「医療情報システムの安全管理に関するガイドライン」

対応のための手引き

Ver1.00

2016 年 3 月 1 日

特定非営利活動法人デジタル・フォレンジック研究会「医療」分科会

一般社団法人メディカルＩＴセキュリティフォーラム

合同委員会

【改定履歴表】

日付	Ver No.	簡単な内容
2016.3.1	1.00	初版

はじめに：

愛知医科大学医療情報部長・特任教授
一般社団法人メディカル IT セキュリティフォーラム　代表理事
深津　博

個人情報の中でも医療情報は、その機微性の高さから、管理・運用に特別な配慮が必要である。医療分野の監督官庁である厚生労働省は、2005 年の個人情報保護法の施行以降、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」（平成 16 年 12 月 24 日通知、平成 18 年 4 月 21 日改正、平成 22 年 9 月 17 日改正）、「医療情報システムの安全管理に関するガイドライン」（最終第 4.2 版：2013 年 10 月）等、様々なガイドラインや通達を提示し、具体的な対応方法や指針を示してきた。

また文部科学省と厚生労働省の共同で、「人を対象として医学系研究に関する倫理指針」（2014 年 12 月）も公表し、診療分野のみならず研究分野における個人情報の取扱いの方針についても、示している。

2015 年の５－７月に発生した、日本年金機構のサイバー攻撃による個人情報の漏えいに端を発する一連のサイバー攻撃事案は、国民に大きな衝撃を与え、個人情報の管理方針についても、再検討をすべき事態となった。

上記の種々の指針のうち、「医療情報システムの安全管理に関するガイドライン第 4.2 版」は、医療機関が、受診者の個人情報を預かって管理するための技術的な対策や運用面での対策について、網羅的に記載したもので、この記載内容を今一度吟味し、それぞれの医療機関において、記載事項が遵守されているか、またどの分野について不十分であるかを把握し、対応策を最新化することが社会的な要請であると考えられる。

しかしながら、ガイドラインの記載内容は技術的な要件を基準として分類・記述されており、医療機関の情報管理担当者が一読してどのような対策を行えばよいのか、という管理する側の視点からの記載がなされていない。このために、実際の対策を検討する側が、内容を把握しづらく、場合により不十分な理解のまま対策を実施することになりかねない状況が存在すると考えられる。

一般社団法人メディカルＩＴセキュリティフォーラムは、このような状況を改善するために、システムの利用者（特に管理する部門）が「何を行えばガイドラインが遵守できるのか」という視点に立った本手引きを作成することを起案し、上記ガイドラインの技術的対策を記載した 6 章部分を中心に、その原案を検討してきた。その過程で、問題意識を共有する特定非営利活動法人デジタル・フォレンジック研究会等と合同で、６章部分のみならず、全ての章について同様の観点で本手引きを作成することに合意し、その作業を進めてきたが、今回その草案が取りまとめられたので、ここに公開するものである。

今後個人情報保護法の改正に伴い、上記ガイドラインの記載内容や、管理体制の変更も考えられるが、その都度必要に応じて、本手引きの更新・改訂も行っていく予定である。

上記のような経緯から、本手引きは、医療機関において医療情報の安全管理を担当している部署のシステム管理者等を主たる対象として書かれている。

本手引きが、医療情報の安全管理担当者にとってより深い理解と、方向性の把握に寄与できれば幸いである。

目　次

■凡例

本手引きでは、医療情報システムの安全管理に関するガイドライン４．２版を『安全管理ガイドライン』と略称する。

また、外部文書は『』、外部文書からの引用は「」で表示している。

１章：契約・合意と責任分界点

医療従事者は、医療行為に伴って文字、画像、検査数値、波形等大量の情報を取り扱い、その一部については法令により、文書化と保存が義務付けられている。また、この保存義務を持つ文書の一部は電子データとして作成・保存することが真正性・見読性・保存性の確保を条件に認められている（安全管理ガイドライン 4 章参照）。

医療機関等は取り扱う情報の安全管理を、さらに、保存義務のある記録の電子保存に当たってはその真正性・見読性・保存性を、医療情報システムの実装及び機関内部の運用管理体制により担保する必要がある。

これらは、医療機関等と患者との間で観念される、医療サービスの提供を主たる目的とする民法上の契約[1]（以下医療契約と呼ぶ）に基づく、善良な管理者としての注意義務（善管注意義務、民法 644 条）とされており、単なる自己の私的財産に対するのと同様の注意では足りず、業務上個人の健康情報を大量に取扱い、法律上秘密保持の義務を有する専門家としての地位に応じ、社会通念上客観的・一般的に要求される注意を払う必要がある。

しかし、当然のことながら医療情報システムの企画・設計・調達・実装・運用・保守・廃棄に至るすべてを医療機関等が自らで完結することはできないため、ベンダをはじめ外部事業者に対する委託が発生する。

その場合、医療機関等が委託した外部事業者（委託先事業者）は単なる＜購買先＞ではなく、医療機関等の業務を補完する存在であるから、医療機関は善管注意義務の一つとして、受託先に対して、提供される機材・サービスの選定や利用に必要な情報の提供を求め、また委託先事業者の管理の実態に応じ、適切な監督を行なう義務を有する[2]。

さらに、情報漏えい等のインシデントが発生した場合には、被害を局限化し、その原因を追究するとともに再発防止策を講じ、患者への説明、監督官庁への報告、損害を発生させた場合にはその補償、場合によっては社会への公表等も必要となるが、実施に当たっては適宜委託元医療機関と委託先事業者が共同して対処する必要がある。

従って、安全管理ガイドラインでは、医療機関と委託先事業者との役割分担の線引きともいえる＜責任分界点＞を明確にした上で、安全管理ガイドライン各章に定める管理策のうち、以下の表に記した事項については契約や SLA[3]等の合意によって双方の間でその内容

---

[1] 法的性質については諸説あるが、民法 656 条に基づく『準委任契約』と考えるのが現在の裁判例の考え方であり、法学界の通説である。

[2] 委託先から個人情報が漏えいした事案につき、委託先に対する適切な監督を行なっていなかったとして委託元の使用者責任（民法 715 条）を認定した判決として、大阪高判平成 13 年 12 月 25 日判自 265 号 11 頁（宇治市住民基本台帳データ漏えい事件控訴審判決。その後最決平成 14 年 7 月 11 日で上告不受理となり確定）、東京高判平成 19 年 8 月 28 日判タ 1264 号 299 頁（エステティックサロン個人情報漏えい事件控訴審判決（確定））などがある。

[3] Service Level Agreement の略記。情報処理や通信に関するサービスを外部から受ける際に、サービス利用者と提供者の間でサービスの内容や水準について合意した事項を文書化したもの。『サービスレベル合意書』『サービス品質保証』などと訳される。

を明確にすることを求めている。

なお、患者への医療契約に基づく責任は一次的に医療機関が負い、委託先事業者は患者に対し直接責任を負わないが、委託先事業者の故意・過失による違法行為と損害との因果関係が認められる場合は、委託先事業者も被害者に対して直接責任を負う場合がある[4]。

表 1 安全管理ガイドラインで記載されている契約等により明らかにすべき事項

分野	内容	ガイドラインの関係項番
情報システムの基本的な安全管理	人的安全対策	6.6
	情報システムの改造と保守	6.8
	災害等の非常時の対応	6.10
	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
診療録及び診療諸記録を外部に保存する際の基準	外部保存を受託する機関の情報の取り扱い、情報の提供	8.1.2B2、3
	個人情報の保護	8.1.3
	外部保存契約終了時の処理について	8.4.2

[4] 大判昭和 12 年 6 月 30 日民集 16 巻 1285 頁

２章：標準化

情報システムにとって可用性、つまり必要な時に必要な分だけ適時且つ適切にシステムを利用することができるという条件は不可欠である。これは医療/非医療を問わず、全ての情報システムに言えることだが、医療情報システムにおいては可用性とは同時に「医療機関等で医療情報を長期間保存する際に、システム更新を経ても旧システムで保存された医療情報を確実に利用できるようにしておくこと」、つまり「相互運用性を確保すること」とをも意味している。

安全管理ガイドラインでは、標準化が不可欠の要素である相互運用性を確保するための厚生労働省標準規格、基本データセット、用語集等について標準化に係る諸規約を解説している。医療情報システムの実運用に際して相互運用性をどのように設計・確保するかという点については安全管理ガイドラインの述べるとおりであるため、ここではさらにもう一歩遡り、医療情報システムの調達に際した留意事項を解説する。

医療情報システムの多くはベンダが提供するものであり、自機関内の情報管理部門が新規に内製化したシステムを用いているケースは非常に少ない。ベンダにより提供・保守される情報システムを利用するということは、言いかえれば、当該事業者がシステム保守を何らかの理由でできなくなった場合、そのシステムの継続利用が困難になる事態を意味している。多くの医療情報システムはパッケージシステムとして導入・運用されており、その設計情報の開示は企業機密であるため契約上不可とされるケースが多い。このような条件下では、システム内部のプログラムソースはどのようにコーディングされているのか、データベースのスキーマはどのように設計されているのか等、システムの設計情報を入手することができないため、別のベンダが提供するシステムへの切替を行うこと、あるいは自前で内製システムを製造することが難しくなる事態を招く。

よって、システムの調達に際しては、別システムへの切り替え・移行を前提とした観点より、システム上で電子的に取り扱う医療データの規格、医療データ交換の規約等、データ移行に必要な情報を自機関が十分に把握できる措置を事前に講じることが望まれる。例えば、該当システムの他システムへのデータ移行に必要な技術設計情報を自機関に開示してもらい、他のベンダが提供するサービスへの切り替え等を円滑に実施可能とする契約条項の実現可否を該当事業者と事前に交渉すること等が一案として考えられる。特に、電子化された医療情報に係る規格・規約が切り替え・移行前システムと同程度の水準にて新しいシステムにおいても利用できるか否かについては、従来と同質の診療上の効率性という観点に加え、患者の保護という観点においても重要になることから、確実に検討しておく必要がある。

３章：システム構築時

３．１ ベンダが提供するシステム機能の確認

安全管理ガイドライン６章では、医療機関等において患者情報を取り扱う上で、「安全管理が十分であることを説明できること、つまり説明責任を果たす」ための技術的・運用的要件が、組織・物理・技術・人等、様々な安全管理措置の観点より整理されている。このような様々なセキュリティ要件を充足する医療情報システムの調達仕様書を情報処理関連事業者単位で作成し、対応していくことは現場にとって負荷の高い業務になるとともに、事業者にとっても、機関単位で用語の異なる多様な仕様書に個別対応することは著しいリソースを要求されることになる。

