個人情報保護に役立つ監査証跡ガイド

――あなたの病院の個人情報を守るために――

財団法人医療情報システム開発センター

■ はじめに

IT 技術の進展に伴い、個人情報保護の重要性が一層高まっています。これは IT 技術による情報管理が、従来の紙を主体とした情報管理とは比較にならないくらい大量で、かつ広範囲な情報漏えいを引き起こすリスクを秘めているからです。このような状況の下、平成 17 年 4 月に「個人情報の保護に関する法律」が完全施行され、一定数以上の個人情報を取り扱う事業者には個人情報の適切な取扱いが義務付けられることになりました。

医療機関で取り扱う患者さんの健康や診療行為に関する情報は、極めて機微度が高い個人情報に分類されます。このような情報がひとたび漏洩したり、その事故発生後の原因究明等の対応が遅れたりすると、損害賠償問題はおろか、社会からの信用失墜に繋がりかねません。このような事態を未然に防ぐためにも、情報セキュリティ管理の実施が望まれます。

本ガイドで紹介する「監査証跡」は、個人情報を取扱う事業者が、個人情報を適切に取扱っていることを説明するために、最も有効な方策と言えるものです。また、個人情報保護法の実施に先立って厚生労働省から発行された「医療情報システムの安全管理に関するガイドライン」においても、監査証跡の実施が義務付けられています。[1]

本ガイドは、この監査証跡の有用性とメカニズム、さらには実施にあたっての体制構築や費用等について、その考え方を医療機関の視点から平易かつ具体的に解説することを目的にしています。

1 「医療情報システムの安全管理に関するガイドライン」（平成 17 年 3 月）
http://www.mhlw.go.jp/shingi/2005/03/s0331-8.html

監査証跡の有用性とメカニズム

監査証跡とは何ですか？

●患者さんの個人情報へのアクセスを監視するための仕組み

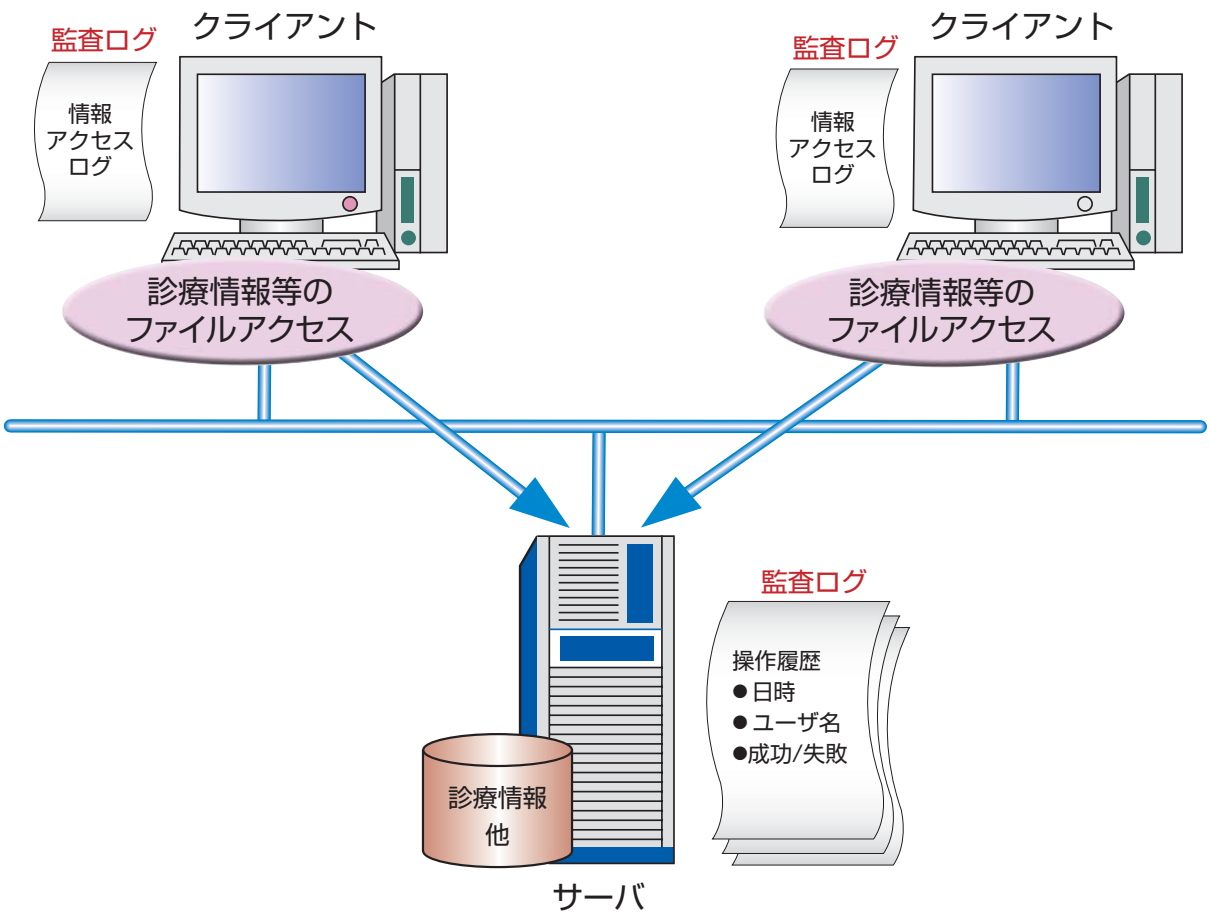
情報システムが適正に運用されているかどうかを確かめるための行為を「監査」と呼びます。情報システムに対する監査では、たとえば、権限を持つ利用者が正しく情報を取り扱っていることや権限を持たない人がアクセスしていないこと等、情報システムを利用して行われる業務に対して、予め設定されたポリシー（ルール）に準じた行動が取られているかが、証拠に基づいて確認されます。

監査証跡は、この監査のための証拠を収集するための一連の仕組みであり、監査対象である情報システムに関する様々な事象の発生から最終結果に至るまでの過程を追跡するための情報収集を行います。この証拠となる情報には、いわゆる「アクセスログ」と呼ばれる情報システムへのアクセス記録から、利用者の作業記録、入退室記録のようなものまで含まれます。（詳細については、「付録 1」をご参照ください）

●監査ログを収集する仕組み

厳密な監査を行うためには、「付録 1」にあげたような情報の多くが必要です。しかし、これらの情報をすべて対象として監査証跡を定義すると、情報システムや組織の運用体制に依存する部分がでてくるため、説明が複雑になります。そこで本ガイドでは少し対象を狭めて、監査証跡は以下のように定義される「監査ログ」を収集する仕組みと考えることにします。

「監査ログ」とは、対象となるその情報システムが保有する個人情報について、「いつ」「誰が」「誰の」情報にアクセスしたかがを第三者が検証可能な形態で残した記録のことをいう。監査ログには当該の情報システムが扱う個人情報に対して、アクセスを行った人のユーザ名（もしくは ID）、アクセスの方法（読み取り／検索等）、アクセスした日時、アクセスの結果（成功／失敗）、及びアクセスされた患者の個人情報等の情報が含まれる。


監査ログ
クライアント
情報
アクセス
ログ
診療情報等の
ファイルアクセス
監査ログ
クライアント
情報
アクセス
ログ
診療情報等の
ファイルアクセス
監査ログ
操作履歴
●日時
●ユーザ名
●成功/失敗
診療情報
他
サーバ

それを導入することで、どのようなメリットが得られるのでしょうか？

●不正アクセスの形跡を捉えることができる

情報へのアクセスの権限を持たない人が、情報を不正に入手しようとする場合があります。このような行為を「不正アクセス」と呼びます。監査証跡を用いることで、このような不正アクセスが未遂に終わったこと、または実際に行われたこと、その両方の事実を監査ログとして記録することができます。

