成等を、使用場面、用途ごとに明確にしている場合は「はい」、そうでない場合は「いいえ」としてください。

### 「８６　機器・ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスが規定されているか？(企 15⑬、シ 9②)」

本項目は、サービス事業者がサービスを提供するために使用する機器・ソフトウェアの改訂履歴を検証するためのプロセス、及び導入の際に実際に行われた作業の妥当性を検証するためのプロセスが規定されている場合は「はい」、そうでない場合は「いいえ」としてください。

### 「８７　機器・ソフトウェアの品質管理に関する作業内容をルールに定めて、策定したルールに基づいて従業者等への教育を実施しているか？(企 15⑪、⑬)」

本項目は、サービス事業者がサービスを提供するために使用する機器・ソフトウェアを、使用開始あるいは更新するときのルールに品質管理に関する作業内容を規定して、その内容に基づく従業者教育を実施している場合は「はい」、そうでない場合は「いいえ」としてください。

### 「８８　システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施しているか？(経 1.2.1、経 3.3.2、企 15⑫、⑬)」

本項目は、サービス事業者がサービスを提供するために使用する機器の構成、ソフトウェアの動作状況を、定期的に内部で監査している場合は「はい」、そうでない場合は「いいえ」としてください。

### 「８９　通信の相手先が正当であることを確認するための相互認証を実施しているか？(シ 13⑫)」

本項目は、医療機関等と外部との通信において、相手先が正当であることを確認するための相互認証を実施している場合は「はい」、そうでない場合は「いいえ」としてください。医療機関等と外部との通信がない場合は「対象外」とし、備考にその旨を記載してください。

### 「９０　ネットワークの転送中に改ざんされていないことを保証する機能を有しているか？(企 15⑦、シ 13⑧、⑨、⑪)」

本項目は、改ざんされないことを保証するものではなく、たとえば通信経路上でデータが変更されていてもそれを検知して再送要求などを実施することによる等により改ざんされていないことを保証するものです。そのた

め、改ざん検知とリカバリ機能を有しているかを確認する質問と同義です。転送中に改ざんされていないことを保証する機能を有している場合は「はい」として、備考にその方式を記載ください。有していない場合は「いいえ」としてください。

### 「９１　サービス事業者の機器・システムはリモートログインの機能を制限しているか？(企 15⑬、シ 7⑫)」

本項目は、目的外利用を防止するためにリモートアクセスの機能について制限を行っているかを確認するものです。サービスを提供する機器等に対してサービス事業者がリモートからアクセスする機能を制限している場合は「はい」、そうでない場合は「いいえ」としてください。

## 見読性の確保について

### 「９２　患者ごとの全ての情報の所在が日常的に管理されているか？(企 8④、企 15⑬、シ 4①)」

媒体の種類に関わらず、患者ごとの情報の全ての所在が速やかに明示できる場合「はい」、そうでない場合は「いいえ」としてください。

### 「９３　電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理しているか、また、見読化手段である機器・ソフトウェア・関連情報等は常に整備された状態になっているか？(企 15⑬、シ 5④)」

電子媒体に保存された全ての情報とその見読化手段を対応付けて管理し、見読化手段の機器等が常に整備された状態になっている場合は「はい」、そうでない場合は「いいえ」としてください。

### 「９４　目的に応じて速やかに検索結果を出力する機能又はサービスがあるか？(企 15⑬、シ 9④)」

見読性とは、保存された情報を目的に対して支障のないレスポンスやスループットと操作性で、肉眼で見読可能な状態にできることです。本項目は、見読性の確保を確認するためのものです。『速やかに』とは、権限保有者からの「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応じて、それぞれの目的に対し支障のない応答時間やスループット、操作方法で提供できることを示します。

