

**データベースシステム、汎用 OS およびファイ
イル保護ソフトを用いた小規模医療施設向
け診療情報電子保存システムの真正性確保
のためのガイドライン**

(Ver.1.00)

**2004年1月19日
IS&C委員会 WG16**

目 次

1 . はじめに.....	4
2 . 背景.....	5
3 . 適用範囲.....	7
4 . 用語解説.....	10
5 . 基本方針.....	11
5 . 1 真正性確保の方法.....	11
5 . 2 システム実装.....	11
6 . システム環境および運用環境.....	14
6 . 1 システム環境.....	14
6 . 2 運用環境.....	15
7 . 脅威の分析.....	16
7 . 1 システムの対象範囲.....	16
7 . 2 アクセス者.....	16
7 . 3 ワークフロー.....	17
7 . 4 システム管理.....	18
7 . 5 組織外部からの脅威.....	19
7 . 6 脅威のまとめ.....	20
8 . 対策手法.....	21
8 . 1 対策方針.....	21
8 . 1 . 1 脅威とその対策手法.....	21
8 . 1 . 2 対策手法の実現部位.....	21
8 . 1 . 3 アクセス者とその権限.....	22
8 . 2 データベースシステムにおける対策手法.....	23
8 . 2 . 1 データベースシステムでの認証.....	23
8 . 2 . 2 アクセス制御と権限管理.....	24
8 . 2 . 3 ログの取得.....	26
8 . 3 OSおよびファイル保護ソフトにおける対策手法.....	28
8 . 3 . 1 OSにおける認証および権限管理.....	28
8 . 3 . 2 ファイル保護ソフトによるデータおよびログの保護.....	28
8 . 3 . 3 システム監査機能.....	30
9 . 診療所電子カルテシステムの対策例.....	31
9 . 1 システム構成.....	31
9 . 2 診療所の職員構成.....	31
9 . 3 電子カルテの管理する情報.....	31
9 . 4 各情報に対するアクセス権.....	32
9 . 5 データベースでの対策.....	32
9 . 5 . 1 アカウントの管理.....	32
9 . 5 . 2 アクセス制御（ロール設定）.....	35

9.5.3	監査ログの実施.....	41
9.6	OSおよびファイル保護ソフトでの対策.....	42
9.6.1	システム構成.....	42
9.6.2	アクセス・ポリシー情報の設定.....	42
付録1	関連文書一覧.....	44
付録2	データベースシステム参考例.....	44
付録3	ファイル保護ソフトウェア参考例.....	44
付録4	カルテの修正とデータベース.....	45

1. はじめに

本ガイドラインでいう「電子保存」とは、平成 11 年 4 月 22 日に当時の厚生省健康政策局、医薬局、保険局の三局長通知として各都道府県知事宛てに発出された「診療録等の電子媒体による保存について」(以下通知と呼ぶ)における電子媒体による保存を指している。通知では、電子媒体による保存を認める文書の範囲、電子媒体に保存する場合の基準、その他留意事項を定めている。同時期に財団法人医療情報システム開発センターより「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」が出ており、通知についての考え方を整理している。(「診療録等の電子媒体による保存に関する解説書」平成 11 年 10 月)

電子媒体に保存する場合の 3 つの基準とは、真正性、見読性、保存性である。また留意事項には「患者のプライバシー保護に留意すること」、運用管理規定を定めること、運用のための組織体制を確立することなどがあげられている。原則として電子保存は当該施設の自己責任によって運用することとされている。自己責任とは、説明責任、管理責任、結果責任を満たす事である。即ち電子保存されていることを第三者に説明する責任、きちんとした管理を行う責任、結果起きたことに対するすべての責任となる。そのためには、電子保存の 3 つ基準と留意事項に対して、技術的に対応が可能なシステムの導入とその運用管理ができていることが必要となる。

上述の「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」によれば、真正性として確保すべき事とは、作成責任者の識別、認証、確定操作の実施、更新履歴の保存、過失や機器による虚偽入力、書き換え、消去及び混同を防止することが上げられる。見読性として確保すべき事は、常に肉眼で見読可能な状態にできることを保証することである。保存性を確保するためには、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、見読可能な状態で保存することが必要である。これらの基準は装置の持つ技術的なレベルだけで担保することは不可能であり、何らかの運用管理があって始めて達成される。技術的なレベルが高ければ運用管理は厳しいものでなくてもよく、逆に技術的なレベルが低くければ運用管理を厳しくしなければならないという相補う関係である。3 つの基準の中で最も運用で担保する事が難しいのは真正性である。一旦確定された情報が、書き換えられあるいは消去されないよう防止すること、またそのことが起こればその事実が履歴として残り検出できることが要求されている。電子保存を行う医療情報システムはそのことを技術的にどこまで担保できるかが問われている。しかしそのための費用をいくらかけてもよいというわけではなく、現実的なももである必要がある。特に診療所のような小規模医療施設においては真正性確保の為に特別の費用をかけることが難しい状況であり、出来るだけ費用のかからない方法でこの課題を解決することが求められている。

そこで本ガイドラインでは小規模医療施設の運用状況も考慮した真正性確保

の課題を解決する方法として、データベースシステム、汎用 OS およびファイル保護ソフトを用いてアクセス権を制約する方法を提案することとした。一般的な汎用製品なので、導入コストを低く抑えられるということと真正性の対策が十分にされていることの説明責任が果たしやすいという面で小規模医療施設向けに適した方法と言える。本ガイドラインは、一般的なデータベースシステム、汎用 OS およびファイル保護ソフトを用いて真正性の確保するためには、どのようにこれらを利用しなければならないのかについてとりまとめたものである。

2. 背景

現在、市場には数多くの電子カルテ製品や画像システムが存在する。これらの製品には診療所などの小規模医療施設向けの製品も存在していて、真正性の確保に関してはいろいろな方法で対策が講じられている。しかし中には真正性の確保の面で不透明なところもあり対策が十分かどうかの疑問も少なくない。

改ざんの防止や検出の技術として以下に示すような技術が一般的とされて、また実際に採用されている。

- (a) ハッシュ値を信頼できる第 3 者機関に預けておいてデータの改ざんを検知する方法
- (b) PDF ファイルに変換しておいて改ざんを防止する方法
- (c) 公開鍵暗号方式を用いた電子署名により改ざんされていないことを保証する方法
- (d) 原本性保証装置を用いデータの改ざんを防止する方法
- (e) 個々のアプリケーションプログラムに独自の改ざん抑止または検知機能を作り込む方法

しかし、これらの技術はその単独の採用では真正性の確保に不十分であったり、費用あるいは簡便さの点に課題を持っている。これらの方法の課題等について以下に示す。

(a) の “ ハッシュ値を信頼できる第 3 者機関に預けておく方法 ” は改ざんの検出に関するものであり、このようなサービス提供業者がまだ限られていることと、このサービスを利用するための費用が必要なことが課題となっている。特に患者毎にハッシュ値を登録するとすると登録回数が 1 日に数百にもなることもあり利用者の費用負担が増す。

(b) の “ PDF ファイルに変換しておいて改ざんを防止する方法 ” では、PDF 化したデータの変更は困難とされているが不可能でなく、また PDF 化する前の元データからの再作成は簡単であり、再作成の可能性がある。したがって元データの改ざん防止手段や他の改ざんの検出手段と併用する必要がある。

(c) の “ 公開鍵暗号方式を用いた電子署名により改ざんされていないことを

保証する方法”はデータの送受信などでは効果が期待でき、また改ざん検出技術として一般的である。しかし診療録のように長期に保存する保存データの改ざん検知に用いるには、暗号解読技術の進歩やコンピュータの処理能力の進歩に対応して長期保存にどう対応するか等の課題がある。長期保存のための課題がありまた仕掛けが煩雑である等、小規模医療施設向けとしての実施するにはまだ課題が多い。また改ざん防止に関しては別の手法を用いる必要がある。

(d)の“原本性保証電子保存装置を用いデータの改ざんを防止する方法”は電子金庫に似た専用のハードウェアが必要となり診療所のような小規模医療施設で導入するには費用面での課題がある。

(e)の“個々のアプリケーションプログラムに独自の改ざん抑止または検知機能を作り込む方法”は、各ベンダーが別々に対応機能を開発しなければならぬこと、製品によっては真正性確保の為の対策が十分に組み込まれない可能性があること、ユーザ側からみて真正性確保が十分に成されていることの検証が難しいこと、またこの検証が難しいということからユーザが真正性の説明責任を果たす上でも説得性に欠ける等の問題をもっている。

なお、アプリケーションプログラムでの対策には限界があることも特記しておかなければならない。通常、電子カルテシステムは汎用のデータベースシステムや、OS上に構築されていることが多いが、データベースシステムや、OSには独自のメンテナンス機能が備わっておりデータベースやファイルを修正、消去、入れ換えなどがアプリケーションプログラムの介在なしの操作可能となっている点である。

また、上記(a)～(e)のいずれの方法も、基本的にデータが登録された時点以降に改ざんされていないことは証明されるが、ある期間に亘って改ざんがなかったことを証明するものではない。ある期間に亘る診療情報を扱う電子カルテでは、記録を追加して再登録を繰り返すことになり、このとき過去の記録データまで書き換えられる恐れが発生し得る。このためには以前のすべての登録データが存在していなければ真正性の保証とならない。またデータの消去への対策も保証されなければならない等の課題がある。

以上に述べるように上記に示す方法はいずれもまだ小規模医療施設向けに最適な方法とは言い難く更なる最適化技術の開発・提供が求められていると言える。さらには上記のいずれの方法も電子カルテに関しては紙カルテイメージに編集した医師作成のカルテファイルに対する対策であり、必ずしも各患者から収集した全診療データを対象としたものであるとは限らない。例えば画像データは医師作成カルテにそのすべてが貼り付けられるわけでもなく、撮影した何枚かの画像の中から代表的な画像のみを貼り付ける運用である。全診療データが保存の対象であるとするならば画像データも含めた全診療データの真正性を確保しなければならないことになる。診療データベースには逐次データの追記が行われているので、ファイル単位の改ざん抑止のようにファイル全体の更新を抑止することではこの問題を解決することは出来ない。すなわちデータベース中の保護対象部のみでの更新・消去抑止などが必要なのであって、このよう

なデータ保護対策はデータベースの管理機能であるデータベースシステムでしか成し得ない。

また、データベース自身も OS のファイルシステムから見ると、単なるファイルに過ぎないのでファイル全体が消去されたり、正当なデータベースシステム以外からアクセスされることが起こり得る。このようなことがないように OS の面からもデータベースの真正性確保の対策が必要となってくる。

アクセス制御やファイル保護を厳密に管理できる OS も存在するが、一般に使用されている汎用 OS では困難である。これらの汎用 OS ではファイル保護ソフトと併用することでアクセス制御やファイル保護を厳密に行うことが可能になる。

このような事情から本ガイドラインでは小規模医療施設の環境状況も考慮したうえで上記の課題を解決すべく新たな方法を提案することとした。

3．適用範囲

本ガイドラインが想定する対象医療施設は診療所などの小規模医療施設とする。想定する施設内ユーザ数は医師、スタッフを含めて 5～10 人程度とする。システム規模はサーバ 1 台、クライアント 5 台程度で、小規模医療施設が費用的に導入可能な規模のレベルとする。当該ユーザの特長としては以下が上げられる。

