JAHIS

ＪＡＨＩＳ標準 20－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.4.0

２０２０年ｘ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

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.4.0

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/サービス事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およ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。今回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）に拡張するため、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 ASP・SaaS・AI・IoT 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 5 版（2017.5 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。

2020 年 x 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。

© JAHIS 2020

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. 記号および略語 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） 6

「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 6

7. チェックリストの解説（製造業者編） 10

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(6.2) 10
物理的安全対策(6.4) 10
技術的安全対策(6.5) 10
情報及び情報機器の持ち出しについて(6.9) 12
災害、サイバー攻撃等の非常時の対応(6.10) 12
外部と個人情報を含む医療情報を交換する場合の安全管理(6.11) 12
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(6.12) 14
真正性の確保について(7.1) 15
見読性の確保について(7.2) 18
保存性の確保について(7.3) 18
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(9.) 20

8. チェックリスト（サービス事業者編） 21

「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 21

9. チェックリストの解説（サービス事業者編） 30

診療録及び診療諸記録を外部に保存する際の基準(8.) 30
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(6.2) 31
組織的安全管理対策（体制、運用管理規程）(6.3) 32
物理的安全対策(6.4) 32
技術的安全対策(6.5) 33
人的安全対策(6.6) 36
情報の破棄(6.7) 37
情報システムの改造と保守(6.8) 38
情報及び情報機器の持ち出しについて(6.9) 41
災害、サイバー攻撃等の非常時の対応(6.10) 43
外部と個人情報を含む医療情報を交換する場合の安全管理(6.11) 44
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(6.12) 48

© JAHIS 2020

真正性の確保について(7.1) 50
見読性の確保について(7.2) 54
保存性の確保について(7.3) 54
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(9.) 56
付録．作成者名簿 58
改訂履歴 59

© JAHIS 2020

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のセキュリティに関して、安全管理ガイドラインへの技術的な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に適応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の説明を求める際の、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、ある型名の製品/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。その中に他製造業者の品（例えば OS やミドルウェア）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。

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			e-文書法に基づいて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	～	６６	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。
６７	～	９３	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。
９４			e-文書法に基づいて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。

© JAHIS 2020

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5版

http://www.mhlw.go.jp/stf/shingi2/0000166275.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%20koumoku.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）・SSL/TLS暗号設定ガイドライン Ver.2.0

https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-2.0.pdf

(4) HIMSS/NEMA Standard HN 1-2013 Manufacturer Disclosure Statement for Medical Device Security

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

和訳版（JIRA 作成）
http://www.jira-net.or.jp/commission/system/info1.html

(5) 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

© JAHIS 2020

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、書き換え、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。

© JAHIS 2020

4. 記号および略語

本書では、次の記号および略語・表記を用います。

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
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

© JAHIS 2020

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	：対象となる製品の製造業者/サービス事業者の名称を記入します。
製品/サービス名称	：製品/サービスの名称・型名を記入します。
バージョン	：製品/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。

※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。

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	：製品/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。

（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。

提供する製品/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。

© JAHIS 2020

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 5 版対応）

製造業者　：	作成日　：
製品名称　：	バージョン　：
医療機関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(6.2)	
1　扱う情報のリストを提示してあるか？(6.2.C1)	はい　いいえ　対象外　備考____
物理的安全対策(6.4)	
2　覗き見防止の機能があるか？(6.4.C5)	はい　いいえ　対象外　備考____
技術的安全対策(6.5)	
3　離席時の不正入力防止の機能があるか？(6.5.C4)	はい　いいえ　対象外　備考____
4　アクセス管理の機能があるか？(6.5.C1)	はい　いいえ　対象外　備考____
4．1　アクセス管理の認証方式は？(6.5.C1) ・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） ・その他（具体的な方法を備考に記入してください） ・上記のうちの二要素を組み合わせた認証 （具体的な組み合わせを備考に記入してください）	 はい　いいえ　対象外　備考____ はい　いいえ　対象外　備考____ はい　いいえ　対象外　備考____ はい　いいえ　対象外　備考____ 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？(6.5.C11 管理者(1)～6.5.C11 管理者(3))	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？(6.5.C3)	はい　いいえ　対象外　備考____
4．2　利用者別、職種別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	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？(6.5.C7)	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？(6.5.C7)	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？(6.5.C8)	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？(6.5.C9)	はい　いいえ　対象外　備考____
6　不正ソフトウェア対策を行っているか？(6.5.C10)	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？(6.5.C12)	はい　いいえ　対象外　備考____
情報および情報機器の持ち出しについて(6.9)	
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？(6.9.C9)	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？(6.9)	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？(6.9.C6、6.9.C7)	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(6.10)	
11　非常時アカウント又は、非常時機能を持っているか？(6.10.C3)	はい　いいえ　対象外　備考____
外部と個人情報を含む医療情報を交換する場合の安全管理(6.11)	
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？(6.11)	はい　いいえ　対象外　備考____
12．1　なりすましの対策（認証）機能を有するか？(6.11.C3)	はい　いいえ　対象外　備考____
12．2　データの暗号化（S/MIME、ファイル暗号化など）が可能か？(6.11.C5)	はい　いいえ　対象外　備考____

© JAHIS 2020

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？(6.11.C4)	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は、安全管理ガイドラインを満たす設定が可能か？(6.11.C4)	はい	いいえ	対象外	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？(6.11.C4、C10)	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？(6.11.C7)	はい	いいえ	対象外	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？(6.11.C7)	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(6.12)				
１３　記名・押印が義務付けられた文書を扱っているか？(6.12.C(1))	はい	いいえ	対象外	備考____
１３．１　HPKI 対応もしくは認定認証局が発行する証明書対応の署名機能があるか？(6.12.C(1))	はい	いいえ	対象外	備考____
１３．２　HPKI 対応もしくは認定認証局が発行する証明書対応の検証機能があるか？(6.12.C(1))	はい	いいえ	対象外	備考____
１３．３　日本データ通信協会認定のタイムスタンプが付与可能か？(6.12.C(2))	はい	いいえ	対象外	備考____
１３．４　日本データ通信協会認定のタイムスタンプが検証可能か？(6.12.C(2))	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？(6.12.C(2))	はい	いいえ	対象外	備考____
真正性の確保について(7.1)				
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？(7.1.C 医療(1).a-1)	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？(7.1.C 医療(1).a-2)	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？(7.1.C 医療(1).a-2)	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？(7.1.C 医療(1).a-3)	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？(7.1.C 医療(2).a-1)	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？(7.1.C 医療(2).a-1)	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？(7.1.C 医療(2).a-2)	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、書き換え、消去及び混同を防止する機能があるか？(7.1.C 医療(2).a-4)	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？(7.1.C 医療(2).b-1)	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？(7.1.C 医療(3)-1)	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？(7.1.C 医療(3)-2)	はい	いいえ	対象外	備考____
１９　代行入力の承認機能があるか？(7.1.C 医療(4))	はい	いいえ	対象外	備考____
１９．１　代行入力が行われた場合、誰の代行が誰によっていつ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？(7.1.C 医療(4)-2)	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を、確定者による「確定操作（承認）」を行う機能があるか？(7.1.C 医療(4)-3)	はい	いいえ	対象外	備考____

© JAHIS 2020

見読性の確保(7.2)				
２０　目的に応じて速やかな検索結果の出力機能があるか？(7.2.C(3))	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？(7.2.C(4))	はい	いいえ	対象外	備考____
２１．１　冗長化手段があるか？(7.2.C(4))	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？(7.2.C(4))	はい	いいえ	対象外	備考____
保存性の確保(7.3)				
２２　いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同が起こらないようにするための防護機能があるか？(7.3.C 医療(1)-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？(7.3.C医療(2)-1)	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？(7.3.C 医療(2)-2)	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？(7.3.C 医療(2)-4)	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？(7.3.C 医療(2)-4)	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？ (7.3.C 医療(2)-5)	はい	いいえ	対象外	備考____
２７　記録媒体が劣化する以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？(7.3.C 医療(3)-1)	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？(7.3.C 医療(4)-1)	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？(7.3.C 医療(4)-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(9.)				
３０　診療録などをスキャナなどにより電子化して保存する機能があるか (9.1.C1)(9.4)	はい	いいえ	対象外	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？ (9.1.C1)	はい	いいえ	対象外	備考____
３０．２　電子署名・タイムスタンプ等を行える機能があるか？ (9.1.C2)(9.4.C2)	はい	いいえ	対象外	備考____

© JAHIS 2020

備考記載欄	

© JAHIS 2020

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(6.2)

「１　扱う情報のリストを提示してあるか？(6.2.C1)」

本項目は、安全管理ガイドライン「6.2.2 取扱い情報の把握」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。「対象外」である場合や、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（6.4）