こうした課題に対して、一般社団法人保健医療福祉情報システム工業会（以下、『JAHIS』）、及び一般社団法人日本画像医療システム工業会(以下、『JIRA』)は、安全管理ガイドラインの６章～９章が求める要件のうち、技術的要件の適応状況をチェックリスト形式で確認できるガイドとして、『「製造業者による医療情報セキュリティ開示書」ガイド』(以下、「MDS」と記載)を公表している。

このガイドの目的は以下の４点とされている。原文をそのまま引用するが、本文の【製造業者】は【ベンダ】と読み替えて頂きたい。

(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。

上述の通り、ベンダによる安全管理ガイドラインへの技術的な適応性を確認するとともに、医療機関等において、技術的要件でカバーされていない範囲については他の機能で実施する、あるいは運用要件の必要性を検討（リスク評価）するために活用することを目的の一つとしている。よって、医療機関等による医療情報システムの調達に際して、当該チェックリストに基づく仕様書を作成し、該当システムにおける技術的な要件充足の有無を判断した上で、どのような全体システム構築と運用を行うかを検討するための有益な材料としてMDSを活用することが推奨される。

なお、MDSでは、安全管理ガイドライン上の「保存義務のある診療録等を電子的に保存する場合の指針」（７章)、「保存義務のある診療録等を医療機関等の外部に保存する場合の指針」（８章)、「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指針」を

踏まえたチェックリストを提供している。そのため、６章～９章までを通貫した包括的なチェックが可能であることも特徴である。

なお、システム機能確認に際しては、ベンダの提供する意図する使用環境、すなわち、機能の目的、使用される状況、使用者のプロファイル、などを考慮に加えることも重要な事項である。

３．２ 工業会が発行している実装用ガイド

上述した MDS をより効果的に活用するため、特に検討が難しいと想定される以下の分野については、個別具体的に参照することが望ましい独立したガイドラインが存在する。その分野とは、①監査証跡、②リモートメンテナンス、③シングルサインオン、④電子署名に係る分野である。

なお、これらのガイドラインは基本的にベンダを対象として作成されていることから、一部は技術的な専門性の高い内容となっている。しかしながら、ベンダが提供するシステム機能の確認に際して、当該ガイドラインの内容を概略的にでも把握した上で、該当技術・機能の実装有無を必要に応じて事業者に確認できるようにすることが、医療機関等のシステム管理者には推奨される。

①監査証跡について

本ガイドでは監査証跡についてアクセスログ等の表現で記載されているが、実際にこれらのログをどの程度の粒度で取得すればよいのか、どのシステムレイヤにおける、どのイベントに係る、どういったメッセージをどのような形式で取得すると、どのような内容が確認（監査）できるのかについては、当然のことながら、システム個別に異なっており、システム管理者の頭痛の種となっていると思われる。JAHIS が公表する『ヘルスケア分野における監査証跡のメッセージ標準規約』はこの悩みを解消するための回答である。本規約は、ISO や IHE 等の動向も踏まえ、医療機関による監査証跡のメッセージ規約の標準化を目指したものであり、医療機関等が個人情報へのアクセスに際した説明責任を果たす上で有用な資料となる。

②リモートメンテナンスについて

大半の医療情報システムでは、高可用性を確保すべく、ベンダによるオンデマンドなリモートメンテナンスを可能とする環境が整備されている。一方、システム保守を外部委託する業者の管理監督、つまり外部委託先管理の観点、または当今話題となるサイバーセキュリティの観点より、リモートメンテナンスに求めるべきセキュリティ要件をどの程度まで充足すべきかについて、安全管理ガイドラインは直接的に言及するまでには至っていない。リモートメンテナンスの設計・運用はベンダによって多種多様であり、閉域網・公衆網・インターネット等の回線種別から、随時接続・常時接続等の回線接続形態、Windows リモートデスクトップ・IP-VPN・サードパーティ製専用ソフトウェア等による接続方式まで、様々な選択肢の組合せが存在する。こうした数ある選択肢のなかで、適切なセキュリティ要件を満たす方式を検討するために医療機関等が参照すべきものとして、JIRA・JAHIS が公表する『リモートサービスセキュリティガイドライン』が存在する。このガイ

ドラインは、国際標準として、ISO TR 11633 Part 1&2 として出版されたものであり、安全管理ガイドラインが求める具体的なリモートメンテナンス上のセキュリティ要件を詳述したものと考えることができる。

③シングルサインオンについて

医療情報システムの多くは、特定のポータルサイトへの ID・パスワードによる認証結果に基づく、その他複数のシステムへのアクセスを可能とするシングルサインオン技術を採用している。電子カルテ・オーダリングシステムを画像診断システムや検査システムの内容を参照しながら利用することが一般的な業務形態においては、シングルサインオンは一度の認証で他システムへのアクセスを可能にする利便性を持つ。その反面、設計を誤れば、本来閲覧すべきできない個人情報へのアクセス、修正すべきでないデータの修正（改ざん）を容易に招くリスクと隣り合わせである。よって、こうした技術の採用について医療機関固有の環境・リスクを踏まえた上で検討することが必要となる。この必要に応えるものが JAHIS の『シングルサインオン実装ガイド』である。このガイドではシングルサインオンの設計に際して留意すべきポイントが様々な事例とともに解説されており、安全管理ガイドラインが求めるアクセス管理の問題系を考える上で有用な資料である。

④電子署名について

安全管理ガイドラインでは医療等に係る文書記録に際して、「厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと」が求められている。電子署名によるタイムスタンプ技術の選定、あるいは改良をどのように行っていくべきか、具体的な実務基準は存在しないため、そのアプローチをどのようにすべきかについては一つの課題である。こうした課題に対して有益な参考資料として、JAHIS の『ヘルスケア PKI を利用した医療文書に対する電子署名規格』が存在する。この文書は安全管理ガイドラインが求める電子署名、タイムスタンプの要件を実装レベルで解説したものであり、業界標準としての水準がどの程度にあるかについて把握する上で有益である。

３．３ 医療機関における管理活動

一方、安全管理ガイドライン 6 章の内容を別の観点で整理したものもある。情報システムの基本的な安全管理に係る要件が想定するリスクをどのようにコントロールすべきかという観点より、医療機関等におけるシステム管理者・利用者が実施すべき事項を＜管理活動＞という単位に分類し、各事項の輪郭を体系的に整理した文書である。これは、一般社団法人メディカルＩＴセキュリティフォーラム（以下、MITSF）:『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４．２版」のガイダンス』（以下、「MITSF ガイダンス」）である。

MITSF ガイダンスでは、安全管理ガイドライン 6 章のうち、以下の節を対象として、管理活動を 13 の単位に整理している。

表 2『「医療情報システムの安全管理に関するガイドライン４．２版」のガイダンス』の対象範囲

安全管理ガイドライン　第 6 章：【情報システムの基本的な安全管理】	対象
6-1：方針の制定と公表	-
6-2：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（ISMS）の実践	○
6-3：組織的安全管理対策	-
6-4：物理的管理対策	○
6-5：技術的安全管理対策	○
6-6：人的安全管理対策	○
6-7：情報の廃棄	○
6-8：情報システムの改造と保守	○
6-9：情報および情報機器の持ち出しについて	○
6-10：災害時の非常時対応	○
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	-
6-12：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	○

表 3 管理活動の区分

No	管理活動
1	リスク評価
2	アカウント/権限の管理
3	パスワード管理
4	ログの点検管理
5	媒体・機器管理
6	入退室管理
7	外部委託先管理
8	無線 LAN 管理
9	廃棄データ管理
10	システム保守管理
11	事業継続管理
12	契約管理
13	電子証明書管理

但し、要件を満たすため MITSF ガイダンスに記載された管理活動を全て一律同じ水準で実施する必要がない点には留意が必要である。上記の管理活動は、＜リスク評価＞という活動の結果に基づき、管理資源を重点的に投入すべき範囲、現状と同等の管理で十分とする範囲、現状では過剰な管理が行われている範囲を識別した上で行われることが望ましい。つまり、自らの医療機関等における現状の技術上・運用上の取組水準と照らし合わせ、本来コントロールすべきリスクが適切に管理されていない範囲を見極めることが重要である。

また、同様に、自らの機関等において医療情報システムがどのように利用・管理されているかという、環境条件の考慮も必要となる。例えば、１人の医師のみが診療結果をクローズドネットワークにおける電子カルテシステムに記録管理する運用が行われ、さらにシステムのメンテナンス自体もその医師が行い、帰宅時には本人以外が開錠できない保管庫に格納しているような小規模な診療所を想定してみよう。そこでは上記の管理活動の多くは必要がないであろう。少なくとも、アカウント/権限の管理、パスワード管理、ログの点検管理等、個人情報への限定されたアクセス、及び情報の毀損・改ざん防止・発見を担保するための活動は必要なく、また外部委託先管理、契約管理等、不限定な第三者による個人情報へのアクセスを監督するための活動も不要となる可能性が高い。このように、個人情報が格納される医療情報システムがどのような環境のもとで利用・管理されているかという点も、管理活動の採用要否に際して影響を及ぼす要素となる。

コントロールすべきリスクが適切に管理されているかを自機関の環境条件を考慮した上で判断するためには、繰り返しとなるが、＜リスク評価＞という活動が重要となる。リスク評価を行う上での準拠枠として、安全管理ガイドラインでは、『ISO（ISO/IEC27001:2005)』、ならびに『JIS（JIS Q 27001:2006)』を「標準的なマネジメントシステム」として紹介しているが、当ガイダンスが整理した管理活動を効率的且つ効果的に実施する上での十分条件となる。この理解が不十分なまま管理活動の採否が判断され、運用されるようであれば、費用対効果の観点、またはリスク管理の観点からは合理性のない取組が行われてしまうことは肝に銘じる必要がある。

医療機関等がリスク評価を行う際に参考すべき資料には、一般財団法人日本情報経済社会推進協会（JIPDEC）が『医療機関向け ISMS ユーザガイド - JISQ27001:2006 (ISO/IEC27001:2005)対応 -』を公表している。本ガイドは財団法人医療情報システム開発センター(MEDIS-DC)、及び IMS 適合性評価制度運営委員会のメンバーを中心に、ISMS の構築あるいは認証取得を検討している医療機関等を対象としたものであり、医療機関等固有の環境・条件を考慮した現実的なガイドとなっている。

