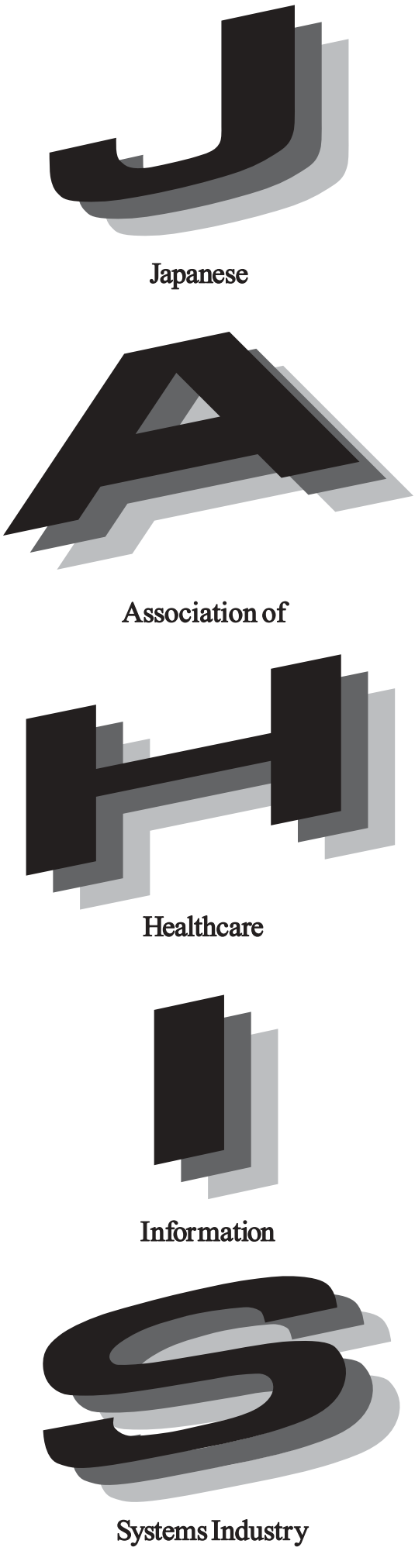
技術文書 03-101



診療録等の電子保存ガイドライン

2003年11月
保健医療福祉情報システム工業会
セキュリティ委員会

目次

１．はじめに

１-１．本ガイドラインの目的

法令により義務付けられている診療録等の保存を電子的に行うことが公に認められたのは、平成11年4月22日付の厚生省健康政策局長、医薬安全局長、保険局長の連名による通知「診療録等の電子媒体による保存について」（以後、「厚生省通知」と表記）である。

また、この厚生省通知に基づいて電子保存システムを運用しようとする医療施設への指導が、「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」として（財）医療情報システム開発センター（ＭＥＤＩＳ－ＤＣ）から発行されている（以後、「ＭＥＤＩＳのガイドライン」と表記）。

厚生省通知およびＭＥＤＩＳのガイドラインでは、電子保存システムの運用は施設の自己責任のもとで厚生省通知の電子保存３条件（真正性、見読性、保存性の確保）および留意事項（運用管理規程、証拠能力・証明力、患者のプライバシー保護）を守ることとなっているが、提示された基準が抽象的であるために電子保存システムを導入しようとする施設では電子保存システムをどの様に実現するか容易に決定しにくい状況にある。

即ち、電子保存３条件等を守る為に必要なセキュリティ保護について、技術的方法でのセキュリティ対策（担保）がどの程度可能なのか、運用でのセキュリティ対策（担保）がどの程度必要かについて自らの判断だけでは決めかねているところが多い。

この様な状況に対し、本ガイドラインではベンダーの団体である保健医療福祉情報システム工業会（以後、「ＪＡＨＩＳ」と表記）の立場から、現在のセキュリティ技術水準を前提にシステムのセキュリティ保護に関して「技術的にどの範囲まで担保することが望ましいか、また技術的に対応しにくい要件を運用でどのように担保することが期待されるか」を具体的に示すことを目的としている。

＜本ガイドラインの利用について＞

本ガイドラインは、ＪＡＨＩＳ会員各社の意見を集約し、「ＪＡＨＩＳ技術文書」の一つとして発行したものである。したがって、会員各社がシステムの開発・更新に当たって、本ガイドラインに基づいた開発・改良を行い、本ガイドラインに準拠していることをその製品のカタログ・仕様書等に示し、さらにその製品のユーザに運用で担保すべきことを説明する場合などに使われることを期待している。

また本ガイドラインを、電子保存システムを導入しようとしている施設が参照し利用することは歓迎するところであるが、当該システムが厚生省通知に合

致しているか否かの判断は、自己責任の下で自ら判断する必要があることをご留意頂きたい。

なお、本ガイドラインで扱うセキュリティ要件は、社会状況にあわせて常に変化するものであり、利用いただく時点で必ずしも適当ではない内容である可能性もある。我々としても継続的に検討を重ねてゆく所存であるが、本ガイドラインの利用者はその点もご留意頂くとともに、お気づきの点をフィードバックして頂けると幸いである。