- ・ 電子保存の為に多く費用がかけられない。
- ・ システム管理の為に特別に訓練された人がいない。
- ・ 院長は病院の責任者であると同時に、システム管理者でもある。

本ガイドラインが対象としている範囲を、平成 13 年 3 月 11 日に財団法人医療情報システム開発センターから出された「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」の通知基準適合チェックリスト(例)を用いて明確化した。その内容を付録の「本ガイドラインが対象としている真正性保証に関する範囲」に示す。

本ガイドラインは、通知に従った診療録の電子保存を行うに際、真正性を確保する方法として、データベースシステム、汎用 OS およびファイル保護ソフトを用いたアクセス権限管理を行う方法について示すものである。

なお、本ガイドラインは小規模医療施設向けの電子カルテシステムやその関連システムを開発・販売するベンダー、および当該医療施設従事者向けに診療録の電子保存システム構築時の参考に供すべく作成されたものである。

表 3 - 1 本ガイドラインが対象としている真正性保証に関する範囲

	項目	内容	対象	本ガイドラインが対象としている真正性保証に関する範囲
真正性	作成責任者の識別および認証	システムは、各種カードとパスワードの組み合わせなどでその操作を行う者を識別して認証できますか？	x	本ガイドラインの適用対象外。
	確定操作	情報の保存タイミングを制御する為に確定操作ができますか？		確定操作自身は本ガイドラインの適用対象外。 確定済み情報を書換不可等の状態で保存するなどの真正性の確保は本ガイドラインの適用範囲。
	識別情報の記録	確定操作を行った利用者の識別情報を保存情報に付加できますか？		確定操作者の識別は本ガイドラインの適用対象外。 確定操作者情報を書換不可等の状態で保存する真正性の確保は本ガイドラインの適用範囲。
	更新履歴の保存	システムは、更新履歴の保存機能がありますか？		更新履歴を書換不可等の状態で保存する真正性の確保は本ガイドラインの適用範囲。
	過失による虚偽入力、書き換え、消去および混同の防止	過失による左記の防止対策は、講じられていますか？		過失による確定情報の書き換え、消去および混同により真正性が損なわれることへの対策は本ガイドラインの適用範囲。
	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	使用する機器あるいはソフトウェアによる左記の防止対策は講じられていますか？		使用する機器、ソフトウェアによる確定情報の書き換え、消去および混同により真正性が損なわれることへの対策は本ガイドラインの適用範囲。
見読性	故意による虚偽入力・書き換え・消去および混同の防止	故意による左記の防止対策は、講じられていますか？		故意による確定情報の書き換え、消去および混同により真正性が損なわれることへの対策は本ガイドラインの適用範囲。 なお、正常なアプリケーションプログラムを通しての故意による虚偽入力・書き換え・消去および混同を目的とした操作は本ガイドラインでも防止出来ないが、もとよりアプリケーションプログラム及び運用では本脅威に対して出来る限りの対策を講じていることが前提であって、アプリケーションプログラム以降の処理である RDBMS、及び OS 層での対策を適用の範囲としている。
	情報の所在管理	システムは、分散保存された情報を関係付ける機能がありますか？	x	本ガイドラインの適用対象外。
	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付けられて管理されていますか？	x	本ガイドラインの適用対象外。
	情報区分管理	システムは、情報の区分を設定できて、その区分にしたがってアクセス権等の設定が可能ですか？		情報区分ごとの利用者資格によるアクセス制限管理、ファイルセキュリティ管理者の設定など本ガイドラインの適用範囲。
	システム運用管理	システムの適切で安全なシステム利用が保証されていますか？		情報区分ごとの利用者資格によるアクセス権限の設定機能、およびファイルセキュリティ管理機能をユーザに開放できないようにすることによるシステムの安全利用に関しては、本ガイドラインの適用範囲。

	利用者管理	利用者管理の手順が明確になっていますか？		各利用者の資格によるデータベースアクセス制限に関しては本ガイドラインの適用範囲。各利用者がどの資格を有しているかについては運用手順などで管理しなければならず本ガイドラインの適用対象外。
保存性	媒体の劣化対策	システムで利用する保存媒体の保証された保存可能期間は何年ですか？その期間が診療録および診療諸記録の法的保存義務年限より短い場合は、新たな媒体に複写できますか？	×	本ガイドラインの適用対象外。
	ソフトウェア・機器・媒体の管理	不適切なソフトウェアによる情報の破壊・混同を起ささないためにソフトウェア・機器・媒体の管理が適切にできるようになっていますか？		真正性を確保しなければならないファイルを特定のデータベースシステム、またはアプリケーションプログラムからのみアクセス可能にすることは本ガイドラインの適用範囲。これによりウイルスなどの不正なソフトの対策となるが機器本体や、システムから離れてしまう媒体の保存性の確保は運用でカバーしなければならず本ガイドラインの対象範囲外。
	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は講じられていますか？	×	本ガイドラインの適用対象外。
	情報保護機能	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ますか？また破壊が起こった場合の回復機能を備えていますか？		故意または過失による確定情報の書き換え、消去および混同により真正性が損なわれることへの対策は本ガイドラインのカバーする範囲。破壊が起こった場合の回復機能（バックアップ・リストア）に関しても本ガイドラインの適用範囲。
その他	相互利用性	相互利用性は、留意していますか？	×	本ガイドラインの適用対象外。
	運用管理規程	管理規程は公開可能ですか？	×	本ガイドラインの適用対象外。
	プライバシー保護	プライバシー保護は、どのように講じられていますか？		利用者の資格によるデータベースアクセス制限に関しては本ガイドラインの適用範囲。各利用者がどの資格を有しているかについては運用でカバーしなければならず本ガイドラインの対象範囲外。
	証拠能力・証明力	証拠能力・証明力は、留意されていますか？		本ガイドラインが適用対象としている部分に関しては、汎用データベース製品、OS製品を用いるので、証拠能力・証明力確保の面では有利。

4 . 用語解説

- ・ 真正性：正当な人が記録した情報が、作成の責任と所在が明確であり、故意または過失による虚偽入力、書換え、消去、および混同が防止されていること。
- ・ 見読性：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出来ること。
- ・ 保存性：記録された情報が必要な期間にわたって真正性を保ち、見読可能な状態で保存されること。
- ・ 原本性保証電子保存装置：真正性、見読性、保存性を備えて電子データを保存できるようにした装置。
- ・ 公開鍵暗号：暗号化鍵と複合化鍵の二つの鍵を持ち、一方を公開することで電子署名を実現することの可能な方式の暗号。
- ・ ハッシュ値：データから生成されたデータの特徴を表す値。
- ・ PDF：Portable Document Format の略。印刷用途等の変更を前提としない共通的な電子文書のデータ交換・保存フォーマット。
- ・ OS：Operating System の略。プログラム、データ、ハードウェアを管理する基本ソフトウェア。
- ・ データベースシステム：データの運用・維持・管理を効果的・効率的に行うソフトウェア。
- ・ RDBMS：Relational Data Base Management System の略。関係データベースモデルに基づいてデータの運用・維持・管理を行うソフトウェア。
- ・ ファイル保護ソフト：汎用 OS にアクセス制御等のファイル保護のセキュリティ機能を追加するソフトウェア。
- ・ リムーバブルメディア：FD、MO、CD、DVD、メモリカードなどの着脱可能な電子媒体。
- ・ SQL：Structured Query Language の略。構造化問合せ言語。データベースシステムに対して問い合わせ・操作等を行うために使用する言語。
- ・ オブジェクト権限：表・ビュー等に対してどの操作が許可されているかという権限。
- ・ ロール：各種複数の権限をセットにして名前をつけたもの。ロールの単位でまとめて権限の付与・削除等が可能になる。
- ・ ビュー：表と同様に扱える実際の表から導き出された仮想的な表。

5 . 基本方針

5 . 1 真正性確保の方法

真正性確保に関して、阻害する要因(脅威)に対しての抑止・予防、阻害された場合の検出・回復の各局面での対策がある。真正性の証明および説明責任と言う観点から重視されるのは一般的に改ざん・消去の検出である。しかし、改ざん・消去を引き起こさないために、その抑止・予防の防止策も同様に重要である。本ガイドラインでは、電子カルテデータの真正性確保のための改ざん・消去の防止および検出の双方の実現を目指す。

改ざんの検出に関して、契約書等の場合は、ある時点に作成されて以後それが改ざんされていないことが証明されれば十分である。しかし、電子カルテデータのような診療プロセスの記録は、診療が始まってからの診療情報が日々追加されるものである。最終のデータだけが登録されてそれ以後の改ざんがないことが証明できても、登録までに改ざんがなかったことの証明にならない。本来記録が追加される毎に登録をして、すべての電子データがそろって初めて最終データが改ざんされていないといえる。以前のデータが消去された場合には、その期間の改ざんの検出はできず、真正性の確保が困難となる。電子カルテのデータが最初に作成されてから診療が続く期間のプロセスにおいて、すべての記録の真正性確保を現実的・効果的に実現する。

改ざん・消去の防止、検出を次の方針で実現する。

(1)改ざん・消去の防止方法

改ざん・消去の防止策として次に示す対策を行う。

アクセス者の適切な認証および適切なアクセス制御を行う

書き換えなしの追記によるデータ処理のみとする。

消去できないようにデータを保護する。

(2)改ざん・消去の検出方法

次のプロセスにより改ざん・消去の検出を行う。

診療情報の書込みについて、確実にすべてのログを取る。

ログを厳密に保存・保護する。

ログを調べることにより、改ざんがあればそれを検出することができる。

ある記録の真正性の証明すなわちここでは改ざん・消去が無いことの証明は、ログを調査して当該記録に関する不正な操作のログが無いことで証明される。この証明においてはログが確実に取得されて保存・保護されていることが重要である。

5 . 2 システム実装

真正性確保のための改ざん・消去の検出および防止を具体的に実現するための機能として次の機能を実装する。

表5 - 1 実装基本機能

No	実装基本機能	目的
1	アクセス者の認証およびアクセス制御	改ざん・消去を防止する。
2	追記による処理	改ざん・消去を防止する。
3	データの保護	改ざん・消去を防止する。
4	書込みのログの取得	すべての書込みのログを取得して改ざん・消去を検出する。
5	ログの保護	改ざん・消去検出のための証拠としてのログを確実に保存・保護する。

真正性の証拠とするには、すべての書込みログの確実な取得およびその確実な保護が必要である。書込みログの確実な取得およびその確実な保護のためにデータベースシステムおよびファイル保護ソフトを採用する。アプリケーションでログを取得することは可能であるが、そのアプリケーション以外からの操作が無かったことの証明が困難である。データベースシステムに制御された情報をデータベースシステムを介さずに操作することは一般に困難である。汎用 OS 上のデータベースシステムに制御されるデータベースやログデータは通常は汎用 OS 上のファイルであり、OS の管理者権限で操作可能である。汎用 OS 単体でそのデータベースやログデータを完全に保護するのは困難であるため、詳細なアクセス制御等を可能にするファイル保護ソフトを用いる。