「２　覗き見防止の機能があるか？(6.4.C5)」

本項目は、安全管理ガイドライン「6.4 物理的安全対策」の考え方に基づいて覗き見防止対策を有するかを確認するものです。

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（6.5）

「３　離席時の不正入力防止の機能があるか？(6.5.C4)」

本項目は、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。

長時間離席の際に不正入力のおそれがある場合に、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？(6.5.C1)」

医療情報システムの利用者の識別・認証が可能である場合は「はい」、できない場合は「いいえ」としてください。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”6.5 技術的安全対策”の”B.考え方“をよく理解した上で回答してください。

「４．１　アクセス管理の認証方式は？(6.5.C1)」

アクセス管理の認証方式として利用可能なものを以下の中からお答えください。（複数回答可）

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）、その他の場合は具体的な認証方式を備考に記入してください。2 要素認証については、具体的な組み合わせ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？(6.5.C11 管理者(1)～6.5.C11 管理者(3))」

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されていることと、安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。

© JAHIS 2020

「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？(6.5C3)」

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に、そのデバイスであるICカード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ことが求められます。

技術的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」として下さい。

「４．２　利用者別、職種別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)」

利用者別、職種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。

「４．３　アクセス記録（アクセスログ）機能があるか？(6.5.C7)」

アクセスログを記録する機能がある場合は「はい」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？(6.5.C7)」

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。

「４．３．２　アクセスログへのアクセス制限機能があるか？(6.5.C8)」

個人情報を含むアクセスログに対して、アクセスする操作者を制限することが可能であり、かつ不当な削除／改ざん／追加等を防止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。

「５　時刻情報の正確性を担保する機能があるか？(6.5.C9)」

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。

「６　不正ソフトウェア対策を行っているか？(6.5.C10)」

不正ソフトウェア対策（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。コンピュータウイルス対策ソフトを使用する場合、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？(6.5.C12)」

無線 LAN を使用している場合に 6.5.C12 を満たすセキュリティ対策機能がある場合は「はい」としてください。なお、無線LANの使用を認めていない場合は「対象外」としてください。具体的な利用可能なセキュリティ機能に関しては備考に記載してください。

※　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。

© JAHIS 2020

情報及び情報機器の持ち出しについて(6.9)

「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？(6.9.C9)」

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が有するか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の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？(6.9)」

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進入防止や情報漏洩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」、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？(6.9.C6、C7)」

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がある場合は「はい」、無い場合は「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(6.10)

「１１　非常時アカウント又は、非常時機能を持っているか？(6.10.C3)」

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。

外部と個人情報を含む医療情報を交換する場合の安全管理(6.11)

「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？(6.11)」

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を有するか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

© JAHIS 2020

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のことを言います。

上記のような通信機能がある場合は「はい」、機能が無い場合は「対象外」としてください。「はい」の場合は、従属質問に回答してください。

「１２．１　なりすましの対策（認証）機能を有するか？(6.11.C3)」

外部との情報交換の際に、機密性保持のために送信元および送信先が正しいことが担保されなくてはなりません。送信元および送信先を偽装するなりすましの対策として、認証機能を有するかどうかを回答してください。

認証機能を有する場合は「はい」、無い場合は「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（S/MIME、ファイル暗号化など）が可能か？(6.11.C5)」

「データの暗号化」とはOSI参照モデル 4層以上のレイヤにて暗号化を施すものを言います。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）機能を有するかを回答してください。その際、IPsecなどOSI 参照モデル3層以下による暗号化（チャネル・セキュリティ）のことでは無いことに注意してください。

データの暗号化が可能な場合は「はい」、暗号化できない場合は「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。

「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？(6.11.C4)」

本項目は、施設内のルータ等を経由して異なる施設間を結ぶ複数のVPNの間で相手先の施設間で自施設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。

有する場合は「はい」、無い場合は「いいえ」としてください。もし、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？(6.11.C4)」

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。

「１２．３．１．１　対応している通信方式はいずれか？(6.11.C4、C10)」

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「はい」、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「いいえ」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。動作保証するネットワークサービスが存在しない場合は「対象外」としてください。

＜「TLS1.2」の場合（いわゆるSSL-VPNではない）＞

- TLSを利用する場合は、相手の確認の手段が「SSL/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。
- 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。

※6.11.C10に示されているように通信の方式として、SSL-VPNは原則として使用してはいけません。原則に反しSSL-VPNを利用する場合は備考にその理由を記載してください。

© JAHIS 2020

「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？(6.11.C4、C10)」

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、もしく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？(6.11.C7)」

本項目は、装置に対し保守会社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「はい」、機能を提供していない場合は「対象外」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？(6.11.C7)」

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。

有する場合は「はい」、有しない場合は「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(6.12)

「１３　記名・押印が義務付けられた文書を扱っているか？(6.12.C(1))」

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「はい」、取り扱っていない場合は「対象外」としてください。

「はい」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、もしくはそれに準ずる措置を行う必要があります。

「１３．１　HPKI 対応もしくは認定認証局が発行する証明書対応の署名機能があるか？(6.12.C(1))」

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 証明書もしくは認定認証局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。署名機能がある場合は「はい」、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。

「１３．２　HPKI 対応もしくは認定認証局が発行する証明書対応の検証機能があるか？(6.12.C(1))」

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

© JAHIS 2020

において HPKI 証明書もしくは認定認証局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。

「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。

「１３．３　日本データ通信協会認定のタイムスタンプが付与可能か？(6.12.C (2))」

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、一般財団法人日本データ通信協会が認定した時刻認証事業者のものを使用することが求められています。付与可能な場合は「はい」、そうでない場合は「いいえ」としてください。

「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。

「１３．４　日本データ通信協会認定のタイムスタンプが検証可能か？(6.12.C (2))」

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、一般財団法人日本データ通信協会が認定した時刻認証事業者のものを使用することが求められています。検証可能な場合は「はい」、そうでない場合は「いいえ」としてください。

「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、備考に当該システムと連携可能なタイムスタンプの検証方法を記載してください。

「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？(6.12.C (2))」

本項目は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 JIS 規格である CAdES、XAdES 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」、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。

真正性の確保について(7.1)

「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？(7.1.C 医療(1).a-1)」

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、特定の装置若しく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。認証を行い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。

安全管理ガイドラインにおいて”「6.5 技術的安全対策 (1) 入力者の識別及び認証」を参照すること”とされていますので、「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？(7.1.C 医療(1).a-2)」

真正性を担保するためには、故意または過失による虚偽入力、書き換え、消去及び混同を防止することが必要

© JAHIS 2020

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らば「はい」、そうでない場合は「いいえ」としてください。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。

「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？(7.1.C 医療(1).a-2)」

本項目は、権限管理の機能を有するかを確認するものです。

権限管理しているならば「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。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。

「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？(7.1.C 医療(1).a-3)」

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に、端末の設置場所を管理するといった運用によってアクセス管理するために、システムが端末を管理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ならば「はい」、そうでない場合は「いいえ」としてください。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？(7.1.C 医療(2).a-1)」

本項目は、真正性を確保して保存を開始する時点を明確にするための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」、そうでない場合は「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？(7.1.C 医療(2).a-1)」

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を有するかを確認するものです。

作成責任者の識別情報と信頼できる時刻源に基づく作成日時とが記録される場合は「はい」としてください。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？(7.1.C 医療(2).a-2)」

本項目は、記録の確定の際には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、書き換え、消去及び混同を防止する機能があるか？(7.1.C 医療(2).a-4)」

真正性の確保のためには、確定後のデータに対し、いかなる追記、変更及び消去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修正・削除が禁止されている場合は「はい」、そうでない場合は「いいえ」としてください。

© JAHIS 2020

「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？(7.1.C 医療(2).b-1)」

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、特定の装置また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」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？(7.1.C 医療(3)-1)」

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、その内容を参照する機能を持っている場合は「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。

「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？(7.1.C 医療(3)-2)」

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。

更新の順序を識別できる機能を持っている場合は「はい」、そうでない場合は「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？(7.1.C 医療(4))」

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。権限として代行権限が付与されているものも承認の中に含みます。

承認機能がある場合は「はい」、そうでない場合は「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、誰の代行が誰によっていつ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？(7.1.C 医療(4)-2)」

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、誰の代行が誰によっていつ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。

機能を持っている場合は「はい」、そうでない場合は「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を、確定者による「確定操作（承認）」を行う機能があるか？(7.1.C 医療(4)-3)」

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。

© JAHIS 2020

機能を持っている場合は「はい」、そうでない場合は「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(7.2)

「２０　目的に応じて速やかな検索結果の出力機能があるか？(7.2.C (3))」

見読性とは、保存された情報を目的に対して支障のない応答速度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、見読性を確保するために、目的に応じて速やかに検索し表示する機能を有するかを確認するものです。『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。

機能を持っている場合は「はい」、そうでない場合は「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？(7.2.C(4))」