平成１５年１１月
保健医療福祉情報システム工業会
セキュリティ委員会

1-2．本ガイドライン記述上の基本方針

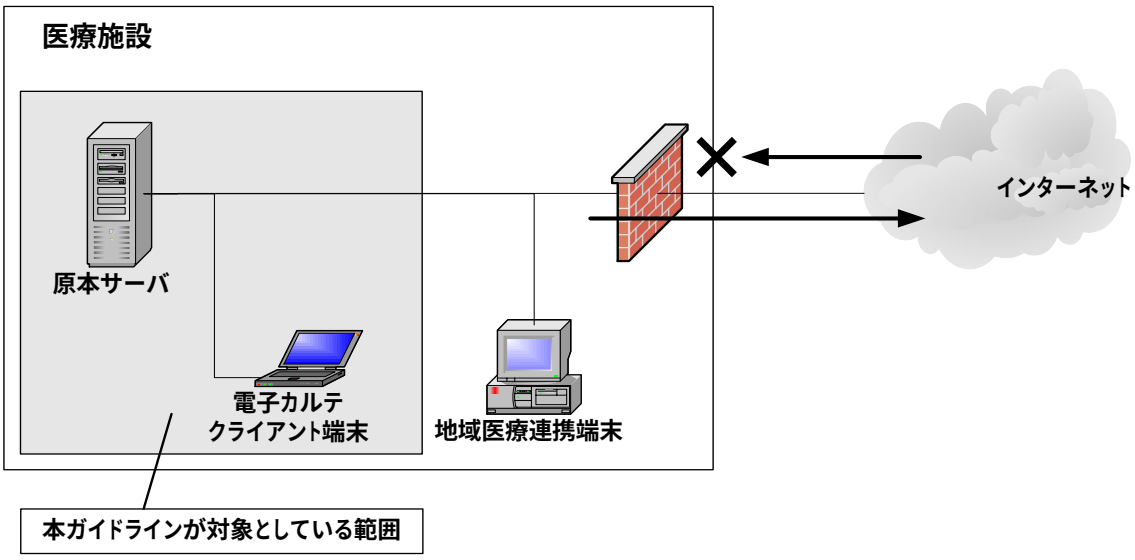
1）本ガイドラインが想定しているシステム

医療施設（但し、診療所は除く）内の診療録等の電子保存機能を含むシステムで、以下の仕様を想定している。

（1）サーバ上で集中管理されている診療録等の情報（データベース）を原本とする。

（2）医療機関は外部と通信回線で接続されており、医療機関内の端末よりインターネット上のホームページの閲覧及びインターネット経由でのメールの送受信が行われている。

（3）原本を集中管理するサーバは当該医療機関外からアクセスできないように対策が施されている。



本ガイドラインが想定しているシステム例

2）本ガイドラインが対象とするシステムの範囲

本ガイドラインで記述されている事項は、医療施設（但し、診療所は除く）内の診療録等の電子保存機能を含むシステムの診療録等の原本情報を保管するサーバと、その情報にアクセスが可能な医療施設内のクライアント端末、及びそれらのサーバや端末上で稼動するソフトウェアを対象としている。

3）ＭＥＤＩＳのガイドラインとの関係

本ガイドラインはＭＥＤＩＳのガイドラインを基にシステムベンダとしての実装要件を具体的にすることを意図して作成したものである。そのためＭＥＤＩＳのガイドラインの項番に沿って記述している。

4）技術的な担保と運用での担保の切り分け

前述の通り、現在のセキュリティ技術水準であれば実装できるであろうものは技術で担保し、技術だけでは要件実現が難しいものは運用で対応することを前提とした（但し、導入施設の方針、ならびに導入システム仕様により、実際の技術要件、運用要件の範囲が相補的に変化することを許容する）。

5）技術的な担保に含めるもの

電子保存システムに実装するセキュリティ機能以外に、システムベンダが顧客に提供すべきマニュアル類も技術的な担保の範囲に含めている。

6）その他の留意事項

電子保存以外の要件（例えば、当該医療機関外からの不正アクセス対策）などは本ガイドラインの対象ではないので、必要に応じて別に検討する必要がある。

２．用語等の定義

１）電子保存システム

診療録等の電子保存機能を有し、その業務機能を中核とする医療施設内の情報システムを「電子保存システム」と称する。

２）システム管理者

電子保存システムの運用主体である医療施設の責任者が、そのシステムの運用管理を委嘱する組織および個人を指す。

３）利用者

システム管理者によって使用の正当性が確認され承認手続きが成された個人を指す。

４）利用者の識別と認証

電子保存システムが利用者を識別する手段として使用する識別コードが必ず存在し、識別コードとしては職員番号やそれに替わり得るシステム管理者によって付与される固有番号等が使われる。また、利用者の識別コードが本人によって使われていることを確認する手段を認証といい、パスワード等の手段が使われる。

５）診療録等の作成責任者

すべての診療諸記録にはその内容に責任を有する医療職が必ず存在する。

電子保存システムに記録される診療録等は通常その内容に責任を有する医療職自ら入力するが、その者を作成責任者という。また、放射線画像や検体検査結果などの医療機器が情報発生源の場合は、電子保存システムの運用施設が当該施設の運用実体を判断して作成責任を明確に定めるものとする。

６）代行入力と作成責任者

診療録の入力において、診療録を作成すべき本人以外の者が作成すべき者の依頼を受けて入力することを代行入力という。代行入力の場合は、代行入力を依頼した本人（作成責任者）の確定操作が行われてはじめて内容および作成責任者が確定するものとする。

７）更新された診療録等の作成責任者

一連の診療録等を複数の医療職が共同で作成（入力）する場合、診療録の作成上の最小単位（作成日時・診療録内容等で分けられる）毎に作成責任者は単独となる。しかし、一旦作成された診療録が別の利用者により更新された場合、その更新範囲の作成責任者は最終の更新者と解釈する。