その構成として概念的な基本構成を図に示す。

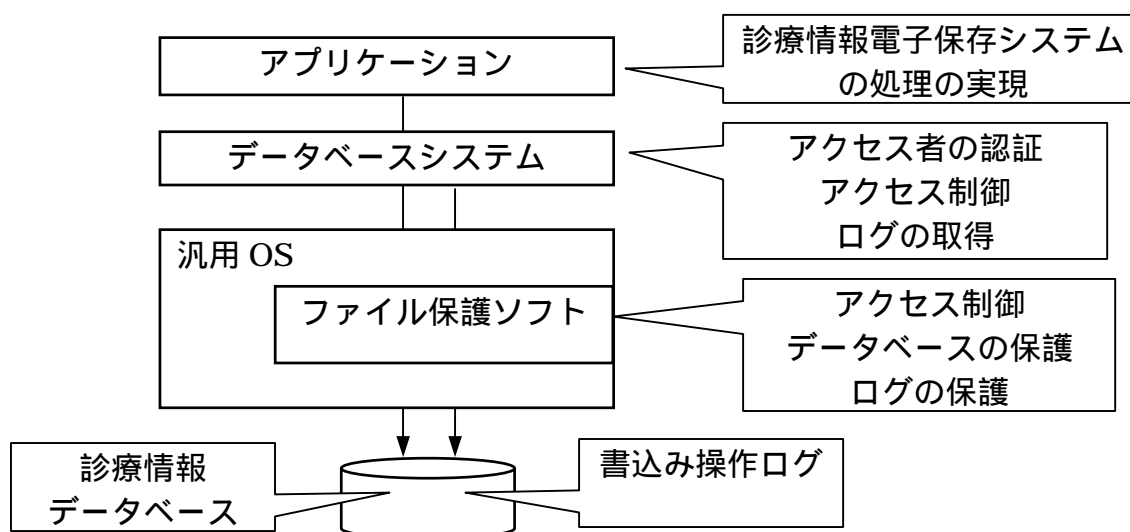


図5 - 1 概念的な基本構成

(1) アプリケーション

下位の層であるデータベースシステムや OS 等の機能を用いて診療情報電子保存システムを実現する根幹部分である。プログラム不良等による真正性の確保への脅威を抑えるために、下位層のデータベースシステムの機能を極力用いるようにして、処理を実現する。

(2) データベースシステム

確実にログを取得するためにデータベースシステムを用いる。データベースシステムとしては RDBMS と呼ばれるデータベースシステムが一般的であり、本ガイドラインでも RDBMS (ANSI X3.135-1999 ISO 9075-1999 に準拠した SQL) を想定する。一般的な商用データベースシステムではセキュリティ対策を講じるための様々なオプション機能等が用意されているが、これらは各製品の独自機能に依存する場合が多く、本ガイドラインでは、各製品等に共通した標準的な機能のみを対象とする。

(3) 汎用 OS およびファイル保護ソフト

高度なアクセス制御機能を持つ OS が存在するが、利用できるソフトが限られることや利用に高度な技術を要するなど一般的でない。一般的な汎用 OS では、通常のシステム管理を実行するためのシステム管理者権限を持つと、すべてのファイルのデータの消去、書換え等が可能となり、真正性確保を容易に阻害される可能性がある。本ガイドラインでは一般的に用いられている汎用 OS を用いて、ファイル保護ソフトを汎用 OS と併用することで、アクセス制御を可能にしてデータベースファイルやログを確実に保護する。

6 . システム環境および運用環境

本章では、本ガイドラインで想定する小規模医療施設向け電子保存システムのシステム環境および運用環境について述べる。

6 . 1 システム環境

図 6.1 に小規模医療施設における電子保存システムの環境例を示す。

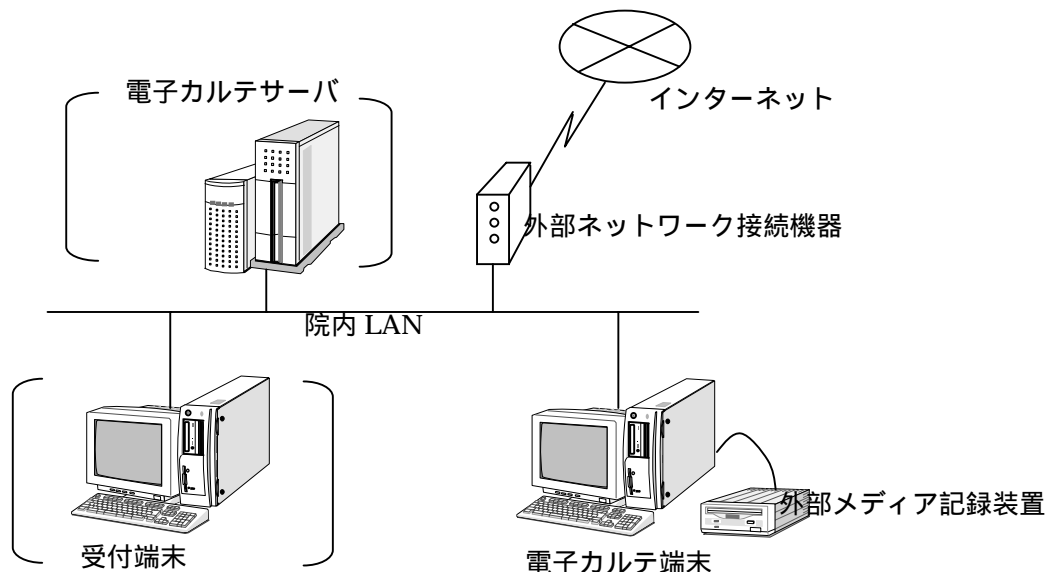


図 6.1 小規模医療施設の電子保存システム環境例

図 6.1 示した各機器の用途及び必須か任意かの構成条件を表 6.1 に整理した。

表 6.1 各機器の用途及び必須か任意かの構成条件

No	機 器	構成条件	用 途
1	電子カルテ端末	必須	電子カルテデータの入力、及び電子カルテの作成を行う。サーバを持たないケースの場合にはデータベースを含めてスタンドアロンの構成をとる。
2	外部メディア記録装置	任意	電子カルテシステムがスタンドアロン構成の場合、作成済みの電子カルテデータを原本として記録保存しておく場合と、電子カルテ装置内ハードディスク保存原本のバックアップをとる場合とがある。
3	外部ネットワーク接続機器	任意	インターネット接続など多くの場合、外部ネットワークに接続されている。
4	受付端末	任意	患者受付や診療費請求計算を行う装置である。同じネットワークに接続されていても、

			電子カルテと連動されている場合と、されていない場合とがある。
5	サーバ	任意	電子カルテデータベース用にサーバ構成をとる場合である。

6.2 運用環境

診療所のような小規模医療施設においては多くの場合、院長は病院の責任者であり、また担当医師であり、かつ電子システムの運用要管理者でもある。このように小規模医療施設においては院長に責任と権限が集中していて、保存データの真正性の説明責任を果たすうえで難しい条件が課せられていると言える。従ってこのような医療施設で使う電子カルテシステムでは、確定データに対する更新履歴が確実に取れかつ更新データの真正性確保が確実に確保できるように、ユーザ開放のシステム操作機能をできる限り制約したシステムの提供が必要となる。

7. 脅威の分析

7.1 システムの対象範囲

本章では、小規模医療施設に導入する電子保存システムにおける、医療情報の真正性保証に対する脅威について記述する。本章で論じる脅威は、図7.1に示すシステム構成において鎖線枠で囲まれた範囲のみを対象とする。外部ネットワーク接続機器より先は、本ガイドラインの対象外とし、また、リムーバブルメディアはその管理運用が施設内で厳格に行われていなければならない。なお、院内LANは施設のネットワーク管理者が適正に管理運用することを前提とする。

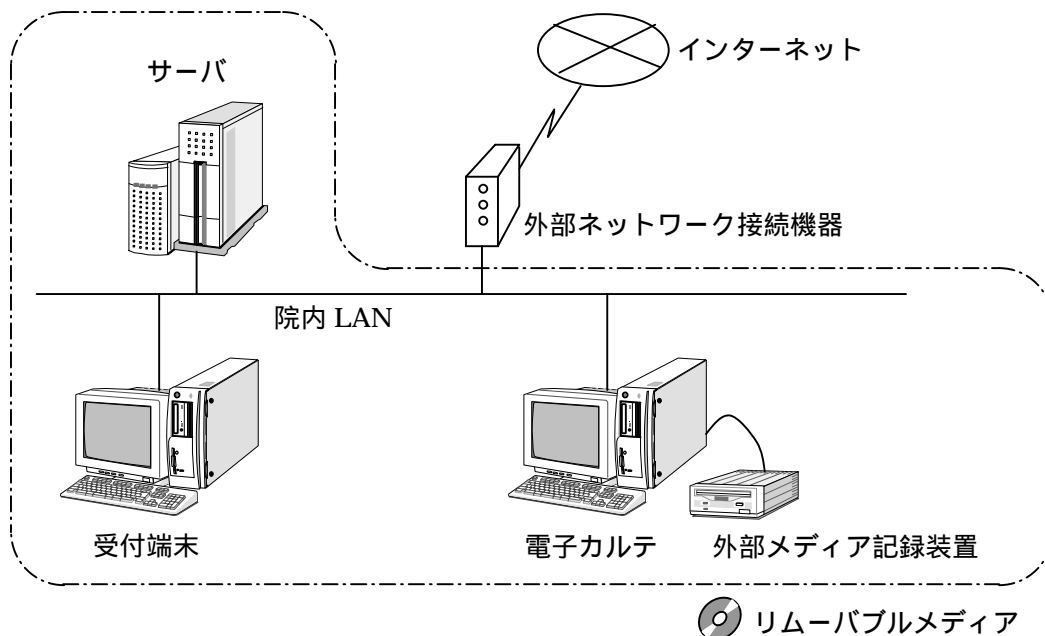


図7-1 電子保存システムにおける対象範囲

7.2 アクセス者

脅威の主体となるシステムの利用、運用、構築などにシステムに関わるアクセス者等は大きくの次のように分類される。

表7-1 アクセス者およびその職務

No	分類	職務	例
1	一般ユーザ	システムを利用して診療情報を保存、参照を行う。	一般事務員 医師、検査技師、看護婦
2	システム管理者	システムを正常に稼働させるための維持・管理に関するこ	システム要員 一般ユーザが兼ねる場合もあ

		とを行う。	る。
3	開発保守ベンダ	システムの開発、初期設定あるいはシステムの故障等の対策を行う。	保守員等
4	組織外部の者	-	侵入者 窃盗者

このシステム構成における脅威について、一般業務のワークフローでの通常のシステム利用に発生する脅威、システムを正常に稼働させるための維持・管理のシステム管理で発生する脅威、組織外部の者等によるその他の脅威の観点から考察する。

表7 - 2 主体者と脅威発生

No	主体者	脅威発生分類	発生業務
1	一般ユーザ	ワークフロー	登録や参照等の一般業務
2	システム管理者	システム管理	バックアップ等 システム保守
3	開発保守ベンダ	システム管理	システム保守 故障修理
4	組織外部の者	組織外部からの脅威	-

