付表1　一般管理における運用管理の実施項目例

A：医療機関の規模を問わない
B：大/中規模病院
C：小規模病院、診療所

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
①	総則	理念（基本方針と管理目的の表明）	A		・情報システムの安全管理に関する方針に基づき、本規程の目的を述べる	・この規程は、〇〇病院（以下「当院」という。）において、情報システムで使用される機器、ソフトウェア及び運用に必要な仕組み全般について、その取扱い及び管理に関する事項を定め、当院において、診療情報を適正に保存するとともに、適正に利用することに資することを目的とする。
		対象情報	A		・対象システム、対象情報を定める ・対象システム、対象情報を安全管理上の重要度に応じて分類し、リスク分析を行う	・対象システムは、電子カルテシステム、オーダエントリシステム、画像管理システム、・・・である。 ・対象システムの扱う情報については、そのシステムごとに別途定義と安全管理上の重要度の分類を行い、リスク分析を行い表に記入し保管すること。
		標準規格	B		・医療機関側でフォローすべき標準規格の列挙を行い、システム改定時に変更の対象とする	・システム管理者は、別表に挙げる標準規格についての変更状況を確認し、システムの変更・改造時の対象とすること。
			C		・ベンダに対しシステムで使われている標準規格に関する情報提供を求め、システム改訂時に変更の対象とする	・システム管理者は、情報システムで使われている標準規格についてベンダへ情報提供を要求し、システムの変更・改造時の対象とすること。
②	管理体制	運用責任者、個人情報保護責任者、システム管理者	B		・運用責任者、個人情報保護責任者、システム管理者、機器管理者、安全管理者等の任命規程	・当院に運用責任者および個人情報保護責任者を置き、病院長をもってこれに充てること。 ・病院長は必要な場合、運用責任者および個人情報保護責任者を別に指名すること。 ・情報システムを円滑に運用するため、情報システムに関する運用を担当する管理者（以下「システム管理者」という。）を置くこと。 ・システム管理者は病院長が指名すること。 ・情報システムに関する取扱い及び管理に関し必要な事項を審議するため、病院長のもとに情報システム管理委員会を置くこと。 ・情報システム管理委員会の運営については、別途定めること。 ・その他、この規程の実施に関し必要な事項がある場合については、情報システム管理委員会の審議を経て、病院長がこれを定めること。
			C		・院長が運用責任者、個人情報保護責任者とシステム管理者を兼ねる場合、その旨を明記する	・当クリニックに運用責任者、個人情報保護責任者およびシステム管理者を置き、院長をもってそれに充てること。 ・院長は必要な場合、システム管理者を別に指名すること。
		マニュアル・契約書等の文書管理体制	A		・別途定めてある文書管理規程に従うことを規程する	・契約書、マニュアル等の文書の管理については、別途規程を定めること。
		監査体制と監査責任者	B		・監査体制（監査の周期、監査結果の評価・対応等）を規程 ・監査責任者の任命規程	・情報システムを円滑に運用するため、情報システムに関する監査を担当する責任者（以下「監査責任者」という。）を置くこと。 ・監査責任者の責務は本規程に定めるものの他、別に定めること。 ・監査責任者は病院長が指名すること。 ・運用責任者は、監査責任者に毎年X回、情報システムの監査を実施させ、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。 ・監査の内容については、情報システム管理委員会の審議を経て、病院長がこれを定めること。 ・運用責任者は必要な場合、臨時の監査を監査責任者に命ずること。
			C		・院内で監査体制を整えることができない場合、第三者監査機関への監査依頼を規程する	・情報システムの監査をXXXとの契約により毎年X回行い、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。

