JAHIS

ＪＡＨＩＳ標準１７－００６

Japanese Association of Healthcare Information Systems Industry

ＪＡＨＩＳ
「製造業者による医療情報セキュリティ開示書」ガイド
Ver.3.0a

２０１７年７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「製造業者による医療情報セキュリティ開示書」ガイド　Ver.3.0a

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。

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のが現状です。このことは、医療機関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：セキュリティ開示書)」の書式を作成しました。この標準的な書式を用いることにより、製造業者と医療機関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、医療機関が医療情報システムによって送信され維持される健康情報に関するリスクアセスメントおよびリスクマネジメントを行うとき、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。

この文書は、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の解説とからなっています。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。

2017 年7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

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のセキュリティ機能に関して、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にとって有用な情報を提供すること。
当該システム導入医療機関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、製造業者により提供される情報をリスクアセスメントの材料とすること。
（3）各製造業者にとって、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）医療機関が製造業者にセキュリティ機能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です。例えば、ある型名の製品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機能の具体的内容の記載を可能としています。

本チェックリスト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。
１３～２８	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。
２９	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、多くの箇所で利用されて標準となることを目指し、さらには各製造業者がホームページなどで公表す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、記入した製造業者が全責任を負います。

2. 引用文献・参考文献

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

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

3. 用語の定義

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。

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
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

5.1 チェックリストの書き方

チェックリストは二部構成となっています。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、備考欄は自由記述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　　：対象となる製品の製造業者の名称を記述します。
製品名称　　：製品の名称・型名を記述します。
バージョン　　：製品のバージョン（版番号）を記述します。
作成日　　：チェックリストの記載日を記述します。

（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。

はい　　：質問に対応している場合に選択します。オプションで対応可能な場合は備考欄にその旨を記述します。
いいえ　　：質問に対応していない場合に選択します。
対象外　　：製品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」に対応する番号を記述します。実際の内容は「備考記載欄」に記述します。備考欄には、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述ください。

（3）備考記載欄

左欄に”備考”にて明示した番号を記述し、右欄に内容の記述を行います。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本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。

5.2 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)	はい	いいえ	対象外	備考____
・生体認証(指紋等)	はい	いいえ	対象外	備考____
・物理媒体（IC カード等)	はい	いいえ	対象外	備考____
・その他（具体的な方法を備考に記入してください）	はい	いいえ	対象外	備考____
・上記のうちの二要素を組み合わせた認証	はい	いいえ	対象外	備考____
4．1．1　パスワードを利用者認識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(1)～6.5.C11(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が出来るか？（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仕組みがあるか？（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.C.12）	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もしく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　非常時機能又は、非常時アカウントを持っているか？（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.C1）
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（SSL/TLS、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____

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____

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

専用線　はい　いいえ　対象外　備考____
公衆網　はい　いいえ　対象外　備考____
IP-VPN　はい　いいえ　対象外　備考____
IPsec－VPN　はい　いいえ　対象外　備考____
TLS1.2　高セキュリティ型、クライアント認証　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.(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.(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.(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.(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.(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.(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.(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.(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.(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.(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.(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.(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.(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.(4)-3)　はい　いいえ　対象外　備考____

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____

２１．１　冗長化の内容は？(7.2.C.(4))

・サーバの冗長化　はい　いいえ　対象外　備考____

・ネットワークの冗長化　はい　いいえ　対象外　備考____

・ストレージの冗長化　はい　いいえ　対象外　備考____

・その他の手段(具体的な方法を備考欄に記入してください)　備考____

２１．２　システム障害に備えた代替え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.(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.(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.(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.(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.(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.(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.(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.(4)-1）　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.）
２９　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.C-1）（9.4.） はい　いいえ　対象外　備考____ ２９．１　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.C-1） はい　いいえ　対象外　備考____ ２９．２　電子署名・タイムスタンプ等を行える機能があるか？（9.1.C-2）（9.4.C-2） はい　いいえ　対象外　備考____

備考記載欄	

６.チェックリストの解説

６．１　「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」と回答してください。「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。

６．２　「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には「はい」、そうでない場合には「いいえ」、対象機器が本項目に該当しない場合は「対象外」と回答してください。補足事項がある場合は、備考に記載してください。

６．３　「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恐れがある場合は、クリアスクリーン等の対策がされている場合には「はい」、そうでない場合には「いいえ」、対象機器が本項目に該当しない場合は「対象外」と回答してください。補足事項がある場合は、備考に記載してください。

６．４　「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」、出来ない場合は「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、本項への回答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“をよく理解してください。

６．４．１　「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載してください。

６．４．１．１　「４．１．１　パスワードを利用者認識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(1)～6.5.C11(3))」