情報が正しく保護されていれば、その情報にアクセスする権限を持たない人がアクセスを試みた場合、アクセスに失敗した記録が監査ログに残ります。この監査ログを調べることによって、不正アクセスが試みられた形跡を検知することができます。

ID やパスワードが不正に利用され、情報へのアクセスが成功してしまった場合には、監査ログには失敗の記録ではなく、成功の記録として残ります。この場合には、他の証拠、たとえば同時に記録している作業履歴や入退出などの記録、もしくは誰かからの指摘などと照合して解析、判断することで、本来の利用者以外による不正なアクセスをつきとめることが可能になります。

●業務上不必要な情報アクセスを識別することができる

情報への正当なアクセスの権限を持つ利用者であっても、本来の業務目的以外で情報を利用しようとする場合があります。このような行為を「目的外アクセス」と呼び、不正アクセスと同様に個人情報への侵害行為に位置づけられます。監査証跡を用いることで、このような目的外アクセスを識別することができるようになります。

目的外アクセスはすべて成功の記録として監査ログに残ります。しかし、監査ログを他の情報、すなわち操作者の属性や患者との関係、業務履歴等と照合することによって、当該のアクセスが業務上必要なものであったかどうかを判断できます。たとえば、業務上必要のない情報の全件検索、他のシステムなどからの要求のないケースでの情報へのアクセス、情報の外部記録媒体（USB メモリなど）への業務上必要のない出力などの記録が残される場合が挙げられます。

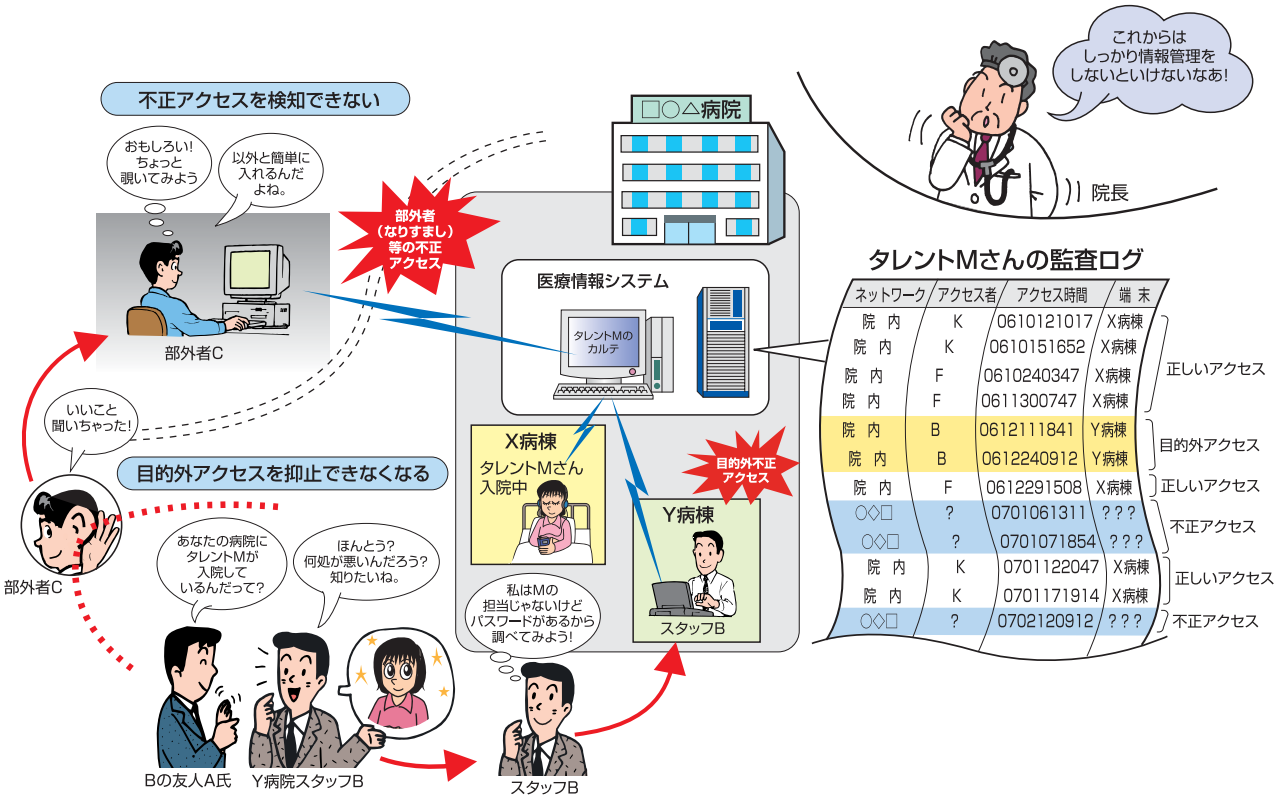
●説明責任を果たす際の証拠となる

ひとたび、個人情報の漏洩事故が発生したり、その事故発生後の原因究明等の対応が遅れたりすると、情報漏えいに対する損害賠償問題はおろか、患者さんや社会からの信用失墜に繋がりかねません。このような事態を未然に防ぐために、医療機関は個人情報を取り扱う医療情報システムの管理を適切に行うとともに、それをきちんと説明できることが必要です。これを「説明責任」と呼びます。この説明責任を全うする際の直接的な証拠となり得る情報が監査ログであり、それを確実に残すための仕組みが監査証跡です。

情報システムに監査証跡の機能が実装されていなければ、いくら利用者の権限管理や情報へのアクセス管理などの強力な機能を持っているとしても、不正アクセスなどの有無を直接的な証拠を元に説明することは、極めて困難な作業です。逆に監査証跡が導入され、有効に機能していれば、直接的な証拠である監査ログを監査することで、問題の有無を比較的容易かつ客観的に証明でき、説明責任を果たすことができます。

●不正な行為の抑止効果がある

また、監査証跡を実施していることを組織内に周知することにより、情報システム利用者の個人情報の取扱いに対する意識を変えることができます。その結果として、個人情報に対する不正アクセス行為の抑止効果が期待できます。