システム障害に備えた冗長化手段や代替え的な見読化手段がある場合は「はい」、そうでない場合は「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？(7.2.C(4))」

本項目は、冗長化の具体的な内容について備考を用いて確認するものです。冗長化手段がある場合は「はい」、そうでない場合は「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？(7.2.C (4))」

本項目は、代替的な見読化手段の具体的な内容について備考を用いて確認するものです。代替え的な見読化手段には一般的な記録形式 (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。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(7.3)

「２２　いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同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？(7.3.C 医療(1)-1」

本項目は、保存性を確保するために、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や混同を防ぐための対策が施さ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。

「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？(7.3.C 医療(2)-1)」

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およ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

© JAHIS 2020

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？(7.3.C 医療(2)-2)」

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、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。

「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？(7.3.C 医療(2)-4)」

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。

そのような機能がある場合は「はい」、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？(7.3.C 医療(2)-4)」

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）を有するかを確認するものです。

そのような機能がある場合は「はい」、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？(7.3.C 医療(2)-5)」

本項目は、システムが保存する情報がき損した場合に、作成しているバックアップデータを用いて、き損前の状態に回復させる機能が提供されているかどう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。

このような機能がある場合は「はい」、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。

「２７　記録媒体が劣化する以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？(7.3.C 医療(3)-1)」

本項目は、記憶媒体の劣化による読み取り不能や不完全な読み取りにより、保存されている情報が滅失あるいは破壊されてしまうことを防止するために、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が有しているかどうかを確認するものです。

機能がある場合は「はい」、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

© JAHIS 2020

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？(7.3.C 医療(4)-1)」

標準形式とは安全管理ガイドライン第5章に記載されている国際標準、業界標準等のことです。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。

機能がある場合は「はい」、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？(7.3.C 医療(4)-2)」

マスタデータベースの入れ替えの際に、医療機関等が運用管理規程と手順書を設け、それにしたがって実施を支援する機能がある場合は「はい」、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(9.)

「３０　診療録などをスキャナなどにより電子化して保存する機能があるか？(9.1.C1)(9.4)」

スキャナなどによる電子化により診療録等の情報を電子保存する機能がある場合は「はい」、機能がない場合は「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？(9.1.C1)」

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」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・タイムスタンプ等を行える機能があるか？(9.1.C2)(9.4.C2)」

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、タイムスタンプを行う機能を有するかを確認するものです。

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。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。

© JAHIS 2020

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 5 版対応）

サービス事業者　：	作成日　：			
サービス名称　：	バージョン　：			
診療録及び診療所記録を外部に保存する際の基準(8)				
1　診療録及び診療所記録の外部保存を受託するか？(8.1.2)	はい	いいえ	対象外	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？(8.1.2.C①)	はい	いいえ	対象外	備考____
1．2　保存場所が、「行政機関等が開設したデータセンター等」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？(8.1.2.C②)	はい	いいえ	対象外	備考____
1．3　保存場所が、「医療機関等が民間事業者等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？(8.1.2.C③)」	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(6.2)				
2　扱う情報のリストを提示してあるか？(6.2.C1)	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）(6.3)				
3　情報システムを運用する際に運用責任者を設置しているか？(6.3.C1)	はい	いいえ	対象外	備考____
4　情報システムを運用する際に、担当者（システム管理者を含む。）を限定しているか？(6.3.C1)	はい	いいえ	対象外	備考____
5　個人情報が参照可能な場所においては、入退管理を定めているか？(6.3.C2)	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？(6.3.C3)	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？(6.3.C4)	はい	いいえ	対象外	備考____
8　個人情報を含む情報システムを再委託している場合、再委託先との契約に安全管理に関する条項を含めているか？ (6.3.C4)	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？(6.3.C5)	はい	いいえ	対象外	備考____
物理的安全対策(6.4)				
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？(6.4.C1)	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？(6.4.C2)	はい	いいえ	対象外	備考____
１２　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か？(6.4.C3)	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？(6.4.C3)	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？(6.4.C3)	はい	いいえ	対象外	備考____
１２．３　個人情報が存在する PC 等の重要な機器に盗難防止用チェーンを設置しているか？(6.4.C3)	はい	いいえ	対象外	備考____

© JAHIS 2020

１３　覗き見防止の機能があるか？(6.4.C5)	はい	いいえ	対象外	備考____
１３．１　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？(6.4.C5)	はい	いいえ	対象外	備考____
技術的安全対策(6.5)				
１４　権限を持たない者による不正入力防止対策が行われているか？(6.5.C4)	はい	いいえ	対象外	備考____
１５　アクセス管理の機能があるか？(6.5.C1)	はい	いいえ	対象外	備考____
１５．１　アクセス管理の認証方式は？(6.5.C1)	はい	いいえ	対象外	備考____
１５．１．１　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？(6.5.C11 管理者(1)～6.5.C11 管理者(3))	はい	いいえ	対象外	備考____
１５．１．１．１　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。(6.5.C11 管理者(1))	はい	いいえ	対象外	備考____
１５．１．１．２　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。(6.5.C11 管理者(2))	はい	いいえ	対象外	備考____
１５．１．１．３　パスワードの有効期限が管理できるか？(6.5.C11 利用者(1))	はい	いいえ	対象外	備考____
１５．１．１．４　文字列制限をチェックすることができるか？(6.5.C11 利用者(1))	はい	いいえ	対象外	備考____
１５．１．１．５　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？(6.5.C11 利用者(2))	はい	いいえ	対象外	備考____
１５．１．１．６　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？(6.5.C11 利用者(2))	はい	いいえ	対象外	備考____
１５．１．１．７　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？(6.5C2)	はい	いいえ	対象外	備考____
１５．１．２　運用管理規程に代替手段が規定されているか？ (6.5C3)	はい	いいえ	対象外	備考____
１５．２　利用者別、職種別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	はい	いいえ	対象外	備考____
１５．３　アクセス記録（アクセスログ）機能があるか？(6.5.C7)	はい	いいえ	対象外	備考____
１５．３．１　アクセスログを利用者が確認する機能があるか？(6.5.C7)	はい	いいえ	対象外	備考____
１５．３．２　アクセスログへのアクセス制限ができるか？(6.5.C8)	はい	いいえ	対象外	備考____
１５．４　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業務日誌等で操作の記録を行っているか？(6.5.C7)	はい	いいえ	対象外	備考____
１５．４．１　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。(6.5.C8)	はい	いいえ	対象外	備考____
１６　時刻情報の正確性を担保する仕組みがあるか？(6.5.C9)	はい	いいえ	対象外	備考____
１７　ウイルス等の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。(6.5.C10)	はい	いいえ	対象外	備考____
１８　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？(6.5.C12)	はい	いいえ	対象外	備考____
１９　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？(6.5.C13(1))	はい	いいえ	対象外	備考____
１９．１　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が提供できるか？(6.5.C13(2))	はい	いいえ	対象外	備考____
１９．２　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？(6.5.C13(3))	はい	いいえ	対象外	備考____
１９．３　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？(6.5.C13(4))	はい	いいえ	対象外	備考____
人的安全対策(6.6)				
２０　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？	はい	いいえ	対象外	備考____

© JAHIS 2020

(6.6(1)C1)	
２１　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？(6.6(1)C2)	はい　いいえ　対象外　備考____
２２　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？ (6.6(1)C3)	はい　いいえ　対象外　備考____
２３　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？ (6.6(2)C1①)	はい　いいえ　対象外　備考____
２４　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？(6.6(2)C1②)	はい　いいえ　対象外　備考____
２５　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？(6.6(2)C1③)	はい　いいえ　対象外　備考____
２６　業務の一部を再委託する場合に、再委託先に対し、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？(6.6(2)C1④)	はい　いいえ　対象外　備考____
２７　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義務契約等の秘密保持の対策を行っているか？ (6.6(2)C2)	はい　いいえ　対象外　備考____
情報の破棄(6.7)	
２８　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？(6.7.C1)	はい　いいえ　対象外　備考____
２８．１　手順には破棄を行う条件を含めているか？(6.7.C1)	はい　いいえ　対象外　備考____
２８．２　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？(6.7.C1)	はい　いいえ　対象外　備考____
２８．３　手順には破棄の具体的な方法を含めているか？(6.7.C1)	はい　いいえ　対象外　備考____
２９　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ものが行うこととし、残存し、読み出し可能な情報がないことを報告できるか？(6.7.C2)	はい　いいえ　対象外　備考____
３０　破棄を再委託した場合、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？(6.7.C3)	はい　いいえ　対象外　備考____
３１　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？(6.7.C4)	はい　いいえ　対象外　備考____
情報システムの改造と保守(6.8)	
３２　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？(6.8.C1)	はい　いいえ　対象外　備考____
３２．１　作業員はサービス事業者自身で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？(6.8.C1)	はい　いいえ　対象外　備考____
３２．２　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規程が含まれているか？(6.8.C1)	はい　いいえ　対象外　備考____
３３　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？(6.8.C2)	はい　いいえ　対象外　備考____
３４　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？(6.8.C2)	はい　いいえ　対象外　備考____
３５　アカウント情報の外部流出等による不正使用の防止に努めているか？(6.8.C3)	はい　いいえ　対象外　備考____
３６　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？ (6.8.C4)	はい　いいえ　対象外　備考____
３７　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	はい　いいえ　対象外　備考____