３．真正性の確保

３-１（１）作成責任者の識別および認証

＜要件＞システムは、作成責任者の識別および認証を利用者ＩＤとパスワード等によって必要な時点で確実に実施できなければならない。

＜技術１＞電子保存システムは利用者の識別・認証をシステムへのログイン時および必要な時点で以下のいずれかの方式で行えること。

① ＩＤ・パスワード方式
② ＩＣカード方式
③ バイオメトリックス方式
④ 上記①～③相当以上の識別・認証方式
⑤ 上記の組み合わせ

＜技術２＞利用者のログイン管理機能として以下のものが備わっていること。

（１）電子保存システムへのログイン情報（ユーザ識別情報、ログイン時刻、使用時間）の採取・記録、および1ヶ月以上の期間のログイン情報を保持・管理する機能

（２）指定期間（年月日・時間帯）のログイン情報をサーチし、例えば以下のような事項の参照が容易に可能なこと

（ａ）利用者別の日別ログイン時刻、使用時間と使用端末ＩＤ

（ｂ）ログイン失敗者別のログイン操作時刻、失敗回数と使用端末ＩＤ

＜運用１＞識別・認証が確実に行なわれるために、以下のような運用上の配慮が払われるよう、利用者教育を徹底すること。

（１）端末操作中にその場を離れる場合は、操作の終了手続きを取るなどにより、他の人が引き続いて（成り済まして）端末操作できない様にすること。

（２）ＩＤ、パスワード方式の場合は、以下のように運用すること。

（ａ）パスワードを他者に教えないこと。

（ｂ）他者にパスワードが漏れないようにすること。

（ｃ）パスワードは、8桁以上でかつ数字、アルファベット、使用が許されている記号等を組み合わせて容易に推測できないものとすること。

（ｄ）3ヶ月に1回以上の頻度でパスワード更新すること。

（ｅ）初期パスワードは必ず速やかに変更すること。

（ｆ）システム管理者は週１回以上、その期間の全利用者のログ

イン時刻、使用時間・回数から統計的に検出される非定常運用状況（例えば、ログイン時間が非常に長時間なケース、ログイン回数が非常に多いケース、複数端末から同時ログインを行なおうとしたケース等）を確認し、問題の発生がないか確認すること。

（3）ＩＣカード方式の場合、他者に貸与しないこと。また、紛失の恐れがあるので、以下を義務づけること。

（ａ）毎日1回の所持確認をすること。

（ｂ）所在不明となった場合は速やかに届け出ること。

＜運用２＞システム管理者から利用者に識別・認証の媒体あるいは情報を提供する場合、システム管理者が直接手渡すか間接的かにかかわらず、その提供ルートを記録すると共に利用者の受領書を受取り一定期間保管すること。

＜運用３＞システム管理者の特権により、電子保存システムの利用者認証を経由せずに当該システムのＤＢ 内容の参照・更新が出来る場合、システム管理者の特権で使用可能な端末の特定化や特権的使用に際しては必ず立ち会い者を付ける等、運用で特権的使用管理を行うこと。

＜運用４＞システム管理者は、利用者ＩＤ 、パスワード等の識別・認証情報が漏洩しないように管理すること。

3-1（2）確定操作

＜要件＞情報の入力後および更新後の記録に際し、入力および更新情報の最終確認と作成責任を明確に認識する確定操作が行われなければならない。

＜技術１＞情報の入力・更新結果を記録しようとする都度、利用者が作成責任を明確に認識できる「確定操作」の機能が備わっていること。

＜技術２＞代行入力の運用が行われる電子保存システムの場合、代行入力の識別と作成責任者が代行入力結果を確認し確定操作を行う機能が備わっていること。

3-1（3）識別情報の記録

＜要件＞確定操作を行った情報の記録とともに、その操作日時並びに利用者識別情報等の情報が確定操作の対象となる情報単位に関連づけて記録されなければならない。

＜技術１＞識別情報として、以下のものが含まれること。
（ａ）利用者が識別できるもの
（ｂ）確定操作日時が識別できるもの
＜運用１＞端末およびサーバのシステム時刻は、正確を期す為に定期的に補正すること。

３-１（４）更新履歴の保存

＜要件＞一旦記録された情報の更新に際しては、更新前の情報と更新後の情報が関連付けられ、それらの関連が相互に識別できるように保存されなければならない。

＜技術１＞更新処理時、以下のどちらかの方法で履歴が保存されること。
（１）更新時、それまでに一旦確定し記録されている情報はそのままとし、更新後の内容を別の記録単位として記録する機能。
（２）更新前の情報と更新後の情報の差分を記録する機能。例えば、更新前のデータを修正する場合は更新前のデータに修正線を入れて更新後のデータと識別できる様にし、データを追加する場合は追加範囲を下線と更新日付で識別すること。
＜技術２＞更新履歴の保存が上記（１）の場合、更新経過を表示し確認する機能が備わっていること。

３-２過失による誤入力、書き換え、消去および混同の防止

＜要件＞利用者に対して、過失を犯さないよう運用操作の面で十分な意識付けと操作訓練が行われなければならない。またシステムの過失対策として、確定操作時に記録範囲を容易に確認できなければならない。さらに、更新中の操作ミス等により更新内容が不確かになった場合などの対策として、その更新内容を取り消す機能が備わっていなければならない。

＜技術１＞確定操作に際し、確定範囲を容易に確認できる機能が備わっていること。
＜技術２＞一旦確定された記録を更新する場合は、更新操作を明示しなければ実施出来ない様な機能になっていること。
＜技術３＞一旦確定操作が行われた記録を取り消す場合、取り消し操作を明示しなければ実施出来ない様な機能になっていること。また、その取り消しも更新履歴として保存できること。
＜技術４＞更新操作中の操作ミス対策として、その更新内容全体を取り消す機

能が備わっていること

＜運用１＞確定操作に際し、必ず記録情報の範囲全体を確認すること。

＜運用２＞入力・更新した情報の内容に不確かなものを感じ、その内容を明確に認識できない場合には、確定操作を行わないこと。

３-３使用する機器、ソフトウェアに起因する虚偽入力・書き換え、消去および混同の防止

＜要件＞システム管理者は電子保存システムに用いる機器及びソフトウェアの新規導入および更新に際し、当該システムの機能および品質の評価を自らの責任で行わなければならない。また日常運用においても、当該システムが正常に機能するよう、点検整備を確実に行わなければならない。