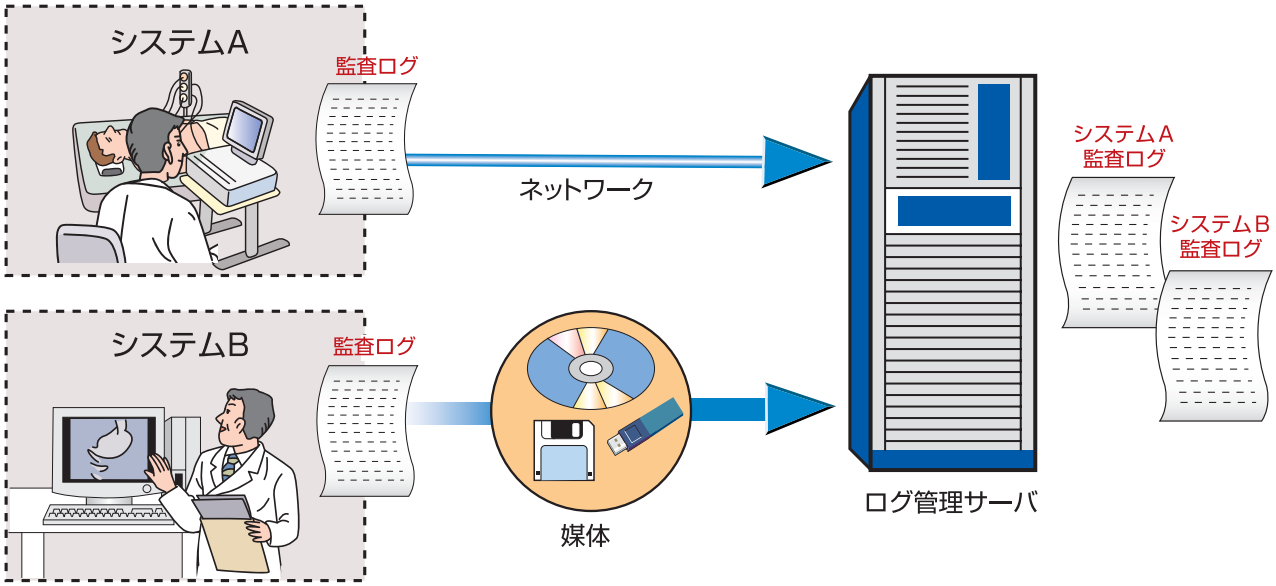


そのような情報をどうやって収集し、調べるのですか？

●監査ログを出力させる仕組み

監査ログの出力は、ある出来事、たとえば新規に個人情報が作成された、個人情報の読み出しが行われたなどが起こったタイミングで行われます。この監査ログを出力させるきっかけとなる出来事のことを「トリガイベント」と呼びます。トリガイベントには特定の情報へのアクセスのタイミングだけでなく、データベースへの検索、ログイン／ログアウトなどの出来事なども含まれます。また、異なるシステム間での個人情報のやりとりが行われる場合は、それぞれのシステムでのこれら個人情報の送信と受信元および送信先の両方で監査ログが出力されます。

トリガイベントによって出力された監査ログの保存方法には、ファイルに記録する、データベースに記録する、ネットワーク経由で外部に出力して外部サーバで保存する、等があります。情報システムが持っている機能だけで監査ログの保存管理を行うことも可能ですし、外部出力機能がある場合は、下図にあるような監査ログ保存用の専用サーバ（以下、「ログ管理サーバ」と呼びます）で集中的に保存管理を行う方法もあります。一般に監査ログの情報量は大きく、特に複数のサブシステムから構成されるような大きなシステムの場合は膨大な量になりますから、効率的な管理と解析のためには「ログ管理サーバ」を設けることが推奨されます。



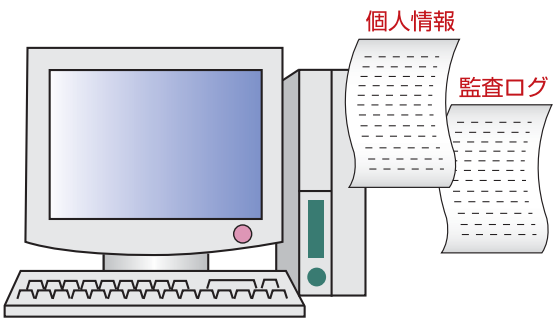
●システムの構成による相違

監査ログはトリガイベントが発生した時点で、その個人情報のあった場所で作成されるのが一般的です。個人情報の所在は医療情報システムの構成によって異なりますので、監査証跡機能の実装形態も、それに依存して異なったものになります。

代表的な医療情報システムのシステム構成には次のようなものがあり、個人情報の所在と監査ログの発生場所を合わせて示します。また、実際には、これらが複合した構成のシステムも存在します。

A) スタンドアロン構成

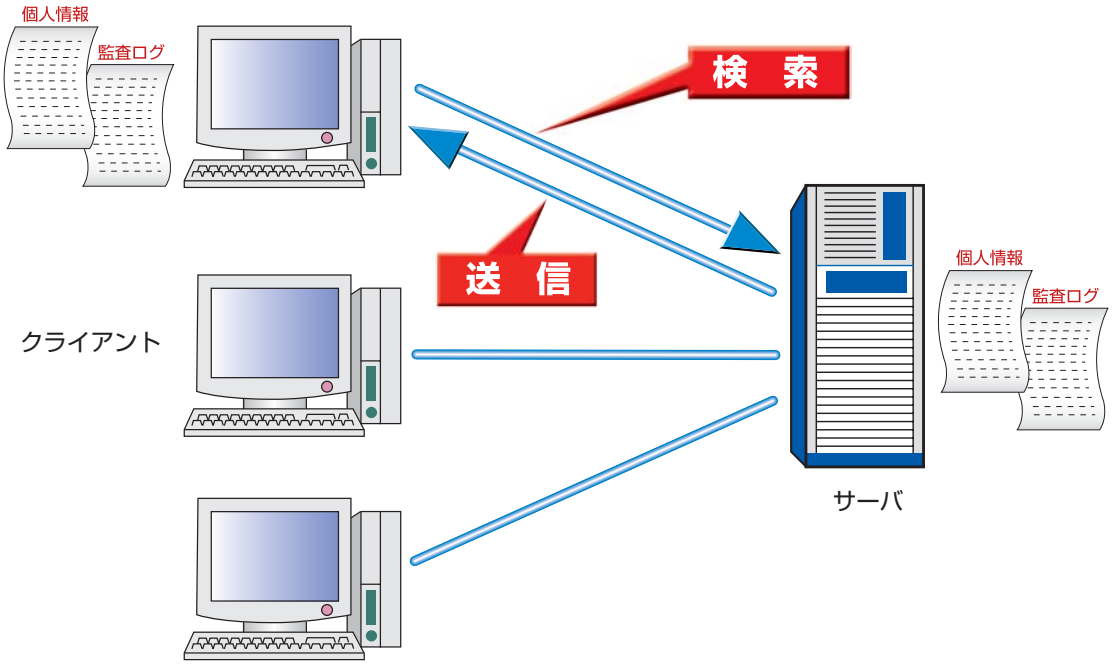
・パソコン一台だけのものです。　例えば、診療所の電子レセプト端末などです。
・個人情報は装置内だけにあり、監査ログも内部で発生、保存されます。



B) サーバ・クライアント構成

・データベースを持つサーバ機と、そこへアクセスするアプリケーションを持つ複数台のクライアント機から構成されるものです。　例えば中大規模病院の電子カルテシステムや放射線科情報システム、PACS などです。

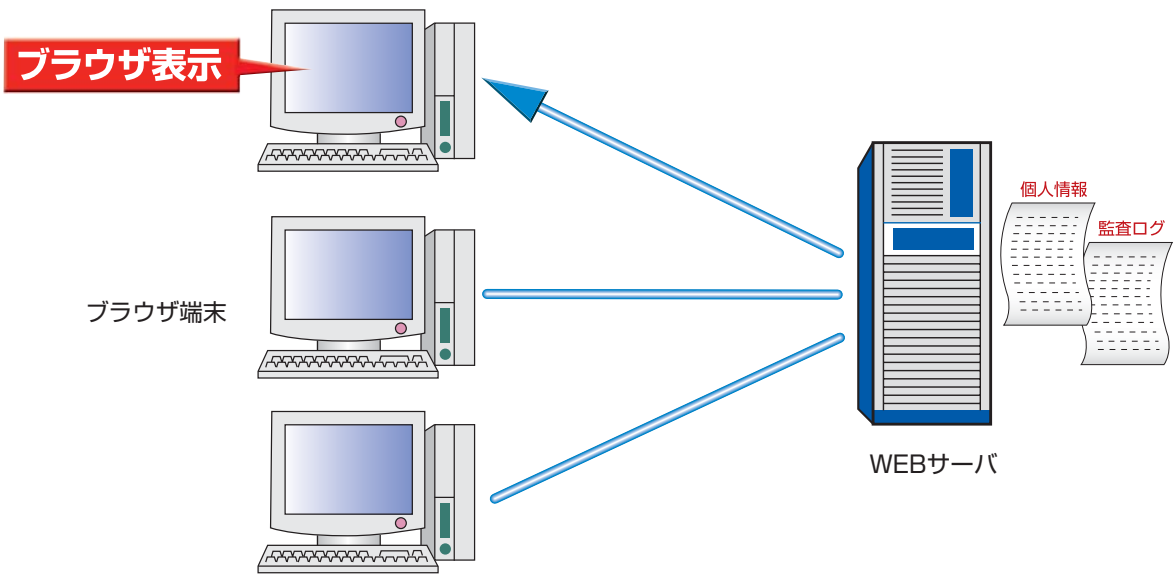
・サーバ機に保存されている個人情報が、クライアントからの検索、要求によりクライアント側へ送られます。監査ログはサーバ側、クライアント側両方で発生します。