© JAHIS 2020

報告を義務付けているか？ (6.8.C4)	
３７．１　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？(6.8.C4)	はい　いいえ　対象外　備考____
３８　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？(6.8.C5)	はい　いいえ　対象外　備考____
３９　メンテナンス終了後は、速やかに医療機関等に作業報告書を提出できるか？(6.8.C5)	はい　いいえ　対象外　備考____
４０　保守を外部委託する場合、保守会社と守秘義務契約を締結しているか？(6.8.C6)	はい　いいえ　対象外　備考____
４１　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？(6.8.C7)	はい　いいえ　対象外　備考____
４２　リモートメンテナンスによる改造や保守を行う場合は、アクセスログを収集するか？(6.8.C8)	はい　いいえ　対象外　備考____
４３　保守業務を再委託している場合、再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？(6.8.C9)	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(6.9)	
４４　持出機器を提供している場合、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？(6.9)	はい　いいえ　対象外　備考____
４４．１　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？(6.9)	はい　いいえ　対象外　備考____
４４．２　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？(6.9.C7)	はい　いいえ　対象外　備考____
４４．３　持ち出した情報機器をネットワークに接続したり、他の媒体を接続する場合、情報漏えいや改ざんの対策を実施しているか？(6.9.C8)	はい　いいえ　対象外　備考____
４５　提供するサービスに係わる情報およ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？(6.9.C1)	はい　いいえ　対象外　備考____
４６　サービス事業者が情報および情報機器を持出する場合、リスク分析の結果を受けて、情報およ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？(6.9.C1)	はい　いいえ　対象外　備考____
４６．１　持ち出した情報および情報機器の管理方法を定めているか？(6.9.C2)	はい　いいえ　対象外　備考____
４６．２　医療機関等の委託による情報を格納した媒体および情報機器の盗難、紛失時の適切な対応を自社方針・規則等に定めているか？(6.9.C3)	はい　いいえ　対象外　備考____
４６．３　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？(6.9.C4)	はい　いいえ　対象外　備考____
４６．４　情報機器について、起動パスワード等を設定しているか？(6.9.C6)	はい　いいえ　対象外　備考____
４６．５　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？(6.9.C6)	はい　いいえ　対象外　備考____
４６．６　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？(6.9.C7)	はい　いいえ　対象外　備考____
４６．７　医療機関等または医療機関等の委託によりサービス事業者が持ち出した情報機器をネットワークに接続したり、他の媒体を接続する場合、情報漏えいや改ざんの対策を実施しているか？(6.9.C8)	はい　いいえ　対象外　備考____
４７　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？(6.9.C5)	はい　いいえ　対象外　備考____
４８　個人保有の情報機器の利用を禁止しているか？(6.9.C10)	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(6.10)	

© JAHIS 2020

４９　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？(6.10.C1)、(6.10.C2)	はい	いいえ	対象外	備考____
５０　非常時アカウント又は、非常時機能を持っているか？ (6.10.C3)	はい	いいえ	対象外	備考____
５０．１　「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？ (6.10.C3)	はい	いいえ	対象外	備考____
５０．２　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？(6.10.C3)	はい	いいえ	対象外	備考____
５０．３　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？(6.10.C3)	はい	いいえ	対象外	備考____
５０．４　標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、関係先への連絡手段を準備しているか？(6.10.C3)	はい	いいえ	対象外	備考____
外部と個人情報を含む医療情報を交換する場合の安全管理(6.11)				
５１～５５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、利用している通信方式それぞれに対して確認が必要です。提供する通信方式に「はい」とし、提供していない通信方式を「対象外」としてください。				
５１　通信方式として専用線に対応しているか？(6.11)	はい	いいえ	対象外	備考____
５１．１　提供事業者に閉域性の範囲を確認しているか？(6.11.C1)	はい	いいえ	対象外	備考____
５１．２　採用する認証手段が定められているか？(6.11.C2)	はい	いいえ	対象外	備考____
５２　通信方式として公衆網に対応しているか？(6.11)	はい	いいえ	対象外	備考____
５２．１　提供事業者に閉域性の範囲を確認しているか？(6.11.C1)	はい	いいえ	対象外	備考____
５２．２　採用する認証手段が定められているか？(6.11.C2)	はい	いいえ	対象外	備考____
５３　通信方式として IP-VPN に対応しているか？(6.11)	はい	いいえ	対象外	備考____
５３．１　提供事業者に閉域性の範囲を確認しているか？(6.11.C1)	はい	いいえ	対象外	備考____
５３．２　採用する認証手段が定められているか？(6.11.C2)	はい	いいえ	対象外	備考____
５４　通信方式として IPsec-VPN ＋IKE に対応しているか？(6.11)	はい	いいえ	対象外	備考____
５４．１　セッション間の回り込み等の攻撃からの防御について対策をしているか？(6.11.C10)	はい	いいえ	対象外	備考____
５４．２　採用する認証手段が定められているか？(6.11.C2)	はい	いいえ	対象外	備考____
５５　チャネル・セキュリティとして TLS1.2 クライアント認証に対応しているか？(6.11)	はい	いいえ	対象外	備考____
５５．１　設定はサーバ/クライアントともに「SSL/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？(6.11.C10)	はい	いいえ	対象外	備考____
５５．２　セッション間の回り込み等による攻撃からの防護について、適切な対策を実施しているか？(6.11.C10)	はい	いいえ	対象外	備考____
５６　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？(6.11.C1)	はい	いいえ	対象外	備考____
５７　ネットワーク上において、盗聴を防止する対策を行っているか？(6.11.C1)	はい	いいえ	対象外	備考____
５８　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？(6.11.C1)	はい	いいえ	対象外	備考____
５９　データ送信元と送信先において、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？(6.11.C2)	はい	いいえ	対象外	備考____
６０　ネットワークの経路制御・プロトコル制御を行える機器もしくは機能を有するか？(6.11.C4)	はい	いいえ	対象外	備考____
６０．１　ネットワークの経路制御・プロトコル制御に関わる機器もしくは機能は、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	はい	いいえ	対象外	備考____

© JAHIS 2020

できるか？(6.11.C4)	
６０．２　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？(6.11.C4)	はい　いいえ　対象外　備考____
６１　ネットワークセキュリティとは別に、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？(6.11.C5)	はい　いいえ　対象外　備考____
６１．１　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？(6.11.C5)	はい　いいえ　対象外　備考____
６２　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が存在するか？(6.11.C6、C8)	はい　いいえ　対象外　備考____
６３　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が存在するか？(6.11.C6)	はい　いいえ　対象外　備考____
６４　リモートメンテナンスサービスを有しているか？(6.11.C7)	はい　いいえ　対象外　備考____
６４．１　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？(6.11.C7)	はい　いいえ　対象外　備考____
６５　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？(6.11.C8)	はい　いいえ　対象外　備考____
６６　患者に情報を閲覧させる機能があるか？(6.11.C9)	はい　いいえ　対象外　備考____
６６．１　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しているか？(6.11.C9)	はい　いいえ　対象外　備考____
６６．２　患者等へ危険性や提供目的について納得できる説明を行える資料を用意しているか？(6.11.C9)	はい　いいえ　対象外　備考____
６６．３　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？(6.11.C9)	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(6.12)	
６７　記名・押印が義務付けられた文書を扱っているか？(6.12.C(1))	はい　いいえ　対象外　備考____
６７．１　HPKI 対応もしくは認定認証局が発行する証明書対応の署名機能があるか？(6.12.C(1))	はい　いいえ　対象外　備考____
６７．２　HPKI 対応もしくは認定認証局が発行する証明書対応の検証機能があるか？(6.12.C(1))	はい　いいえ　対象外　備考____
６７．３　日本データ通信協会認定のタイムスタンプが付与可能か？(6.12.C(2))	はい　いいえ　対象外　備考____
６７．４　日本データ通信協会認定のタイムスタンプが検証可能か？(6.12.C(2))	はい　いいえ　対象外　備考____
６７．５　保存期間中の文書の真正性を担保する仕組みがあるか？(6.12.C(2))	はい　いいえ　対象外　備考____
６８　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？(6.12.C(3))	はい　いいえ　対象外　備考____
真正性の確保について(7.1)	
６９　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？(7.1.C 医療(1).a-1)	はい　いいえ　対象外　備考____
６９．１　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？(7.1.C 医療(1).a-2)	はい　いいえ　対象外　備考____
６９．２　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？(7.1.C 医療(1).a-2)	はい　いいえ　対象外　備考____
６９．３　サービス事業者内の利用者の権限管理の機能があるか？(7.1.C 医療(1).a-2)	はい　いいえ　対象外　備考____
６９．４　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？(7.1.C 医療(1).a-2)	はい　いいえ　対象外　備考____
６９．５　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	はい　いいえ　対象外　備考____