使用目的に応じて、適切な時間内に結果が出力できる機能またはサービスを有している場合は「はい」、有していない場合は「いいえ」としてください。

### 「９５　システム障害に備えた冗長化手段や代替的な見読化手段はあるか？(企 11.2、企 15⑬、シ 11①、シ 11.1)」

システム障害に備えた冗長化手段や代替的な見読化手段を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。

### 「９５．１　冗長化手段があるか？(企 11.2、企 15⑬、シ 11.1)」

本項目は、冗長化の具体的な内容について確認するものです。冗長化手段を有している場合は「はい」、有していない場合は「いいえ」、対象システムが本項目に該当しない場合は「対象外」としてください。「はい」の場合は、具体的な内容を備考に記載してください。

### 「９５．２　システム障害に備えた代替的な見読化手段があるか？(企 15⑬、シ 11①)」

本項目は、代替的な見読化手段の具体的な内容について確認するものです。代替的な見読化手段には、①一般的な記録形式（例えば PDF、XML、JPEG などのファイルフォーマット）で記録しておくことによって、標準的な

見読化装置で見読可能とする方法と、②別の専用の代替的な見読化手段を用意する方法とがあります。いずれかの方法を有している場合は「はい」、有していない場合は「いいえ」としてください。代替的な手段の具体的な内容を備考に記載してください。

## 保存性の確保について

### 「９６　不正ソフトウェアによる情報の破壊、混同等が起こらないように、システムで利用するソフトウェア、機器及び媒体の管理を行っているか？(経 3.4、企 15⑥、⑬、シ 7④、シ 8③、シ 8.1)」

本項目は、保存性を確保するために、コンピュータウイルスなどの不適切なソフトウェア等による情報の破壊、混同等を防ぐための適切な管理が行われているかを確認するものです。
行われている場合は「はい」、行われていない場合は「いいえ」としてください。

### 「９７　記録媒体及び記録機器の院内での保管及び取扱いについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？また、クラウドサービスを提供する場合において、サービス事業者による記録媒体及び記録機器の保管及び取扱いについて SLA 等の文書に含めて医療機関等に提供されているか？(企 15③、④、⑬、シ 12.2)」

保存性の確保のために、医療機関等には、記録媒体及び記録機器の保管及び取扱いについての運用管理規程の作成と、関係者への教育が求められます。本項目は、その運用管理規程作成のために、機器における記録媒体や記録機器の保管や取り扱い（例えば、記録媒体の品質保証期間、保存場所の推奨環境等）について、取扱説明書等の文書として提供されているかを確認するものです。またクラウドサービスを提供する場合においては、サプライチェーンの構成を明確にし、クラウドサービス事業者間の責任分解点を明示した SLA 等が必要です。

以上のような取扱説明書や SLA などで運用管理規程作成のための情報が、提供されている場合は「はい」、そうでない場合は「いいえ」、対象となる製品が記憶媒体や記録機器を有さない場合は「対象外」としてください。

### 「９８　情報の保存やバックアップについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？(企 15③、④、⑬、企 15.1、シ 12.2)」

保存性の確保のために、医療機関等は、情報を保存する場所や、その場所ごとの保存可能容量、期間、リスク、レスポンス、バックアップ頻度、バックアップ方法等を運用管理規程にまとめ、関係者に周知することが求められます。本項目は、その運用管理規程作成のために、機器における情報の保存方式やバックアップ手順について、取扱説明書等の文書として提供されているかを確認するものです。

提供されている場合は「はい」、そうでない場合は「いいえ」、対象となる製品が記憶媒体や記録機器を有さない場合は「対象外」としてください。

### 「９９　システムが保存する情報へのアクセスについて、履歴を残しているか？(経 4.2、企 5①、④、企 15⑬、シ 17①)」

本項目は、保存性確保のために機器に求められる、情報に対するアクセス履歴を保存する機能を有するかを確認するものです。ここでのアクセス履歴とは、医療情報システムの動作に関するアプリケーションログだけではなく、保存された情報に対する通常の操作以外でのアクセス（例：データベースへの直接ブラウズ等）にも対応するものです。