C) WEB サーバ構成

・サーバ・クライアント構成と同じような構成ですが、サーバ側に WEB サーバ機能を持ち、クライアント機から WEB ブラウザでアクセスするものです。WEB 型電子カルテシステム、院内画像配信システムなどです。

・WEB サーバ機に保存されている個人情報が、クライアントの WEB ブラウザで表示されます。通常クライアント側には個人情報は残りません。監査ログもサーバ側だけで発生します。

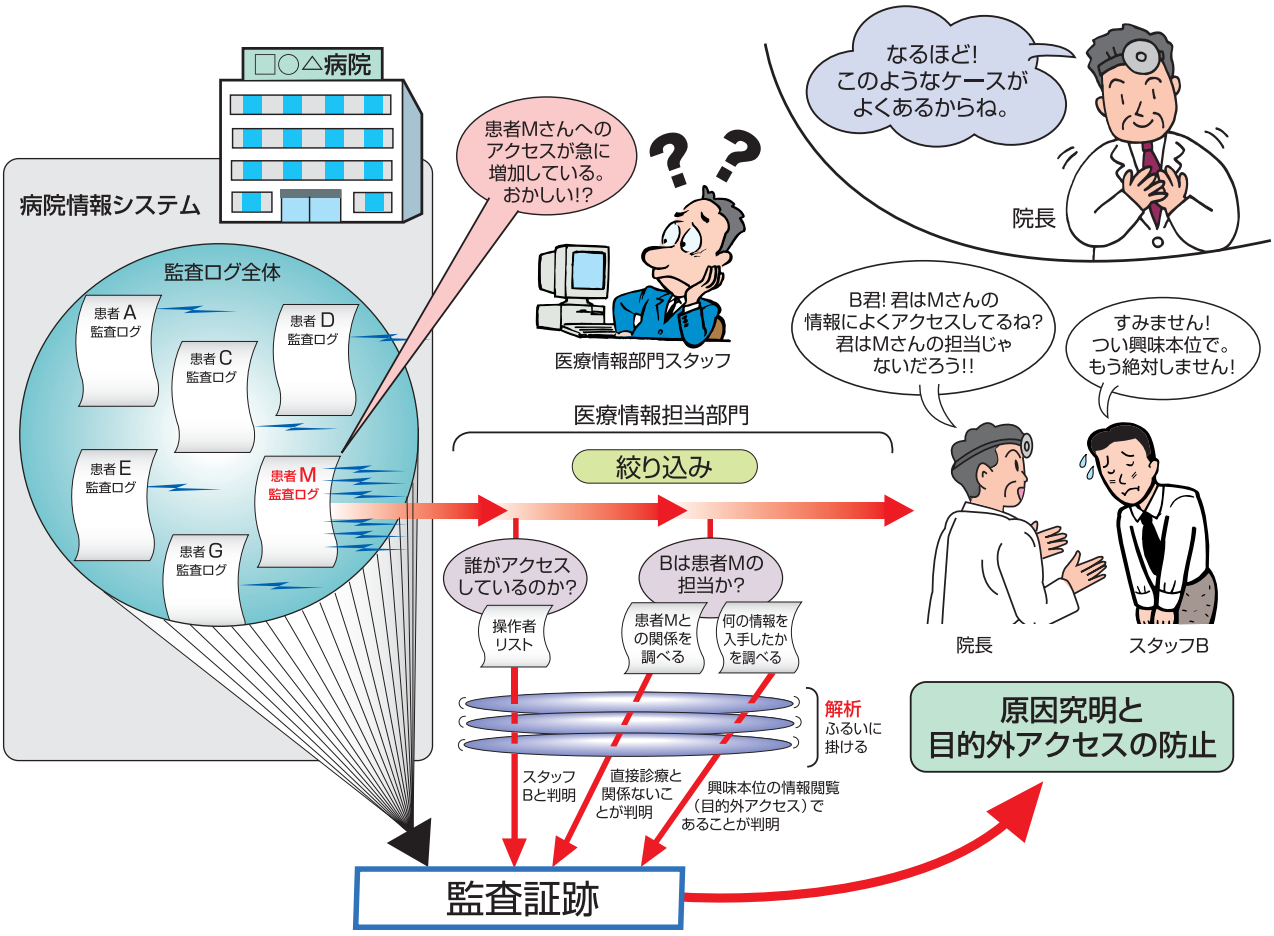


●収集された監査ログの解析

収集された監査ログの解析は、まず収集された監査ログの整理することから始めます。収集したログから特定の条件に該当する監査ログのメッセージ内容だけの抽出、あるいは件数の算出、監査ログの並び替え等を行います。

監査ログの整理ができたら、次にこれらの前後関係や、他の方法で記録されている操作者の作業履歴、権限ポリシー規約ポリシー等を合わせて検討し、不適切なアクセスや異常なアクセスがないかを調べます。この作業は人の手で行うことも可能ですが、監査ログの解析用のソフトウェアも製品化されています。このようなソフトウェア製品（以下、「ログ管理ソフトウェア」と呼びます）を利用すると、人手で行うよりも迅速かつ詳細な解析ができる場合があります。詳しくは本ガイドの「既存システムの変更箇所は？　また、いくらくらい費用がかかりますか？」における「ログ管理ソフトウェア」の項をご参照ください。

一般的には監査ログの件数は膨大であり、全部の監査ログを調べることは非常な困難を伴うことがあります。そのような場合には適宜サンプリングするか、特定の時間帯や患者の情報に絞って行うことも考慮する必要があります。