© JAHIS 2020

クセスを防止する機能があるか？(7.1.C 医療(1).a-3)	
６９．６　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？(7.1.C 医療(1).a-3)	はい　いいえ　対象外　備考____
７０　システムは記録を確定する機能があるか？(7.1.C 医療(2).a-1)	はい　いいえ　対象外　備考____
７０．１　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？(7.1.C 医療(2).a-1)	はい　いいえ　対象外　備考____
７０．２　「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？(7.1.C 医療(2).a-2)	はい　いいえ　対象外　備考____
７０．３　確定された記録に対して、故意による虚偽入力、書き換え、消去及び混同を防止する機能があるか？(7.1.C 医療(2).a-4)	はい　いいえ　対象外　備考____
７１　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？(7.1.C 医療(2).b-1)	はい　いいえ　対象外　備考____
７２　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？(7.1.C 医療(3)-1)	はい　いいえ　対象外　備考____
７２．１　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？(7.1.C 医療(3)-2)	はい　いいえ　対象外　備考____
７３　代行入力の承認機能があるか？(7.1.C 医療(4))	はい　いいえ　対象外　備考____
７３．１　代行入力が行われた場合、誰の代行が誰によっていつ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？(7.1.C 医療(4)-2)	はい　いいえ　対象外　備考____
７３．２　代行入力により記録された診療録等を、確定者による「確定操作（承認）」を行う機能があるか？(7.1.C 医療(4)-3)	はい　いいえ　対象外　備考____
７４　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？(7.1.C 医療(5)-1)	はい　いいえ　対象外　備考____
７５　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？(7.1.C 医療(5)-2)	はい　いいえ　対象外　備考____
７６　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盛り込んでいて、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？(7.1.C 医療(5)-3)	はい　いいえ　対象外　備考____
７７　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？(7.1.C 医療(5)-4)	はい　いいえ　対象外　備考____
７８　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？（7.1.C 外部(1))	はい　いいえ　対象外　備考____
７９　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？(7.1.C 外部(2))	はい　いいえ　対象外　備考____
８０　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？（7.1.C 外部(3))	はい　いいえ　対象外　備考____
見読性の確保について(7.2)	
８１　患者ごとの情報の全ての所在が日常的に管理されているか？（7.2.C(1))	はい　いいえ　対象外　備考____
８２　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は対応づけて管理され、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ているか？(7.2.C(2))	はい　いいえ　対象外　備考____
８３　目的に応じて速やかに検索結果を出力する機能もしくはサービスがあるか？(7.2.C(3))	はい　いいえ　対象外　備考____
８４　システム障害に備えた冗長化手段や代替え的な見読化手段はあるか？(7.2.C (4))	はい　いいえ　対象外　備考____

© JAHIS 2020

８４．１　冗長化手段があるか？(7.2.C (4))	はい	いいえ	対象外	備考____
８４．２　システム障害に備えた代替的な見読化手段があるか？(7.2.C (4))	はい	いいえ	対象外	備考____
保存性の確保について(7.3)				
８５　いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同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？(7.3.C 医療(1)-1)	はい	いいえ	対象外	備考____
８６　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、医療機関等への SLA 等が文書として提供されているか？(7.3.C 医療(2)-1)	はい	いいえ	対象外	備考____
８７　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？ (7.3.C 医療(2)-2)	はい	いいえ	対象外	備考____
８８　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？(7.3.C 医療(2)-4)	はい	いいえ	対象外	備考____
８８．１　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？(7.3.C 医療(2)-4)	はい	いいえ	対象外	備考____
８９　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？(7.3.C 医療(2)-5)	はい	いいえ	対象外	備考____
９０　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？(7.3.C 医療(4)-1)	はい	いいえ	対象外	備考____
９１　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？(7.3.C 医療(4)-2)」	はい	いいえ	対象外	備考____
９２　外部保存を受託する機関は、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？(7.3.C 外部(1))	はい	いいえ	対象外	備考____
９３　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？(7.3.C 外部(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(9.)				
９４　診療録などをスキャナなどにより電子化して保存する機能があるか？(9.1.C1)(9.4)	はい	いいえ	対象外	備考____
９４．１　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？(9.1.C1)	はい	いいえ	対象外	備考____
９４．２　電子署名・タイムスタンプ等を行える機能があるか？(9.1.C2)(9.4.C2)	はい	いいえ	対象外	備考____

© JAHIS 2020

備考記載欄	

© JAHIS 2020

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を外部に保存する際の基準(8.)

「1　診療録及び診療諸記録の外部保存を受託するか？(8.1.2)」

外部保存を受託する場合は「はい」、そうでない場合は「いいえ」としてください。
本質問の回答が「はい」の場合は、従属質問のいずれかを「はい」としてください。保存場所が複数「はい」の場合は、それぞれ個別のチェックリストを作成してください。
本章の各事項は、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。

「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？(8.1.2.C①)」

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む。

- 敷地内の適切に管理する場所に自ら堅牢性の高い設備環境を用意している。(8.1.2.C①(ア))
- 保存を委託した病院、診療所及び患者の許可なく診療録等を取り扱わない規定がある。(8.1.2.C①(イ))
- 保存を受託した診療録等について分析等を行う場合は、委託した病院、診療所及び患者の同意を得た上で、不当な利益を目的としない場合に限ることの規定がある。(8.1.2.C①(ウ))
- 匿名化された情報を取り扱う場合においても、匿名化の妥当性の検証を検証組織で検討することや、取扱いをしている事実を患者等に掲示等を使って知らせる等、個人情報の保護に配慮した上で実施することを規定している。(8.1.2.C①(エ))
- 情報を保存している機関に患者がアクセスし、自らの記録を閲覧するような仕組みを提供する場合は、情報の保存を受託した病院、診療所は適切なアクセス権を規定し、情報漏えいや、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を規定している。(8.1.2.C①(オ))

医療機関等とのサービス契約において、個人情報保護法の本人同意に関する除外規定以外の例外条件を設ける場合は「いいえ」として、備考に例外内容を具体的に記載してください。

「1．2　保存場所が、「行政機関等が開設したデータセンター等」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？(8.1.2.C②)」

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む。

- 保存業務に従事する個人若しくは従事していた個人に対して、個人情報の内容に係る守秘義務や不当使用等の禁止について、法律や条例により罰則が適用されることになっている。(8.1.2.C②(ア))
- 適切な外部保存に必要な技術及び運用管理能力を有することを、システム監査技術者及び Certified Information Systems Auditor（ISACA 認定）等の適切な能力を持つ監査人の外部監査を受ける等して、定期的に確認している。(8.1.2.C②(イ))
- 保存された情報の分析、解析等を実施しないことを、医療機関等との契約書等に明記できる。(8.1.2.C②(ウ))
- 保存された情報を独自に提供しないように、医療機関等との契約書等に明記できる。(8.1.2.C②(エ))
- 外部保存を受託する事業者側が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、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している。(8.1.2.C②(エ))

© JAHIS 2020

医療機関等とのサービス契約において、個人情報保護法の本人同意に関する除外規定以外の例外条件を設ける場合は「いいえ」として、備考に例外内容を具体的に記載してください。

「１．３　保存場所が、「医療機関等が民間事業者等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？(8.1.2.C③)」

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む。

- 管理者や電子保存作業従事者等に対する守秘に関連した事項、違反した場合のペナルティ、保存した情報の取扱いに対しての監督を受けることについて、医療機関等との契約書において明記できる。(8.1.2.C③(ア))
- 医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していることを説明できる資料がある 。(8.1.2.C③(イ))
- 医療機関等との契約書において、受託事業者が総務省・経済産業省の「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」等を遵守すること、並びに少なくとも定期的に確認報告等をすることを明確に定めること。(8.1.2.C③(ウ))
- 保存された情報を契約で取り交わした保守作業に必要な範囲を超えて閲覧してはならないこと、保守に関しては、「6.8 情報システムの改造と保守」を遵守することを、医療機関等との契約書に明記できる。(8.1.2.C③(エ))
- 保存した情報を分析、解析等を実施してはならないこと、匿名化された情報であっても同様であることを、医療機関等との契約書に明記できる。(8.1.2.C③(オ))
- 保存された情報を独自に提供しないことを、医療機関等との契約書等に明記できる。(8.1.2.C③(カ))
- 保存された情報の提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、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している。(8.1.2.C③(カ))
- 医療機関等から下記資料を求められた場合には、提供する用意がある。(8.1.2.C③(キ))
  - (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
  - (b) 医療情報等の安全管理に係る実施体制の整備
  - (c) 実績等に基づく個人データ安全管理に関する信用度
  - (d) 財務諸表等に基づく経営の健全性