そのような機能を有している場合は「はい」、有していない場合は「いいえ」、対象となる製品が情報を保持しない場合は「対象外」としてください。「はい」ならば、従属質問に回答してください。

**「９９．１　システムが保存する情報へのアクセスについてその履歴を管理しているか？(経 4.2、企 5②、企 15⑬、シ 17①)」**

本項目は、アクセス履歴を管理しているかを確認するものです。
管理している場合は「はい」、していない場合は「いいえ」、対象となるシステムが情報を保持しない場合は「対象外」としてください。

**「１００　システムが保存する情報がき損した時に、バックアップされたデータ等を用いて、き損前の状態に戻せるか、又はもし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしているか？(経 3.4.1、企 15⑬、シ 11①、シ 18①、シ 18.1)」**

本項目は、システムが保存する情報がき損した場合に、事前に作成したバックアップデータを用いるなどして、き損前の状態に回復させることができるかを確認するものです。もし、戻せない場合は損なわれた範囲が容易に分かるようにする必要があります。
上記の運用ができる場合は「はい」、できない場合は「いいえ」、対象となるシステムが情報を保存しない場合は「対象外」としてください。
き損前と同一状態に戻した際には、バックアップからの復元であることを記録することが望ましいです。

**「１０１　システムの移行の際に診療録等のデータを、標準形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式にて出力及び入力できる機能があるか？(企 15⑬、シ 5①、シ 5.2)」**

標準形式とは「厚生労働省標準規格」を始めとする業界標準や国際標準等で定められた形式のことです。変換が容易なデータ形式とは CSV、XML 等のような、特定のアプリケーションに依存しないデータ形式のことです。本項目は、システム更新時の移行が迅速に行えるように、上記のようなデータ形式で診療録等のデータを出力及び入力できる機能を有しているかを確認するものです。
機能を有している場合は「はい」、有していない場合は「いいえ」、対象となるシステムが情報を保存しない場合は「対象外」としてください。

**「１０２　マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能またはサービスを備えているか？(企 15⑬、シ 5②)」**

本項目は、過去の記録については当時のマスタを参照して表示するなど、システムやサービスで対応することができるかを問うています。
マスタデータベースの変更の際に、過去の診療記録等の情報に対する内容の変更が起こらないような機能を備えている場合、または機能としては備えていないものの、内容の変更が起らない形で変更作業を実施するサービスを提供できる場合は、「はい」、できない場合は「いいえ」、対象となるシステムが情報を保存しない場合は「対象外」としてください。

**「１０３　外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持できるか？(シ 5③)」**

以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持できる場合は、「はい」、できない場合は「いいえ」としてください。

**「１０４　SLA 等に医療機関等に対して設備の条件を提示して、記録媒体、回線または設備が劣化した場合は SLA 等の要件を満たすように更新できるか？(企 15⑤、シ 12⑤、シ 12.2)」**

本項目は、SLA 等で提示した条件に対して適切に運用管理できるかを確認するものです。適切に運用管理できる場合は「はい」、できない場合は「いいえ」としてください。

## 診療録等をスキャナ等により電子化して保存する場合について

### 「１０５　診療録などをスキャナなどにより電子化して原本として保存する機能があるか？」

スキャナなどによる電子化により法令等で作成又は保存を義務付けられている診療録等の情報を原本として電子保存する機能がある場合は「該当」、機能がない場合は「非該当」としてください。「該当」ならば、従属質問に回答してください。

### 「１０５．１　光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いているか？(企 16①、シ 16①)」

スキャナ等による電子化においては、医療に関する業務等に支障が生じないように、スキャンによる情報量低下を防ぎ、保存義務を満たす情報として必要な情報量を確保することが求められます。本項目は、安全管理ガイドラインに例示されているユースケース毎に個別に定められた規格・基準を満たす形でスキャナを使用しているかを確認するものです。

使用している場合は「はい」、そうでない場合は「いいえ」、サービス事業者から医療機関等にスキャナを提供しない場合は「対象外」としてください。どのユースケースに適合するシステムかについては、備考に記載してください。