＜技術１＞電子保存システム本体および電子保存システムの関連機器、ソフトウェアを提供するベンダーは、提供するものが、本ガイドラインを技術的にどのように担保しており、また顧客が実施すべき運用上の対策が何かを説明するものを書面で提供すること。

＜運用２＞システム管理者は、電子保存システム本体および電子保存システムに用いる機器及びソフトウェアの新規導入および更新に際し、そのマニュアルの内容を十分に確認し疑義のないようにしておくこと。また、一連の運用操作を行い、正常動作を確認すること。

＜運用３＞システム管理者は、システムの点検整備をマニュアル通りに実施すること。

＜運用４＞システム管理者は、システム監査を専門家に委託して毎年1回以上実施すること。また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ずること。

＜運用５＞システム管理者は品質管理の面で利用者に対し以下の指導を行うこと。

（１）サーバ管理室の入室 ；正当な理由があってもシステム管理者が随行すること。

（２）端末の管理 ； システム管理者の認めていない以下の行為を禁止すること。

（ａ）許可されていない端末機器の接続

（ｂ）許可されていないネットワークへの接続

（ｃ）アプリケーション・ソフトウェアの導入

（３）ウィルス対策ソフトの導入 ： システム管理者の指示が速やかに実施されること。

（４）システム異常時の対応 ； 速やかにシステム管理者に連絡し、その指示に従うこと。

３-４故意による虚偽入力・書き換え・消去および混同の防止

＜要件＞故意による虚偽入力等の対策として、利用者の識別・認証が確実に行われると共に（本件は「３-１．（１）」で確定済）、正当な利用者であっても、当人が関与していない患者の情報を参照、入力および更新を行うことを抑制する手段が提供されなければならない。

＜技術１＞アクセス権の基本機能として以下のものが満たされること。

（１）電子保存システムの業務メニュー単位でその業務の運用操作が可能か否かを職務および利用者単位に規定できること。

（２）必要に応じて、上記以上に細かいアクセス権を設定できること。例えば、情報の種類（区分）や内容に応じた参照・更新制限が必要に応じてできること。

＜技術２＞情報へのアクセス（参照・入力・更新）に際し、その処理内容をログ出力（アクセスログ）し、誰がどのような情報の入力・更新を行ったか識別できること。

＜技術３＞アクセスログの解析機能として、例えば以下のものを備えること。

（１）情報の種別を指定し、その種別の情報にアクセスした実績（アクセス拒否やパスワード入力エラー等を含む処理内容）を指定した日時（時間帯）で時間軸に沿って画面等に表示する機能。

（２）利用者を指定し、その利用者がアクセスした実績（情報の種別とその処理内容）を指定した日時（時間帯）で時間軸に沿って画面等に表示する機能。

（３）端末IDを指定し、その端末からアクセスした実績（情報の種別とその内容）を指定した日時（時間帯）で時間軸に沿って画面等に表示する機能。

（４）管理上のスクリーニングチェック機能として、特殊な時間帯にアクセスした累積時間順の利用者リストや、指定期間内にアクセスした患者情報件数順の利用者リスト等を表示する機能。

（５）日時の順序性チェックなどにより、端末の不正な時刻変更を検出できる機能。

＜運用１＞システム管理者は、アクセス権の設定・更新を必要に応じて行うこと。

＜運用２＞システム管理者は、アクセスログを必要な期間に渡って安全に保存

し、後からの分析調査が行えるようにすること。

＜運用３＞アクセスログ管理は、スクリーニングチェックに関しては1回／週以上の頻度で行い、その他の機能は必要に応じて実施すること。また、個室等の他人の眼が届かない所に置かれる端末の操作状況については、更に十分な管理を行うこと。

＜運用４＞抑制効果を高めるため、当該医療機関の責任者は違反者に対する罰則規程等を定め、利用者全員に予め通知しておくこと。

４．見読性の確保

4．（1）情報の所在管理

＜要件＞電子保存の対象とする情報の範囲を明確にし、また電子保存対象の情報が複数の機器や媒体に分散記録されていてもその情報の所在を一元的に管理できること。

＜技術１＞記録された情報が複数の機器に分散記録されていても、必要に応じて必要な情報の所在が迅速に把握され、容易に見読されること。なお、「迅速」とは運用目的に則し十分な時間内に見読可能なことをいう。

＜技術２＞記録された情報が媒体に保存されている場合は、各媒体を機器に装着することで、対象患者、および記録内容が容易に見読されること。

＜運用１＞電子保存の対象とする情報については、当該医療機関の責任者がこれを定め、それを施設従事者に周知徹底すること。

＜運用２＞記録媒体の管理について、当該医療機関の責任者がその管理方法について運用規則を定め、正しく運用・管理されるよう監督すること。

4．（2）見読化手段の管理

＜要件＞保存の対象となっている全ての情報は、保存開始後のシステム増設や更新あるいはソフトウェアのバージョンアップが有っても容易に見読することができるよう、情報の記録形式（記録媒体、記録フォーマット）の違いにそれぞれ対応した見読化手段が管理されていること。

＜技術１＞電子保存システムに用いる機器及びソフトウェアの新規導入および更新に際し、電子保存の対象とする情報に対して従来と同等以上の見読手段を確保すること。

＜技術２＞電子保存システムが扱う情報項目、マスタ、利用者の変更にともない、保存された情報が影響を受けないよう履歴管理などの手段を確保すること。

＜運用１＞システム管理者は、電子保存システムに用いる機器及びソフトウェアの新規導入および更新に際し、全ての情報の見読手段が継続して確保されるよう、十分に配慮すること。