		患者及びシステム利用者からの苦情・質問の受付体制	A		・患者及びシステム利用者からの苦情・質問受付窓口の設置 ・受付後の処置を規程	・患者及び利用者からの、情報システムについての苦情・質問を受け付ける窓口を設けること。 ・苦情・質問受け付け後は、その内容を検討し、速やかに必要な措置を講じること。
		事故対策	A		・緊急時あるいは災害時の連絡、復旧体制並びに回復手段を規程する	・システム管理者は、緊急時及び災害時の連絡、復旧体制並びに回復手順を定め文書化し、利用者に周知の上、常に利用可能な状態におくこと。
		システム利用者への教育・訓練など周知体制	A		・各種規程書、指示書、取扱説明書等の作成 ・定期的な利用者への教育、訓練	・システム管理者は、情報システムの取扱いについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におくこと。 ・システム管理者は、情報システムの利用者に対し、定期的に情報システムの取扱い及びプライバシー保護に関する研修を行うこと。
③	管理者及び利用者の責務	システム管理者や運用責任者の責務	A		・機器、ソフトウェア導入時の機能確認 ・運用環境の整備と維持 ・情報の安全性の確保と利用可能な状況の維持 ・情報の継続的利用の維持 ・不正利用の防止 ・利用者への教育、訓練 ・患者または利用者からの問合せ・苦情窓口設置	・情報システムに用いる機器及びソフトウェアを導入するに当たって、システムの機能を確認すること。 ・情報システムの機能要件に挙げられている機能が支障なく運用される環境を整備すること。 ・診療情報の安全性を確保し、常に利用可能な状態に置いておくこと。 ・機器やソフトウェアに変更があった場合においても、情報が継続的に使用できるよう維持すること。 ・システム管理者は情報システムの利用者の登録を管理し、そのアクセス権限を規程し、不正な利用を防止すること。 ・情報システムを正しく利用させるため、作業手順書の整備を行い利用者の教育と訓練を行うこと。 ・患者及び利用者からの、情報システムについての問い合わせや苦情を受け付ける窓口を設けること。
		監査責任者の責務	B		・監査責任者の役割、責任、権限を規程	・情報システムを円滑に運用するため、情報システムに関する監査を担当する責任者（以下「監査責任者」という。）を置くこと。 ・監査責任者の責務は本規程に定めるものの他、別に定めること。
			C		・第三者機関へ監査依頼している場合は、監査実施規程は不要 ・監査結果に対する対応を規程	・情報システムの監査をXXXとの契約により毎年X回行い、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。
		利用者の責務	B		・自身の認証番号やパスワードあるいはICカード等の管理 ・利用時にシステム認証を必ず受けること ・確定操作の実施による入力情報への責任の明示 ・権限を超えたアクセスの禁止 ・目的外利用の禁止 ・プライバシー侵害への配慮 ・システム異常、不正アクセスを発見した場合の速やかな運用管理者へ通知 ・離席対策	・利用者は、自身の認証番号やパスワードを管理し、これを他者に利用させないこと。 ・利用者は、情報システムの情報の参照や入力（以下「アクセス」という。）に際して、認証番号やパスワード等によって、システムに自身を認識させること。 ・利用者は、情報システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示すること。 ・利用者は、与えられたアクセス権限を越えた操作を行わないこと。 ・利用者は、参照した情報を、目的外に利用しないこと。 ・利用者は、患者のプライバシーを侵害しないこと。 ・利用者は、システムの異常を発見した場合、速やかにシステム管理者に連絡し、その指示に従うこと。 ・利用者は、不正アクセスを発見した場合、速やかにシステム管理者に連絡し、その指示に従うこと。 ・利用者は、離席する際は、ログアウトすること。
			C		・利用者が限定される運用の場合、その旨を明記し、責任の所在を明確にする ・目的外利用の禁止 ・プライバシー侵害への配慮 ・システム異常時の対応を規程	・利用者は、XXX、XXX、XXXである。 ・利用者は、参照した情報を、目的外に利用しないこと。 ・利用者は、患者のプライバシーを侵害しないこと。 ・利用者は、システムの異常を発見した場合、速やかにシステム管理者に連絡し、その指示に従うこと。 ・利用者は、不正アクセスを発見した場合、速やかにシステム管理者に連絡し、その指示に従うこと。