なお、管理活動区分のうち、事業継続管理の内容を検討する際には、JOINT NEMA/COCIR/JIRA SECURITY AND PRIVACY COMMITTEE(SPC)による『ブレークグラス── ヘルスケアシステムへの非常時アクセスを許すことへのアプローチ』が有効な参照先である。当該ガイドでは医療情報システムへの非常時アクセスが中心的なテーマとして解説されているが、災害下において通常システムが機能不全に陥り、当該システムに格納された診療データを非診療端末等で利用せざるを得ない事態を想定し、医療データを汎用性の高いツールで再現できる環境の準備の検討についても、事業継続管理における「見読性」の維持という観点から重要であるため、あわせて留意されたい。

４章：電子保存の３原則との対応

４．１ 電子保存の3原則とは

法令により作成・保存する義務のある記録（安全管理ガイドライン 3.1 参照）の電子化に当たっては、安全管理ガイドライン 7 章に電子データとして作成・保存することを認める条件が記載されている。

これが以下の 3 点からなる、いわゆる「電子保存の 3 原則」である。

（1） 正当な権限に於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、第三者からみて作成の責任の所在が明確であること（真正性：安全管理ガイドライン7.1）

（2） 電子媒体に保存された内容を、権限保有者からの診療、患者への説明、監査および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と操作方法で、肉眼で見読可能な状態にできること（見読性：同7.2）

（3） 記録された情報が法令等で定められた期間（付録３参照）にわたって真正性を保ち、見読可能にできる状態で保存されること（保存性：同7.3）

この原則は、平成 6 年 3 月 29 日の厚生省健康政策局長通知『エックス線写真等の光磁気ディスク等への保存について』で初めて打ち出され、後にその対象が診療録等のデータにも拡げられたものであるが、これは記録作成・保存の義務を課した制度・規定が、いずれも記録が紙・フィルムであることを前提として構築されていることから、「紙・フィルムとは異なる特性を持った電子データを書面と同等に取り扱うためにはいかなる要素が必要か」を検討した結果、打ち出されたものである。

よって、電子保存の 3 原則はあくまで安全管理ガイドライン 6 章その他の基準・ガイドライン等に基づいた安全管理策（安全対策）の実施が前提であり、電子保存の 3 原則が一般に考えられている情報セキュリティの原則に代わるものではない。

４．２ 電子保存の3原則と情報セキュリティの関係

一般に、情報セキュリティとは、情報に関する以下の特性を維持することと定義されている。

（1） 機密性：許可されていない個人、エンティティ（情報にアクセスしようとする人、他の情報システム・装置等のこと）またはプロセスに対して、情報を使用させず、また、開示しない特性（『JIS Q27000:2014[5]』 2.12）

（2） 完全性：正確さ及び完全さの特性（『JIS Q27000:2014』 2.40）

（3） 可用性：認可されたエンティティが要求したときに、アクセス及び使用が可能である特性（『JIS Q27000:2014』 2.9）

上記の要素を情報セキュリティの 3 要素、又は機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の英語の頭文字を取って情報セキュリティの CIA と

[5] ISO/IEC27000 の公式日本語訳文であり、対応する国内規格である。

呼んだりするが、『ISO/IEC 13335-1』（GMITS）の発行（同規格の前身となる Technical Report の発行開始は 1996 年）以降、セキュリティの対象に応じて以下の 4 特性を独立した要素として追加する考え方が有力であり（『JIS Q13335-1:2006』4.3、『JIS Q27000:2014』2.33 注記）、これらを情報セキュリティの拡張 7 要素と呼ぶ。

（4） 真正性：ある主体又は資源が，主張どおりであることを確実にする特性（『JIS Q13335-1:2006 2.3）、エンティティは、それが主張するとおりのものであるという特性（『JIS Q27000:2014』 2.8）

（5） 責任追跡性：あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できることを確実にする特性（『JIS Q13335-1:2006』 4.3、『JIS Q27000:2014』 2.33注記）

（6） 否認防止：ある活動又は事象が起きたことを，後になって否認されないように証明する能力（『JIS Q13335-1:2006』 2.16）、主張された事象又は処置の発生、及びそれを引き起こしたエンティティを証明する能力（『JIS Q27000:2014』 2.54）

（7） 信頼性：意図した動作及び結果に一致する特性（『JIS Q13335-1:2006』 2.17）、意図する行動と結果が一貫しているという属性（『JIS Q27000:2014』 2.62）

そして、これらの要素を損なう状況が発生し、自組織に損失が発生するリスクが情報セキュリティリスクである。

なお、安全管理ガイドラインでは、医療情報システムの構築・運用において情報セキュリティリスクを低減するための基本的な管理策（安全対策）については 6 章、電子保存の 3 原則の確保に関する管理策は 7 章に規定されている。

しかし、電子保存の 3 原則は医療情報システムに必要なセキュリティ対策の一要素として位置づけることが可能である。具体的には、電子保存の 3 原則における真正性は情報セキュリティの拡張 7 要素でいう責任追跡性・真正性・否認防止と、見読性は完全性・可用性・信頼性と、保存性も同じく完全性・可用性・信頼性の各要素とそれぞれ結びつけることができる。

よって、医療情報システムに情報セキュリティを組み込む際には、電子保存の 3 原則についても情報セキュリティによって確保されるべき要素の一つとして理解し、その観点から管理策を検討することが有効である。

すなわち、電子保存の 3 原則を担保するためには 7 章の管理策に 6 章の管理策を併用する必要がある。また、電子保存の 3 原則の対象外である記録データについても、情報セキュリティリスク低減のため有効と考えられる場合は、6 章の管理策に加え 7 章の管理策を参考にすることが有用である。

５章：クラウドを利用した外部保管

５．１ 外部保管先としてのクラウドとは

安全管理ガイドライン８章では「診療録及び診療諸記録を外部に保存する際の基準」として、診療録等を外部保存する受託機関を選定する基準を３つ挙げているが、このうち医療機関等が一般的に採用する基準は「病院、診療所が自ら堅牢性の高い設備環境を用意し、近隣の病院、診療所の診療録等を保存する、ASP・SaaS 型のサービスを提供するような場合」であり、その際に最も利用される傾向が高いサービスは、情報処理関連事業者が提供する＜クラウド＞サービスと想定される。

当今、情報技術環境の進展により、＜クラウド＞という単語が巷間を賑わせており、一般企業同様、医療機関等においても診療録等をクラウドサービスへ外部保存する運用を採用しているところも増加している。前述の通り、安全管理ガイドラインでは「診療録及び診療諸記録を外部に保存する際の基準」が 8 章に定められており、この管理要件が遵守され、且つ、「データセンター等の情報処理関連事業者が、経済産業省が定めた『医療情報を受託管理する情報処理事業者向けガイドライン』や総務省が定めた『ASP・SaaS における情報セキュリティ対策ガイドライン』及び『ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン』の要求事項を満たしていることを確認の上、契約等でその遵守状況を明らかに」するかぎりにおいて、当該事業者が提供するクラウドサービスにて診療録等を保管・利用することに特に問題はない。

しかし、クラウドサービス上で診療録等を利用・管理する場合には、同時にクラウドコン ピューティングという仕組を実現する技術的な要件に係るリスクを検討する必要がある。そもそもクラウドとは何か？クラウド自体がまさにその名の通り、雲のようにつかみどころのないバズワードとして流通していたサービス初期とは異なり、現在ではある程度までその実態の輪郭を掴める程度には情報が整理されてきている。米国国立標準技術研究所（NIST: National Institute of Standards and Technology）では、クラウドコンピューティング（＝＜クラウド＞）を「共用の構成可能なコンピューティングリソース（ネットワーク、サーバ、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ提供されるもの」[6]と定義し、SaaS/PaaS/IaaS といったサービスモデル、プライベート・パブリック・ハイブリットといった実装モデルにより分類・整理を行っているが、こうした技術専門的な話は省略し、ここではクラウドが何故好まれるのかという点を中心に話を進める。

５．２ 何故クラウドは好まれるのか

日本では経済産業書が『平成 24 年度我が国情報経済社会における基盤整備』（2013 年 11 月）にて、クラウドコンピューティングを「ネットワークから提供される情報処理サービスで、ネットワークとの接続環境さえあれば，ネットワークに接続している特定のコンピュータ通信ネットワーク等の情報処理基盤を意識することなく，情報通信技術の便益やア

---

[6] NIST：SP800-146：Cloud Computing Synopsis and Recommendations の日本語訳である、情報処理推進機構『クラウドコンピューティングの概要と推奨事項』より引用

プリケーションを享受可能にするものをいう」と定義している。多分に技術的な観点からの説明ではあるが、より経済的な観点からみると、NIST、及び経済産業省の定義ともに共通する内容として、以下二つの利点が挙げられる。

- 情報処理関連事業者が管理するシステム資源を利用することで、システム導入までの期間を短縮できるという利点
- 複数の利用者がシステム資源を共同利用する仕組みのもと，仮に単独で利用者がリソースの調達・管理を行う際に求められる負担・コストを抑え，安価なシステム利用を可能にするという利点

これらは短期間で安価にシステムを調達できる（イニシャルコストの低下）とともに、継続的な利用に際した運用上の費用（ランニングコストの低下）を抑えられるという利点をも意味しており、利用企業にとってはシステム経費の削減に直結する。また、サービス提供をする情報処理関連事業者にとってもコスト低下に見合ったシステム維持・管理負担の低減が期待できる。そのため、情報処理関連事業者はクラウドの魅力を語り、利用企業は相次いで自前のシステムを捨て、クラウドサービスへ積極的に移行・切替を行っている状況である。

５．３ クラウド利用に伴う技術的なリスク

医療機関等でも自機関内部でのシステム運用からクラウド上でのシステム利用への移行・切替を行う事例も発生している。しかし、クラウドを利用することには様々なリスクが伴っていることには留意が必要である。

クラウド利用も一種のシステムの外部委託という観点からは従来の外部委託先管理と共通するリスクも存在している。こうした外部委託先として管理すべきクラウドのリスクについては既に様々に議論されている。よって、ここではクラウドの利用に伴う固有の技術的なリスクの要点を解説する。このリスクとはクラウドの特徴に係る４つのカテゴリにおおむね分類可能である。具体的には、①マルチテナント、②サプライチェーン、③データセンターの所在地、④ベンダロックインとなる。