7.3 ワークフロー

ここではシステムのアプリケーションとして設計された機能を用いる医療施設での標準的なワークフローおよび緊急時のワークフローを図7 - 2 に示し、その脅威と手段について表7 - 3 に示す。

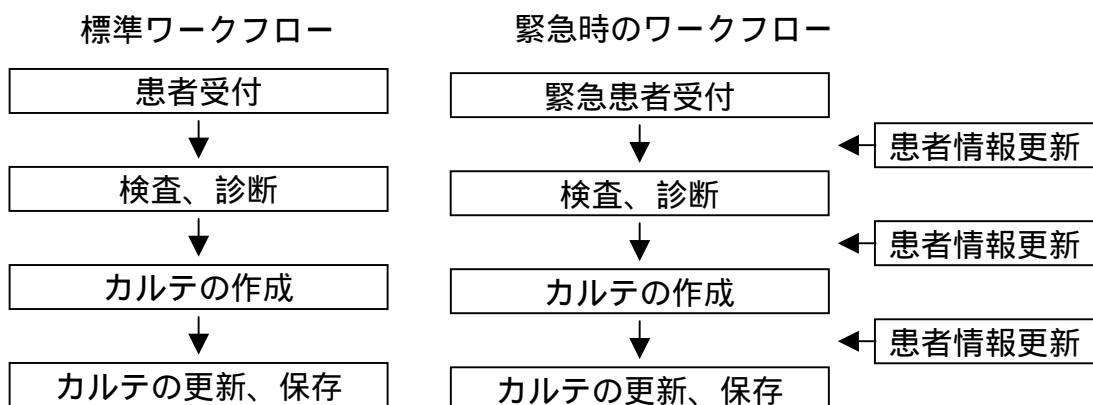


図7 - 2 医療施設でのワークフロー

表7 - 3 ワークフローにおける脅威と手段

No	ワークフロー	脅威	手段
1	患者受付	不正データ作成	誤操作 データの入力ミス 悪意のある利用
2	患者情報更新	不正データ作成	誤操作 データの入力ミス 悪意のある利用
3	検査、診断	不正データ作成	誤操作 データの入力ミス 悪意のある利用
4	カルテの作成 カルテの更新 カルテの登録	不正なデータアクセス データ改ざん データ漏洩	誤操作 データの入力ミス 悪意のある利用 他人のパスワードを取得 ログアウトしていないシステムを利用 ユーザ権限を越えてシステムを利用 正規ユーザ・正規ユーザ権限で悪意のある利用

悪意のないシステム利用行為はすべて誤操作として記述している

7.4 システム管理

システム管理における脅威と手段について表7 - 4に示す。

表 7 - 4 システム管理における脅威と手段

No	システム管理	脅威	手段
1	データのアーカイブ	不正なデータアクセス データ漏洩 システムクラッシュ	OSのコマンドを利用 データベースシステムの コマンドを利用 他人のパスワードを取得 ユーザ権限を越えてシス テムを利用 不正プログラムを利用
2	データのバックアップ・リストア	不正なデータアクセス データ改ざん データ漏洩 システムクラッシュ	OSのコマンドを利用 バックアップデータにア クセス リムーバブルメディアに アクセス 正規ユーザ・正規ユーザ権 限で悪意のある利用 不正プログラムを利用
3	管理作業	不正なデータアクセス データ改ざん データ漏洩 データ消去	OSのコマンドを利用 データベースシステムの コマンドを利用 データベースに直接アク セス 不正プログラムを利用

7.5 組織外部からの脅威

組織外部の者による脅威と手段について表 7 - 5 に示す。

表 7 - 5 組織外部の者による脅威と手段

No	組織外部の者	脅威	手段
1	ハッカー	不正なログイン 不正なデータアクセ ス データ改ざん データ漏洩 システムクラッシュ	他人のパスワードを取得 ユーザ権限を取得してシス テムを利用 ネットワークを經由して侵入 ネットワークの脆弱性を利用
2	ウィルス	データの消去 システムクラッシュ	メールやサイト閲覧による感 染

7.6 脅威のまとめ

前節までに、小規模医療施設に導入する電子保存システムにおける医療情報の真正性保証に対する脅威と手段について述べてきた。脅威の手段をまとめ、本ガイドラインの適用範囲とするものと適用範囲外とするものを表7-6示す。

表7-6 本ガイドラインの対象範囲

No	脅威の手段	対象	備考
1	誤操作	×	運用規定でカバーする
2	データの入力ミス	×	運用規定でカバーする
3	悪意のある利用	×	運用規定でカバーする*1
4	データベースシステムのコマンドを利用		-
5	データベースへの直接アクセス		-
6	ユーザ権限を越えてシステムを利用		
7	ユーザ権限を取得してシステムを利用		
8	バックアップデータにアクセス		
9	OSのコマンドを利用		
10	ウィルスなどの不正プログラムを利用		
11	システムデータにアクセス		
12	他人のパスワードを取得	×	運用規定でカバーする
13	リムーバブルメディアにアクセス	×	運用規定でカバーする
14	ネットワークを経由して侵入		
15	ネットワークの脆弱性を利用		
16	メールやサイトの閲覧による感染		
17	リムーバブルメディアにアクセス	×	運用規定でカバーする

1 脅威そのものはシステムで防ぐことはできないが、本ガイドラインに示すシステムを導入することにより、抑止効果を期待できる。

8 . 対策手法

8 . 1 対策方針

8 . 1 . 1 脅威とその対策手法

第7章で分析した脅威に対しての対策はそれぞれ次の対策手法で対策する。

表 8 - 1 脅威とその対策手法

No	脅威の手段	対策手法
1	データベースシステムのコマンドを利用	アクセス者の認証・アクセス制御 書込みのログの取得
2	データベースへの直接アクセス	データの保護
3	ユーザ権限を越えてシステムを利用	アクセス者の認証・アクセス制御 書込みのログの取得 追記による処理
4	ユーザ権限を取得してシステムを利用	アクセス者の認証・アクセス制御 書込みのログの取得 追記による処理
5	バックアップデータにアクセス	書込みのログの取得 データの保護
6	OS のコマンドを利用	データの保護 ログの保護
7	ウィルスなどの不正プログラムを利用	データの保護 ログの保護
8	システムデータにアクセス	データの保護 ログの保護
9	ネットワークを經由して侵入	アクセス者の認証 データの保護 ログの保護
10	ネットワークの脆弱性を利用	アクセス者の認証 データの保護 ログの保護
11	メールやサイトの閲覧による感染	アクセス者の認証 データの保護 ログの保護

8 . 1 . 2 対策手法の実現部位

各対策手法の各機能を実現する部位は次のようにする。

表 8 - 2 対策機能の実現部位

No	基本機能	実現部位
1	アクセス者の認証・アクセス制御	データベースシステム、OS
2	追記による処理	アプリケーションソフト
3	データの保護*1	OS、ファイル保護ソフト
4	書込みログの取得	データベースシステム
5	ログの保護*1	OS、ファイル保護ソフト

*1 アクセス制御機能であるが保護対象別に扱う。

使用されている汎用 OS・データベースシステムに関する知識を持つ者がユーティリティ等を使って直接データベースシステムにアクセスして操作を行ったり OS 上の権限を不正に利用する等の方法でその制限を回避し得るといった危険を内在しており、アクセス制御について可能な限り OS・データベースシステムの機能を用いて高度なアクセス制御を実現する。

追記による処理についてはアプリケーションで実現する。その詳細はここでは触れない。

8.1.3 アクセス者とその権限

アクセス者を次のように分類して、それぞれ必要最小限の権限を付与するものとする。

表8 - 2 アクセス者の分類とその権限

No	分類	権限	備考
1	一般ユーザ	職務に従った利用権限でシステムを利用する権限のみを持つ。	一般事務員 医師、検査技師、看護婦
2	システム管理者	システムの維持・管理に最小限必要な管理者権限を持つ。データベースおよびファイル保護ソフトの管理者権限は持たない。	システム要員
3	開発保守ベンダ	すべての権限を持つ。	保守員等
4	組織外部の者	無し	侵入者等

(1) 一般ユーザ

システムを利用して診療情報を保存、参照を行う一般ユーザについては、事務担当、検査技師、医師等の職務により権限が詳細化して、必要な機能のみが利用でき

るようにデータベースシステムにより管理・認証する必要がある。

(2) システム管理者

組織内でシステムを正常に稼働させるための維持・管理に関することを行うシステム管理者は、その実行に必要な最小限の権限を与える。OS 機能については管理者権限を与える。しかしデータベースの管理者権限およびファイル保護ソフトの管理者権限は与えない。維持管理に必要な定期的なバックアップ等のデータベース管理者権限で実施する機能についてはアプリケーション上で自動実行プログラム等を実装すること等によりシステム管理者が実行可能なようにする。

(3) 開発保守ベンダ

システムの開発、初期設定あるいはシステムの故障等の対策を行う開発保守ベンダは、その職務の実行に必要な権限を持つ。データベース管理者権限、ファイル保護ソフトの管理者権限を持ち、システムに必要な設定等を適切に行う。

アクセス者の認証を適切に行わなければならない。通常、パスワードを使用するがパスワードの管理は厳密に行う。

8.2 データベースシステムにおける対策手法

データベースシステムではアクセス者の認証、アクセス制御および書込み口グの取得を行う。

8.2.1 データベースシステムでの認証

(1) ユーザアカウントの管理

ユーザアカウントについては多くの製品においてデータベースシステムをインストールした際にデモ用のアカウントやオブジェクト等が生成される場合があるが、実システム上ではこのような不要なアカウントは全て削除ないしロックしておくものとする。

(2) データベースシステム管理者パスワードの管理

- ・ インストール後、デフォルトのパスワードは必ず変更する。また定期的変更を行う。
- ・ エンドユーザには開示を行わず、必要な保守業者等のみが保持するものとして運用で保護を行う。

(3) アプリケーションでのプレーンテキストによるパスワード格納は避ける

アプリケーションがデータベースシステムに接続する場合、接続用ユーザ

名・パスワードをスクリプトファイル等テキストベースのファイルにプレーンテキストの形で格納することは漏洩防止のため行わない。

8.2.2 アクセス制御と権限管理

(1) アプリケーションに付与する権限の最小化

アプリケーションが独自にユーザを管理している場合、データベースシステムに対してアプリケーションが単一のユーザ（スキーマ）になり、かつユーザ情報をデータベースシステムに渡さないシステム構造をとると、データベースシステム側では各ユーザを識別できないため結果的にアプリケーションに大きな権限を付与することになる。この場合不正アクセスを受け、アプリケーションが OS 上で保持している権限が乗っ取られた場合これに対応するデータベースシステム上の権限が行使できるため、格納された情報を改ざん、または削除される等被害を大きくする可能性がある。したがってアプリケーションが持つ権限を必要最小限のものに限定することが重要となる（図 8.2-1）。