④	一般管理における運用管理事項	来訪者の記録・識別・入退の制限等の入退管理規程	B	・IDカード利用による入退者の制限、名札着用の実施 ・PCの盗難防止チェインの設置 ・防犯カメラの設置 ・施錠	・入退者の名簿記録と妥当性チェックなどの定期的チェック	・個人情報が保管されている機器の設置場所及び記録媒体の保存場所への入退者は名簿に記録を残すこと。 ・入退出の記録の内容について定期的にチェックを行うこと。
			C	・施錠	・スタッフの常駐	・個人情報が保管されている機器の設置場所及び記録媒体の保存場所は、スタッフの常駐または施錠できる部屋に設置すること。
		情報システムへのアクセス制限の決定方針及び、記録、点検等のアクセス管理	B	・ID、パスワード等により診療録データへのアクセスにおける識別と認証を行う ・監査ログサーバを設置し、アクセスログの収集を行う。	・管理規則に則ったハードウェア・ソフトウェアの設定を行う ・情報区分とアクセス権限に基づくアクセスできる診療録等の範囲を定め、アクセス管理を行う ・誰が、いつ、誰の情報にアクセスしたかを記録し、定期的な記録の確認を行う	・システム管理者は、職務により定められた権限によるデータアクセス範囲を定め、必要に応じてハードウェア・ソフトウェアの設定を行うこと。また、その内容に沿って、アクセス状況の確認を行い、監査責任者に報告をすること。
			C	（上記技術的対策が行えない場合）	・システム操作業務日誌を備え、システムを操作するものはシステム操作業務日誌に操作者氏名、作業開始時間、作業終了時間、作業内容、作業対象を記載する ・システム管理者は定期的にシステム操作業務日誌をチェックし、記載内容の正当性を確認する	・システム管理者はシステム操作業務日誌を設置すること。 ・利用者は、操作者氏名、作業開始時間、作業終了時間、作業内容、作業対象をシステム操作業務日誌に記載すること。 ・システム管理者は定期的にシステム操作業務日誌をチェックし、記載内容の正当性を評価すること。
		個人情報を含む記録媒体の管理（保管・授受等）規程	A		・保管、バックアップ作業を的確に行う	・保管、バックアップの作業に当たる者は、手順に従い行い、その作業の記録を残し、システム管理者の承認をうること。
		個人情報を含む媒体の廃棄の規程	A	・技術的に安全（再生不可）な方式で破棄を行う	・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事者の特定、具体的な破棄の方法を含めること	・個人情報を記した媒体の廃棄に当たっては、安全かつ確実に行われることを、システム管理者が作業前後に確認し、結果を記録に残すこと。
		リスクに対する予防、発生時の対応方法	A		・情報に対する脅威を洗い出し、そのリスク分析の結果に対し予防対策を行う ・リスク発生時の連絡網、対応、代替手段などを規程する	・システム管理者は、業務上において情報漏えいなどのリスクが予想されるものに対し、運用管理規程の見直しを行うこと。また、事故発生に対しては、速やかに運用責任者に報告し利用者に周知すること。
		技術的と運用的対策の分担を定めた文書の管理規程	A	・6章全般に基づいて取られる技術的対策	・左記の項と対応する、運用事項	・各システムはその設計時、運用開始時に技術的対策と運用による対策を、基準適合チェックリストに記載し、必要時には第三者への説明に使える状態で保存すること。 ・システムの保守時には、基準適合チェックリスト記載にしたがっていることを確認すること。 ・システム改造時は、最新の基準適合チェックリストに従って、技術的対策と運用による対策の分担を見直すこと。
		無線LANに関する事項	A	・ステルスモード、ANY接続拒否設定、不正アクセス対策、暗号化を行う。	・利用者への規則の説明を行う ・電波発生機器の利用に当たっての規則を定める	・システム管理者は、無線LANアクセスポイントの設定状態を適宜確認すること。 ・システム管理者は、無線LAN利用規則を院内関係者および利用可能性のある入院患者へ説明をすること。

		電子署名・タイムスタンプに関する規程	A	・電子証明書による電子署名環境 ・タイムスタンプ付与環境 ・電子署名の検証環境	・利用する電子証明書がガイドラインが求める信用性を有していることを記載した文書の作成 ・署名が必要な文書に電子署名があることの確認手順の作成 ・タイムスタンプを付与する作業手順の作成 ・電子的な受領文書の電子署名検証手順の作成	・システム管理者は、電子署名、タイムスタンプに関する作業手順を定めること。 ・システム管理者は、電子的に受領した文書に電子署名が有る場合の、署名検証手順を定めること。
⑤	業務委託の安全管理措置	委託契約における安全管理・守秘条項	A		・包括的な委託先の罰則を定めた就業規則等で裏付けられた守秘契約を締結すること	・業務を当院外の所属者に委託する場合は、守秘事項を含む業務委託契約を結ぶこと。契約の署名者は、その部門の長とする。また、各担当者は委託作業内容が個人情報保護の観点から適正に且つ安全に行われていることを確認すること。
		再委託の場合の安全管理措置事項	A		・委託先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先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	・業務委託の契約書には、再委託での安全管理に関する事項を含むこと
		システム改造及び保守での医療機関関係者による作業管理・監督、作業報告確認	A	・保守要員用のアカウントを設定する ・保守作業におけるログの取得と保存	・保守要員用のアカウントを確認する ・保守作業等の情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行うこと ・清掃など直接情報システムにアクセスしない作業の場合、定期的なチェックを行うこと ・保守契約における個人情報保護の徹底 ・保守作業の安全性についてログによる確認	・システム管理者は、保守会社における保守作業に関し、その作業者および作業内容につき報告を求め適切であることを確認すること。必要と認めた場合は適時監査を行うこと。
⑥	情報および情報機器の持ち出しについて	持ち出し対象となる情報および情報機器の規程	A		・組織としてリスク分析を実施し、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で定めること	・システム管理者は、情報および情報機器の持ち出しに関しリスク分析を行い、持ち出し対象となる情報および情報機器を規程し、それ以外の情報および情報機器の持ち出しを禁止すること。 ・持ち出し対象となる情報および情報機器は別表としてまとめ、利用者に公開すること。
		持ち出した情報および情報機器の運用管理規程	A		・持ち出した情報および情報機器の管理方法を定めること ・情報が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握すること	・情報および情報機器を持ち出す場合は、所属、氏名、連絡先、持ち出す情報の内容、格納する媒体、持ち出す目的、期間を別途定める書式でシステム管理者に届け出て、承認を得ること。 ・システム管理者は、情報が格納された可搬媒体および情報機器の所在について台帳に記録すること。そして、その内容を定期的にチェックし、所在状況を把握すること。
		持ち出した情報および情報機器への安全管理措置	A	・情報機器に対して起動パスワードを設定すること。 ・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。	・設定にあたっては推定しやすいパスワードなどの利用を避けたり、定期的にパスワードを変更する等の措置を行うこと ・持ち出した情報を、例えばファイル交換ソフト（Winny等）がインストールされた情報機器で取り扱わないこと。医療機関等が管理する情報機器の場合は、このようなアプリケーションをインストールしないこと	・持ち出す情報機器について起動パスワードを設定すること。そのパスワードは推定しやすいものは避け、また定期的に変更すること。 ・持ち出す情報機器について、ウイルス対策ソフトをインストールしておくこと。 ・持ち出した情報を、別途定められている以外のアプリケーションがインストールされた情報機器で取り扱わないこと。 ・持ち出した情報機器には、別途定められている以外のアプリケーションをインストールしないこと。
		盗難、紛失時の対応策	A	・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。	・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	・持ち出した情報および情報機器の盗難、紛失時には、直ちにシステム管理者に届け出ること。 ・届け出を受け付けたシステム管理者は、その情報および情報機器の重要度にしたがって、別途定めるとおり対応すること。
		利用者への周知徹底方法	A		・運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと	・システム管理者は、情報および情報機器の持ち出しについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におくこと。 ・システム管理者は、利用者に対し、情報および情報機器の持ち出しについて研修を行うこと。また、研修時のテキスト、出席者リストを残すこと。