①マルチテナント

クラウドでは、利用者毎に専用のシステムが用意される通常のシステム利用とは異なり，情報処理関連事業者が提供する同一システムを複数のシステム利用者が共同利用するというマルチテナントという特徴を有する。ここで言う通常のシステム利用とは、ASP サービスのように、情報処理関連事業者が利用者単位にシステムを用意し、インターネット等のネットワークを経由して、利用者がそれぞれ専用のサービスを利用するシングルテナントの形態をも含む。クラウドでは、同一のシステムを様々な仮想化技術により資源分割することで、各利用者が好きな時に好きなだけ用意された資源を利用できるようにしている。こうした条件下では、例えば他の利用者と同一の IP アドレスを利用していた場合、他の利用者が諸事情によりブロックされることに伴い自分もサービスから締め出されてしまう可能性、他の利用者を標的とした外部攻撃が発生し、サービスダウンが発生した場合、同じシステムを共有する自分までもがサービスを利用できなくなる可能性も考えられる。つまり、他の利用者の動向によって自分のサービスの利用可能性が制限されるリスクである。

また、データベースの共同利用が行われている場合、外部からの攻撃やベンダの管理不備により、自データが他の利用者のデータと混在し、本来見られるべきでないデータが他の利用者に閲覧される可能性が考えられる。他利用者が司法当局から疑惑を持たれ、証拠保全のため設備全体を押収される事態も発生例がある。

加えて、データが様々なサーバに分散管理されていることにより、サービス利用を終了する際に、データの削除・廃棄を情報処理関連事業者に要求しても、事業者としてもどこに何のデータが分散管理されているか把握できないため、そもそもデータの削除・廃棄を証明すること自体が不可能になる可能性も考えられる。これらの可能性は単なる絵空事ではなく、実際に発生したケースを前提にして記載していることには注意頂きたい。

②サプライチェーン

多くのクラウドサービスは単独の情報処理関連事業者のみでなく、複数の情報処理関連事業者により管理されていることが一般的である。つまり、利用者が窓口としている情報処理関連事業者は、自社のサービスを提供する上で、外部のクラウドサービスを利用（外部委託）し、さらにその外部も別のサービスを利用する等、複数社による各サービスを組み合わせ、利用者には一本化したサービスとして提供するサプライチェーン（サービスの複合的な組合せ）アプローチが採用されている。これは同時に窓口としている情報処理関連事業者をどれほど強力に管理しようとも、当該事業者の外部委託先（利用者からすれば再委託先・再々委託先等）の管理監督方針自体が十分でなければ、サービスの信頼性自体が損なわれる。クラウドを利用する際の契約は複数の利用者に向けた約款となっていることが多く、通常のシステム調達のような個別契約の形態は少ない。情報処理関連事業者が提示する約款のなかには、自身がサービス提供する上で外部委託を行う別ベンダの管理監督義務を免責しているケースもあるため、短期間で導入し、安価で利用できるクラウド利用時に慎重に定款をチェックしていない場合、こうした問題に直面することになる[7]。

③データセンターの所在地

①でも触れた通り、仮想化技術を採用したクラウドでは、データは様々なデータセンターのサーバへ分散処理・管理される。そのため、削除・廃棄の証明が技術的に困難になることはもちろんのこと、海外にデータセンターを設置している情報処理関連事業者においては、データの差し押さえが発生するリスクを常に抱えている。例えば、アメリカにデータセンターを設置していれば、米国自由法（USA Freedom Act）（旧・米国愛国者法：USA PATRIOT Act）や電子通信プライバシー保護法（Electronic Communications Privacy Act）で法的な強制のもとでの差し押さえが発生する可能性がある。イギリスであれば捜査権限規制法（Regulation of Investigatory Powers Act）、中国であればデータ規制捜査権限法等、海外当局の強制差し押さえが発生すれば、サービス利用の継続性が損なわれるリスクがあ

[7] 例えば、契約を結んでいるA社という情報処理関連事業者はシステム、A社の外部委託先であるB社という情報処理関連事業者がネットワークを提供しているパターンを想像してみよう。B社でネットワーク障害が発生したため、A社のシステムが利用できなくなった。しかし、A社のシステム自体では障害は発生していない場合、B社に本来責任が発生するが、約款ではB社に対する外部委託責任がA社には存在しないと記載されている場合、A社の管理責任を利用者は責めることはできず、またB社とはそもそも契約関係にすらないため、利用者は大抵泣き寝入りとなる。このようにサプライチェーンアプローチが採用されたサービスでは、各情報処理関連事業者の責任分界点が不明確になりやすい。

る。多くの情報処理関連事業者は自社サービスを提供する上でのデータセンターの所在地域を開示していないケースが多く、利用者はこうしたリスクと隣り合わせである点を留意する必要がある。

なお、本リスクは、総務省『ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン』、経済産業省『医療情報を受託管理する情報処理事業者向けガイドライン』にそれぞれ記載されている通り、医療機関等にクラウドサービスを提供する民間の情報処理関連事業者においては適切に対応されていることが前提となる。これらのガイドラインでは民間の情報処理関連事業者に対する要求事項[8]として国内法の適用範囲にデータを保管することが求められている。「データセンターが国内法のおよぶ範囲に制限されている理由はデータセキュリティの問題ではない。国内外でデータセキュリティ対策に優劣があるとは考えられず、むしろ事業者の努力に依存している。この制限は、行政的な可用性の問題で、他国の事情で日本の行政行為が制限されないためにある。」[9]よって、法律により作成・保管が義務付けられた行政文書でもある診療録が国内法の適用が及ばない海外のデータセンターに保管されることにより、日本の行政行為が制限されることがあってはならない。

④ベンダロックイン

ベンダロックインとは、特定のベンダ技術・サービスに大きく依存することにより、他ベンダの技術・サービスへの移行・切り替えが出来なくなり、結果的に特定ベンダのサービスを利用し続けなければならなくなる事態である。これは、安易にクラウドサービスを利用し、データ・プログラムの多くを当該情報処理関連事業者が提供するサービスに合わせてカスタマイズしすぎたため、他のサービスへの移行・切り替えには技術調査等に莫大の費用を要することになってしまい、自らの他システムとのインタフェースすらこのサービスを中心に検討しなければならなくなる状況を意味する。一般のシステム外部委託であれば、個別契約のなかで切り替え時の交渉権を盛り込むことも可能かもしれないが、クラウドという約款ベースの利用形態ではそもそもこういった交渉権すら発生しないケースがあることは留意すべきである。

５．４ 医療機関等でクラウド利用を行う際に事前検討すべきこと

上記のようにクラウドの特徴を踏まえた観点からの固有リスクとしては、マルチテナント、サプライチェーン、データセンター所在地、ベンダロックインという 4 つが挙げられる。

---

[8] 総務省ガイドライン：「所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の適用が及ぶ場所に設置すること」
経済産業省ガイドライン：「扱う情報として、法令により作成や保存が定められている文書を含む場合には、医療情報システム及び医療情報が国内法の執行が及ぶ範囲にあることを確実とすることが必要である」

[9] 第 35 回医療情報学連合大会 35th JCMI(Nov.,2015) 山本隆一：「外部保存に関する諸規制とその解決策」より引用

これをさらに、医療機関等におけるシステムの技術的な安全管理の観点に当てはめると、次の通りリスクの高いサービスであることが判明する。

つまり、クラウドというサービスを利用するに際して、利用者は、マルチテナントという観点から他の利用者（医療機関等にとどまらない他の利用者）の影響による想定外の制約を受けるとともに、サービス終了時のデータ廃棄の証明を受けることが技術的に難しい可能性がある。

データ廃棄のみでなく、データ保管という点においても、事業者によっては、データ保管期間の制約、及び契約終了に伴うデータ返却作業において費用負担を利用者に求める可能性も想定する必要がある。

また、サプライチェーンという観点からは情報処理関連事業者の責任分界が不明確であり、突然のサービス品質の低下（あるいは利用不可）という事態と隣り合わせとなる。

加えて、ベンダロックインという観点からは相互運用性を著しく損なう可能性があることを考慮しなければならない。

上記のリスクの一部については発生可能性自体が非常に低いものもある。ただし、クラウドを医療機関等におけるシステムとして採用するのであれば、少なくとも上記のリスクに対する合理的なコントロールが設計・運用される必要がある。具体的にどのような管理水準とするのかについては各機関の判断に委ねられるが、こういったリスクが顕在化し、不測の事態に陥った場合、患者や当局（厚生労働省）へ合理的な説明を行うことが可能であるのか、そういった観点も踏まえた上で、医療機関等におけるクラウドの利用を慎重に検討し、その得失を認識して、有効に活用していく姿勢が必要である。

５．５ 委託主体がクラウド選定をする際に参考すべき認定・認証制度

本節では、医療機関等が、診療録等の電子媒体による外部保存を、クラウドサービスを提供する民間の情報処理関連事業者に委託する場合に留意すべき事項を示す。

５．１でも前述した通り、情報処理関連事業者を選定する際には、安全管理ガイドラインは「データセンター等の情報処理関連事業者が経済産業省が定めた『医療情報を受託管理する情報処理事業者向けガイドライン』や総務省が定めた『ASP・SaaS における情報セキュリティ対策ガイドライン』及び『ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン』の要求事項を満たしていることを確認の上、契約等でその遵守状況を明らかにしなくてはならない」ことを求めている。

上記の２ガイドラインは、個人情報法保護の面から民間事業者が満たすべき要求事項が定められている。外形条件として、事業者は P マークまたは適切な範囲での ISMS 取得を必要としている。一方、医療機関等、外部保存を委託する側が事業者を選定するに当たって留意すべき事項は、安全管理ガイドライン 8 章に記載されているが、ここでは民間の情報処理関連事業者に委託する場合に参考にできる認定・認証制度について記載する。

①ASP・SaaS の安全・ 信頼性に係る情報開示認定制度

クラウドサービスの利用者が、民間の情報処理関連事業者やサービスを選定する際に、比較、評価するための認定制度として、一般財団法人マルチメディア振興センターが実施して

いる『ASP・SaaS の安全・ 信頼性に係る情報開示認定制度』[10]がある。当該認定制度への申請時に記載する申請書 B の 93 項目の審査対象項目は、安全管理ガイドラインの内容とも重なるものが多く、医療機関等が該当事業者を選定する際の評価項目として考慮すべきものである。例えば、データセンターの立地条件のうち、大規模災害等に備えて安全な情報の保存場所を選定する必要性の観点より国内の設置場所の情報、あるいは事業継続性の高い民間事業者を選定する必要性の観点より事業者の経営上の安定性についての情報が審査されており、事業者を選定する上で有用な参考情報となる。

②民間事業者による医療情報の外部保存及び ASP・SaaS サービスに係る適合性評価制度

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: Health Information Security Performance Rating Organization)が、総務省『ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン』、及び経済産業省『医療情報を受託管理する情報処理事業者向けガイドライン』に基づく観点から、医療機関等向けに提供される ASP・SaaS サービスが当該ガイドラインに適合しているかについて評価を行う制度[11]である。安全管理ガイドラインが情報処理関連事業者に要求するガイドラインの遵守有無を確認する上で有益である。