医療機関等とのサービス契約において、個人情報保護法の本人同意に関する除外規定以外の例外条件を設ける場合は「いいえ」として、備考に例外内容を具体的に記載してください。

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(6.2)

「２　扱う情報のリストを提示してあるか？(6.2.C1)」

本項目は、安全管理ガイドライン「6.2.2 取扱い情報の把握」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。「対象外」である場合や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。

© JAHIS 2020

組織的安全管理対策（体制、運用管理規程）(6.3)

「3　情報システムを運用する際に運用責任者を設置しているか？(6.3.C1)」

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、運用責任者の設置を問うものです。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　情報システムを運用する際に、担当者（システム管理者を含む。）を限定しているか？(6.3.C1)」

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、運用担当者の設置を問うものです。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。

「5　個人情報が参照可能な場所においては、入退管理を定めているか？(6.3.C2)」

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？(6.3.C3)」

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？(6.3.C4)」

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再委託している場合、再委託先との契約に安全管理に関する条項を含めているか？(6.3.C4)」

個人情報を含む医療情報システムの業務を再委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。個人情報を含む医療情報システムの業務を再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？(6.3.C5)」

組織的安全管理対策に関する事項とは、「理念」、「体制」、「契約書・マニュアル等の文書の管理」、「リスクに対する予防、発生時の対応の方法」、「機器を用いる場合は機器の管理」、「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(6.4)

「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？(6.4.C1)」

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

© JAHIS 2020

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？(6.4.C2)」

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か？(6.4.C3)」

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していない場合は「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？(6.4.C3)」

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？(6.4.C3)」

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。

「１２．３　個人情報が存在する PC 等の重要な機器に盗難防止用チェーンを設置しているか？(6.4.C3)」

個人情報が存在する PC 等の重要な機器に盗難防止用チェーンを設置している場合は「はい」、そうでない場合は「いいえ」としてください。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。

「１３　覗き見防止の機能があるか？(6.4.C5)」

本項目は、安全管理ガイドライン「6.4 物理的安全対策」の考え方に基づいて覗き見防止対策を有するかを確認するものです。

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。

「１３．１　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？(6.4.C5)」

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(6.5)

「１４　権限を持たない者による不正入力防止対策が行われているか？(6.5.C4)」

本項目は、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。

© JAHIS 2020

「１５　アクセス管理の機能があるか？(6.5.C1)」

医療情報システムの利用者の識別・認証が可能である場合は「はい」、できない場合は「いいえ」としてください。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”6.5 技術的安全対策”の”B.考え方“をよく理解した上で回答してください。

「１５．１　アクセス管理の認証方式は？(6.5.C1)」

アクセス管理の認証方式として利用可能なものを以下の中からお答えください。（複数回答可）
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）、その他の場合は具体的な認証方式を備考に記載してください。

「１５．１．１　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？(6.5.C11 管理者(1)～6.5.C11 管理者(3))」

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されていることと、安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。

「１５．１．１．１　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？(6.5.C11 管理者(1))」

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。

「１５．１．１．２　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？(6.5.C11 管理者(2))」

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。

「１５．１．１．３　パスワードの有効期限が管理できるか？(6.5.C11 利用者(1))」

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。

「１５．１．１．４　文字列制限をチェックすることができるか？(6.5.C11 利用者(1))」

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。

「１５．１．１．５　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？(6.5.C11 利用者(2))」

類推しやすいパスワード（「administrator」、「12345678」、「password」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。

「１５．１．１．６　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？(6.5.C11 利用

© JAHIS 2020

者(2))」

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。

「１５．１．１．７　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？(6.5C2)」

パスワードを暗号化したり、ハッシュ化したりするなどして、管理者にもわ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。

「１５．１．２　運用管理規程に代替手段が規定されているか？(6.5C3)」

本人の認証情報が利用できない際に、緊急時の代替手段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。

「１５．２　利用者別、職種別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)」

利用者別、職種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。

「１５．３　アクセス記録（アクセスログ）機能があるか？(6.5.C7)」

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。

「１５．３．１　アクセスログを利用者が確認する機能があるか？(6.5.C7)」

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。

「１５．３．２　アクセスログへのアクセス制限ができるか？(6.5.C8)」

アクセスログへのアクセス制限ができる場合は「はい」、そうでない場合は「いいえ」としてください。

「１５．４　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で操作の記録を行っているか？(6.5.C7)」

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で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。

「１５．４．１　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？(6.5.C8)」

システムにアクセスログへのアクセス制限機能が無い場合、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。

「１６　時刻情報の正確性を担保する仕組みがあるか？(6.5.C9)」

システムに時刻情報の正確性を担保する仕組みがある場合は「はい」、そうでない場合は「いいえ」としてください。

© JAHIS 2020

「１７　ウイルス等の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？(6.5.C10)」

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。

「１８　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？(6.5.C12)」

無線 LAN を使用している場合に 6.5.C12 を満たすセキュリティ対策機能がある場合は「はい」としてください。なお、無線 LAN の使用を認めていない場合は「対象外」としてください。具体的な利用可能なセキュリティ機能に関しては備考に記載してください。

※ 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。

「１９　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？(6.5.C13(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場合は「はい」、そうでない場合は「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。

「１９．１　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が提供できるか？(6.5.C13(2))」

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

「１９．２　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？(6.5.C13(3))」

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。

「１９．３　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？(6.5.C13(4))」

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(6.6)

「２０　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？(6.6(1)C1)」

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。

「２１　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？(6.6(1)C2)」

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。

「２２　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

© JAHIS 2020

まれているか？(6.6(1)C3)」

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。

「２３　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？(6.6(2)C1①)」

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。

「２４　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？(6.6(2)C1②)」

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。

「２５　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？(6.6(2)C1③)」

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。

「２６　業務の一部を再委託する場合に、再委託先に対し、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？(6.6(2)C1④)」

業務の一部を再委託し、再委託契約の中で、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」と同等の義務を再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。再委託していない場合は「対象外」としてください。

「２７　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義務契約等の秘密保持の対策を行っているか？(6.6(2)C2)」

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(6.7)

「２８　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？(6.7.C1)」

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。

「２８．１　手順には破棄を行う条件を含めているか？(6.7.C1)」

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。

© JAHIS 2020

「２８．２　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？(6.7.C1)」

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。

「２８．３　手順には破棄の具体的な方法を含めているか？(6.7.C1)」

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。

「２９　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ものが行うこととし、残存し、読み出し可能な情報がないことを報告できるか？(6.7.C2)」

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ものが行うこと、および、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ものが破棄し、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。

「３０　破棄を再委託した場合、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？(6.7.C3)」

本項目は、サービス事業者が情報の破棄を再委託した場合、委託業者の監督およ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再委託しない場合は「対象外」、サービス事業者が委託業者の監督およ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。

「３１　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？(6.7.C4)」

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。

情報システムの改造と保守(6.8)

「３２　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？(6.8.C1)」

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、外部委託を含む作業員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。

「３２．１　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？(6.8.C1)」

外部委託を含む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、再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。

「３２．２　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規

© JAHIS 2020

定が含まれているか？(6.8.C1)」

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。

「３３　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？(6.8.C2)」

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。

「３４　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？(6.8.C2)」

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。

「３５　アカウント情報の外部流出等による不正使用の防止に努めているか？(6.8.C3)」

本項目は、作業員個人のアカウント情報の外部流出等による不正使用の防止の観点による対策が運用管理規程に含まれる等、適切に管理されていることを問うものです。

該当する場合は「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。

「３６　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？(6.8.C4)」

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。

「３７　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？(6.8.C4)」

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。

「３７．１　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？(6.8.C4)」

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。

「３８　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？(6.8.C5)」

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

© JAHIS 2020

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。

「３９　メンテナンス終了後は、速やかに医療機関等に作業報告書を提出できるか？(6.8.C5)」

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後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、契約等で作業終了後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後、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。

「４０　保守を外部委託する場合、保守会社と守秘義務契約を締結しているか？(6.8.C6)」

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

保守会社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。

「４１　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？(6.8.C7)」

本項目は、障害対応時等で原因特定や解析等のためにやむを得ず障害発生時のデータ（個人情報を含む）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、「医療機関等およ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。

「４２　リモートメンテナンスによる改造や保守を行う場合は、アクセスログを収集するか？(6.8.C8)」

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。

「４３　保守業務を再委託している場合、再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？(6.8.C9)」

本項目は、保守業務を再委託している場合、再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。

再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。再委託を行っていない場合は「対象外」としてください。

© JAHIS 2020

情報及び情報機器の持ち出しについて(6.9)