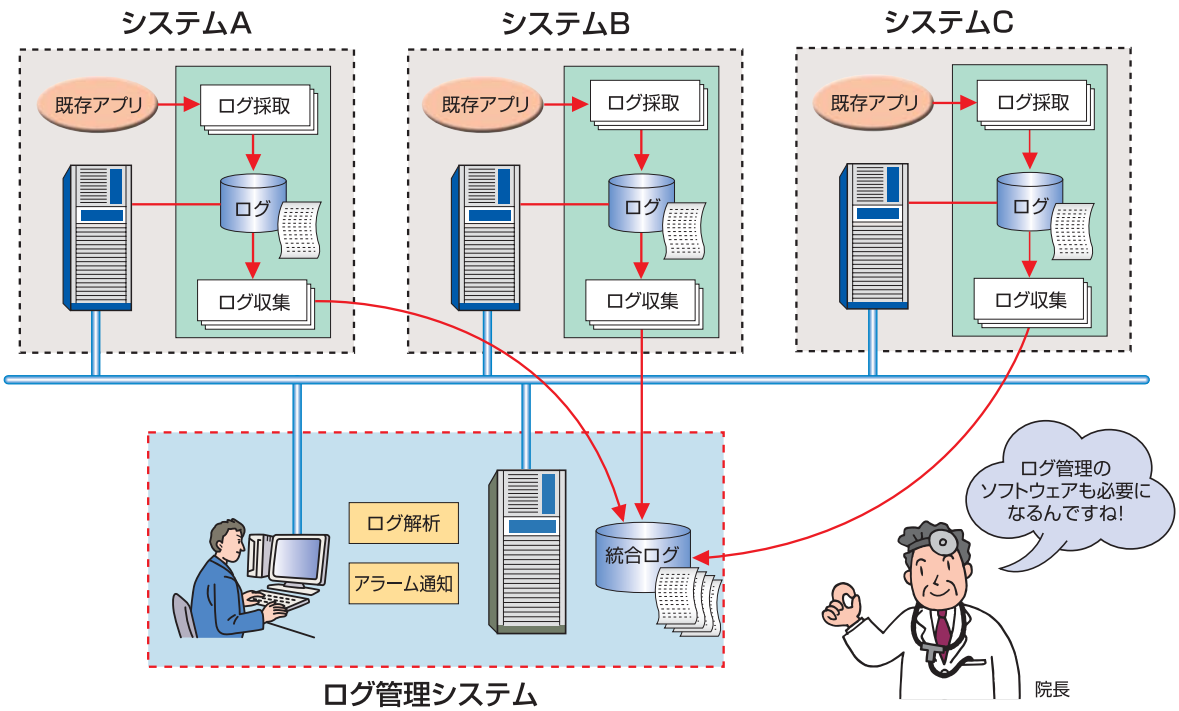
監査証跡を導入する

既存システムの変更箇所は？　また、いくらくらい費用がかかりますか？

●既存システムの改修と追加設備

監査証跡は監査ログを収集し解析するための一連の仕組みです。したがって、既存システムには解析の用途に利用できる監査ログを出力させる機能が必要です。既存システムがこの機能を持たない場合には、追加実装が必要になります。

次に、各システムで発生した監査ログを収集して整理（時系列での並べ替え等）する機能と、その整理されたデータを解析して不正なアクセス等を識別する機能が必要です。これらの機能は別々に用意しても構いませんが、２つの機能を統合した「ログ管理システム」として実装することもできます。「ログ管理システム」は、複数のベンダーからソフトウェアが製品化されていますので、それらを活用することで導入を比較的容易にすることが期待できます。



●監査ログを発生、蓄積する機能の追加

A) 既存システムのソフトウェア改修

既存の業務ソフトウェアが既に監査ログを発生、蓄積する機能を有している場合には、この改修は必須ではありません。ただし、複数のシステムで構成される情報システムの場合、可能であれば後に述べるログの標準化のための改修を行うことが推奨されます。

既存のシステムがこの機能を持たない場合には、定められたトリガイベントが発生した際に、定められた標準形式の監査ログを発生、蓄積する機能の実装が必要です。これらの改修（試験も含む）

に掛かる費用は、システムの規模にもよりますが、50 万円から 500 万円程度と想定されます。既存システムの仕様に大きく依存するところですので、貴院の情報システムの導入ベンダーとよくご相談ください。

B) ハードウェアの増強

上記のソフトウェアの改修に伴って、一時的にログを保管しておく記憶領域ためのハードウェア（メモリ、補助記憶装置など）の追加が必要になる場合があります。このような設備の増強にかかる費用は、既存のシステムのハードウェア構成（PC サーバ、UNIX サーバなど）により価格の開きがあり、一概には言えませんが、1 システムあたり 10 万円、全体でも 100 万円も見込んでおけば十分と思われます。これも詳細については、貴院の情報システムの導入ベンダーとよくご相談ください。

●ログ管理システムの追加

A) ログ管理サーバ（ハードウェア）

監査ログを一元的に集約、蓄積し、解析を行うためのサーバ（ハードウェア）です。　ログ管理サーバは、既存システムのどれかのサーバと相乗りさせることも考えられますが、性能確保や管理上の観点から独立したものにすることが推奨されます。ハードウェアスペック（CPU 性能、メモリ容量、補助記憶装置容量、バックアップ装置など）は、ログを収集する対象となるシステム数、発生するログの量などに依存します。また、収集したログの改ざん防止対策として、タイムスタンプ機能もしくはライトワンス型の媒体へのバックアップ装置があることが望ましいといえます。これらを含めて、50 万円～ 100 万円程度で用意できるでしょう。

B) ログ管理ソフトウェア

ログ管理ソフトウェアは、医療機関が独自にソフトウェアを開発することも可能ですし、ベンダーのログ管理ソフトウェア製品を採用することも可能です。もし貴院がソフトウェアの開発力をお持ちの場合は、貴院の運用にあったログ解析機能の開発に挑戦するのもよい試みだと思われます。ベンダーのログ管理ソフトウェア製品を採用する場合は、その製品の解析機能とカスタマイズ能力を十分検討した上で採用することを推奨します。独自開発、既存製品の採用にかかわらず、次の 2 つの機能は必須です。

●ログ収集の機能

各業務システムで出力された監査ログを収集し、蓄積する機能です。収集する方式には、各業務サーバにエージェントソフトウェアをインストールして、エージェントソフトウェアが定期的にログ管理サーバに送信する方式や、一般的な FTP などのファイル転送機能などを使って送信する方式などがあります。

●ログ解析機能

不正なアクセスの可能性があるアクセスパターンの判別などを自動的に行う機能です。不正を検知してから対処までの時間を短縮できるために有効な機能です。ソフトウェアの規模（すなわち、開発に要する費用、もしくはソフトウェア製品の価格）は、解析の仕様に大きく依存しますので、監査に関する基本方針（ポリシー）に合った仕様とする必要があります。

また、ログの管理機能の一つとして不正アクセスと思われる事象が発生したときに管理者にメールで通知する機能なども考えられます。

これらの機能を持つ一般的なログ管理ソフトウェアの価格は、300 万円～ 500 万円程度です。これに加えて、通常は導入価格の 10 ～ 20%が年間の保守費用として必要となります。

●構築人件費

ログ管理機能構築に必要な項目は以下のとおりです。

●ログ管理サーバ構築（OS 及びミドルウェア、ログ管理ソフトウェアのインストール）

●システム試験（各業務システムから適切にログが収集され、解析が正常に機能することを確認）

●運用試験（医療施設に監査運用方針にあった運用ができることを確認）

ログ管理システムの構築にかかる工数は構成されるシステムの数に依存しますが、0.5 人月～ 2 人月程度と考えられますので、50 万～ 250 万円程度となります。

●運用人件費

監査証跡に関する運用時の作業としては、ログの監査作業と異常なログを発見したときもしくは不正と思われる事象が発覚した際の詳細の解析作業です。

ログの監査の運用については、監査方針（ポリシー）や毎日発生するログの量により異なってきます。定期的にログを検査する場合でも、毎日行う場合、週次など一定期間毎に行うなども考えられます。また、何か事象（VIP が入院した、不正と思われる事象など）が発生したときにのみ行う運用も監査方針（ポリシー）によって選択肢の 1 つとなります。

監査の体制ですが、日常の監査は複数の担当者が交代で監査を行うのが、相互の点検内容の検証もできるため（相互牽制）、望ましいと言えます。また、異常なログを発見したときの詳細の解析をするためには、運用体制などの業務知識が必要となるため、必要に応じてシステム管理部門の担当者に他部門の要員を加えて行うことになります。現実的には数名が兼務でログ監査を担当し、平常時は 0.2 ～ 0.3 人月程度の工数の確保が必要だと思われます。