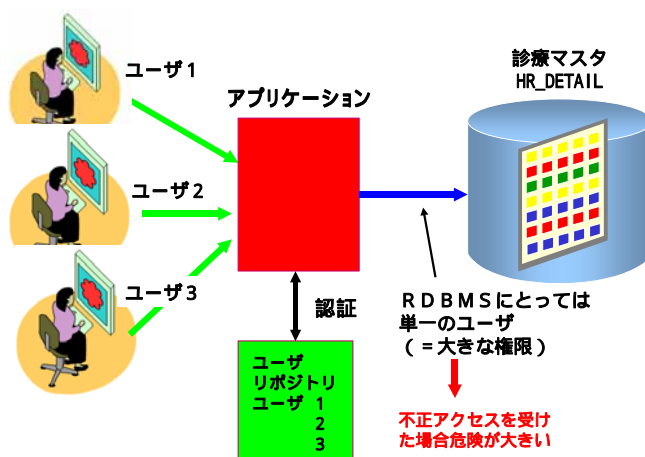


図8.2-1 アプリケーションでユーザ管理した場合の問題

(2) システム権限・オブジェクトに対する権限の最小限の付与

医療機関においてもその資格（医師・看護師・検査技師・医事会計部門等）によって閲覧・改変等に関わるアクセス権限を業務上必要な最小限にとどめることを原則とする。これを実装するための留意すべき点として次のようなものがある。

- ・一般的なオペレーションを行うだけのユーザに対してはシステム全体に関する権限の付与はほとんど必要ないため、CONNECT 権限等最小限にする。CREATE TABLE などの権限が必要な動作がある場合はあらかじめそれらを組み込んだプロシージャを作成し、その実行権限のみを付与するのが望ましい。
- ・オブジェクト権限については表ないしビューの SELECT, INSERT, UPDATE, DELETE の各権限をユーザに割り付けるものとする。またプロシージャを用いる場合はその実行権限を限定したユーザに付与す

るものとする。

(3) ビューを使ったアクセス制御

表に格納されている情報のうちユーザの属性(部門・職責など)によって参照できる物を制限するため、閲覧を許可する行・列のみを抽出したビューを作成し、ユーザに対しては当該ビューに対するアクセス権(SELECT,DELETE,UPDATE,INSERT 権)を必要なものだけ付与する方法をとることができる(図8.2-2)。

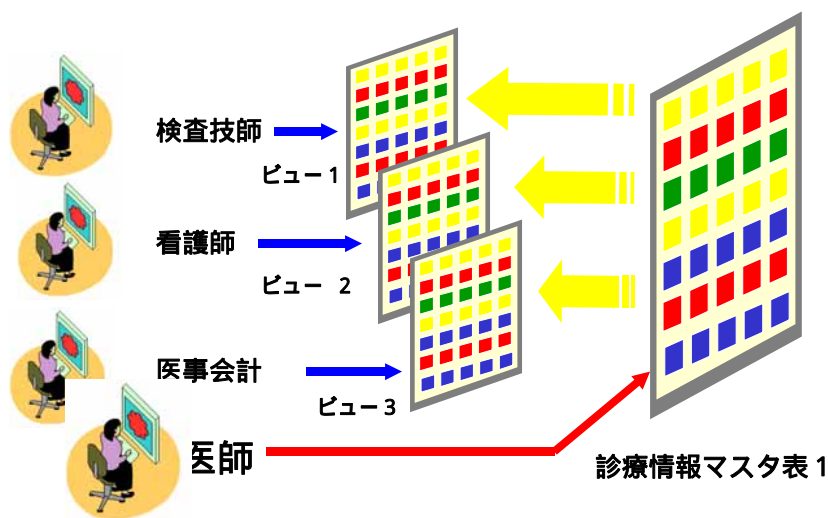


図8.2-2ビューを使ったアクセス制御

(4) ロールを使った権限の管理

ユーザ数が増加した場合、ユーザごとに個別の権限管理を行うことは運用上難しくなる可能性がある。データベースシステム側でユーザの資格に対応させた複数の権限をまとめたロールを作成し、割り当てる方式をとることが望ましい(図8.2-3)。

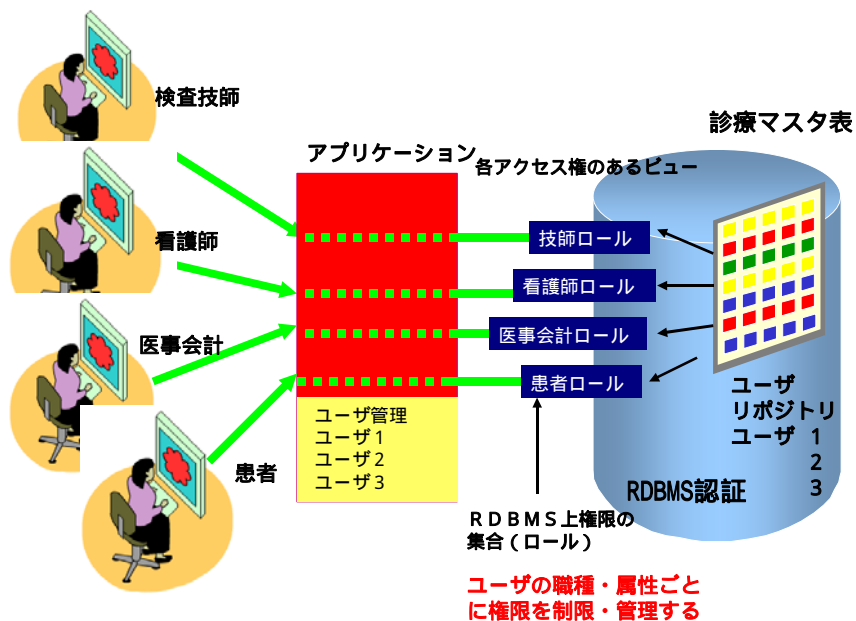


図8.2-3 ロールを使った権限の管理

この場合、アプリケーションでユーザを管理する方式となり、ユーザアカウント、その資格、データベースシステム上のロールとの対応をアプリケーション側で管理する必要がある（表 8.2-1）。

表 8.2-1 ユーザと属性・ロールの対応例

ユーザ名	資格	ロール名
ユーザ 1	検査技師	技師ロール A
ユーザ 2	検査技師	技師ロール B
ユーザ 3	外科医師	外科ロール
ユーザ 4	内科医師	内科ロール
ユーザ 5	看護師	看護師ロール
ユーザ 6	医事会計	会計ロール
ユーザ 7	患者	患者ロール

8.2.3 ログの取得

重要な情報を格納した各オブジェクト（表・ビュー）に対して特定の SQL 文に対する監査を行う。特に重要情報に対する UPDATE, DELETE, INSERT のアクションについて監査を行うことが必要である。このとき、アクセスしたユーザ名、日時、使用した SQL 文の内容、成功・失敗の区別などの情報が記録されている必要がある。実現のためには以下のような方法をとることができる。

- ・ 各データベースシステムに搭載されている監査機能を利用してこれを実現す

る。

- ・ 個別にデータベースシステムの更新トリガ機能を利用して別の表に記録情報を格納する。

監査証跡（ログ）の保存についてはデータベースシステム内部の専用の表に格納する、ないし OS 上のファイルに出力するといった方法があるがファイルに出力して、データベースシステム管理者がアクセスできないような管理を行うことが監査証跡（ログ）の客観性を保つ上では望ましい。

8.3 OSおよびファイル保護ソフトにおける対策手法

OS およびファイル保護ソフトでアクセス者の認証およびアクセス制御、データの保護、ログの保護を行う。

データベースシステムに制御されるデータベースやログデータはOS上のファイルであり、OSの管理者権限で操作可能である。汎用のOS単体でそのデータベースやログデータを完全に保護するのは困難である。データの保護、ログの保護を確実に保護するため、汎用OSに追加して詳細なアクセス制御を可能にするファイル保護ソフトを用いる。

8.3.1 OSにおける認証および権限管理

汎用のOSでは、一般にOSに登録されたユーザは利用者権限と管理者権限の2種類である。OS利用者権限は通常のアプリケーションの利用に関するリソースを扱うことができるが、OSの設定等重要なリソースを操作することはできない。OS管理者権限はOS上のすべての操作の権限を持つ。

データの保護やログの保護を行うファイル保護ソフトに関して、その設定に関するファイル保護ソフト管理者権限は開発保守ベンダのみが持つようにして、医療施設等のシステム管理者に開示しない。

表8.3-1 アクセス者のOSおよびファイル保護ソフトの権限

No	分類	権限	備考
1	一般ユーザ	OS 利用者	一般事務員 医師、検査技師、看護婦
2	システム管理者	OS 管理者	システム要員
3	開発保守ベンダ	OS 管理者 ファイル保護管理者	保守員等

8.3.2 ファイル保護ソフトによるデータおよびログの保護

一般的なシステムにおいては、パスワードの漏洩等でOS管理者の権限を得た場合、OSのシステム機能を利用し、ファイルから電子カルテシステムに格納されているデータを手入、改ざん、消去することが可能である。またネットワークを介した不正アクセス者がOS管理者権限を手入した場合やウィルス等による消去等に対抗しなければならない。

したがって、真正性保証が必要な電子カルテシステムにおいては、OS管理者権限でのファイルアクセスに対し制限を設けるため、ファイル保護ソフトによるファイルアクセス制御機能によりデータやログの保護等の必要な保護を行う。

(1) 保護対象

保護すべきファイルは以下の通りである。

- ・ 電子カルテシステムで使用するデータベースのデータが格納されるファイル
- ・ 監査ログファイル等のデータベースには格納しないファイル
- ・ その他電子カルテシステムで独自に使用する対情報漏洩、改ざん施策が必要なファイル
- ・ ファイルアクセス制御機能を収容したプログラムファイル

(2) 保護方式および実装部位

ファイルにアクセスできるアプリケーションプログラム(以降プロセスとする)を特定する機能と、OS管理者権限に対してファイルアクセス制限を設けることができる部位として、ファイルアクセス制御機能をOSレベルに実装する。その実装部位を図8.3-1に示す。

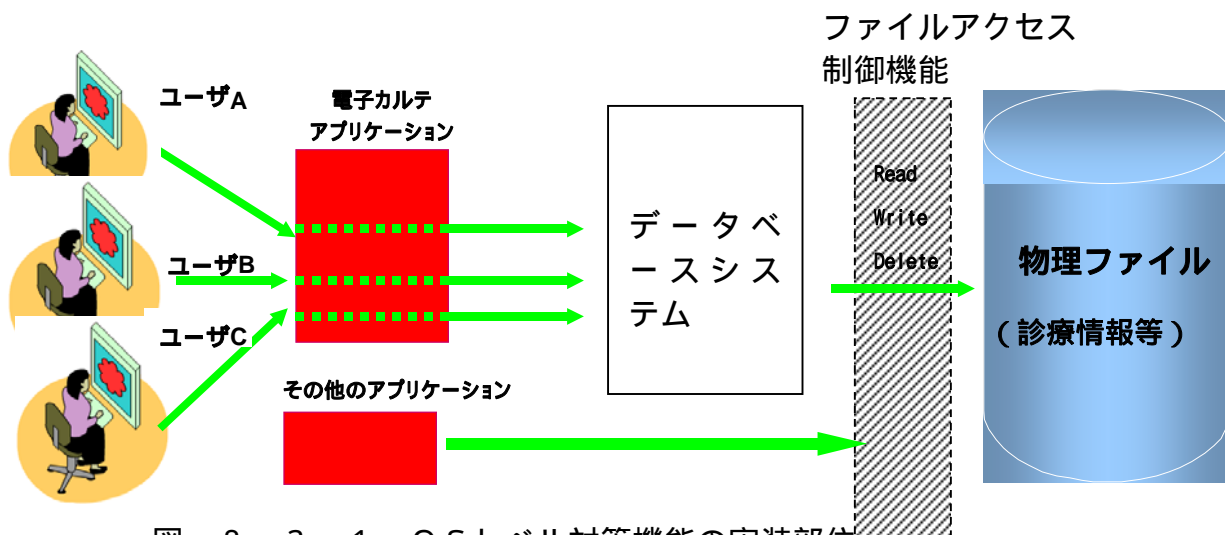


図 8.3-1 OSレベル対策機能の実装部位

ファイルアクセス制御機能が持つ機能は以下の通りである。

アクセス制御対象の物理ファイルを特定する機能

- ・ の物理ファイルに対してアクセスを許可するプロセスを特定する機能

の物理ファイルに対してアクセスを許可するユーザを特定する機能
のプロセスが発行するアクセス種別 (Read/Write/Delete/
Rename) を特定する機能