③STAR 認証

英国規格協会（British Standards Institute :BSI）とクラウドセキュリティアライアンス（Cloud Security Alliance :CSA）が共同創設した制度[12]である。『ISO/IEC 27001』，及び CSA によるクラウドコントロールマトリックスを組合せた観点から，クラウドサービスを提供する情報処理関連事業者におけるセキュリティ管理態勢の成熟度を評価している。対象事業体におけるセキュリティ管理態勢の程度を把握する上で参考となる。

④クラウド情報セキュリティ監査制度

特定非営利活動法人 日本セキュリティ監査協会（JASA : Japan Information Security Audit Association）傘下のクラウドセキュリティ推進協議会（JCISPA）により制定された，クラウドのセキュリティに特化した監査制度[13]である。クラウドサービスを提供する情報処理関連事業者による情報セキュリティマネジメントの取組状況に係る監査が，機密性/可用

---

[10] 一般社団法人マルチメディア振興センターホームページ参照
http://www.fmmc.or.jp/asp-nintei/about.html

[11] 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ホームページ参照
http://www.hispro.or.jp/open/kekka-top.htm

[12] BSI グループジャパン株式会社ホームページ参照
http://www.bsigroup.com/ja-JP/STAR/

[13] 特定非営利活動法人 日本セキュリティ監査協会ホームページ参照
http://jcispa.jasa.jp/cloud_security/

性/完全性という三つの軸から適切に行われているかを評価するものであり、対象事業者における情報セキュリティに係る PDCA サイクルの成熟度を把握する上で参考となる。

なお、上記以外にも、クラウドサービスの提供・利用のための情報セキュリティ管理対策を定めた国際規格としての ISO/IEC 27017、パブリッククラウドにおける個人情報保護の国際規格としての ISO/IEC 27018 が存在し、これらの規格への準拠状況を審査する ISMS 適合性認証もクラウドサービスを検討する上で有用である。

６章：スキャナによる電子化

安全管理ガイドラインには、「診療等の都度電子化・原本化」、「過去に蓄積された紙媒体等の電子化・原本化」、「原本は紙媒体のままでの運用利便性のための電子化」の分類で具体的規定が述べられている。電子化対象文書がこの中のどの分類に当たるのかは、慎重な検討の上で決めることである。

使用するスキャナ装置の精度については、画一的な基準は無いので、用途に応じて各実施機関で検討する必要がある。「診療の用途に差し支えない精度」を対象毎にあらかじめ利用目的に則して運用規定等で定めることである。

安全管理ガイドライン附表の運用管理規定例にある様に、「スキャナ読取の対象にする文書」を、スキャナ精度の正当性とともに規定文書にしておくことが必要である。これにより、初期の状態から、運用の便利さに伴い無検討のまま対象文書が拡大していくことの防止に役立つことになる。

なお、デジタル複合機等の機器をスキャンに使用する場合は、情報セキュリティの観点から、スキャン後の機器上（メモリ、ハードディスク）に保存された電子データは放置せず、確実に削除処理することが推奨される。特に機器の保守事業者がリモートメンテナンスを目的として当該機器をインターネットに接続している場合は、スキャン機器のメモリに残存する電子化された診療録等が外部の不特定多数の目に晒されるリスクが存在する。

2013 年には日本の学術関係機関に設置された、大手国内メーカ製の複合機上のデータがインターネットより誰にでも閲覧可能な初期設定であったことから、健診結果や身分証明等の個人情報が外部に漏えいしていた事件が発生し、情報処理推進機構(IPA)が複合機に係るセキュリティ対策の重要性を注意喚起する事態[14]に至っている。さらにその後も大手損保会社の代理店において同様の事案が発生しており、スキャン機器に係るセキュリティ対策は今や情報漏洩という観点で重要となっている。仮にインターネットに接続していない場合であっても、本来権限のない内部要員が電子化された診療録等にアクセスするというセキュリティリスクが潜在しており、そのためスキャン後には機器上に電子データは不要に保存せず、適時に削除する運用が求められる。

なお、「過去に蓄積された紙媒体等の電子化・原本化」は安全管理ガイドライン 9.3 に述べられている通り、厳しい実施条件を付されている。「どのように精密な技術を用いても、元の紙等の媒体の記録と同等にはならない」(9.1 共通の要件)ので、証拠性の観点から原本化の検討は重要である。

実施に当たっては、紙等を原本のまま保存することに運用上著しく障害がある場合に限定されており、安全管理ガイドライン 9.3 の条件を満たすことも実施上の制約が大きい上に、蓄積された文書には様々な様態があり、一律機械的にスキャンすることも作業的負担が大きい。

---

[14] 情報処理推進機構ホームページ参照
https://www.ipa.go.jp/about/press/20131108.html
https://www.ipa.go.jp/security/ciadr/vul/20160106-printer.html

従って、本文書においては「過去に蓄積された紙媒体等のスキャナ等による電子化・原本化」は推奨しない。

７章：地域医療連携システムの構築

この章では、複数医療機関による医療情報の交換の構成を対象とする。情報交換システム（たとえば、遠隔画像診断、臨床検査等、診療等を目的とした業務の第三者委託（安全管理ガイドライン「4.3 (3) 医療機関等の業務の一部を委託することに伴い情報が「一時的に外部に保存」される場合」）は本文書では５章（クラウドを利用した外部保管）に含めているため、ここでの対象としない。

７．１ システム仕様に関して

医療機関への電子カルテの普及が進みつつある今日、医療機関の連携による医療サービスの実現には期待が高いものがある。しかしながら、電子カルテ間の連携様式はベンダにより異なっているため、連携システム構築のハードルが高く、かつ広域連携が困難となっている。

医療連携システムの形態としては、HELICS 標準として『地域医療連携における情報連携基盤技術仕様』が日本 IHE 協会から発行され、これに準拠した『システム実装ガイド』が JAHIS より発行されている。

標準規格を用いたシステム構築仕様は、医療連携の標準化を推進しており、現在世界各国で採用が進んでおり、わが国でも上記の標準化に当たっては厚生労働省の費用が投じられている。

地域医療連携情報システムを構築する際に、参加施設の情報システム間で患者（個人）の識別情報および医療情報等を共用するのに必要な情報連携基盤の仕様を定めたものであり、参考にすべきものである。

７．２ 運用管理に当たって

複数医療施設による医療情報連携には、個別医療機関でのシステム構築とは異なる観点からの考慮が必要である。

注意すべき点は、複数医療施設による情報共用と外部保存/バックアップとの違いである。

外部保存/バックアップは医療機関が自らの記録保管義務を果たすために、外部機関に情報の保管を委託するものであり、データがそこにあるからといって直ちにこれが共有等に利用できると考えるのは誤りである。

複数医療機関で情報共有し、医療連携や医学研究への活用など情報の二次的利用に用いる場合には、 目的に応じて、患者への通知や同意取得を必要とするなど、本来は相当程度煩雑な手続きが必要である。

個別医療機関にはシステム管理者が存在するが、連携システムにも統一的管理が必要であり、そのための管理組織が必要である。

統一的管理を行うため、地域医療連携システムの管理組織の、医療機関／行政組織／その他の別に応じて、安全管理ガイドライン 8 章の分類に準拠した参加各機関による契約・合意に基づいた運営等の対策が必要である。

この中で、参加する医療機関間でのポリシーに関する合意、共有情報の定義やアクセス権限管理、各医療機関の責任範囲、相互運用性の確保などについての取決めを定めなければならない。

安全管理ガイドライン付録に、参考として「外部機関と診療情報等を連携する場合に取り決めるべき内容」が挙げられている。

地域医療連携においては、運営主体が管理する情報システムにおいて保管される情報が多い。関与する医療機関、ネットワーク上のサービス機能提供事業者、ネットワーク機能提供の通信事業者間の責任の在り方は、安全管理ガイドライン「4.3 例示による責任分界点の考え方の整理（1） 地域医療連携で「患者情報を交換」する場合」において、詳細に説明されている。

安全管理ガイドライン「4.3（1）(c) 外部保存機関が介在する場合に対する考え方」においては、「保存する情報は外部保存機関に委託することになる」ため、「管理者の権限や義務の範囲が他施設や通信事業者にも及び」委託先に対する監督義務があり「通常運用における責任、事後責任は医療機関等にある」とされている。従って、「これを他の医療機関等と共用しようとする場合は、双方の医療機関等における管理責任の分担を明確にし、共用に対する患者の同意も得ておく必要がある」。同意の取り方には共用目的により異なる。

情報漏えいに対するセキュリティに関しては、各参加医療機関でレベルの統一を行わなければならず、一機関の対策レベル低下が連携システムを通して全参加機関にとっての脅威となり得る。

ネットワーク上の留意点に関しては、安全管理ガイドライン 6.11 に記載があるが、考慮すべき事項はネットワークの問題には止まらない。安全管理ガイドライン付録等を参考にし、取決め事項を定めることを推奨する。

付録１：外部参照文書

安全管理ガイドラインが参照する外部文書を以下に一覧として整理する。

4.2.2 第三者提供における責任分界

8.1.3 個人情報の保護

個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）第 23 条及び「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」

5.1.1 厚生労働省標準規格

厚生労働省における保健医療情報分野の標準規格（「厚生労働省標準規格」）

5.1.2 基本データセット

・医療情報システムにおける相互運用性の実証事業報告書

・JAHIS 基本データセット適用ガイドライン

5.1.3 用語集・コードセット

MEDIS 標準マスター類

5.2 データ交換のための国際的な標準規格への準拠

保健医療福祉情報システム工業会（JAHIS）が定める標準データ交換規約

6.1 方針の制定と公表

JIS Q 15001:2006（個人情報保護マネジメントシステム-要求事項）

6.2 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（ISMS）の実践

ISO（ ISO/IEC27001:2005）ならびに JIS（JIS Q 27001:2006）

6.5 技術的安全対策

「広帯域電力線搬送通信機器による医療機器への影響に関する医療関係者等からの照会に対する対応について」（平成 18 年 11 月 9 日付薬食安発第 1109002 号）

6.9 情報及び情報機器の持ち出しについて

「スマートフォン・クラウドセキュリティ研究会最終報告～スマートフォンを安心して利用するために実施されるべき方策～（総務省；平成 24 年 6 月）

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

「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書（保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム；HEASNET）；平