パスワードを利用者認識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」、出来ない場合は「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。

６．４．１．２　「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」を、運用により行うことを求める場合には「いいえ」として下さい。

６．４．２　「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、職種別のアクセス管理機能がある場合は「はい」としてください。

６．４．３　「４．３　アクセス記録(アクセスログ)機能があるか？（6.5.C7)」

製品に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。

６．４．３．１　「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)」

アクセスログにおいて操作者、アクセスした時間(ログイン時刻、操作時間)、アクセスした個人情報を特定し、確認を行う手段がある場合は「はい」としてください。

６．４．３．２　「４．３．２　アクセスログへのアクセス制限が出来るか？（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」としてください。

６．５　「５　時刻情報の正確性を担保する仕組みがあるか？（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」としてください。

６．６　「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（たと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」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。

６．７　「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.C.12)」

無線 LAN を使用している場合に C.12 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。

６．８　「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には「はい」、制限する機能が無い場合には「いいえ」、ソフトウェアのインストール自体が出来ない場合には「対象外」としてください。

６．９　「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出来るか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には「はい」、出来ない場合には「いいえ」、外部入出力装置を持たない場合には「対象外」としてください。

６．１０　「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もしく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もしくは暗号化機能がある場合には「はい」、無い場合には「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には「対象外」としてください。

６．１１　「１１　非常時機能又は、非常時アカウントを持っているか？（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が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には「はい」、無い場合には「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）には「対象外」としてください。

６．１２　「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.C1）」

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のことを言います。

上記のような通信機能がある場合には「はい」、無い場合には「いいえ」としてください。「はい」の場合は、１２．１～４の質問に回答してください。

６．１２．１　「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欄に記載記入してください。

６．１２．２　「１２．２　データの暗号化（SSL/TLS、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」、機能を有しない場合は「いいえ」としてください。補足説明が必要な場合は、使用している暗号の仕様を備考欄に記入してください。

６．１２．３ 「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、ファイアーウォールなど)、もしく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、１２．３．１～１２．３．２の質問に回答してください。

６．１２．３．１ 「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。

６．１２．３．１．１「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」として備考欄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。

６．１２．３．２ 「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。

６．１２．４ 「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、１２．４．１の質問にも回答してください。

提供している場合は「はい」、していない場合は「いいえ」としてください。

６．１２．４．１ 「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。

６．１３ 「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。
「はい」の場合は、１３．１以降の５項目の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。

６．１３．１　「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作成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。
作成機能がない場合は「対象外」となります。作成機能がある場合、「はい」の場合は備考に対応している証明書を記載してください。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ますので、可能ならば備考に当該システムと連携可能な署名機能の提供方法を記載してください。

６．１３．２　「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。
参照機能がない場合は「対象外」となります。検証機能がある場合、「はい」の場合は備考に対応している証明書を記載してください。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ますので、可能ならば備考に当該システムと連携可能な署名検証機能の提供方法を記載してください。

６．１３．３　「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。
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」となります。作成機能がある場合、「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ますので、可能ならば備考に当該システムと連携可能なタイムスタンプの付与方法を記載してください。

６．１３．４　「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。
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」となります。参照機能がある場合はタイムスタンプの検証機能が必要になります。「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ますので、可能ならば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。

６．１３．５　「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、もしく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。

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」となります。「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ますので、可能ならば備考に当該システムと連携可能な真正性確保手段を記載してください。

６．１４　「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.(1).a-1)」

本項目は、電子カルテシステムなどで PC など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。そうでない場合は「対象外」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) 入力者及び確定者の識別認証」を参照すること”とされていますので、「はい」ならば、１４．１と１４．２の質問に回答してください。

６．１４．１　「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.(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」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」に記入してください。

６．１４．２　「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.(1).a-2）」

本項目は、上記質問で区分管理を行っていない場合においての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」を選択してください。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」に記入してください。

６．１５　「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.(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」を選択してください。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」に記入してください。

６．１６　「１６　システムは記録を確定する機能があるか？（7.1.C.(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」を選択してください。そうでない場合は「いいえ」を選択してください。「はい」ならば、１６．１～１６．３の質問に回答してください。

６．１６．１　「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.(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」を選択してください。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」を選択してください。

６．１６．２　「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.(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」を選択してください。そうでない場合は「いいえ」を選択してください。

６．１６．３　「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.(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」を選択してください。そうでない場合は「いいえ」を選択してください。

６．１７　「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.(2).b-1）」

本項目は、装置が確定機能は有していない場合、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」を選択してください。記録されない場合には「いいえ」を選択してください。

６．１８　「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.(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、その内容を参照する機能を持っている場合には「はい」、そうでない場合には「いいえ」、対象機器が本項目に該当しない場合は「対象外」と回答してください。補足事項がある場合は、備考に記載してください。