●費用トータル試算　　300 床程度の地域中核病院を想定

300 床程度の地域中核病院を想定した場合の費用試算をまとめると概ね以下のとおりになります。

No.	項　目（下線は必須）	初期導入費用（円）	ランニング費用（年額）[注1]	
1	既存ハードウェアの増強	0 万円～　100 万円	0 万円～　20 万円	
2	既存業務ソフトウェアの改修	50 万円～　500 万円	―	
3	ログ管理サーバ（ハードウェア）	50 万円～　100 万円	60 万円～ 100 万円	必須項目
4	ログ管理ソフトウェア	300 万円～　500 万円	60 万円～ 100 万円	必須項目
5	構築人件費	50 万円～　250 万円	―	必須項目
6	運用人件費（0.2 人月と想定）	―	100 万円～ 300 万円	必須項目
	合計 [注2]	400 万円～1,350 万円	160 万円～ 420 万円	

注 1 ：ハードウェア、ソフトウェアの保守費用を導入費用の 20%と想定しています。

注 2 ：最小値は必須でない項目を除外した値で計算しています。

当院には情報システムがいくつもあるのですが、全部に入れるのですか？

●個人情報にアクセスするところは全部入れる

複数のシステムで構成され、また、例えばそれぞれの異なるシステム間で個人情報のやりとりを行っている場合、個人情報を渡した先のシステムが監査対象でないと一貫性が保てなくなります。したがって個人情報を扱うすべてのシステムに監査証跡の導入が望まれます。

●システム全体として機能する監査証跡

さらにシステム全体として機能する監査証跡であれば、より正確な監査が行えます。例えば同一の利用者 ID で異なるシステムに同時にログインがされており、かつその端末が離れた場所にある場合、どちらかのログインがなりすましによって行われている可能性が高いことが分かります。これ以外にもシステム全体として監査を行うことのメリットは大きく、個々のシステム単位での監査だけでなく、システム全体の監査を行うことは非常に有用です。

●標準化が導入を容易に

上記のように監査証跡はシステム全体に適用することが望まれますが、現状では監査ログ出力のタイミング、内容、保存方式仕様等については、システム開発ベンダーの独自仕様になっています。そのため医療機関がシステム全体での監査証跡を実施するためには、監査ログの標準化が緊急の課題となっています。

標準化の動向としては、国内では JAHIS（保健医療福祉情報システム工業会）が「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」を制定しホームページ（http://www.jahis.jp/）で公開しています。この規約は個人情報保護のための最低限のトリガイベントと監査ログ内容を規定したもので、世界的な監査ログの標準化の流れに沿ったものになっています。

監査ログが標準化され、対応した医療情報システムを導入することで、監査ログの収集、保管、分析の標準化が可能になります。さらに対応したログ管理サーバで一元的に管理することでログ分析をまとめて行うことができ、監査上のチェック漏れの防止とともにより詳細な監査が可能になります。

では私たち病院スタッフは、実際に何をすればよいのでしょうか？

●組織としてのポリシーの策定

監査ログを収集して検査することは、患者さんの個人情報を大切に扱うためですが、結果的に事故がなかったらよいというだけなら、そこまでしなくても大丈夫かも知れません。でも重要なことは患者さんの個人情報を大切に扱っていることを説明できることです。患者さんに病状や、治療方法を説明するときには、検査結果を示し、医学的に適切であることを示して説明すると思います。情報の安全管理も同じで、結果的に安全だった、というだけでは納得は得られません。安全に十分注意していることを説明し、納得してもらうことが重要です。そのためには何をすればよいでしょうか。

まず、もっとも基本的なことを文書で宣言します。これを基本方針（ポリシー）といいます。個人情報保護法の全面施行でほとんどの医療機関には個人情報保護に関する基本方針を作成されたと思い

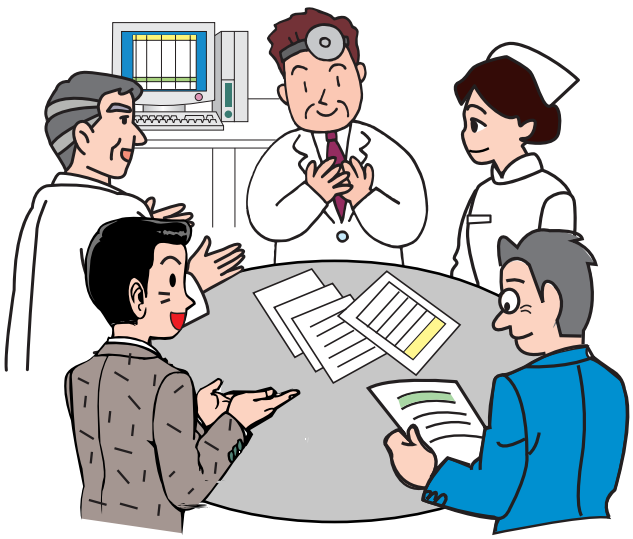
ます。その中に個人情報の安全管理に関する決意表明があると思いますが、なければ加えたほうが良いでしょう。

●具体的なルール策定と院内体制の構築

さてポリシーで決意表明をしたら、それを実現する方法を具体的に決めます。実際にはルールを作りそのルールを実施する体制を構築します。電子化された情報はモラルや安全意識が高いといわれている医療従事者であってもばらばらに対応していたのでは安全に管理することはできません。紙のカルテは風に飛ばされても追いかけることはできますが、電子化情報は大変な高速で移動しますので、追いかけることは不可能です。ルールを決めて組織的に対応しなければなりません。ルールに含めるべき内容は「付録 1」を参照してください。ただしルールは努力すれば実行できるものでなくてはなりません。不可能なことや、実行することが大変でとても業務をしながらでは実行できないことがルールに書かれていると、最初から無視されてしまいます。

医療現場は臨機応変が重要です。しかしある人がルールに書かれていないことを臨機応変に行って、そのこと自体はやむをえないこと、正しいことであっても、それをそのまま胸にしまっておくと、困ったことになります。ほかの人はルール通りに行われていると思い込んでいますし、同じようなことが再び起こった場合、別の人が別の対応してしまい、結局安全に管理していることが説明できなくなります。最悪の場合はそれぞれの思い込みの違いから安全性に破綻を来たしてしまうかもしれません。

医療行為の安全性を確保するためにヒヤリハットの収集や、スタッフ同士の報告・連絡・相談が重要であることはよくご存知でしょう。情報の安全管理もまったく同様です。その医療機関の中で順調に管理されているか、予想外のことがどのくらい起こっているのか、ルールは無理なく守られているのか、そのようなことが組織的に集められ、また必要なことは速やかに院内に伝達されなければなりません。このような体制がしっかり作られていることが説明できるためには必要です。



●ベンダーとの協調による機能実装、導入

さて医療情報システムはレセコンのような単純なものから電子カルテのような複雑なものまでありますが、それぞれシステムが持っている機能が異なります。このガイドの対象である監査ログの収集や検査に関する機能も様々です。一般にシステムの機能は価格に強く関係します。高度な機能を備えたシステムを導入すれば価格は高くなります。そのかわりシステムを使う医療従事者の作業は楽になるかも知れません。つまりシステムの機能と利用者の運用方法は密接に関係しています。そして、その二つを総合して情報の安全が守られます。ルールを作って守ると書きましたが、ルールはシステムの機能によって変わってきます。どの医療機関でもルールは簡単で実行することが楽なものが良いに決まっていますが、そのためには高度な機能を持つシステムを導入しなければならなくなり、導入経費や維持経費が高くなってしまいます。経費には限りがありますので、妥協点をうまく見つける必要があります。そのためにはシステムを提供するベンダーとよく相談し、導入を進める必要があります。しかし、予算に限りがあるからといって監査ログを記録する機能がないシステムを導入することはあまりに危険です。