4．（3）情報区分管理

＜要件＞情報の確定状況、利用範囲、更新履歴、機密度等に応じた情報区分を設定でき、情報区分に応じてアクセス権の設定ができること。

＜技術１＞アクセス権管理のため、記録された情報は例えば以下のような情報区分が設定されること。
①記録の対象患者識別情報、②記録者識別情報、③情報発生日時、④情報記録日時、⑤確定者識別情報、⑥確定日時、⑦情報の種類・カテゴリー、⑧機密度、⑨記録システム識別等
＜技術２＞情報区分に応じてアクセス権（参照、更新（新規記録を含む））の設定が可能であること。
＜運用１＞システム管理者は情報区分の定義とアクセス権の設定条件を、システム導入に際し運用管理規程に明確に定めること。

4．（4）システム運用管理

＜要件＞電子保存システムに記録された全ての情報は、目的に応じた適切な速度で見読できるようシステム管理者によって予めその必要条件が定められ、その為に必要な運用管理が行われること。

＜技術１＞電子保存システムの提供ベンダーは、記録された全ての情報が目的に応じて速やかに表示または印刷できるよう、日常の運用保守マニュアルを整備し、当該システムに添付すること。
＜技術２＞システム障害等により見読不可能な事態が生じても、そのシステムの運用目的に則した適切な時間内に復旧する手段を提供すること。
＜運用１＞システム管理者は、システムの利用可能時間を利用者に周知徹底すること。
＜運用２＞システム管理者は、コンピュータ設置場所の使用環境条件（温度、湿度等）を適切に管理すること。
＜運用３＞システム管理者は、システムの保守点検内容（正常動作を確認する為のチェック項目・頻度、保守項目・間隔、実施体制等）やデータ・バックアップ内容を明確に定め、定期的に実施すること。
＜運用４＞システム管理者は、システムの障害等の理由によるシステム停止を何段階か想定し、その個々の対応方針を定めて予め利用者に周知徹底すること。特に、システム障害時の連絡体制、対応体制は明確にすること。
＜運用５＞システム管理者は、システムの保守点検の結果やデータ・バックアップ内容履歴を管理記録として1 年以上の期間保存すること。
＜運用６＞データバックアップは世代管理を行い、厳重に管理された場所に保管すること。

4．（５）利用者管理

＜要件＞システム利用者の管理規程を定め、規程通りに運用すること。また管理規程に基づき、利用する職員のアクセス権限の設定と定期的な利用者の教育・訓練を行い、不正な利用を防止すること。

＜技術１＞システムには、利用者登録機能とその利用者の職務条件に基づく、アクセス権の登録・更新機能が備わっていること。

＜運用１＞システム管理者は、システムの利用者に関し以下の管理手順を定め管理すること。

（１）システムの利用を認められる人の条件と利用申請手続きの明示、およびシステム登録手続の速やかな実行

（２）システムの利用が取り消される条件（及び、利用が認められない条件）とその事実が認識された時点での速やかな実行

＜運用２＞システム管理者は、利用者のアクセス権に関し以下の管理手順を定め管理すること。

（１）利用者のアクセス権の設定条件の明示、およびその管理

５．保存性の確保

５．（１）媒体の劣化対策

＜要件＞電子保存システムの媒体（情報保存媒体）は、当該システムの運用施設が必要とする保存期間内は記録された情報が品質劣化等で欠落しないよう管理されなければならない。

＜技術１＞電子保存システムの提供ベンダーは、平常使用環境の維持を条件として、使用している情報保存媒体の情報保存期間の目処を具体的に示すこと。

＜技術２＞バックアップ用情報保存媒体のベンダーは、使用頻度と保存環境を条件として情報保存期間の目処を具体的に示すこと。

＜運用１＞システム管理者は、ベンダーが提示した使用環境を確保し、情報保存期間の目途内で情報保存が行われるように情報保存媒体を管理すること。

＜運用２＞システム管理者は、ベンダーが提示した期間を越えて情報保存を行う場合には、新たに他の情報保存媒体にコピーを行なう等の対策をとること。

５．（２）ソフトウェア・機器・媒体の管理

＜要件＞不適切なソフトウェアによる情報の破壊・混同を起こさないために、ソフトウェア・機器・情報保存媒体の管理を適切に行なわなければならない。

＜技術１＞電子保存システムの提供ベンダーは、適切な品質管理基準に基づいた試験を実施し、その試験結果について納入先の承認を受けること。

＜技術２＞利用されるソフトウェアの改変やウィルスの侵入を防止または検出し、速やかに復元できる仕組みを設けること。

＜運用３＞システム管理者は、ソフトウェア・機器・情報保存媒体のバージョン管理や所在管理を実施し、常に正しい動作環境で運用すること。

５．（３）継続性の確保

＜要件＞電子保存システムの変更に際して、利用する機器やソフトウェアに変更があった場合においても、以前のシステムで蓄積した情報が継続的に利用可能でなければならない。

＜技術１＞電子保存システムの変更に際し、旧システムで保存されていて継続

して保存すべき情報は、システム管理者の求めに応じて、漏れなく速やかに汎用的な形式（ＣＳＶ等）で出力する機能を備えていること。

＜運用１＞電子保存システムに蓄積されている情報の内、継続して保存すべき情報が明確に定義されていること。

５．（４）情報保護機能

＜要件＞故意または過失による情報の破壊が起こらないための機能を備えていなければならない。また自然災害等を含め、破壊が起こった場合の回復機能を備えていなければならない。

＜技術１＞利用者の操作ミスがあっても、それにより情報が破壊されない仕組みを備えること。

＜技術２＞アクセス権限を所有しない者が、直接あるいは外部ネットワークを通じて、データやプログラムに不正にアクセスすることを防止する機能を備えること。

＜技術３＞情報やプログラムの破壊が生じた際に容易かつ速やかに復旧させる手段を備えていること。

＜運用１＞故意による情報およびシステムの破壊が起こらないよう、サーバ室への入退出及び鍵の管理、外部ネットワークからのアクセス制限管理を徹底すること。

＜運用２＞過失による情報やシステムの破壊が起こらないよう、業務に関係のないソフトウェアのインストールや端末の目的外使用禁止等のルールを定め、遵守するよう利用者の教育を徹底すること。