⑦	外部の機関と医療情報を交換する場合	安全を技術的、運用的面から確認する規程	A	・6.11章に基づいて取られる技術的対策	・左記の項と対応する、運用事項	・システム管理者は、外部の機関と医療情報を交換する場合、リスク分析を行い、安全に運用されるように別途定める技術的および運用的対策を講じること。 ・技術的対策が適切に実施され問題がないかを定期的に監査を行って確認すること。
		リスク対策の検討文書の管理規程	A		・上記のリスク対策の検討文書を作成し管理する	
		情報処理事業者との通常運用時、事故処理時それぞれで責任分界点を定めた契約文書の管理と契約状態の維持管理規程	A		・医療機関等の間の情報通信に関連する医療機関等、通信事業者やシステムインテグレータ、運用委託事業者等、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 ・またその契約状態を維持管理する規程を定めていること	・外部の機関と医療情報を交換する場合、相手の医療機関等、通信事業者、運用委託業者などとの間で、責任分界点や責任の所在を契約書等で明確にすること。 ・上記契約状態が適切に維持管理されているか定期的に監査を行って確認すること。
		リモートメンテナンスの基本方針	A	・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。	・遠隔保守を行う事業者との間で、責任分界点、責任の所在を契約書等で明確にすること	・外部の保守会社からリモートメンテナンスを受ける場合、相手の保守会社等、通信事業者、運用委託業者などとの間で、責任分界点や責任の所在を契約書等で明確にすること。 ・上記契約状態が適切に維持管理されているか定期的に監査を行って確認すること。
		従業者による医療機関等の外部からアクセスする場合の運用管理規程	A	・医療機関等の内部のシステムに不正な侵入等を防止する技術的対策	・外部からアクセスを許容する機器及びその状態を規定する ・外部からアクセスを許容した機器が、その許容状態を保持しているのかを確認する	・外部からアクセスを許容する機器については別途定める規程に従ったものに限定すること。その機器が許可された際の状態を保持していることを定期的に確認すること。
⑧	災害等の非常時の対策	BCPの規程における医療情報システムの項	A		・医療サービスを提供し続けるためのBCPの一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと	・災害、サイバー攻撃などにより一部医療行為の停止など医療サービス提供体制に支障が発生する非常時の場合、別途定める事業継続計画(BCP)にしたがって運用を行うこと。 ・どのような状態を非常時と見なすかについては、別途定める基準、手順に従って運用責任者が判断すること。
		システムの縮退運用管理規程	A	・技術的な縮退運用時機能	・システムが縮退運用を行っている際の、運用管理規程	・システムの縮退運用時や非常時の運用に関して運用管理規程を作成し、利用者に周知の上、常に利用可能な状態におくこと。
		非常時の機能と運用規程	A	・技術的な非常時用機能	・正常復帰後に、代替手段で運用した間のデータ整合性を図る規約 ・「非常時のユーザアカウントや非常時用機能」の管理手順	
		報告先と内容一覧	A		・サイバー攻撃で広範な地域での一部医療行為の停止など医療サービス提供体制に支障が発生する場合は、別途定める所管官庁への連絡を行うこと	・災害、サイバー攻撃などにより一部医療行為の停止など医療サービス提供体制に支障が発生した場合、別途定める一覧の連絡先に連絡すること。
⑨	教育と訓練	マニュアルの整備	A		・マニュアルの整備	・システム管理者は、情報システムの取扱いについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におくこと。
		定期または不定期なシステムの取り扱い及びプライバシー保護やセキュリティ意識向上に関する研修	A		・定期または不定期な電子保存システムの取扱及びプライバシー保護に関する教育、研修	・システム管理者は、利用者に対し、定期的に情報システムの取扱い及びプライバシー保護に関する研修を行うこと。また、研修時のテキスト、出席者リストを残すこと。
		従事者に対する人的安全管理措置	A		・守秘契約、業務規程 ・退職後の守秘規程 ・規程遵守の監査	・本院の業務従事者は在職中のみならず、退職後においても業務中に知った個人情報に関する守秘義務を負う。