「４４　持出機器を提供している場合、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？(6.9)」

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がある場合は「はい」、制限する機能が無い場合は「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。

「４４．１　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？(6.9)」

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。「いいえ」の場合は、備考にその理由を記載してください。

「４４．２　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？(6.9.C7)」

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」、医療機関等ならびに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。

「４４．３　持ち出した情報機器をネットワークに接続したり、他の媒体を接続する場合、情報漏えいや改ざんの対策を実施しているか？(6.9.C8)」

本項目は、持ち出した情報機器をネットワークに接続したり、他の媒体を接続する場合、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、および管理区域外から持ち込んだ情報機器を医療機関等ならびにサービス事業者のネットワーク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。

「４５　提供するサービスに係わる情報およ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？(6.9.C1)」

本項目は、医療機関等ならびにサービス事業者が情報（個人情報または各種データ）および情報機器（PC、スマートフォン、USB メモリ、SSD カード等の情報を格納できる機器やメディア等）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およ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」、情報およ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。

© JAHIS 2020

「４６　サービス事業者が情報および情報機器を持出する場合、リスク分析の結果を受けて、情報およ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？(6.9.C1)」

本項目は、サービス事業者が情報およ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およ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および情報機器を持出さない場合は「対象外」としてください。

「４６．１　持ち出した情報および情報機器の管理方法を定めているか？(6.9.C2)」

本項目は、サービス事業者が持ち出した情報およ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。

「４６．２　医療機関等の委託による情報を格納した媒体および情報機器の盗難、紛失時の適切な対応を自社方針・規則等に定めているか？(6.9.C3)」

本項目は、情報を格納した媒体およ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。

「４６．３　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？(6.9.C4)」

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。

「４６．４　情報機器について、起動パスワード等を設定しているか？(6.9.C6)」

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もの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。

「４６．５　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？(6.9.C6)」

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、6.5.C11 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。

「４６．６　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？(6.9.C7)」

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。

「４６．７　医療機関等または医療機関等の委託によりサービス事業者が持ち出した情報機器をネットワークに接続したり、他の媒体を接続する場合、情報漏えいや改ざんの対策を実施しているか？

© JAHIS 2020

(6.9.C8)」

本項目は、医療機関等ならびに医療機関等の委託によりサービス事業者が、持ち出した情報機器をネットワークに接続したり、他の媒体を接続する場合、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、「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」に準じた設定を行う必要があります。また、公衆無線 LAN 等、6.5.C12 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。

「４７　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？(6.9.C5)」

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。

「４８　個人保有の情報機器の利用を禁止しているか？(6.9.C10)」

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(6.10)

「４９　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？(6.10.C1)、(6.10.C2)」

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。

「５０　非常時アカウント又は、非常時機能を持っているか？(6.10.C3)」

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提供できる機能を有するかを確認するものです。例えば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。

「５０．１　「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？(6.10.C3)」

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。

「５０．２　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

© JAHIS 2020

う適切に管理及び監査できる情報を提供できるか？(6.10.C3)」

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。

「５０．３　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？(6.10.C3)」

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。

「５０．４　標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、関係先への連絡手段を準備しているか？(6.10.C3)」

標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した際、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。

外部と個人情報を含む医療情報を交換する場合の安全管理(6.11)

本節の質問は、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「はい」とし、対応していない通信方式を「対象外」としてください。

「５１　通信方式として専用線に対応しているか？(6.11)」

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

「５１．１　提供事業者に閉域性の範囲を確認しているか？(6.11.C1)」

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。閉域性の範囲について、通信方式の提供事業者に確認を行い、確認した内容を備考に記載してください。

「５１．２　採用する認証手段が定められているか？(6.11.C2)」

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）

「５２　通信方式として公衆網に対応しているか？(6.11)」

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

「５２．１　提供事業者に閉域性の範囲を確認しているか？(6.11.C1)」

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。閉域性の範囲について、通信方式の提供事業者に確認を行い、確認した内容を備考に記載してください。

© JAHIS 2020

「５２．２　採用する認証手段が定められているか？(6.11.C2)」

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)

「５３　通信方式として IP-VPN に対応しているか？(6.11)」

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

「５３．１　提供事業者に閉域性の範囲を確認しているか？(6.11.C1)」

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。閉域性の範囲について、通信方式の提供事業者に確認を行い、確認した内容を備考に記載してください。

「５３．２　採用する認証手段が定められているか？(6.11.C2)」

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)

「５４　通信方式として IPsec-VPN ＋IKE に対応しているか？(6.11)」

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

「５４．１　セッション間の回り込み等の攻撃からの防御について対策をしているか？(6.11.C10)」

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。(6.11.B 参照)
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。

「５４．２　採用する認証手段が定められているか？(6.11.C2)」

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等)

「５５　チャネル・セキュリティとして TLS1.2 クライアント認証に対応しているか？(6.11)」

本項目は、専用線、公衆網、IP-VPN、IPsec-VPN を用いずにチャネル・セキュリティとして TLS1.2（いわゆる SSL-VPN ではない）で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「はい」、そうでない場合は「対象外」としてください。

© JAHIS 2020

※6.11.C10 に示されているように通信の方式として、SSL-VPN は原則として使用してはいけません。原則に反し SSL-VPN を利用する場合は備考にその理由を記載してください。

「５５．１　設定はサーバ/クライアントともに「SSL/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？(6.11.C10)」

TLS を利用する場合は、相手の確認の手段が「SSL/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。

「５５．２　セッション間の回り込み等による攻撃からの防護について、適切な対策を実施しているか？(6.11.C10)」

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。

「５６　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？(6.11.C1)」

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、ウイルス混入等）　そうでない場合は「いいえ」としてください。

「５７　ネットワーク上において、盗聴を防止する対策を行っているか？(6.11.C1)」

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。

「５８　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？(6.11.C1)」

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。

「５９　データ送信元と送信先において、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？(6.11.C2)」

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、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。

「６０　ネットワークの経路制御・プロトコル制御を行える機器もしくは機能を有するか？(6.11.C4)」

本項目は、施設内のルータ等を経由して異なる施設間を結ぶ複数の VPN の間で相手先の施設間で自施設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。

© JAHIS 2020

「６０．１　ネットワークの経路制御・プロトコル制御に関わる機器もしくは機能は、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？(6.11.C4)」

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。

「６０．２　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？(6.11.C4)」

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。

「６１　ネットワークセキュリティとは別に、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？(6.11.C5)」

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等）

「６１．１　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？(6.11.C5)」

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。電子政府推奨暗号を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。

「６２　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が存在するか？(6.11.C6、C8)」

本項目は、医療機関等に対して、脅威に対する管理責任の範囲を示せるか問う項目です。管理責任の範囲を示す文書等が存在する場合は「はい」とし、記載してある文書等を備考に記載してください。存在しない場合は「いいえ」としてください。
（責任範囲となる例：情報送信／受信時、操作開始時、ネットワーク不通・遅延時、認証時、障害時、情報交換中止時）

「６３　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が存在するか？(6.11.C6)」

文書等が存在する場合は「はい」、存在しない場合は「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）

「６４　リモートメンテナンスサービスを有しているか？(6.11.C7)」

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「はい」、有していない場合は「対象外」としてください。

「６４．１　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

© JAHIS 2020

有しているか？(6.11.C7)」

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。

「６５　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？(6.11.C8)」

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。

「６６　患者に情報を閲覧させる機能があるか？(6.11.C9)」

本項目は患者に対しても情報を閲覧する機能の有無について問うものです。閲覧する機能があれば「はい」、機能が無い場合は「対象外」としてください。

「６６．１　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しているか？(6.11.C9)」

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れば「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 個人認証等の技術を用いた対策の実施等）

「６６．２　患者等へ危険性や提供目的について納得できる説明を行える資料を用意しているか？(6.11.C9)」

本項目は、患者への情報閲覧のサービスや機能を提供する際に、納得できる説明資料を用意しているかを問う項目です。説明資料がある場合は「はい」としてください。説明資料がない場合は「いいえ」としてください。

「６６．３　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？(6.11.C9)」

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(6.12)

「６７　記名・押印が義務付けられた文書を扱っているか？(6.12.C(1))」

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「はい」、取り扱っていない場合は「対象外」としてください。「はい」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

© JAHIS 2020

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。

「６７．１　HPKI 対応もしくは認定認証局が発行する証明書対応の署名機能があるか？(6.12.C(1))」

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 証明書もしくは認定認証局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。署名機能がある場合は「はい」、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。

「６７．２　HPKI 対応もしくは認定認証局が発行する証明書対応の検証機能があるか？(6.12.C(1))」

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 証明書もしくは認定認証局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。

「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。

「６７．３　日本データ通信協会認定のタイムスタンプが付与可能か？(6.12.C(2))」

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、一般財団法人日本データ通信協会が認定した時刻認証事業者のものを使用することが求められています。付与可能な場合は「はい」、そうでない場合は「いいえ」としてください。