＜運用３＞故意又は過失による情報の破壊に対し、速やかに復旧させるための手順を整備し、実施可能な体制を整えておくこと。

６．相互利用性の確保

＜要件＞異なる医療施設間、および同一医療施設内の異なるシステム間での情報交換が容易に可能でなければならない。

＜技術１＞電子保存システムの異機種および異システム間の情報交換が必要に応じて可能なように、システムに蓄積されている診療録等の全てが、汎用の媒体や通信を介して汎用のデータ形式で出力可能なこと。

７．運用管理規程

＜要件＞電子保存システムを運用する医療施設は明確なセキュリティポリシーを有し、実用的な運用管理規程を設け、それらは公開可能な水準でなければならない。

＜運用１＞電子保存システムの適切な運用を確保・維持するため「情報セキュリティ基本方針」および「情報セキュリティ対策基準」からなる「情報セキュリティポリシー」を策定し、必要に応じ公開できること。

＜運用２＞電子保存システムの運用管理規程は、ＭＥＤＩＳ のガイドラインを参考に作成され、必要に応じて公開できること。

８．プライバシー保護

＜要件＞電子保存システムを運用する医療施設では、最低水準として個人情報保護法のレベルが保証されていなければならない。

＜注意事項＞平成15年5月成立の「個人情報保護関連5法」の理念に従い、対応し、今後作成される予定となっている医療分野における個人情報保護に関する法令またはガイドラインに従うこと。

９．証拠能力・証明力

＜要件＞電子保存システムの導入・運用に際し、当該システム機能及びシステム運用条件が、医療関連訴訟に於いても十分な証拠能力および証明力を有するものと認められるようにすること。

＜運用１＞診療録の証拠能力が担保されるよう、日常診療において適切かつ定常的に診療内容が記録されるように努めること。また、診療時にその場で記録できない状況の場合、すみやかに記録すること。

＜運用２＞証明力を云々される場合を想定し、３条件（特に真正性の確保）を

当然として、さらに診療記録の内容が疾患上の問題点、診断結果および診療計画等、医学的に妥当な診療経過が包含されるように努めること。

以上

付録１　厚生省通知（診療録等の電子媒体による保存について）

写

健政発第５１７号
医薬発第５８７号
保発第８２号
平成１１年4月２２日

各都道府県知事　殿

厚生省健康政策局長

厚生省医薬安全局長

厚生省保険局長

診療録等の電子媒体による保存について

診療録等の記載方法については、「診療録等の記載方法について」（昭和６３年５月６日付け厚生省健康政策局総務・指導・医事・歯科衛生・看護・薬務局企画・保険局医療課長、歯科医療管理官連名通知）により、作成した医師等の責任が明白であれば、ワードプロセッサー等いわゆるＯＡ機器により作成することができるものと解されているところであるが、診療録等の電子媒体による保存の可否については、これまで明らかにされていないところである。

そこで、今般、下記１に掲げた文書等（以下「診療録等」という。）について、下記２に掲げる基準を満たす場合には、電子媒体による保存を認めるとともに、その実施に際し、留意すべきことを下記３のとおり示すこととしたので、御了知の上、関係者に周知方をお願いする。

この基準は、診療録等の電子媒体による保存を行うに際してのものであり、診療録等の情報活用を行うに際しての基準ではないことから、各医療機関においては、保存された診

療録等の情報が発生源入力システム、新旧のシステム等のシステムにおいて、支障なく利用されるように注意を払うよう、合わせて関係者に周知方をお願いする。

なお、本通知をもって、「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」（平成６年３月２９日付け健政発第２８０号厚生省健康政策局長通知）は廃止する。

また、この通知は電子媒体による保存を義務付けるものではなく、紙媒体により保存する場合には従来どおりの取扱いとする。

さらに、本年３月１１日、高度情報社会医療情報システム構築推進事業による診療録等の電子媒体による保存に関するガイドライン及び運用管理規程例の検討の結果が取りまとめられたところであるので、参考までに送付する。

記

１　電子媒体による保存を認める文書等

(1)　医師法（昭和２３年法律第２０１号）第２４条に規定されている診療録

(2)　歯科医師法（昭和２３年法律第２０２号）第２３条に規定されている診療録

(3)　保健婦助産婦看護婦法（昭和２３年法律第２０３号）第４２条に規定されている助産録

(4)　医療法（昭和２３年法律第２０５号）第２１条、第２２条及び第２２条の２に規定されている診療に関する諸記録及び同法第２２条及び第２２条の２に規定されている病院の管理及び運営に関する諸記録