成 19 年 2 月」

6.12 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

・2008年4月の情報セキュリティ政策会議「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA1及びRSA1024に関わる移行指針」

・JIS X 5092:2008 CMS利用電子署名(CAdES)の長期署名プロファイル、JIS X 5093:2008 XML署名利用電子署名(XAdES)の長期署名プロファイル)

・「電子署名に係る地方公共団体の認証業務に関する法律」（平成14 年法律第153号）

・「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの安全な長期保存のために－」（総務省、平成16 年11 月）

8.1.2 外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準

・経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン」

・総務省「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」

9 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

日本医学放射線学会電子情報委員会「デジタル画像の取り扱いに関するガイドライン 2.0 版（平成 18 年 4 月）

付録２：本文書が言及する外部文書類

本文書にて言及した、安全管理ガイドライン以外の、ガイドライン・規格類について、各章毎に以下に一覧として整理する。なお、これらのガイドライン・規格類は各所管団体により適宜更新されるため、常に最新版を参照することが推奨される。

【3 章】

所管団体・組織	ガイドライン類
一般社団法人保健医療福祉情報システム工業会(JAHIS) / 一般社団法人日本画像医療システム工業会(JIRA)	「製造業者による医療情報セキュリティ開示書」ガイド
	リモートサービスセキュリティガイドライン
一般社団法人保健医療福祉情報システム工業会(JAHIS)	ヘルスケア分野における監査証跡のメッセージ標準規約
	シングルサインオン実装ガイド
	ヘルスケア PKI を利用した医療文書に対する電子署名規格
国際標準化機構（ISO） / 国際電気標準会議（IEC)	ISO/IEC27001:2005
日本工業規格(JIS)	JIS Q 27001:2006
一般社団法人メディカルＩＴセキュリティフォーラム(MITSF)	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４．２版」のガイダンス
一般財団法人日本情報経済社会推進協会（JIPDEC）	医療機関向け ISMS ユーザガイド - JISQ27001:2006 (ISO/IEC27001:2005)対応
JOINT NEMA/COCIR/JIRA SECURITY AND PRIVACY COMMITTEE	Break-Glass An Approach to Granting Emergency Access to Healthcare Systems （ブレークグラス:医療システムへの緊急アクセスのためのアプローチ） （注：JIRA ホームページより、「システム部会活動内容」中の「セキュリティ委員会」に和訳がある）

【4 章】

所管団体・組織	ガイドライン類
国際標準化機構（ISO）/ 国際電気標準会議(IEC)	ISO/IEC27000:2014
	ISO/IEC 13335-1（GMITS）
日本工業規格(JIS)	JIS Q13335-1:2006
	JIS Q27000:2014

【5 章】

所管団体・組織	ガイドライン類
経済産業省	医療情報を受託管理する情報処理事業者向けガイドライン
総務省	ASP・SaaS における情報セキュリティ対策ガイドライン
	ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン
米国国立標準技術研究所（NIST: National Institute of Standards and Technology） ※日本語訳は情報処理推進機構(IPA)による。	SP800-146 : Cloud Computing Synopsis and Recommendations ※クラウドコンピューティングの概要と推奨事項（IPA による日本語訳）
国際標準化機構（ISO） / 国際電気標準会議（IEC）	ISO/IEC27017:2015 ISO/IEC27018:2014

【7 章】

所管団体・組織	ガイドライン類
日本 IHE 協会（Integrating the Healthcare Enterprise-Japan）	地域医療連携における情報連携基盤技術仕様
一般社団法人保健医療福祉情報システム工業会(JAHIS)	IHE-ITI を用いた医療情報連携基盤実装ガイド

なお、本文には明記していないものの、地域医療連携システムの構築を検討する際には、以下のガイドラインも有益であるため、併せて参考とすることが推奨される。

- 日本 IHE 協会（Integrating the Healthcare Enterprise-Japan）

地域医療連携情報システム構築 ハンドブック 2010―IHE XDS による HIE（Health Information Exchange）の構築―

- 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）
  地域医療介護連携サービスの安全管理評価

付録３　医療機関等においての主な法的作成保管義務のある書類と保管期間等

作成義務者	作成すべき書類	保管義務者	保管期間
医師	診療録	病院、診療所の管理者、作成医師	5 年間
	処方せん	薬局開設者 (調剤済み処方せん)	調剤済みとなった日から 3 年間 (調剤済み処方せん)
歯科医師	診療録	病院、診療所の管理者、作成歯科医師	5 年間
	歯科技工に関する指示書	病院、診療所又は歯科技工所の管理者	当該歯科技工が終了した日から 2 年間
薬剤師	調剤録	薬局開設者	最終の記入の日から 3 年間
助産師	助産録	病院、診療所又は助産所の管理者、作成助産師	5 年間
診療放射線技師	照射録	(診療放射線技師)	―
歯科衛生士	業務記録	歯科衛生士	3 年間
救急救命士	救急救命処置録	病院、診療所の管理者、消防機関の長、救急救命士	記載の日から 5 年間
病院	病院日誌 各科診療日誌 処方せん 手術記録 看護記録 検査所見記録 エックス線写真 紹介状 入院患者・外来患者数を明らかにする帳簿	病院	作成から 2 年間

作成義務者	作成すべき書類	保管義務者	保管期間
特定生物由来製品の取扱病院、診療所、薬局	特定生物由来製品の使用の対象者の氏名、住所その他厚労省令で定める事項の記録	特定生物由来製品の取扱病院、診療所、薬局の管理者	当該特定生物由来製品を使用した日から20年間
保険医	診療録	保険医療機関	完結の日から5年間
保険薬剤師	調剤録	保険薬局	完結の日から3年間
保険医療機関	療養の給付の担当に関する帳簿、書類その他の記録	保険医療機関	完結の日から3年間
保険薬局	療養の給付に関する処方せん、調剤録	保険薬局	完結の日から3年間
人を対象とする医学系研究を実施する研究機関	侵襲（軽微な侵襲を除く）を伴い、介入を行う研究に用いられる情報及び当該情報に係る資料	研究機関（研究を実施する法人、行政機関及び個人事業主）	研究の終了について報告された日から5年経過日、又は研究結果の最終公表日から3年経過日の、いずれか遅い日までの期間（倫理指針）

補足：購買・契約担当者、及び利用者が理解すべき安全管理ガイドライン４章～８章の要件

１ 目的

安全管理ガイドラインのうち、第１章から第６章は「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」、第７章は「保存義務のある診療録等を電子的に保存する場合の指針」、第８章は「保存義務のある診療録等を医療機関等の外部に保存する場合の指針」が記述されている。

これらの内容については、医療情報システムの調達・導入から設計・開発、運用・利用までの各フェーズにおいて様々な立場で関与する関係者が遵守すべき諸要件として一まとめに記述されている。

医療情報システムの導入・運用管理を担うシステム管理者はこれらの内容を網羅的に理解し、システムの調達・保守に際した、外部委託先となる情報処理関連事業者の選定業務等に従事する購買・契約担当者との協議、あるいは日々の業務において医療情報システムを利用する者への教育を行うことが求められている。他方、購買・契約担当者、あるいは利用者がその業務遂行の上で安全管理ガイドラインのうち、何を理解・遵守しなければならないかについては、その全体像が把握しづらい。

そのため、本文書では、安全管理ガイドラインのうち、医療情報システムの調達・契約（外部委託先業者との契約含む)、設計・開発、運用・利用の各フェーズにて安全管理を遵守するための実務的な内容を記述している第４章から第８章について、購買・契約担当者、あるいは利用者が安全管理ガイドラインの遵守に基づく業務遂行を行うための利便に資すべく、以下の立場より理解すべき事項を要点化し、一覧とした。

- 購買・契約担当者が、医療情報システム調達に際した合意・契約文書に記載する必要がある事項。具体的には、医療情報処理製品・技術の導入（購入）・保守等、外部の情報処理関連事業者との契約・合意（または調整・交渉時）に際して最低限理解しておくべき事項
- システム利用者がシステム管理者による運用管理規程、または教育の下、医療情報システムを用いて日々の医療上、あるいは関連業務を遂行する上で最低限理解しておくべき事項。

なお、安全管理ガイドラインより内容を抜粋する関係上、文脈依存的な意図や前後の脈絡が十分に反映されない可能性がある。そのため、当該内容はあくまでリファレンスとして参考し、要件の詳細については安全管理ガイドライン本文に当たられることを推奨する。

２ 購買・契約担当者として理解すべき事項

4：電子的な医療情報を扱う際の責任のあり方

- 関係者間での電子的な医療情報の取扱いについての責任分界の取り決め
- 「医療機関等の管理者の情報保護責任の内容と範囲」及び「他の医療機関等や事業者に情報処理の委託や他の業務の委託に付随して医療情報を委託する場合と第三者提供した場合」について

4.1：医療機関等の管理者の情報保護責任について

- 通常運用における責任について（4.1.(1)）
- 事後責任について（4.1.(2)）

4.2.1：委託における責任分界

- 通常運用における責任について（4.2.1.(1)）
- 事後責任について（4.2.1.(2)）

4.2.2：第三者提供における責任分界

- 善後策を講ずる責任

4.3：例示による責任分界点の考え方の整理

- 地域医療連携で「患者情報を交換」する場合(4.3.(1))

5：情報の相互運用性と標準化について

- 医療療情報システムの導入時や、現に保有する医療情報システムの運用にあたって、ベンダに対して、

  ・標準化に対する基本スタンス
  ・次項以下に掲げる標準（GLを参照）に対応していないならばその理由
  ・将来のシステム更新、他社システムとの接続における相互運用性に対する対応案

  等の説明を受ける等して一定の理解を等しくしておく必要がある。

5.3：標準規格の適用に関わるその他の事項

- 最後に注意しなければならない点として外字の問題がある

6.6：人的安全管理対策

＜B. 考え方＞

- 第三者については、そもそも医療機関等の医療情報システムに触れてはならないものであるため、物理的安全管理対策や技術的安全管理対策によって、システムへのアクセスを禁止する必要がある。
- 万が一、第三者によりシステム内の情報が漏えい等した場合については、不正アクセス行為の禁止等に関する法律等の他の法令の定めるところにより適切な対処等をする必要がある。

＜C. 最低限のガイドライン＞

(1) 従業者に対する人的安全管理措置

- 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。
- 従業者の退職後の個人情報保護規程を定めること。

(2) 事務取扱委託業者の監督及び守秘義務契約

- 医療機関等の事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。
  - 受託する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結すること。
  - 委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。

6.7：情報の廃棄

＜C.最低限のガイドライン＞

- 外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策 (2) 事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。