●日々のログ収集とログ解析、ログ情報の保護

監査ログを記録するシステムを導入すれば監査ログは自動的に収集されます。まず、ログ自体を安全に管理することが重要です。この節の最初に述べた、安全であることを説明するための基礎証拠ですので、少なくとも一定期間は不正に書き換えられない状態で保存しなければなりません。定期的にCD-R などの媒体にコピーし、施錠されて、鍵がしっかり管理されているロッカーなどに、定められた期間保存しておけばよいでしょう。期間は自主的に定めて問題ありませんが、一般に 2 年以上は必要です。また監査ログはこのガイドで目指している患者さんの個人情報保護の説明責任を果たすこと以外の目的にも利用できます。しかし、乱用すれば仲間内の監視や中傷の道具にもなりかねません。監査ログの利用目的、利用権限はしっかり決めておきましょう。

また保存とは別に定期的に検査を行う必要があります。いくら監査ログを採取しても誰も見ないのであれば意味がありません。とは言っても少し規模の大きな医療機関では監査ログは膨大な量になり、すべて目を通すことは難しいものです。このガイドに紹介されているようなツールを使えば楽にはなりますが、それでもすべて検査することは大きな負担になります。やむを得ず抜き取り検査をすることになります。無作為に日や患者を選び、対象となるログを詳細に検査し、問題が少しでもあればさらに対象を広げて検査をするという方法が一般的です。また特別に興味を引く状況（有名人、職員やその家族が受診・入院した場合など）を重点的にチェックすることも有効です。そして検査したことを院内に周知することが重要です。

費用対効果をどのように考えればよいでしょうか？

●定量的な費用対効果を考えられる性質のものではない

監査証跡を費用をかけずに実現はできませんが、定量的な「費用効果」を云々することには意味が乏しいと考えて下さい。不正アクセスによる被害発生に対して、その金銭的損害の算定は条件設定によって大きく変わり意味の乏しいものとなります。むしろ、定性的な効果を考えて実施すべき性質のものです。患者個人情報の保護を図ることは医療機関としての責務であり、その手段として、「医療情報システムの安全管理に関するガイドライン」（2005.3 厚生労働省発行）では「C．最低限のガイ

ドライン」に記載されています。費用対効果が見込めないからと言って、やらなくても良いという性質のものではありません。

●セキュリティ事故の損害見積もりには費用効果が予測困難

個人情報の価値は情報主体本人の主観に依存し、金銭的価値に客観性がありません。人によっては「社会的立場が損なわれ金銭での補償が.できない被害」になることがあり得ます。また、患者情報の漏えいの発生（疑いを持たれただけでも）対応費用も考える必要があります。これらを金銭で補償することを見積もることは、一般には極めて困難です。

どうしても損害金額を見積もる必要がある場合には、「NPO 日本ネットワークセキュリティ協会（JNSA）」から公表されている、「個人情報漏えい賠償額算出式」（「付録 3」）が参考になります。ただし、この算定式が社会的に確定したわけではなく、実際には情報主体者の個人的事情と被害感覚によりますので、あくまで参考に留める必要があります。

●患者個人情報守秘の重要性の教育効果もある

監査証跡への投入費用を組織内部に開示することで「教育効果」を期待することもできます。収益を期待できないことに費用を出していると言うことは、不必要なアクセスを排除することにそれだけの価値を認めているというメッセージになります。

●医療従事者を外部の疑いから守る仕組みでもある

監査証跡を実施していないと、客観的に証拠をもって「不必要なアクセスを行った」ことや「情報漏えい」の疑いを晴らすことができません。従事者が安心して業務に取り組めることを支える仕組みでもあります。

●風評被害の予防対策

「院内で興味で見ている」、「あの医療施設からは情報が漏れやすい」といった風評により患者の減少が予想されますが、患者数の減少があっても、それに影響するような風評があったかどうか、また本当にその影響であったかどうかも正確にはわからないものです。しかし、積極的な対策の開示で風評が立つ要因が防げる面もあります。

上述のように、費用面からだけで監査証跡の効果を考えることはできません。投入可能費用に限界があるのは現実ですから、それぞれの医療機関で全般的セキュリティ方針を立てる中で、どう考えてどう実施するかを決めることが重要です。

おわりに

監査証跡を実施することは、従来に無かった新しい取り組みです。情報の電子化に伴い、個人情報保護の重要性が言われる今において、究極の個人情報といわれる健康情報を預かる医療機関としては、基本的安全対策です。患者さんや地域、施設内部関係者に安心していただくためにも、積極的に取り組みましょう。

本ガイドによって医療機関の皆様に監査証跡をご理解いただき、大切な患者さんの個人情報保護の一助となりますことを、執筆者一同願ってやみません。

[付録 1] セキュリティリスクに対する管理策としての監査証跡実装

●経済産業省の情報セキュリティ管理基準

経済産業省の情報セキュリティ管理基準 Ver1.0
（http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex01.pdf）

上記によれば、システムアクセスおよびシステム使用状況の監視について以下のような管理を行うことを求めています。本管理基準は、本ガイドの目的とする個人情報保護のみならず、情報セキュリティ監査全般を取り扱っています。本管理基準を参照することは情報セキュリティ監査全般についての理解の助けになります。また、医療情報システムの安全管理に関するガイドラインの要求事項よりもより具体的な記載がなされていますので、個人情報保護に関する監査証跡の検討においても具体的な管理策選択の参考になります。

7.7	システムアクセスおよびシステム使用状況の監視
	目的：認可されていない活動を検出するため
7.7.1	例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査およびアクセス制御の監視を補うために、合意された期間保存すること
7.7.1.1	監査記録には、利用者 ID を含めること
7.7.1.2	監査記録には、ログオンおよびログオフの日時を含めること
7.7.1.3	監査記録には、可能ならば、端末の ID 又は所在地を含めること
7.7.1.4	監査記録には、システムへのアクセスを試みて、成功および失敗した記録を含めること
7.7.1.5	監査記録には、データ、他の資源へのアクセスを試みて、成功および失敗した記録を含めること
7.7.2	情報処理設備の使用状況を監視する手順を確立すること
7.7.2.1	個々の設備に対して要求される監視レベルは、リスクアセスメントによって決めること
7.7.2.2	監視項目には、認可されているアクセスについて、利用者 ID を含むこと
7.7.2.3	監視項目には、認可されているアクセスについて、その重要な事象の日時を含むこと
7.7.2.4	監視項目には、認可されているアクセスについて、その事象のタイプを含むこと
7.7.2.5	監視項目には、認可されているアクセスについて、アクセスされたファイルを含むこと
7.7.2.6	監視項目には、認可されているアクセスについて、使用されたプログラム・ユーティリティを含むこと
7.7.2.7	監視項目には、すべての特権操作について、監督者アカウントの使用の有無を含めること
7.7.2.8	監視項目には、すべての特権操作について、システムの起動および停止を含めること
7.7.2.9	監視項目には、すべての特権操作について、入出力装置の取付け・取外しを含めること
7.7.2.10	監視項目には、認可されていないアクセスの試みについて、失敗したアクセスの試みを含めること
7.7.2.11	監視項目には、認可されていないアクセスの試みについて、ネットワークのゲートウェイおよびファイアウォールについてのアクセス方針違反および通知を含めること
7.7.2.12	監視項目には、認可されていないアクセスの試みについて、侵入検知システムからの警告を含めること
7.7.2.13	監視項目には、システム警告又は故障について、コンソール警告又はメッセージを含めること