⑩	監査	B		・定期的な監査の実施 ・監査責任者の任命、役割、責任、権限を規程 ・監査結果の検討、規程見直しといった手順の規程	・情報システムを円滑に運用するため、情報システムに関する監査を担当する責任者（以下「監査責任者」という。）を置くこと。 ・監査責任者の責務は本規程に定めるものの他、別に定めること。 ・監査責任者は病院長が指名すること。 ・システム管理者は、監査責任者に毎年X回、情報システムの監査を実施させ、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。 ・監査の内容については、情報システム管理委員会の審議を経て、病院長がこれを定めること。 ・システム管理者は必要な場合、臨時の監査を監査責任者に命ずること。
		C		・第三者機関に監査を委託している場合、その旨を記載する	・情報システムの監査をXXXとの契約により毎年X回行い、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。
⑪	その他	A		・運用管理規程の公開について規程 ・運用管理規程の改定の規程	

付表2　電子保存における運用管理の実施項目例

A：医療機関の規模を問わない
B：大/中規模病院
C：小規模病院、診療所

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
①	真正性確保	作成者の識別及び認証	B	・利用者識別子、パスワードによる識別と認証	・利用者識別子とパスワードの発行、管理 ・パスワードの最低文字数、有効期間等の規程 ・認証の有効回数、超過した場合の対処 ・利用者への認証操作の義務づけ ・識別子、パスワードの他人への漏えいやメモ書きの禁止 ・利用者への教育 ・緊急時認証の手順規程	・システム管理者は、電子保存システムの利用者の登録を管理し、そのアクセス権限を規程し、不正な利用を防止すること。 ・パスワードの最低文字数、有効期間等を別途規程すること。 ・認証の有効回数、超過した場合の対処を別途規程すること。 ・利用者は、自身の認証番号やパスワードを管理し、これを他者に利用させないこと。 ・利用者は、電子保存システムの情報の参照や入力（以下「アクセス」という。）に際して、認証番号やパスワード等によって、システムに自身を認識させること。 ・システム管理者は、電子保存システムを正しく利用させるため、利用者の教育と訓練を行うこと。
				・ログアウト操作、自動ログアウト機能、スクリーンセーブ後の再認証等	・利用者への終了操作義務づけ ・離席時の対処の規程と周知	・利用者は、作業終了あるいは離席する際は、必ずログアウト操作を行うこと。
			A	・運用状況において作成者が自明の場合は、技術的対策なし	・作成責任者を明記すること ・定期的な実施状況の監査	・電子保存システムにおいて保存されている情報の作成責任者はXXであること。
		情報の確定手順と、作成責任者の識別情報の記録	B	・技術的に入力した情報の確定操作を行う機能	・利用者への確定操作法の周知・教育 ・代行入力の場合、責任者による確定を義務づけ	・利用者は、電子保存システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示すること。 ・代行入力の場合、入力権限を持つ者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
			B	・技術的に情報に作成責任者の識別情報を記録する機能	・利用者への確定操作法の周知・教育	・利用者は、電子保存システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示すること。 ・代行入力の場合、入力権限を持つ者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
			A	・運用において確定の状況が自明の場合は、「確定」操作はなし	・「確定」を定義する状況を運用規程に明記する	・本規程が対象とする情報システムの作成データの「確定」については、付表に記す。[付表として、各システムの操作における「確定」の定義を行う。”xx機器のyy釦操作の時点”、”確定操作”等]
		更新履歴の保存	B	・技術的に更新履歴を保管し、必要に応じて更新前の情報を参照する機能	・利用者への確定操作法の周知・教育	・利用者は、電子保存システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示すること。 ・代行入力の場合、入力権限を持つ者が最終的に確定操作を行い、入力情報に対する責任を明示すること。