### 「１０５．２　電子署名等を付与する機能があるか？(経 4.1、企 16③、⑦、シ 1①、シ 15①)」

本項目は、改ざん防止のために、スキャンした電子情報に対して安全管理ガイドラインに適合する電子署名等を付与する機能を有するかを確認するものです。

機能を有している場合は「はい」、有していない場合は「いいえ」としてください。いずれの場合も他のシステムと組み合わせて機能を実現する場合はその実現方式を備考に記載してください。電子署名を付与する必要がない情報のみを扱う場合は「対象外」としてください。

### 「１０６　診療録などをスキャナなどにより電子化して参照情報として保存する機能があるか？」

スキャナなどによる電子化により法令等で作成又は保存を義務付けられている診療録等の情報を参照情報として電子保存する機能を有している場合は「該当」、有していない場合は「非該当」としてください。「該当」ならば、従属質問にも回答してください。

### 「１０６．１　光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いているか？(企 16①、シ 16①)」

スキャナ等による電子化においては、医療に関する業務等に支障が生じないように、スキャンによる情報量低下を防ぎ、保存義務を満たす情報として必要な情報量を確保することが求められます。本項目は、安全管理ガイドラインに例示されているユースケース毎に個別に定められた規格・基準を満たす形でスキャナを使用しているかを確認するものです。

使用している場合は「はい」、そうでない場合は「いいえ」、サービス事業者から医療機関等にスキャナを提供しない場合は「対象外」としてください。どのユースケースに適合するシステムかを備考に記載してください。

# 付録．作成者名簿

作成者（社名五十音順）

| | | |
|---|---|---|
| 渡邊　克也 | イーグロース（株） | |
| 武者　義則 | ウィーメックスヘルスケアシステムズ（株） | ◎JAHIS 主査 |
| 有馬　一閣 | （株）NTT データ | |
| 木戸　須美子 | キヤノンメディカルシステムズ（株） | |
| 下野　兼揮 | （株）グッドマン | ◎JIRA 主査 |
| 高野　博明 | コニカミノルタ　（株） | |
| 平田　泰三 | JAHIS 特別委員 | |
| 野津　勤 | （株）システム計画研究所 | |
| 山本　智仁 | セコム　（株） | |
| 松元　恒一郎 | （一社）電子情報技術産業協会 | |
| 日高　昇治 | （一社）日本クラウド産業協会 | |
| 村松　和彦 | 日本光電工業（株） | |
| 村田　公生 | 富士フイルム（株） | |
| 梶山　孝治 | 富士フイルムヘルスケア（株） | |
| 茗原　秀幸 | 三菱電機（株） | |

# 改訂履歴

| 改定履歴 | | |
|---|---|---|
| 日付 | バージョン | 内容 |
| 2013/04 | Ver. 1.0 | 初版 |
| 2014/11 | Ver. 2.0 | 安全管理ガイドライン 7~9 章対応、タイトルの変更 |
| 2017/7 | Ver. 3.0 | 安全管理ガイドライン第 5 版対応等 |
| 2017/11 | Ver. 3.0a | 誤記の修正 |
| 2021/03 | Ver. 4.0 | 安全管理ガイドライン第 5.1 版対応等<br>サービス事業者対応、タイトルの変更 |
| 2023/06 | Ver. 4.1 | 安全管理ガイドライン第 5.2 版対応等 |
| 2024/＊＊ | Ver.5.0 | 安全管理ガイドライン第 6.0 版対応等 |

（ＪＡＨＩＳ標準　２４－＊＊＊）

２０２４年＊月発行

ＪＡＨＩＳ「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書」
ガイド　Ver. 5.0

発行元　一般社団法人　保健医療福祉情報システム工業会
〒１０５－０００４　東京都港区新橋２丁目５番５号
(新橋２丁目ＭＴビル５階)

電話　03-3506-8010　　FAX　03-3506-8070