の情報を『アクセス・ポリシー情報』と呼ぶ。

アクセス・ポリシー情報に基づき、全ての条件が満たされた場合のみ物理ファイルへのアクセスを許可するものとする。

また、アクセス・ポリシー情報はOSの管理する一般ファイルとは異なり、ファイルアクセス制御機能からのみ管理されることが望ましい。

8.3.3 システム監査機能

OS が持つ監査機能と、ファイルアクセス制御機能が持つ監査機能を利用し、下記監査情報を記録することにより、不正操作の試みを検出することができる。不正操作の試みが記録されることを知らしめることで不正操作の抑止効果を期待できる。表 8.3-3 にその詳細を示す。

表 8.3 - 3 システム監査機能

OS が持つ監査機能	OS へのログイン/ログアウト
ファイルアクセス 制御機能が持つ監査機能	<ul style="list-style-type: none">・アクセス・ポリシーに違反したファイルアクセスがあった場合の不正アクセスログ取得機能・取得した不正アクセスログの表示機能

9 . 診療所電子カルテシステムの対策例

9 . 1 システム構成

以下に電子カルテシステムの構成図に示す。



図9 . 1 システム構成図

電子カルテシステムは、WEB 型の電子カルテシステムで、サーバ室のサーバマシンにWEBサーバとDBサーバが導入されている。クライアントは受付、事務室、診察室1、診察室2、検査室、放射線室に設置され、放射線室にはX線一般撮影用のCR装置がある。クライアントマシン、サーバマシン、CR装置はすべてネットワーク接続されている。

9 . 2 診療所の職員構成

- (1) 医師 - 2名
- (2) 検査技師 - 1名
- (3) 放射線技師 - 1名
- (4) 看護師 - 6名
- (5) 医事会計 - 2名

9 . 3 電子カルテの管理する情報

- (1) 診療情報 (所見、診療方針 (診療計画)、紹介状など)
- (2) 検体検査情報 (血液検査などの検体検査)

- (3) X線検査情報 (CR、CT、MRなどのX線検査)
- (4) 処方情報(処方、注射など)
- (5) 患者基本情報 (氏名、住所、電話番号、生年月日、保険情報など)
- (6) レセプト情報 (診療報酬請求)

9.4 各情報に対するアクセス権

表9.1 各情報に対するアクセス権

	診療情報		検体検査情報		X線検査情報		処方情報		患者基本情報		レセプト情報	
	R	W	R	W	R	W	R	W	R	W	R	W
医師												×
検査技師		×				×		×		×	×	×
放射線技師		×		×				×		×	×	×
看護師		×		×		×		×		×	×	×
医事会計		×		×		×		×				

記号「R」は参照権限、「W」は書込権限を示す。

記号「 」は利用可能、「×」は利用不可を示す。

検体検査情報は、医師が検査依頼を書き、検査技師が結果を書く。

X線検査情報は、医師が検査依頼を書き、放射線技師が結果を書く。

9.5 データベースでの対策

9.5.1 アカウントの管理

(1) ロールを使った権限の管理

アプリケーション利用者が必要最低限の権限しか与えないよう、アプリケーションで使用できるロール名とDBアカウントを決定する。

表9.2 ロール名とDBアカウント表

No	属性	ロール名	DBアカウント
1	アプリケーション	DB_KarteApp	KarteApp

2	医師	DB_MedDoctor	MedDoctor
3	検査技師	DB_MedTechnologist	MedTechnologist
4	放射線技師	DB_RadTechnologist	RadTechnologist
5	看護師	DB_GenNurse	GenNurse
6	医事会計	DB_Accountant	Accountant

(2) アプリケーションでのユーザ管理

アプリケーションアカウントと DB アカウントの対応はアプリケーションが管理する。以下に対応管理の例を示す。アプリケーションは USER_TABLE などを作成し、アプリケーションアカウントが利用する DB アカウントを管理する。

表9.3 アプリケーションアカウントと DB アカウント

No.	アプリケーション アカウント	属性	DB アカウント	備考 (利用者名)
1	Yamakawa	医師	MedDoctor	山川健一
2	Kimura	医師	MedDoctor	木村太一
3	Sakamoto	検査技師	MedTechnologist	坂本洋一
4	Ueda	放射線技師	RadTechnologist	上田耕一
5	Sugiyama	看護師	GenNurse	杉山彩子
6	Ootuka	看護師	GenNurse	大塚礼子
7	Mizuno	看護師	GenNurse	水野優子
8	Fujii	看護師	GenNurse	藤井明子
9	Nakata	看護師	GenNurse	中田悦子
10	Endou	看護師	GenNurse	遠藤京子
11	Nakamura	医事会計	Accountant	中村真一
12	Suzuki	医事会計	Accountant	鈴木純一

9.5.2 アクセス制御（ロール設定）

（1） テーブル一覧

以下に電子カルテアプリケーションのテーブル一覧を示す。

表9.4 電子カルテアプリケーションテーブル一覧

項目	テーブル名	テーブル名
1	患者基本テーブル	TBL_PATIENT
2	診察テーブル	TBL_EXAMINATION
3	カルテテーブル	TBL_KARTE
4	カルテ履歴テーブル	TBL_KARTE_REVISION
5	検体検査テーブル	TBL_TEST
6	検体検査履歴テーブル	TBL_TEST_REVISION
7	検体検査マスタテーブル	TBL_MST_TEST
8	処方テーブル	TBL_PRESCRIPTION
9	処方履歴テーブル	TBL_PRESCRIPTIN_REVISION
10	処方マスタテーブル	TBL_MST_PRES
11	画像検査テーブル	TBL_IMAGE
12	画像検査履歴テーブル	TBL_IMAGE_REVISION
13	画像検査マスタテーブル	TBL_MST_IMAGE
14	レセプトテーブル	TBL_RECEIPT
15	レセプト履歴テーブル	TBL_RECEIPT_REVISION
16	レセプトマスタテーブル	TBL_MST_RECIEPT
17	診察予約テーブル	TBL_RESERVATION
18	単位マスタテーブル	TBL_MST_UNIT

(2) テーブル構造

以下に、電子カルテのテーブル構造を示す。

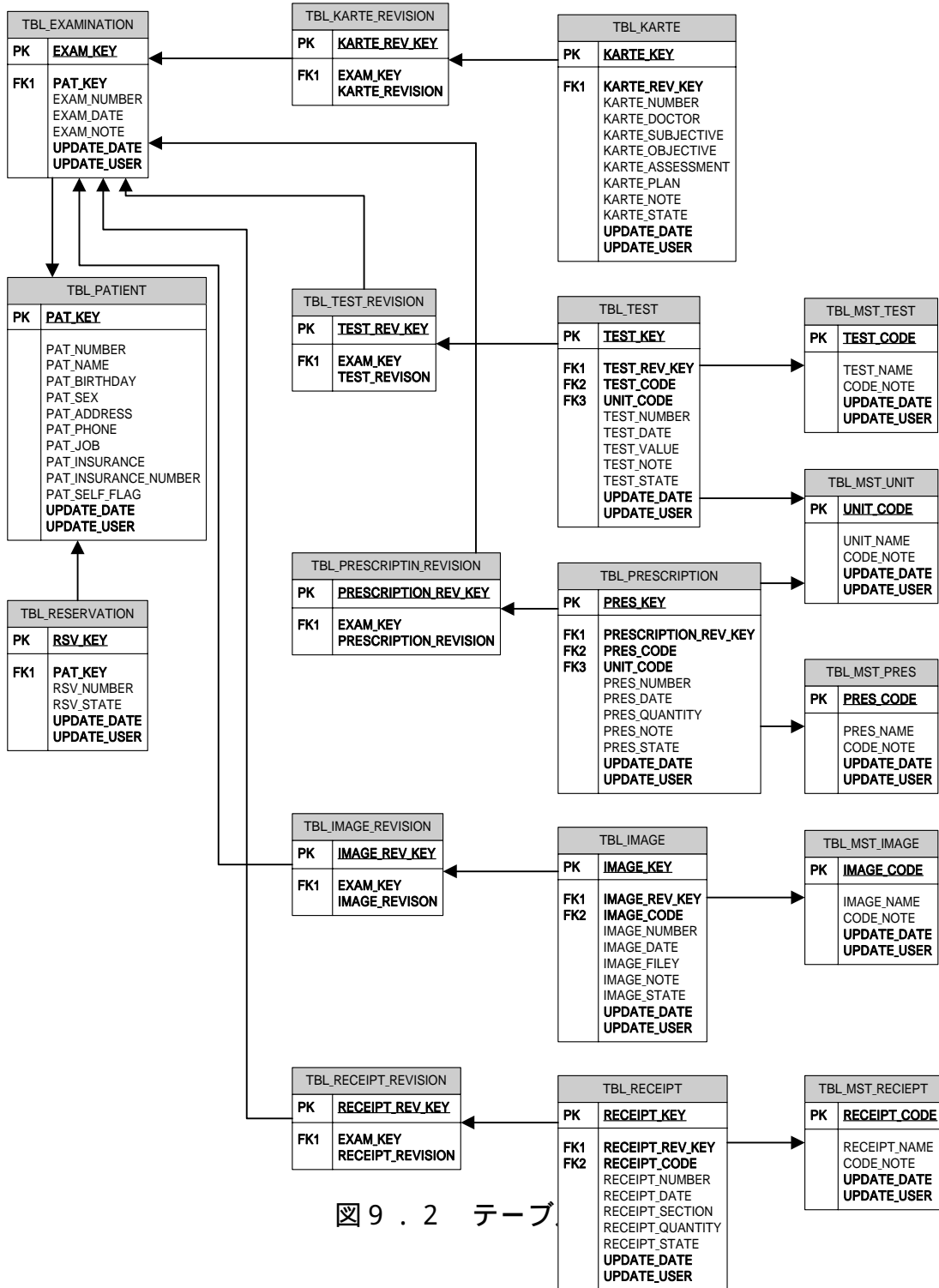


図 9.2 テーブ

(3) アクセス権

各テーブルオブジェクトの操作毎に、属性のアクセス権を決定する。
電子カルテアプリケーションは追記型のため Update、Delete は一切行えない。

表 9 . 5 オブジェクトに対するアクセス権 (その 1)