		代行操作の承認記録	A	・技術的に更新履歴を保管し、必要に応じて更新前の情報を参照する機能	・代行者を依頼する可能性のある担当者に、確定の任務を徹底すると同時に適宜履歴の監査を行う	・代行入力の場合、入力権限を持つ者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
		機器・ソフトウェアの品質管理、動作状況の内部監査規程	A		・定期的な機器、ソフトウェアの動作確認。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の規定。	・システム管理者は、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すること。
②	見読性確保	情報の所在管理	A	・技術的に情報の論理的所在確認を行う	・情報機器・媒体のリストを作成し、物理的所在場所の確認を行う	システム管理者は定期的に情報の所在確認を行うこと。
		見読化手段の管理	A	見読に必要な機器（モニタ、プリンタ等）の整備を行う	・見読化手段の維持、管理（例えば、モニタ・プリンタの管理やネットワークの管理）要件を明記する	・電子保存に用いる機器及びソフトウェアを導入するに当たって、保存義務のある情報として電子保存された情報毎に見読用機器を常に利用可能な状態に置いておくこと。
		見読目的に応じた応答時間とスループット	A	・応答時間の確保が出来る、システム構成、機器の選定。	・システム利用における見読目的の定義と、システム管理により業務上から要請される応答時間の確保を行う	・システム管理者は、応答時間の劣化がないように維持に努め、必要な対策をとること。
		システム障害対策	A	・システムの冗長化	・システム障害時に備えた機器・システムの維持体制を決める ・データのバックアップ	・システム管理者は障害時の対応体制が最新のものであるように管理すること。 データバックアップ作業が適切に行われている事を確認すること。
③	保存性確保	ソフトウェア・機器・媒体の管理	A		・定期的な機器、ソフトウェアの動作確認 ・媒体の保存場所、その場所の環境、入退出管理	・システム管理者は、電子保存システムで使用されるソフトウェアを、使用の前に審査を行い、情報の安全性に支障がないことを確認すること。 ・電子保存システムの記録媒体を含む主要機器は管理者によって入退室管理された場所に設置すること。 ・システム管理者は、定期的にソフトウェアのウィルスチェックを行い、感染の防止に努めること。 ・設置場所には無水消火装置、漏電防止装置、無停電電源装置等を備えること。 ・設置機器は定期的に点検を行うこと。
		不適切な保管・取り扱いによる情報の滅失、破壊の防止策	A		・作業の管理を行う ・データのバックアップを行う ・業務担当者の変更に当たっては、教育を行う	・システム管理者は新規の業務担当者には、操作前に教育を行うこと。
		記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止策	A		・記録媒体劣化以前の情報の複写を規程	・記録媒体は、記録された情報が保護されるよう、別の媒体にも補助的に記録すること。 ・品質の劣化が予想される記録媒体は、あらかじめ別の媒体に複写すること。
		媒体・機器・ソフトウェアの整合性不備による復元不能の防止策	A	・マスタDB変更時に過去の情報に対する内容変更が起こらない機能 ・標準形式でのデータ入出力機能	・システムの移行時のデータベースの不整合、機器・媒体の互換性不備に備えたシステム変更・移行時の業務計画の作成 ・定期的なバグフィックスやウイルス対策の実施	・機器・媒体やソフトウェアの変更に当たっては、データ移行のための業務計画を作ること。

④	相互運用性確保	システムの改修に当たっての、データ互換性の確保策	A	・標準的な規約（例えば、HL7、DICOM、HELICS、IHE等）に従った情報形式を持つシステム構築	・システム更新時の継続性確保策 ・異なる施設間の場合、契約により責任範囲を明確にすることを規程	・機器やソフトウェアに変更があった場合においても、電子保存された情報が継続的に使用できるよう維持すること。
		システム更新に当たっての、データ互換性の確保策	A			
(4)	スキャナ読み取り書類の運用	スキャナ読取の対象にする文書の規程	A		・対象文書を定める	・システム管理者は、適宜、業務において規程通りの運用がなされていることを確認すること。
		スキャナ読み取り電子情報と原本との同一性を担保する情報作成管理者の任命	A	・適切な精度のスキャナの使用	・スキャナ読み取りの運用管理を規程する	
		スキャナ読み取り電子情報への作業責任者の電子署名及び認証業務に関する法律に適合した電子署名・タイムスタンプ	A	・電子署名・タイムスタンプ環境の構築		
		診療の都度、スキャンするタイミングの規程	A	・タイムスタンプ機能	・情報が作成されてから、または情報を入手してから一定期間以内(1～2日程度以内)にスキャンを行うことを運用管理規程で定め、遅滞なくスキャンを行うこと	