６．１８．１　「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.(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には「はい」、そうでない場合には「いいえ」、対象機器が本項目に該当しない場合は「対象外」と回答してください。補足事項がある場合は、備考に記載してください。

６．１９　「１９　代行入力の承認機能があるか？（7.1.C.(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承認機能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」、対象機器が本項目に該当しない場合は「対象外」と回答してください。「はい」ならば、１９．１と１９．２の質問に回答してください。

６．１９．１「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.(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には「はい」、そうでない場合には「いいえ」、対象機器が本項目に該当しない場合は「対象外」と回答してください。補足事項がある場合は、備考に記載してください。

６．１９．２「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.(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。

機能を持っている場合には「はい」、そうでない場合には「いいえ」、対象機器が本項目に該当しない場合は「対象外」と回答してください。補足事項がある場合は、備考に記載してください。

６．２０　「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」、そうでない場合には「いいえ」、対象機器が本項目に該当しない場合は「対象外」と回答してください。補足事項がある場合は、備考に記載してください。

６．２１　「２１　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)）」

見読性確保のためには、システムの一系統に障害が発生した場合でも、通常の診療等に差支えない範囲で診療録等を見読可能にすることが必要です。その対策としてはシステムの冗長化があります。冗長化とは、信頼性を高めるための技法のひとつで、システムやネットワークの予備構成をとることです。例えば、デュプレックスシステム、デュアルシステム、フォルトトレラントシステム、マルチプロセッサシステム等です。本項目は、そのような冗長化手段や代替え的な見読化手段を有しているかを確認するものです。

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」と回答してください。　補足事項がある場合は、備考に記載してください。「はい」ならば、２１．１ならびに２１．２の質問に回答してください。

６．２１．１　「２１．１　冗長化の内容は？(7.2.C.(4))」

本項目は、冗長化の具体的な内容を確認するものです。それぞれの内容について持っている場合は「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」と回答してください。補足事項がある場合は、備考に記載してください。

６．２１．２　「２１．２　システム障害に備えた代替え的な見読化手段があるか？（7.2.C.(4)）」

本項目は、見読性の確保を項目２１でのシステムの冗長化ではなく、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機能を有しているかを確認するものです。

有する場合は「はい」、そうでない場合は「いいえ」と回答してください。代替的な手段の具体的な内容については備考にご記入下さい。

６．２２　「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.(1)-1）」

保存性とは、記録された情報が法令等で定められた期間に渡って真正性と見読性を確保することです。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。

そのための対策が施されている場合は「はい」、されていない場合は「いいえ」、そもそも原理的に影響を受けないことが明白な場合（例：ソフトウェアをインストールする機能がない）は「対象外」と回答してください。

６．２３　「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.(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。

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」と回答してください。

６．２４　「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.(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」と回答してください。

６．２５　「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.(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」と回答してください。「はい」ならば、２５．１の質問に回答してください。

６．２５．１　「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.(2)-4）」

本項目は、項目２５の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」と回答してください。

６．２６　「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.(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。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なっていることでも構いません。
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」と回答してください。

６．２７　「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.(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」と回答してください。

６．２８　「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.(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」、対象となる製品が情報を保存しない場合は「対象外」と回答してください。

６．２９　「２９　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.C-1）（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には「はい」、ない場合には「いいえ」と回答してください。「はい」ならば、２９．１、２９．２の質問に回答してください。

６．２９．１　「２９．１　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.C-1）」

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」と回答してください。どのユースケースに適合する

システムかについては「備考欄」に記載してください。

６．２９．２　「２９．２　電子署名・タイムスタンプ等を行える機能があるか？（9.1.C-2）（9.4.C-2）」

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。

機能がある場合には「はい」、ない場合には「いいえ」と回答してください。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欄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）

下野　兼揮	(株)グッドマン	◎JAHIS 主査
五十嵐　隆史	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
野津　勤	(株)システム計画研究所	
西田　慎一郎	(株)島津製作所	
藤咲　喜丈	日本光電工業(株)	
梶山　孝治	(株)日立製作所	
村田　公生	富士フイルム(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
2017/07	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（安全管理ガイドラインの C 項の項番訂正ならびに誤植の修正）
2018/01	同上	誤記の訂正（項目番号の訂正：下記正誤表に記載）

正誤表

P.1　「１．適用範囲」

誤）

１～１３　　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。

１４～２８　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。

正）

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。

１３～２８　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。

（ＪＡＨＩＳ標準　１７－００６）

２０１７年7月発行

ＪＡＨＩＳ「製造業者による医療情報セキュリティ開示書」ガイド　Ver. 3.0a

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