(5)　歯科技工士法（昭和３０年法律第１６８号）第１９条に規定されている指示書

(6)　薬剤師法（昭和３５年法律第１４６号）第２８条に規定されている調剤録

(7)　救急救命士法（平成３年法律第３６号）第４６条に規定されている救急救命処置録

(8)　保険医療機関及び保険医療養担当規則（昭和３２年厚生省令第１５号）第９条に規定されている診療録等

(9)　保険薬局及び保険薬剤師療養担当規則（昭和３２年厚生省令第１６号）第６条に規定されている調剤録

(10)　歯科衛生士法施行規則（平成元年厚生省令第４６号）第１８条に規定されている歯科衛生士の業務記録

２　基準

法令に保存義務が規定されている文書等に記録された情報（以下「保存義務のある情報」という。）を電子媒体に保存する場合は次の３条件を満たさなければならない。

(1)　保存義務のある情報の真正性が確保されていること。

○　故意または過失による虚偽入力、書換え、消去及び混同を防止すること。

○　作成の責任の所在を明確にすること。

(2) 保存義務のある情報の見読性が確保されていること。

○ 情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。

○ 情報の内容を必要に応じて直ちに書面に表示できること。

(3) 保存義務のある情報の保存性が確保されていること。

○ 法令に定める保存期間内、復元可能な状態で保存すること。

3 留意事項

(1) 施設の管理者は運用管理規程を定め、これに従い実施すること。

(2) 運用管理規程には以下の事項を定めること。

① 運用管理を総括する組織・体制・設備に関する事項

② 患者のプライバシー保護に関する事項

③ その他適正な運用管理を行うために必要な事項

(3) 保存されている情報の証拠能力・証明力については、平成８年の高度情報通信社会推進本部制度見直し作業部会報告書において説明されているので、これを参考とし十分留意すること。

(4) 患者のプライバシー保護に十分留意すること。

付録２　MEDIS-DC ガイドライン

法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン

１．はじめに

今回の通知は規制緩和の一環であり、電子媒体に保存したい施設が自己責任において実施することを妨げないことを確認するためのものであり、電子媒体に保存することを強制するものではない。本ガイドラインは今回の通知をもとに現状に合わせて具体的方策を説明したもので、今後の技術的進歩等に合わせ、見直す必要がある。

２．自己責任について

自己責任とは、当該施設が運用する電子保存システムの説明責任、管理責任、結果責任を果たすことを意味する。

なお、電子保存システムとは、法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存のために使用される機器、ソフトウェア及び運用に必要な仕組み全般をいう。

説明責任とは、当該システムが電子保存の基準を満たしていることを第三者に説明する責任である。

管理責任とは、当該システムの運用面の管理を施設が行う責任である。

結果責任とは当該システムにより発生した問題点や損失に対する責任である。

３．真正性の確保について

真正性とは、正当な人が記録し確認された情報に関し第三者から見て作成の責任と所在が明確であり、かつ、故意又は過失による、虚偽入力、書き換え、消去、及び混同が防止されていることである。

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の記録内容を誤ることをいう。

３－１作成の責任の所在を明確にすること。

作成の責任の所在を明確にするためには、責任の無い人が責任の有る人に成りすまして入力すること、及び一旦記録した内容が責任のある人による後からの追記・書き換え・消去等によって責任の所在が曖昧になることを防止しなければならない。

なお、一つの記録は責任のある人だけが入力するわけではなく代行入力者の存在、記録の共同責任者による追記･書き換え･消去があり得ることを想定しておく必要がある。

作成の責任の所在を明確にするために以下の対策を実施する必要がある。

（1）作成責任者の識別及び認証

作成責任者（入力者と作成責任者とが異なる時は入力者も）の識別及び認証（ＩＤ・パスワード等）が行われること。

（2）確定操作

作成責任者による入力の完了、代行入力の場合は作成責任者による確認の完了、及び一旦確定した情報の作成責任者本人及び作成共同責任者による情報の追記、書き換え及び消去等の責任を明確にするために「確定」操作が行われること。

（3）識別情報の記録

「確定」操作に際し、その作成責任者の識別情報が記録情報に関連付けられること。

（4）更新履歴の保存

一旦確定された情報は、後からの追記・書き換え・消去の事実を正しく確認できるよう、当該事項の履歴が保存され、その内容を容易に確認できること。

3－2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。

過失による誤入力、書き換え、消去及び混同は、単純な入力ミス、誤った思い込み、情報の取り違えによって生じるが、内容的に明らかな過失であっても技術的に過失と認識することが困難な場合が多い。従って、確定操作を行う前に十分に内容の確認を行うことを運用規程等に定めることが望ましい。

3－3使用する機器、ソフトウェアに起因する虚偽入力、書き換え・消去・混同を防止すること。

虚偽入力、書き換え・消去・混同は、不適切な機器・ソフトウェアの使用によって発生する可能性がある。

従って、機器やソフトウェアの導入及び更新に際して、医療機関が自らその品質管理を行うこと。

3－4故意による虚偽入力、書き換え、消去、混同を防止すること。

第三者の責任のある人への成りすましによる虚偽入力、書き換え、消去及び混同に対しては、少なくとも責任者の識別・認証等により防止すること。

なお、責任のある人の不正の意を持った虚偽入力および改竄（確定された情報に対する書き換え、消去、混同）は、もとより違法行為である。

4．見読性の確保について

見読性とは、電子媒体に保存された内容を必要に応じて肉眼で見読可能な状態に容易にできることである。

なお、"必要に応じて"とは『診療、患者への説明、監査、訴訟等に際して、その目的に応じて』という意味である。

また、『容易に』とは、『目的にあった速度、操作で見読を可能にすること』を意味する。

見読性を脅かす原因としては、例えば下記のものが考えられる。

①情報が分散されて情報の相互関係が不明になる。
②システムや関連情報が更新されて旧情報の見読ができなくなる。
③情報の所在が判らなくなったり、アクセス権等が不明になる。
④システムの正常動作ができなくなる。