オブジェクト	操作	アプリケーション	医師	検査技師	放射線技師	看護師	医事会計
患者基本テーブル (TBL_PATIENT)	Select						
	Insert	×	×	×	×	×	
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
診察テーブル (TBL_EXAMINATION)	Select						
	Insert	×		×	×	×	×
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
カルテテーブル (TBL_KARTE)	Select						
	Insert	×		×	×	×	×
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
カルテ履歴テーブル (TBL_KARTE_REVISION)	Select						
	Insert		×	×	×	×	×
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
検体検査テーブル (TBL_TEST)	Select						
	Insert	×			×	×	×
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
検体検査履歴テーブル (TBL_TEST_REVISION)	Select						
	Insert		×	×	×	×	×
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×

表9.6 オブジェクトに対するアクセス権(その2)

オブジェクト	操作	アプリケーション	医師	検査技師	放射線技師	看護師	医事会計
検体検査マスタテーブル (TBL_MST_TEST)	Select						
	Insert		×	×	×	×	×
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
処方テーブル (TBL_PRESCRIPTION)	Select						
	Insert	×		×	×	×	×
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
処方履歴テーブル (TBL_PRESCRIPTIN_REVISION)	Select						
	Insert		×	×	×	×	×
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
処方マスタテーブル (TBL_MST_PRE)	Select						
	Insert		×	×	×	×	×
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
画像検査テーブル (TBL_IMAGE)	Select						

	Insert	x		x		x	x
	Update	x	x	x	x	x	x
	Delete	x	x	x	x	x	x
画像検査履歴テーブル (TBL_IMAGE_REVISION)	Select						
	Insert		x	x	x	x	x
	Update	x	x	x	x	x	x
	Delete	x	x	x	x	x	x
画像検査マスターテーブル (TBL_MST_IMAGE)	Select						
	Insert		x	x	x	x	x
	Update	x	x	x	x	x	x
	Delete	x	x	x	x	x	x

表9.7 オブジェクトに対するアクセス権(その3)

オブジェクト	操作	アプリケーション	医師	検査技師	放射線技師	看護師	医事会計
レセプトテーブル (TBL_RECEIPT)	Select						
	Insert	×	×	×	×	×	
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
レセプト履歴テーブル (TBL_RECEIPT_REVISION)	Select						
	Insert		×	×	×	×	×
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
レセプトマスタテーブル (TBL_MST_RECEIPT)	Select						
	Insert		×	×	×	×	×
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
診察予約テーブル (TBL_RESERVATION)	Select						
	Insert	×	×	×	×	×	
	Update	×	×	×	×	×	×
	Delete	×	×	×	×	×	×
単位マスタテーブル (TBL_MST_UNIT)	Select						

	Inser t		×	×	×	×	×
	Updat e	×	×	×	×	×	×
	Delet e	×	×	×	×	×	×

9.5.3 監査ログの実施

監査ログは更新トリガ機能を利用して別のテーブルに更新情報を格納する。
 記録する内容は、 実行日時、 アプリケーションアカウント、 使用した
 SQL 文、 実行結果（成功・失敗）を記録する。

9.6 OSおよびファイル保護ソフトでの対策

9.6.1 システム構成

OSおよびファイル保護ソフトでの対策事例のシステム構成図を図9.6.1に示す

本システム構成において、保護対象ファイルは

- (1) 医療情報用DBファイル
- (2) 監査ログファイル

とする。また、保護対象ファイルへのアクセスを許可するアクセス経路は図中の で示される経路に限定し、その他の のアクセス経路での保護対象ファイルへのアクセスは禁止される。

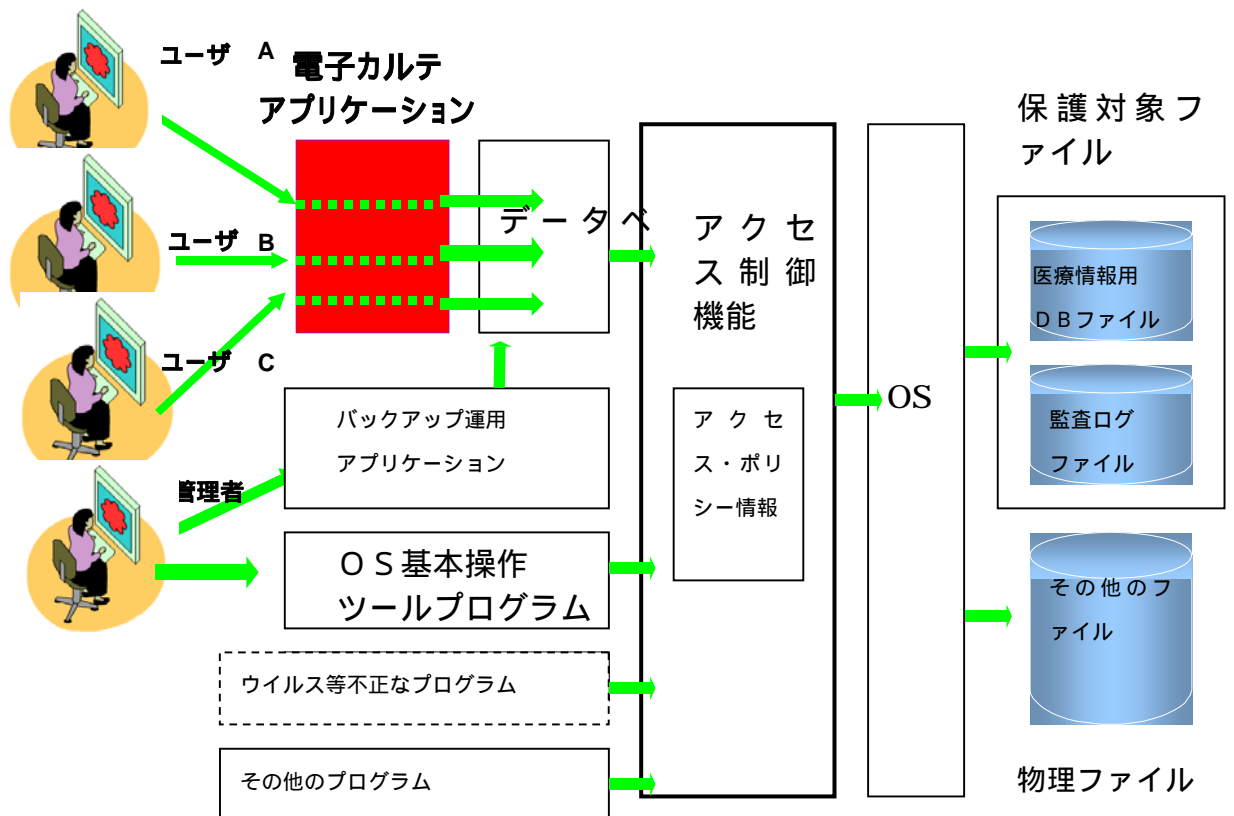


図9.6.1 システム構成図

9.6.2 アクセス・ポリシー情報の設定

図 9.6.1 のシステム構成におけるアクセス・ポリシー情報の設定例を表 9.6.1 に示す。

表 9.6.1 アクセス・ポリシー設定例

保護対象	プロセス	OS アカウ ント	アクセス種 別	備考
医療情報用 DB ファイル	DBMS	一般ユー ザ	R/W/D/X	DBMS 以外からのアク セスを禁止する
監査ログファ イル	DBMS	一般ユー ザ	R/W/D/X	同上

アクセス種別： R:読み込み D:削除 W:書き込み X:実行

付録1 関連文書一覧

- ・ 厚生省通知「診療録等の電子媒体による保存について」
http://www.medis.or.jp/2_kaihatu/denshi/file/99_517.pdf
- ・ 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」
http://www.medis.or.jp/2_kaihatu/denshi/file/99_11-24.pdf

付録2 データベースシステム参考例

データベースシステム参考例

名称	Oracle Database	DB2	SQL server	HiRDB
開発元	オラクル	IBM	マイクロソフト	日立
動作OS	Windows系 Linux系 Unix系	Windows系 Linux系 Unix系	Windows系	Windows系 Linux系 Unix系
種別	ソフト製品	ソフト製品	ソフト製品	ソフト製品

(注1) 参考例であり、これ以外にも存在する。

付録3 ファイル保護ソフトウェア参考例

ファイル保護ソフトウェア参考例

名称	Hacker Safe	Miracle Hazard	SELinux
開発元	日立	ミラクルリナックス	米国家安全保障局
対象OS	Windows系	Linux系, Unix系	Linux系
種別	ソフト製品	ソフト製品	フリー

(注1) 参考例であり、これ以外にも存在する。

(注2) データベースシステムの参考例との組み合わせについて保証しているものではない。個々の組み合わせおよび動作条件での確認が必要である。

付録4 カルテの修正とデータベース (1) カルテデータの表示イメージ

患者番号	0001
患者名	miura kenichi
生年月日	1965.03.05
性別	男
住所	東京都
電話番号	03-1234-5678
職業	会社員
保険区分	
保険証番号	001-123456

診察番号	1
診察日	2002.07.01
医師名	yamakawa kenichi
主訴	2～3日前から咳と痰がからみ、咽頭の不快感がある。以前より他院にて、高血圧と糖尿病の薬を処方されている。運動はキチンとしている。週末にイベントがあるので、おかしいと思ったときから手持ちの薬を飲み始めていたが直らない。
所見	咽頭軽度発赤あり。体調自体は良好。活気あり。やや乾いた感じの咳がみられる。
評価	本日より高血圧と糖尿病の管理を始める。今回、急性上気道炎の併発あり。
方針	採決に血糖の管理状態把握。併せて運動の継続と薬の服用について指導を行った。

白血球数	77.0	x 10 ⁴
赤血球数	540	x 10 ⁴
ヘモグロビン	16.4	g / dL
ヘマトクリット	47.5	%
血小板数	21.4	x 10 ⁴

患者番号	0001
患者名	miura kenichi
生年月日	1965.03.05
性別	男
住所	東京都
電話番号	03-1234-5678
職業	会社員
保険区分	
保険証番号	001-123456

診察番号	2
診察日	2003.07.07
医師名	yamakawa kenichi
主訴	昨日朝から鼻汁と頭痛。咳は少しでる程度。花粉症は毎年ある。いつも2月ころから。でも花粉症の症状とは違う。
所見	咽頭発赤あり。咳は乾性。
評価	急性上気道炎。
方針	鼻炎と咽頭炎用の内服薬処方。いままで薬剤アレルギーなし。

白血球数	71.0	x 10 ⁴
赤血球数	518	x 10 ⁴
ヘモグロビン	15.7	g / dL
ヘマトクリット	46.6	%
血小板数	23.4	x 10 ⁴

(2) カルテデータのDB格納イメージ

患者基本テーブル

患者キー	患者番号	患者名	生年月日	性別	住所	電話番号	職業	保険区分	保険証番号	本人フラグ	更新日
1	0001	miura kenichi	1965.03.05	男	東京都	03-1234-5678	会社員		001-123456	TRUE	2002.07.01
2	0002	shinoda momoko	1950.05.14	女	東京都	03-9876-5432	主婦		002-654321	FALSE	2003.07.07