「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。

「６７．４　日本データ通信協会認定のタイムスタンプが検証可能か？(6.12.C(2))」

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、一般財団法人日本データ通信協会が認定した時刻認証事業者のものを使用することが求められています。検証可能な場合は「はい」、そうでない場合は「いいえ」としてください。

「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検証機能がない場合は「対象外」としてください。

「６７．５　保存期間中の文書の真正性を担保する仕組みがあるか？(6.12.C(2))」

本項目は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 JIS 規格である CAdES、XAdES などの機能、又はそれと同等の真正性を確保する

© JAHIS 2020

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」、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。

「６８　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？(6.12.C(3))」

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」、そうでない場合は「いいえ」としてください。

真正性の確保について(7.1)

「６９　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？(7.1.C 医療(1).a-1)」

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、特定の装置若しく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。入力者及び確定者の認証機能があるならば「はい」、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。

「６９．１　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？(7.1.C 医療(1).a-2)」

真正性を担保するためには、故意または過失による虚偽入力、書き換え、消去及び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らば「はい」、そうでない場合は「いいえ」としてください。機能が不要ならば「対象外」としてください。

「６９．２　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？(7.1.C 医療(1).a-2)」

本項目は、権限管理の機能を有するかを確認するものです。

権限管理しているならば「はい」、そうでない場合は「いいえ」としてください。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。

「６９．３　サービス事業者内の利用者の権限管理の機能があるか？(7.1.C 医療(1).a-2)」

本項目は、一般ユーザではなく、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。サービス事業者が利用をできない等の場合は「対象外」としてください。

「６９．４　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？(7.1.C 医療(1).a-2)」

本項目は、一般ユーザではなく、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。サービス事業者が利用をできない等の場合は「対象外」としてください。

© JAHIS 2020

「６９．５　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？(7.1.C 医療(1).a-3)」

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確認するものです。
利用可能な端末を管理する機能を有するならば「はい」、そうでない場合は「いいえ」としてください。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。

「６９．６　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？(7.1.C 医療(1).a-3)」

本項目は、一般ユーザではなく、サービス事業者内の利用者に対して権限管理の機能を確認するものです。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ならば「はい」、そうでない場合は「いいえ」としてください。機能が不要ならば「対象外」としてください。

「７０　システムは記録を確定する機能があるか？(7.1.C 医療(2).a-1)」

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」、そうでない場合は「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。

「７０．１　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？(7.1.C 医療(2).a-1)」

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。
作成責任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。

「７０．２　「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？(7.1.C 医療(2).a-2)」

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。

「７０．３　確定された記録に対して、故意による虚偽入力、書き換え、消去及び混同を防止する機能があるか？(7.1.C 医療(2).a-4)」

真正性の確保のためには、確定後のデータに対し、いかなる追記、変更及び消去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修正・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。

「７１　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

© JAHIS 2020

者の識別情報、作成日時を含めて記録する機能があるか？（7.1.C 医療(2).b-1)」

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、特定の装置若しく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。

「７２　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？(7.1.C 医療(3)-1)」

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持っている場合は「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。

「７２．１　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？(7.1.C 医療(3)-2)」

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に、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持っている場合は「はい」、そうでない場合は「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。

「７３　代行入力の承認機能があるか？(7.1.C 医療(4))」

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。権限として代行権限が付与されているものも承認の中に含みます。

承認機能がある場合は「はい」、そうでない場合は「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。

「７３．１　代行入力が行われた場合、誰の代行が誰によっていつ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？(7.1.C 医療(4)-2)」

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、誰の代行が誰によっていつ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。

機能を持っている場合は「はい」、そうでない場合は「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。

「７３．２　代行入力により記録された診療録等を、確定者による「確定操作(承認)」を行う機能があるか？(7.1.C 医療(4)-3)」

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。

© JAHIS 2020

機能を持っている場合は「はい」、そうでない場合は「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。

「７４　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？(7.1.C 医療(5)-1)」

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。

「７５　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？(7.1.C 医療(5)-2)」

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。

「７６　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盛り込んでいて、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？(7.1.C 医療(5)-3)」

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、それを教育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。

「７７　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？(7.1.C 医療(5)-4)」

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。

「７８　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？(7.1.C 外部(1))」

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、備考に状況を記載してください。

「７９　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？(7.1.C 外部(2))」

本項目は、改ざんされないことを保証するものではなく、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。そうでない場合は「いいえ」としてください。

「８０　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？(7.1.C 外部(3))」

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。

© JAHIS 2020

見読性の確保について(7.2)

「８１　患者ごとの情報の全ての所在が日常的に管理されているか？(7.2.C(1))」

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。

「８２　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は対応づけて管理され、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ているか？(7.2.C(2))」

電子媒体に保存された全ての情報に関し見読化手段が常に対応付けられている場合は「はい」、そうでない場合は「いいえ」としてください。

「８３　目的に応じて速やかに検索結果を出力する機能もしくはサービスがあるか？(7.2.C(3))」

見読性とは、保存された情報を目的に対して支障のない応答速度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、見読性を確保するために、目的に応じて速やかに検索し表示する機能を有するかを確認するものです。『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の出力ができるように見読化手段を備えている場合は「はい」、そうでない場合は「いいえ」としてください。

「８４　システム障害に備えた冗長化手段や代替え的な見読化手段はあるか？(7.2.C (4))」

システム障害に備えた冗長化手段や代替え的な見読化手段がある場合は「はい」、そうでない場合は「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。

「８４．１　冗長化手段があるか？(7.2.C (4))」

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。冗長化手段がある場合は「はい」、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。

「８４．２　システム障害に備えた代替的な見読化手段があるか？(7.2.C (4))」

本項目は、代替的な見読化手段の具体的な内容をについて確認するものです。代替的な見読化手段には一般的な記録形式（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。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(7.3)

「８５　いわゆるコンピュータウイルスを含む不適切なソフトウェア等による情報の破壊・混同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？(7.3.C 医

© JAHIS 2020

療(1)-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や混同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。

「８６　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、医療機関等への SLA 等が文書として提供されているか？(7.3.C 医療(2)-1)」

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およ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。

「８７　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？(7.3.C 医療(2)-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、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。

「８８　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？(7.3.C 医療(2)-4)」

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。
そのような機能がある場合は「はい」、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。

「８８．１　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？(7.3.C 医療(2)-4)」

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。

「８９　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

© JAHIS 2020

うにしているか？(7.3.C 医療(2)-5)」

本項目は、システムが保存する情報がき損した場合に、作成しているバックアップデータを用いて、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。

「９０　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？(7.3.C 医療(4)-1)」

標準形式とは安全管理ガイドライン第５章に記載されている国際標準、業界標準等のことです。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。
機能がある場合は「はい」、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。

「９１　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？(7.3.C 医療(4)-2)」

マスタデータベースの入れ替えの際に、医療機関等が運用管理規程と手順書を設け、それにしたがって実施を支援するサービスやしくみ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。

「９２　外部保存を受託する機関は、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？(7.3.C 外部(1))」

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。

「９３　SLA 等に医療機関等に対して設備の条件を提示していて、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？(7.3.C 外部(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(9.)

「９４　診療録などをスキャナなどにより電子化して保存する機能があるか？(9.1.C1)(9.4)」

スキャナなどによる電子化により診療録等の情報を電子保存する機能がある場合は「はい」、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。

「９４．１　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？(9.1.C1)」

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

© JAHIS 2020

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」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。

「９４．２　電子署名・タイムスタンプ等を行える機能があるか？(9.1.C2)(9.4.C2)」

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、タイムスタンプを行う機能を有するかを確認するものです。

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。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。

© JAHIS 2020

付録．作成者名簿

作成者（社名五十音順）

日高　昇治	（一社）ASP・SaaS・AI・IoT クラウド産業協会	
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	◎JAHIS 主査
高野　博明	コニカミノルタ　（株）	
葉賀　功	コニカミノルタ　（株）	
平田　泰三	シーメンスヘルスケア（株）	◎JIRA 主査
松元　恒一郎	（一社）電子情報技術産業協会	
野津　勤	（株）システム計画研究所	
西田　慎一郎	（株）島津製作所	
山本　智仁	セコム　（株）	
長谷川　博司	ソフトウェアサービス（株）	
村松　和彦	日本光電工業（株）	
梶山　孝治	（株）日立製作所	
武者　義則	日立ヘルスケアシステムズ（株）	
渡邊　克也	PHC（株）	
村田　公生	富士フイルム（株）	
茗原　秀幸	三菱電機（株）	

© JAHIS 2020

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
2020/xx	Ver.4.0	サービス事業者対応、タイトルの変更

（ＪＡＨＩＳ標準　２０－ｘｘｘ）
２０２０年ｘ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. 4.0

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

(無断複写・転載を禁ず)

© JAHIS 2020