付表3　外部保存における運用管理の例

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
①、⑨	管理体制と責任	管理体制の構築、受託する機関の選定、責任範囲の明確化、契約	B		管理体制の構築、受託する機関の評価・選定、契約	この規程は、〇〇病院(以下「当院」という)において、診療録及び診療諸記録(以下「診療記録」という)の、ネットワークを経由してXXにおいて保管する為の仕組みと管理に関する事項を定めたものである。本規程の付表に、当院における管理体制(運用責任者、システム管理者、各作業実務者(外部の実業務委託者を含む))、XXへの監査体制(監査者)、を定める。 　なお、システム管理者は、保管を委託するXXは「医療情報システムの安全管理に関するガイドライン」が定める「外部保存を受託する機関の選定基準」を満たしていることを適宜確認すること。XXが民間等のデータセンターである場合には、経済産業省が定めた「医療情報を受託管理する事業者向けガイドライン」や業務形態によっては総務省が定めた「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に準拠していることを確認すること。
			C		管理体制の構築、受託する機関の評価・選定、契約	この規程は、〇〇病院(以下「当院」という)において、診療録及び診療諸記録(以下「診療記録」という)の、ネットワークを経由してXXにおいて保管する為の仕組みと管理に関する事項を定めたものである。運用責任者は院長とし、運用内容の管理実務および監査は△△に委託する。また、保管を受託するXXの評価、管理・監査を受託する△△への評価を添付する。 　なお、院長は、保管を委託するXXは「医療情報システムの安全管理に関するガイドライン」が定める「外部保存を受託する機関の選定基準」を満たしていることを△△に適宜確認すること。XXが民間等のデータセンターである場合には、経済産業省が定めた「医療情報を受託管理する事業者向けガイドライン」や業務形態によっては総務省が定めた「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に準拠していることを確認すること。
		受託する機関への監査	A		受託する機関に対する保管記録の監査規程作成、契約	システム管理者は、XXにおける「診療記録」の保管内容を示す記録を監査し、正しいことを確認する。異常の発見時には直ちに運用責任者に報告すると共に、XXと契約の責任分担に基づき対処に着手する。また、これらの確認記録を残す。
					受託する機関での管理策の承認、実施監査規程作成、契約	システム管理者は、XXにおける受信「診療記録」の管理策を精査し、承認する。その管理策の実施状況を必要時に監査する。異常の発見時には直ちに運用責任者に報告すると共に、XXに対し対処を指示し、結果を確認する。また、これらの監査記録を残す。
		責任の明確化	A		通常運用における責任、事後責任の分界点を定める	運用責任者は、定められた責任体制が維持されていることを確認する。
		動作の監査	B	委託する機関での送信記録、受託する機関での受信記録の保持	委託する機関での送信記録、受託する機関での受信記録の合致監査	システム管理者は、XXから「診療記録」の受信記録を受け取り、送信した「診療記録」との合致を確認する。また、確認した旨の作業記録を残す。異常の発見時には直ちに運用責任者に報告すると共に、XXと契約の責任分担に基づき対処に着手する。
			C	(監査目的に耐える記録レベル、保存期間であること)	監査(上記を含む全)を第三者へ委託した場合は、定期的報告(6ヶ月程度)を受けること	運用責任者は、監督を委託した△△から、『XXからの「診療記録」の受信記録、送信した「診療記録」との合致を確認した』旨の報告を受け、確認後に報告内容の保管を行う。また、異常発生時には直ちに報告を受け、△△と共に対処に着手する。
		不都合な事態への対処	A		受託する機関との間で、不都合な事態(異常の可能性も含む)の責任対処作業範囲を定める	運用責任者は「診療記録」流出の危険があると判断した時には、直ちに外部保存の運用を停止する。
②	外部保存契約終了時の処理		A		保管データの破棄契約と管理者による確認、守秘義務契約	【契約事項として】当院とXXとの契約終了時には、それまでに保管を受託した全ての「診療記録」を当院に戻す(あるいは、利用不可能な形で廃棄する)こととし、その結果につき当院の監査を受けるものとする。また、XXが受託期間中に異常への対応等で「診療記録」の内容にアクセスした場合、その内容についての守秘義務は、本保管委託契約終了後も有効である。
③	真正性確保	相互認証機能の採用	A	SSL/TLSあるいは相互認証付きVPNの使用	認証局を使う場合は、両機関間でお互いに相手方の証明書を認証可能な認証局を選定する事。 双方が合意すれば、特に独立した第三者の認証局である必要性は無い。	システム管理者は、記録による動作の監査において、委託する機関、受託する機関双方のなりすましが無い事を確認する。
		通信上で「改ざんされていない」ことの保証	A	SSL/TLSあるいはメッセージ認証付きのVPNの使用	認証局を使う場合は、両機関間でお互いに相手方の証明書を認証可能な認証局を選定する事。双方が合意すれば、特に独立した第三者の認証局である必要性は無い。	システム管理者は、記録による動作の確認において、通信上の改ざんの発見に努める。
④	見読性確保	情報の所在管理 見読化手段の管理 見読目的に応じた応答時間とスループット システム障害対策	A		付表2の見読性確保と同じ技術的対策・運用的対策がとられていることの確認	システム管理者は、XXにおける見読性対策が適切である事を確認する。監査者は必要に応じてXXの設備を監査する。
⑤	保存性確保	外部保存を受託する機関での保存確認機能	A	受託する機関との間で、改ざんされることの無いデータとして保存された事を確認できる機能　、たとえばネットワークを介したStrageへの保管確認機能、あるいは　保存を委託する機関への保管内容送信機能(1時間～1日単位)	・付表2の保存性確保と同じ技術的対策・運用的対策がとられていることの確認 ・受託先での保存が確認された時点まで委託元でのデータ削除を行わない作業規程	システム管理者は、XXにおける保存性対策が適切である事を確認する。監査者は必要に応じてXXの設備を監査する。
		標準的なデータ形式及び転送プロトコルの採用	A	DICOM、HL7、標準コードの使用あるいはこれらへの変換機能		
		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確保	A		継続性の保証契約を交わす	【契約事項として】当院とXXは互いに各自のシステム変更に当たっては、相互にデータ通信の継続性に配慮し、変更内容が外部保存の障害にならないように協議をする。