リレーション

診察テーブル

患者キー	診察キー	診察番号	診察日	医師名	主訴	所見	評価	方針	備考	状態	更新日
1	1	1	2002.07.01	yamakawa kenichi	2～3日前から咳と痰が	咽頭軽度発赤あり。体	本日より高血圧と糖	採決に血糖の管理	併せて運動の		2002.07.01
1	2	2	2003.07.07	yamakawa kenichi	昨日朝から鼻汁と頭痛	咽頭発赤あり。咳は	急性上気道炎。	鼻炎と咽頭炎用	の内服薬処方。い		2003.07.07

リレーション

臨床検査マスタータブル

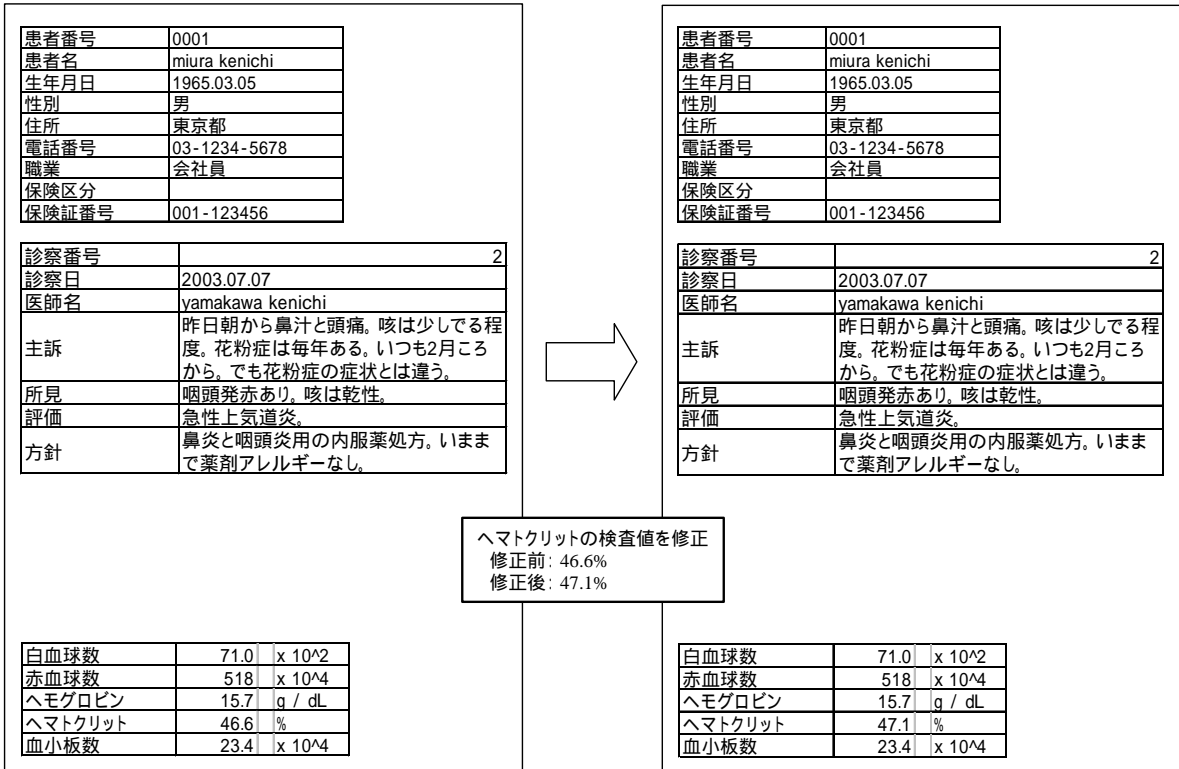
臨床検査コード	臨床検査名	備考	更新日	更新者	更新フラグ
1	白血球数		2002.04.01	sakamoto youichi	FALSE
2	赤血球数		2002.04.01	sakamoto youichi	FALSE
3	ヘモグロビン		2002.04.01	sakamoto youichi	FALSE
4	ヘマトクリット		2002.04.01	sakamoto youichi	FALSE
5	血小板数		2002.04.01	sakamoto youichi	FALSE

リレーション

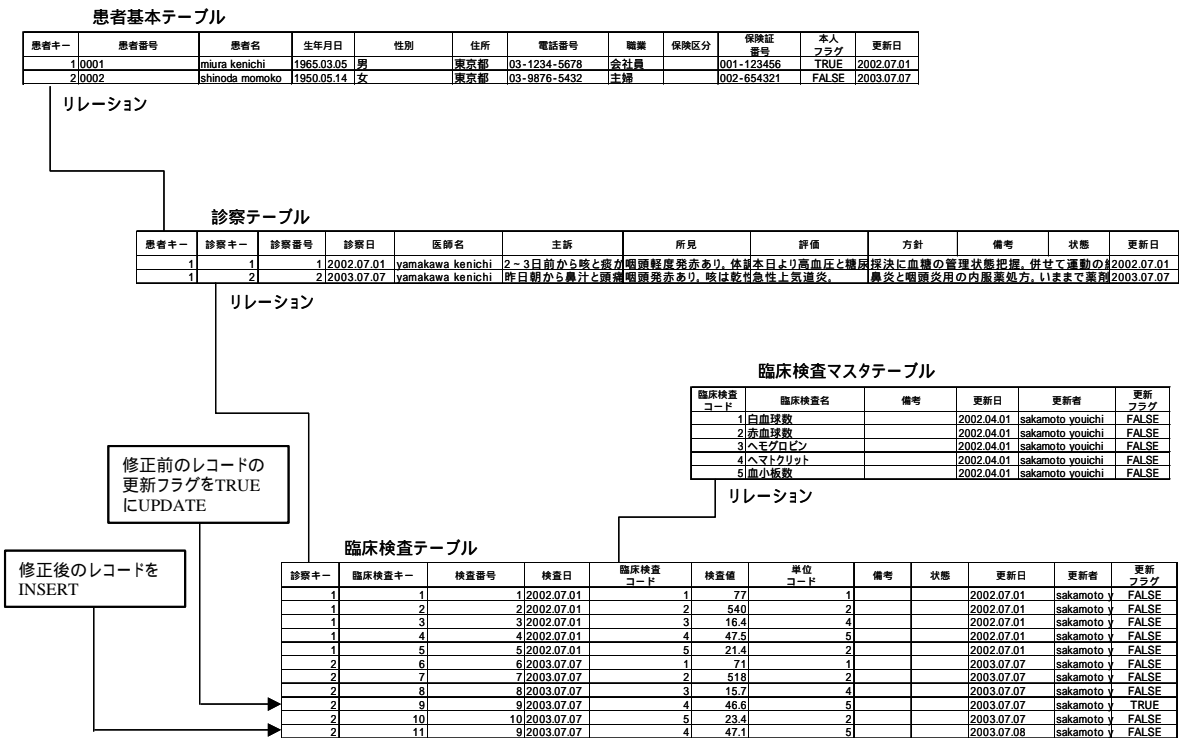
臨床検査テーブル

診察キー	臨床検査キー	検査番号	検査日	臨床検査コード	検査値	単位コード	備考	状態	更新日	更新者	更新フラグ
1	1	1	2002.07.01	1	77	1			2002.07.01	sakamoto	FALSE
1	2	2	2002.07.01	2	540	2			2002.07.01	sakamoto	FALSE
1	3	3	2002.07.01	3	16.4	4			2002.07.01	sakamoto	FALSE
1	4	4	2002.07.01	4	47.5	5			2002.07.01	sakamoto	FALSE
1	5	5	2002.07.01	5	21.4	2			2002.07.01	sakamoto	FALSE
2	6	6	2003.07.07	1	71	1			2003.07.07	sakamoto	FALSE
2	7	7	2003.07.07	2	518	2			2003.07.07	sakamoto	FALSE
2	8	8	2003.07.07	3	15.7	4			2003.07.07	sakamoto	FALSE
2	9	9	2003.07.07	4	46.6	5			2003.07.07	sakamoto	FALSE
2	10	10	2003.07.07	5	23.4	2			2003.07.07	sakamoto	FALSE

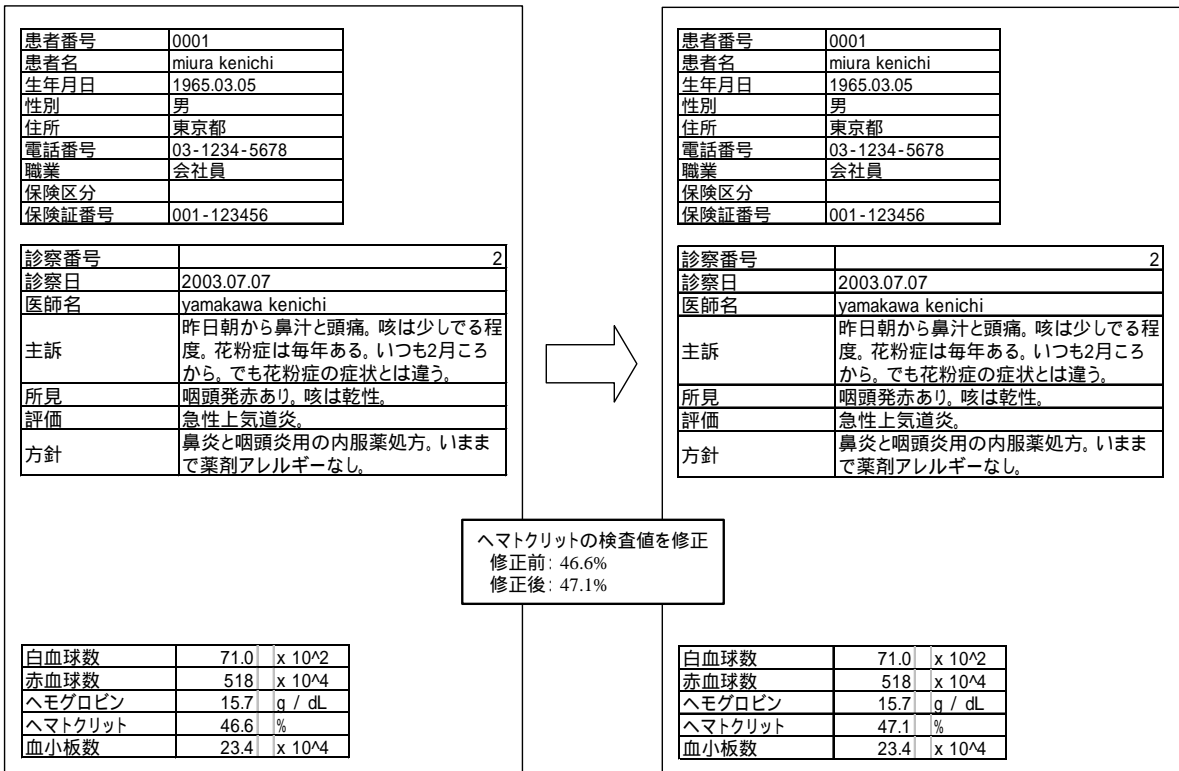
(3) カルテデータの表示イメージ：検査値の修正



(4) カルテデータの DB 格納イメージ：検査値の修正



(5) カルテデータの表示イメージ：診療情報の修正



(6) カルテデータの DB 格納イメージ：診療情報の修正