6.8：情報システムの改造と保守

＜B. 考え方＞

- 保守会社との保守契約の締結にあたっては、再委託する事業者への個人情報保護の徹底等について保守会社と同等の契約を求めることが重要である

＜C. 最低限のガイドライン＞

- 動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めること。
- アカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。
- 保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと。
- 保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。
- 保守会社と守秘義務契約を締結し、これを遵守させること。
- 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。
- リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。
- 再委託が行われる場合は、再委託する事業者にも保守会社の責任で同等の義務を課すこと。法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、

雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。

6.10：災害時の非常時対応

＜B. 考え方＞

- 業務を受託する事業者との間の連絡体制や受託する事業者と一体となったトラブル対処方法等が明示されるべきである

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

＜B. 考え方＞

- 送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威から守らなければならない

B-1. 医療機関等における留意事項

- 盗聴防止については、例えばリモートログインによる保守を実施するような時も同様である。その場合、医療機関等は上記のような留意点を保守委託事業者等に確認し、監督する責任を負う

B-2. 選択すべきネットワークのセキュリティの考え方

- 情報セキュリティに対する分析を行った上で、コスト・運用に対して適切なネットワークを選択する必要がある。この整理を実施した上で、ネットワークにおけるセキュリティの責任分界点がネットワークを提供する事業者となるか、医療機関等になるか、もしくは分担となるかを契約等で明らかにする必要がある

Ⅱ. オープンなネットワークで接続されている場合

- ネットワーク導入時に業者等に委託をするが、その際には、リスクの説明を求め、理解しておくことも必要である
- チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、事前にサービス提供者との契約をよく確認して、チャネル・セキュリティが確実に確保されるようにしておく必要がある

＜C.最低限のガイドライン＞

- 医療機関等の間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等多くの組織が関連する。そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。
  - 診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定
  - 送信元の医療機関等がネットワークに接続できない場合の対処
  - 送信先の医療機関等がネットワークに接続できなかった場合の対処
  - ネットワークの経路途中が不通または著しい遅延の場合の対処においても次の事項において契約や運用管理規程等で定めておくこと。
  - 通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。

- 患者等に対する説明責任の明確化。
- 事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。
- 交換した医療情報等に対する管理責任及び事後責任の明確化。
- 個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。

➢ リモートメンテナンスを実施する場合は、必要に応じて適切な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ログインを防止すること。また、メンテナンス自体は「6.8 情報システムの改造と保守」を参照すること。

➢ 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。また上記1 及び4 を満たしていることを確認すること。

7.1 真正性の確保について

➢ ネットワークを通じて外部に保存を行う場合、委託元の医療機関から委託先の外部保存施設への転送途中で、診療録等が書き換えや消去されないように、また他の情報との混同が発生しないよう、注意する必要がある。

(1) 故意または過失による虚偽入力、書き換え、消去及び混同の防止

システムの改造や保守等で診療録等にアクセスされる可能性がある場合には、真正性確保に留意し、「6.8 情報システムの改造と保守」に記載された手続きに従う必要がある

＜C.最低限のガイドライン＞

【医療機関等に保存する場合】

(5) 機器・ソフトウェアの品質管理

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が明らかにされており、システムの仕様が明確に定義されていること。

【ネットワークを通じて医療機関等の外部に保存する場合】

➢ 医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。

(1) 通信の相手先が正当であることを認識するための相互認証を行うこと

診療録等のオンライン外部保存を受託する機関と委託する医療機関等が、お互いに通信目的とする正当な相手かどうかを認識するための相互認証機能が必要である。

(2) ネットワーク上で「改ざん」されていないことを保証すること

ネットワークの転送途中で診療録等が改ざんされていないことを保証できること。なお、可逆的な情報の圧縮・回復ならびにセキュリティ確保のためのタ

グ付けや暗号化・平文化等は改ざんにはあたらない。

(3) リモートログイン機能を制限すること

保守目的等のどうしても必要な場合を除き行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。

なお、これらの具体的要件については、「6.11 外部と診療情報等を含む医療情報を交換する場合の安全管理」を参照すること。

7.2 見読性の確保について

＜B. 考え方＞

- ネットワークを通じて外部に保存する場合は、これらのことに適切に対応することに加えて、外部保存先の機関の事情により見読性が損なわれることを考慮に含めた十分な配慮が求められる

7.3 保存性の確保について

＜B. 考え方＞

(5)障害等によるデータ保存時の不整合

委託する医療機関等は、医療機関内部のデータを消去する等の場合には、外部保存を受託する機関において、当該データが保存されたことを確認してから行う必要がある

＜C.最低限のガイドライン＞

【ネットワークを通じて医療機関等の外部に保存する場合】

- 医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。

(1) データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと

保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップまたは変更されることが考えられる。その場合、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しなくてはならない

(2) ネットワークや外部保存を受託する機関の設備の劣化対策を行うこと

ネットワークや外部保存を受託する機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策を行うこと

8.1.2 外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準

＜B. 考え方＞

1. 外部保存を受託する機関の選定基準

①病院、診療所、医療法人等が適切に管理する場所に保存する場合

②行政機関等が開設したデータセンター等に保存する場合

③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に保存する場合

- 法令上の保存義務を有する医療機関等は、システム堅牢性の高い安全な情報の保存場所を選定する必要がある。
- 事業者等が、本章の他の項の要求事項、本ガイドラインの他の章で言及されている、責任のあり方、安全管理対策、真正性、見読性、保存性及びC項で定める情報管理体制の確保のための全ての要件を満たす必要がある。
- それらのサービス形態によって、経済産業省の定めた「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」の要求事項も満たす必要がある。

2. 情報の取り扱い

①病院、診療所、医療法人等が適切に管理する場所に保存する場合

- 病院、診療所等であっても、保存を受託した診療録等について分析等を行おうとする場合は、委託した病院、診療所及び患者の同意を得た上で、不当な営利、利益を目的としない場合に限る

②行政機関等が開設したデータセンター等に保存する場合

- 外部保存を受託する事業者を選定する場合、医療機関等はそれらが実施されないことの確認、もしくは実施させないことを明記した契約書等を取り交わす必要がある。

③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に保存する場合

- 外部保存を受託する事業者が医療機関等から委託を受けて情報を保存する場合、不当な営利、利益追求を目的として情報を閲覧、分析等を行うことはあってはならず、許されない。
- 医療機関等は契約も含め、その遵守状況を十分確認する必要がある。
- 外部保存を受託する事業者に暗号鍵を預託する場合においては、暗号鍵の使用について厳重な管理が必要である。
- 暗号鍵の使用に当たっては、非常時に限定することとし、使用における運用管理規程の策定、使用したときにその痕跡が残る封印等の利用、情報システムにおける証跡管理等を適切に実施し、外部保存を受託する事業者による不正な利用を防止する措置をとらなければならない。

3. 情報の提供

①病院、診療所、医療法人等が適切に管理する場所に保存する場合

- 情報の保存を受託した病院、診療所、医療法人等は適切なアクセス権限を規定し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないように配慮しなくてはならない。
- それら情報の提供は、原則、患者が受診している医療機関等と患者間の同意で実施されるものであり、情報の保存を受託した病院、診療所、医療法人等が患者からの何らの同意も得ずに実施してはならない。

②行政機関等が開設したデータセンター等に保存する場合

- 保存された情報を外部保存を受託する事業者が独自に保存主体の医療機関等以外に提供してはならない。
- 外部保存を受託する事業者を通じて保存された情報を保存主体の医療機関以外にも提供する場合は、あくまで医療機関等同士の同意の上で実施されなくてはならず、当然、患者の同意も得た上で実施する必要がある。
- 外部保存を受託する事業者がアクセス権の設定を受託している場合は、医療機関等もしくは医療機関等との間で同意を得た患者の求めに応じて適切な権限を設定する等し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにしなくてはならない。
- このような形態で外部に診療録等を保存しようとする医療機関等は、外部保存を受託する事業者に対して、契約書等でこれらの情報提供についても規定する必要がある。

③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に保存する場合

- 保存された情報を外部保存を受託する事業者が独自に保存主体の医療機関等以外に提供してはならない。これは匿名化された情報であっても同様である。
- 外部保存を受託する事業者を通じて保存された情報を保存主体の医療機関以外にも提供する場合は、あくまで医療機関等同士の同意で実施されなくてはならず、当然、個人情報の保護に関する法律に則り、患者の同意も得た上で実施する必要がある。
- 外部保存を受託する事業者がアクセス権の設定を受託している場合は、医療機関等もしくは医療機関等との間で同意を得た患者の求めに応じて適切な権限を設定する等し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにしなくてはならない。
- このような形態で外部に診療録等を保存しようとする医療機関等は、外部保存を受託する事業者に対して、契約書等でこれらの情報提供についても規定しなくてはならない。

＜C.最低限のガイドライン＞

①病院、診療所、医療法人等が適切に管理する場所に保存する場合

- 保存を受託した診療録等を委託した病院、診療所や患者の許可なく分析等を目的として取り扱わないこと。
- 病院、診療所等であっても、保存を受託した診療録等について分析等を行おうとする場合は、委託した病院、診療所及び患者の同意を得た上で、不当な営利、利益を目的としない場合に限ること。
- 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、取り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。
- 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、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないように配慮すること。

②行政機関等が開設したデータセンター等に保存する場合

- 法律や条例により、保存業務に従事する個人も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が規定され、当該規定違反により罰則が適用されること。
- 医療機関等は保存された情報を、外部保存を受託する事業者が分析、解析等を実施しないことを確認し、実施させないことを明記した契約書等を取り交わすこと。
- 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者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、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにさせること。

③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に保存する場合

- 医療機関等が、外部保存を受託する事業者と、その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や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行えること。
- 受託事業者が民間事業者等に課せられた経済産業省の「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省の「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」等を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。
- 保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。なお保守に関しては、「6.8 情報システムの改造と保守」を遵守すること。
- 外部保存を受託する事業者が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。これらの事項を契約に明記し、医療機関等において厳守させること。
- 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者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、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにさせること。
- 医療機関等において（ア）から（カ）を満たした上で、外部保存を受託する事業者の選定基準を定めること。少なくとも以下の4 点について確認すること。

  (a) 医療情報等の安全管理に係る基本方針・取扱規程等の整備
  (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

8.1.3 個人情報の保護

＜C.最低限のガイドライン＞

(1) 診療録等の外部保存委託先の事業者内における個人情報保護

- 適切な委託先の監督を行うこと

  診療録等の外部保存を受託する事業者内の個人情報保護については「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」において考え方が示されている。「Ⅲ 医療・介護関係事業者の義務等」の「4. 安全管理措置、従業者の監督及び委託先の監督（法第20 条～第22 条)」及び本指針6 章を参照し、適切な管理を行うこと