これらの見読性を脅かす原因を除去し必要に応じて容易に見読性を確保するためには以下の対策を実施する必要がある。

（1）情報の所在管理

分散された情報であっても、患者別等の情報の所在が可搬型媒体を含めて管理されていること。

（2）見読化手段の管理

保存情報を見読するための手段が対応づけられて管理されていること。

そのために保存情報に対応した、機器、ソフトウェア、関連情報等が整備されていること。

（3）情報区分管理

情報の確定状態、利用範囲、更新履歴、機密度等に応じた管理区分を設定し、アクセス権等を管理すること。

（4）システム運用管理

運用手順を明確にし適切で安全なシステムの利用を保証すること。

（5）利用者管理

システムに対するアクセス権限の割り当てを制御するため、利用者管理の手順を明確にすること。

利用者の管理手順では、利用者の登録から抹消までの利用者の状況の変化に応じたアクセス権限の変更を可及的速やかに行うこと。

5．保存性の確保について

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をいう。

保存性を脅かす原因としては、例えば下記のものが考えられる。

①不適切な保管・取り扱いを受けることによる診療情報及び、その真正性、見読性を確保するための情報の滅失、破壊。
②記録媒体の劣化による読み取り不能又は不完全な読み取り。
③ウィルスや不適切なソフトウェア等による情報の破壊および混同等。
④システムの移行、マスターＤＢ、インデックスＤＢの移行時の不整合、機器・媒体の互換性不備による情報復元の不完全、見読可能な状態への復元の不完全、読み取り不能。
⑤故意又は過失による誤操作に基づく情報の破壊。
⑥業務継続計画の不備による媒体・機器・ソフトウェアの整合性不備による復元不能。

これらの保存性を脅かす原因を除去するために真正性、見読性で述べた対策を施すこと及び以下に述べる対策を実施することが必要である。

（１）媒体の劣化対策
記録媒体の劣化する以前に情報を新たな記録媒体に復写すること。

（２）ソフトウェア・機器・媒体の管理
いわゆるコンピュータウィ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。

（３）継続性の確保
システムの変更に際して、以前のシステムで蓄積した情報の継続的利用を図るための対策を実施すること。
なお、システム導入時にデータ移行に関する情報開示条件を明確にすること。

（４）情報保護機能
故意又は過失による情報の破壊が起こらないよう情報保護機能を備えること。
また、万一破壊が起こった場合に備えて、必要に応じて回復できる機能を備えること。

６．相互利用性について

電子保存された情報の効率的な相互利用を可能とするために、システム間のデータ互換性が確保されることが望ましい。効率的な相互利用とは、同一施設内又は異なる施設間で複数のシステムが存在する場合、それぞれのシステム内の情報を交換して、より効率的な情報の利用を行うことをいう。なお、異なる施設間で情報の交換を行う場合には、契約等により責任範囲を明確にし、管理の責任の所在を明らかにする必要がある。

７．運用管理規程について

各施設にあった運用管理規程を作成し、遵守すること。なお、運用管理規程にはシステムの導入に際して、「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関する基準」を満足するために技術的に対応するか、運用によって対応するかを判定し、その内容を公開可能な状態で保存する旨の規定を盛り込むこと。

８．プライバシー保護について

管理者は利用者にプライバシー保護意識の徹底を図り、運用上のアクセス権を設定し、プライバシー侵害の恐れがある場合には、調査し適切な対応を行わなければならない。

（参考）証拠能力・証明力について

訴訟における証拠能力・証明力については「高度情報通信社会推進本部制度見直し作業部会報告書　平成８年６月」に以下のように述べられている。

①刑事訴訟

電子データの存在自体を立証する場合は、非供述証拠であり、刑事訴訟法上の伝聞法則の適用はなく、したがって、要証事実との関連性が立証できれば証拠能力が認められる。通常、プリントアウトした書面を証拠として提出することになるため、電子データの内容が正確に出力されていることの立証が必要とされている。

また、電子データの内容の真実性を立証する場合は、供述証拠であり、文書に準ずるものと考えられることから、証拠能力が認められるためには、要証事実との関連性に加え、刑事訴訟法上の伝聞法則の例外が認められるための要件の具備が必要とされている。この場合、商業帳簿等業務の通常の過程において作成された書面については、一般に業務の遂行に際して規則的、機械的かつ継続的に作成されるもので、作為の入り込む余地が少なく、正確に記載されるものと一般に期待されていることから、証拠能力が認められている。これ以外の書面についても特に信用すべき状況の下に作成されていることが認められれば、証拠能力が認められるが、商業帳簿等と同様に信用性の高い書面であることが必要とされている。

さらに、証明力については裁判官の自由な判断に委ねられているが、その判断は電子データの正確性等の評価に依存するものとされている。

以上から、電子データの証拠能力及び証明力の確保については、データの入力及び出力の正確性を確保するとともに、データの改変の可能性を減殺することなどにより電子データの信頼性を高め、かつこれに対する責任の所在を明かにする必要がある。

そのためには、書類の内容、性格に応じた電子データの真正性、見読性及び保存性の確保措置を講ずる必要がある。

なお、紙で作成又は受領した証ひょう類の電子化については、紙に記録される紙質、筆跡等の情報が電子データには記録されないため、犯罪捜査・立証上問題が多いと指摘されており、電子データによる保存を認めるに当たっては、その点に十分配意する必要がある。

②民事訴訟

民事訴訟においては、証拠能力についての制限はなく、また、証明力については裁判官の自由な判断に委ねられてる。

電子データによって保存された書類を証拠とする場合、その証明力の判断においては、データの入力及び出力の正確性、データの改変の可能性が問題となり、電子データの信頼性を高め、かつこれに対する責任の所在を明らかにすることが必要であるが、この点については、書類の内容、性格に応じた電子データの真正性、見読性及び保存性の確保措置を講ずる必要がある。

なお、書類の電子データによる保存の認容をどの程度とするかは、そのデータにより証明しようとする事柄についての挙証責任を官と民のいずれが負担するかについても関係するので、その点も踏まえ、検討することが必要である。

（技術文書 03-101）

診療録等の電子保存ガイドライン

2003年11月

発行：保健医療福祉情報システム工業会
セキュリティ委員会

〒105-0001　東京都港区虎ノ門１丁目19-9
（虎の門ＴＢＬビル　6F）
TEL：03-3506-8010　FAX：03-3506-8070

（無断複写・転載を禁ず）