⑥	診療録等の個人情報を電気通信回線で伝送する間の個人情報保護策	秘匿性の確保のための適切な暗号化	A	メッセージの暗号化が可能な通信手段 暗号の強度は、電子署名法に準じること		
		通信の起点・終点識別のための認証	A	SSL/TLSあるいは相互認証付きVPNの使用 暗号の強度は、電子署名法に準じること	認証局を使う場合は、両機関間でお互いに相手方の証明書を認証可能な認証局を選定する事 双方が合意すれば、特に独立した第三者の認証局である必要性は無い。	システム管理者は、記録による動作の監査において、委託する機関、受託する機関双方が正当である事を確認する。
⑦	外部保存を受託する機関内での個人情報保護策	外部保存を受託する機関における個人情報保護	A		受託する機関と受託する機関側における業務従事者への教育、守秘義務	監査者は必要に応じてXXを監査する。【契約事項として】①XXは当院から受けた保管委託を再委託してはならない ②XXは「診療記録」の保管業務に従事する従業員に対して「個人情報保護の重要性」の教育を年1回行う。また、その業務を離れた後も有効な守秘契約を当該従業員と交わすこと。
		外部保存を受託する機関における診療情報へのアクセス禁止	A	アクセス制御機能とアクセスログ機能、監査目的に耐えるログ保存期間であること	委託する機関によるアクセスログの監査	監査者は、XXにおける保管された「診療記録」及びアクセスログへのアクセス記録を監査する。
		外部保存を受託する機関における障害対策時のアクセス通知	A	アクセス制御機能とアクセスログ機能、監査目的に耐えるログ保存期間であること	アクセス許可、秘密保持に関する契約と委託する機関によるアクセスログの監査	【契約事項として】XXにおいては正当な理由無く、保管した「診療記録」及びアクセスログにアクセスしてはならない。出来る限り事前に当院の許可を得ることとし、やむを得ない事情で許可を得ずアクセスした場合は遅滞無く当院に報告するものとする。また、目的外に利用してはならないし、正当で明確な目的が無く他の媒体などに保管してはならない。
		外部保存を受託する機関におけるアクセスログの完全性とアクセス禁止	A	アクセスログファイルへのアクセス制御とアクセスログ機能、監査目的に耐えるログ保存期間であること	委託する機関によるアクセスログへのアクセスの監査	
⑧	患者への説明	外部保存を行っている旨を院内掲示等を通じて周知すること	A		外部保存を行っている旨を院内掲示等を通じて周知すること	運用責任者は、外部保存している事の患者への周知（例、掲示内容）が計られていることを適宜確認する。
						付録 1. 管理体制・受託する機関との責任分担規程 2. XXに保管を委託する「診療記録」の定義 3. XXへの監査事項 4. XXとの契約

A：医療機関の規模を問わない
B：大／中規模病院
C：小規模病院、診療所

付録　（参考）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

外部の機関と診療情報共有の連携等を行う場合に、連携する機関の間で取り決めるべき内容の参考として以下に記載する。

1. 組織的規約
   理念、目的
   管理と運営者の一覧、各役割と責任
   医療機関と情報処理事業者・通信事業者等との責任分界点
   免責事項、知的財産権に関する規程
   メンバの規約（メンバ資格タイプ、メンバの状況を管理する規約)、資金問題
   など

2. 運用規則
   管理組織構成、日常的運営レベルでの管理方法
   システム停止の管理（予定されたダウンタイムの通知方法、予定外のシステムダウンの原因と解決の通知、など)、データ維持、保存、バックアップ 、不具合の回復
   など

3. プライバシ管理
   患者共通ID（もし、あるならば）の管理方法
   文書のアクセスと利用の一般則
   役割とアクセス権限のある文書種別の対応規約
   患者同意のルール
   非常時のガイド(ブレークグラス、システム停止時、等の条件)
   など

4. システム構造
   全体構造、システム機能を構成する要素、制約事項
   連携組織外部との接続性（連携外部の組織とデータ交換方法）
   など

5. 技術的セキュリティ
   リスク分析
   認証、役割管理、役割識別(パスワード規約、2要素、認証、等の識別方法)
   可搬媒体のセキュリティ要件
   など

6. 構成管理
   ハードウェアやソフトウェアの機能更新、構成変更等の管理方法、新機能要素の追加承認方法
   など

7. 監査
   何時、誰が監査し、適切な行動が取られるか

8. 規約の更新周期