8.4.2 外部保存契約終了時の処理について

- 診療録等の外部保存を委託する医療機関等は、受託する事業者に保存されている診療録等を定期的に調べ、終了しなければならない診療録等は速やかに処理を行い、処理が厳正に執り行われたかを監査する義務を果たさなくてはならない。
- 外部保存を受託する事業者も、医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を医療機関等に明確に示す必要がある。
- これらの廃棄に関わる規定は、外部保存を開始する前に委託契約書等にも明記をしておく必要がある。
- ネットワークを通じて外部保存する場合は、外部保存システム自体も一種のデータベースであり、インデックスファイル等も含めて慎重に廃棄しなければならない。
- 電子媒体の場合は、バックアップファイルについても同様の配慮が必要である。
- 確実に情報が廃棄されたことを、外部保存を委託する医療機関等と受託する事業者とが確実に確認できるようにしておかなくてはならない。

3 利用者として理解すべき事項

6.4：物理的安全対策

＜C. 最低限のガイドライン＞

- 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すること。
- 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、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることが出来ない対策を講じること。ただし、本対策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。
- 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すること。例えば、以下のことを実施すること。
  - 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。
  - 入退者の記録を定期的にチェックし、妥当性を確認する。
- 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すること。
- 窃視防止の対策を実施すること

6.5：技術的安全対策

＜B.考え方＞

(1) 利用者の識別及び認証

このような本人の識別・認証に用いられる情報は本人しか知り得ない、または持ち得ない状態を保つ必要がある。例えば、本人の識別・認証に用いられる情報が第三者に漏れないように以下のようなリスクに対処しなければならない。

- ID とパスワードが書かれた紙等が貼られていて、第三者が簡単に知ることができてしまう。
- パスワードが設定されておらず、誰でもシステムにログインできてしまう。
- 代行作業等のためにID・パスワードを他人に教えており、システムで保存される作業履歴から作業者が特定できない。
- 容易に推測できる、あるいは、文字数の少ないパスワードが設定されており、容易にパスワードが推測できてしまう。
- パスワードを定期的に変更せずに使用しているために、パスワードが推測される可能性が高くなっている。
- 認証用の個人識別情報を格納するセキュリティ・デバイス（IC カード、USB キー等）を他人に貸与する、または持ち主に無断で借用することにより、利用者が特定できない。
- 入力者が端末から長時間、離席する場合には、正当な入力者以外の者による入力を防止するため、クリアスクリーン等の防止策を講じるべきである。
- 利用者の識別や認証、署名等を目的として、IC カード等のセキュリティ・デバイスに個人識別情報や暗号化鍵、電子証明書等を格納して配布する場合は、これらのセキュリティ・デバイスが誤って本人以外の第三者の手に渡ることのないような対策を講じる必要がある

(2) 情報の区分管理とアクセス権限の管理

重要なことは、付与する利用権限を必要最小限にすることである

＜C.最低限のガイドライン＞

- 本人の識別・認証にユーザID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。
- 入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力の恐れがある場合には、クリアスクリーン等の防止策を講じること。
- 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。
- アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも

利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した患者が特定できること。

- 情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容）を必ず行うこと。
- システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時には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すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（たとえばパターンファイルの更新の確認・維持）を行うこと。
- パスワードは定期的に変更し（最長でも2 ヶ月以内)、極端に短い文字列を使用しないこと。英数字、記号を混在させた8 文字以上の文字列が望ましい。
- 類推しやすいパスワードを使用しないこと。
- 無線LAN の適用に関しては、総務省発行の「安心して無線LAN を利用するために」を参考にすること。

6.7：情報の廃棄

＜B.考え方＞

- 破棄は確実に行う必要がある

＜C.最低限のガイドライン＞

- 「6.1 方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。
- 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確認すること。

6.9：情報及び情報機器の持ち出し

＜C.最低限のガイドライン＞

- 運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。
- 情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。
- 情報機器に対して起動パスワードを設定すること。設定にあたっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。
- 盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。
- 持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネットワークに接続する場合は「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」の規定を順守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線LAN を利用できる場合があるが、公衆無線LAN は6.5 章C-11 の基準を満たさないことがあり、使用する場合は6.11 章で述べている基準を満たした通信手段を使うこと。

6.10：災害時の非常時対応

＜B. 考え方＞

- BCP として事前に周知しておく必要がある事項は事前に対応策を知ってもらい、信頼してもらっておくべきである。

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

＜B. 考え方＞

B-2. 選択すべきネットワークのセキュリティの考え方

- 選択するセキュリティ技術の特性を理解し、リスクの受容範囲を認識した上で、必要に応じて説明責任の観点から患者等にもそのリスクを説明する必要がある

B-4.患者等に診療情報等を提供する場合のネットワークに関する考え方

- 情報を提供する医療機関等が患う者等の納得が行くまで十分に危険性を説明し、その提供の目的を明確にする責任がある

＜C.最低限のガイドライン＞

- 情報の主体者となる患者等へ危険性や提供目的の納得できる説明を実施し、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すること。

7.1 真正性の確保について

＜B. 考え方＞

B-1. 虚偽入力、書換え、消去及び混同を防止すること

- 作成責任者（情報を作成、書き換え、消去しようとする者）は、情報の保存を行う前に情報が正しく入力されており、過失による書き換え・消去及び混同がないことを確認する義務がある

B-2. 作成の責任の所在を明確にすること

- 一旦記録された情報を追記・訂正・消去することもごく日常的に行われるものと考えられるが、追記・訂正・消去するごとに責任者が明確になっている必要がある。

(1) 作成責任者の識別及び認証

- 医療機関等の運用上、代行入力を容認する場合には、必ず入力を実施する個人毎にID を発行し、そのID でシステムにアクセスしなければならない
- 日々の運用においてもID、パスワード等を他人に教えたり、他人のID でシステムにアクセスしたりすることは、システムで保存される作業履歴から作業者が特定できなくなるため、禁止しなくてはならない

＜C.最低限のガイドライン＞

【医療機関等に保存する場合】

(1) 作成者の識別及び認証

a. 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

- 装置の管理責任者や操作者が運用管理規程で明確にされ、管理責任者、操作者以外による機器の操作が運用上防止されていること。
- 当該装置による記録は、いつ・誰が行ったかがシステム機能と運用の組み合わせにより明確になっていること。

(2) 記録の確定手順の確立と、作成責任者の識別情報の記録

a. 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

- 「記録の確定」を行うにあたり、作成責任者による内容の十分な確認が実施できるようにすること。

(4) 代行操作の承認機能

- 代行操作により記録された診療録等は、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。

7.2 見読性の確保について

＜C. 最低限のガイドライン＞

- 紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者毎の情報の全ての所在が日常的に管理されていること

7.3 保存性の確保について

＜B. 考え方＞

(2)不適切な保管・取扱いによる情報の滅失、破壊

サーバ室等への入室は、許可された者以外が行うことができないような対策を施す必要がある。

＜C.最低限のガイドライン＞

【医療機関等に保存する場合】

- 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うこと

➢ 記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を施すこと。

8.1.2 外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準

＜B. 考え方＞

3. 情報の提供

①病院、診療所、医療法人等が適切に管理する場所に保存する場合

● 情報の保存を受託した病院、診療所、医療法人等は適切なアクセス権限を規定し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないように配慮しなくてはならない

②行政機関等が開設したデータセンター等に保存する場合

● 外部保存を受託する事業者がアクセス権の設定を受託している場合は、医療機関等もしくは医療機関等との間で同意を得た患者の求めに応じて適切な権限を設定する等し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにしなくてはならない。

③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に保存する場合

● 外部保存を受託する事業者がアクセス権の設定を受託している場合は、医療機関等もしくは医療機関等との間で同意を得た患者の求めに応じて適切な権限を設定する等し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにしなくてはならない。

＜C.最低限のガイドライン＞

①病院、診療所、医療法人等が適切に管理する場所に保存する場合

②行政機関等が開設したデータセンター等に保存する場合

③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に保存する場合

● 情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないように配慮すること

8.1.3 個人情報の保護

＜C.最低限のガイドライン＞

(1) 診療録等の外部保存委託先の事業者内における個人情報保護

● 外部保存実施に関する患者への説明

診療録等の外部保存を委託する施設は、あらかじめ患者に対して、必要に応じて患者の個人情報が特定の外部の施設に送られ、保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得る必要がある。

● 診療開始前の説明

患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を、院内掲示等を通じて説明し理解を得た上で診療を開始すること。

● 患者本人に説明をすることが困難であるが、診療上の緊急性がある場合

意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明をし、理解を得る必要がある。

● 患者本人に説明することが困難であるが、診療上の緊急性が特にない場合

乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得ること。ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。

執筆・監修者一覧

氏名	所属名
礒部　佳奈子	特定非営利活動法人デジタル・フォレンジック研究会　事務局
一原　武司	一般社団法人メディカルＩＴセキュリティフォーラム　事務局長 三井物産セキュアディレクション株式会社
伊藤　英一	新潟県立新発田病院　循環器内科・情報システム部
江原　悠介	一般社団法人メディカルＩＴセキュリティフォーラム PwC あらた監査法人 システム プロセス アシュアランス　マネージャー
緒方　健	おがたコンサルティング　代表
川島　史子	株式会社 PLUS F　代表取締役
佐藤　智晶	青山学院大学　法学部　准教授
田中　友佳子	特定非営利活動法人デジタル・フォレンジック研究会　事務局
野津　勤	特定非営利活動法人デジタル・フォレンジック研究会「医療」分科会　幹事
深津　博	一般社団法人メディカルＩＴセキュリティフォーラム　代表 愛知医科大学医学部付属病院　医療情報部長・特任教授
舟橋　信	一般社団法人メディカルＩＴセキュリティフォーラム　理事 特定非営利活動法人デジタル・フォレンジック研究会　理事
丸谷　俊博	特定非営利活動法人デジタル・フォレンジック研究会　理事・事務局長

（五十音順）

発行者　特定非営利活動法人デジタル・フォレンジック研究会「医療」分科会
一般社団法人メディカルＩＴセキュリティフォーラム
合同委員会

住所　〒141-0022　東京都品川区東五反田 1-4-1　ハニー五反田第２ビル３Ｆ
（ＩＤＦ事務局）
ＴＥＬ　03(5420)1805　　ＦＡＸ　03(5420)3634
E-mail　j-sfc_wg1@digitalforensic.jp