7.7.2.14	監視項目には、システム警告又は故障について、システム記録例外事項を含めること
7.7.2.15	監視項目には、システム警告又は故障について、ネットワーク管理警報を含めること
7.7.3	監視の結果は、定期的に見直すこと
7.7.3.1	監視結果の見直しの頻度は、関係するリスクによって決めること
7.7.3.2	考慮すべきリスク要因には、業務手続に与える重要性の度合を含めること
7.7.3.3	考慮すべきリスク要因には、関係ある情報の価値、取扱いに慎重を要する度合又は重要性に関する度合を含めること
7.7.3.4	考慮すべきリスク要因には、システムへの侵入および誤用の過去の経験を含めること
7.7.3.5	考慮すべきリスク要因には、システム相互接続の範囲（特に、公衆ネットワーク）を含めること
7.7.4	システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること
7.7.4.1	セキュリティのための監視を目的とする重要な事象の識別を補助するために、適切なメッセージタイプを予備の記録として自動的に複製すること
7.7.4.2	ファイルへ応答指令信号を送る適切なシステムユーティリティ若しくは監査ツールを使用することを考慮すること
7.7.4.3	記録の検証の責任を割り当てるとき、検証する者と活動を監視されている者との間で、役割の分離を考慮すること
7.7.4.4	記録機能のセキュリティに対して注意すること
7.7.4.5	管理策は、認可されていない変更および運用上の問題から保護することを目標とすること
7.7.5	コンピュータの時計は正しく設定すること
7.7.5.1	コンピュータ又は通信装置にリアルタイムの時計を作動する機能がある場合、合意された標準時（たとえば、万国標準時に（ＵＣＴ）又は現地の標準時）に合わせること
7.7.5.2	コンピュータ内の時計は、有意な変化があるかチェックして、あればそれを修正する手順があること

[付録 2] 院内の監査実施ルールと体制の例

●監査実施ルールの例

個人情報に対する目的外アクセスの防止のための監査の実施ルールとして、以下の内容を参考にしてルールを構築してください。

A）定期的な監査と臨時の監査についてルールを定める

- 監査のタイミングについてルールを定めましょう。
- 監査には定期監査と臨時監査があります。
- 臨時監査は監査人の判断で行えるように規定しておくと迅速な対応が行えます。

例「年に 2 回の定期監査を行う、また VIP の受診や情報漏えいの恐れなどの特別な事象が発生した場合など監査人が必要と認めるときは臨時の監査を行う。」

B）監査の際のチェック項目とチェック方法を定める

- アクセスした時間、アクセスした場所、対象患者 ID（VIP や病院関係者とその親族など）などから対象ログの抽出方針を定め、目的外アクセスが行われていないかの確認方法を規定しましょう。

例「深夜時間帯や別の診療科、病棟などからのアクセスがあった場合はアクセス内容について精査する。また、VIP や病院関係者とその親族の受診があった場合は当該患者情報へのアクセス内容について精査する。また、定期監査においては、無差別抽出した監査証跡についてのアクセス内容についても精査する。」

C）監査ログなどの監査記録の参照権限を限定する

- 監査ログの利用目的は監査に限定されます。
- 監査ログの目的外利用を防止するためのルールを策定しましょう。

例「監査ログは監査目的にのみ利用すること。監査ログの閲覧についてはその目的を明確にした上で監査人の承認を得なければならない。監査人は目的外利用がないように適切に監査ログを管理すること。」

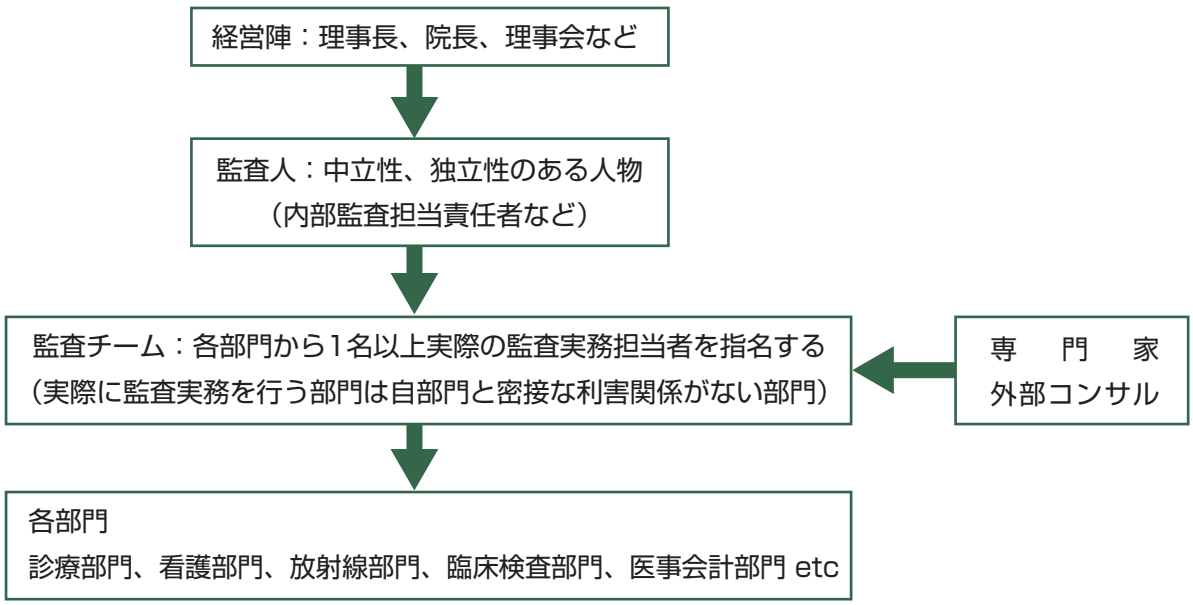
D） 監査メンバーの独立性を求める

- 監査は利害関係者が行ってはなりません。
- 内部監査を行う場合には、監査スタッフの選定は中立性や独立性を考慮して定めなければなりません。

例「監査スタッフの選定に当たっては独立性（密接な利害関係がないこと、公正かつ客観的に判断をおこなうこと）、職業倫理と誠実性、専門能力を確認し、中立性を確保すること。」

●監査体制

- 監査体制は、内部監査においても、外部監査においても、情報セキュリティ監査人を中心に監査チームを編成して実施します。
- 監査チームは独立性（密接な利害関係がないこと、公正かつ客観的に判断をおこなうこと）、職業倫理と誠実性、専門能力が求められます。
- 監査チームには必要に応じて、ネットワークスペシャリスト、システムアナリスト、ビジネスコンサルタント、技術士、弁護士、公認会計士などの専門職の支援をあおぐことを考慮したほうがよいでしょう。
- 専門職からのアドバイスや監査手続きの補助または代行があっても監査の結果については情報セキュリティ監査人が負うこととなります。



監査体制の例（内部監査）

[付録 3] 想定損害賠償額の算定式

● NPO 日本ネットワークセキュリティ協会（JNSA）の報告書

2005 年度 情報セキュリティインシデントに関する調査報告書
（http://www.jnsa.org/result/2005/20060803_pol01/index.html）

・＜情報漏えいによる被害想定と考察 （想定損害賠償額の算定）＞（2006.7.31）
・個人情報漏えいにおける想定損害賠償額の算出（P27 ～ P33）

この中で、1 件当たりの損害額として、下記の算定式が記載されています。

> 想定損害賠償額＝漏えい個人情報価値×情報漏えい元組織の社会的責任度×事後対応評価
>
> 漏えい個人情報価値＝基礎情報価値×機微情報度×本人特定容易

各パラメータの値は、以下のとおりです。

> 医療機関の社会的責任度＝ 2
> 基礎情報価値＝ 500
> 医療情報の機微度＝ 101
> 氏名＋住所があるデータの本人特定容易度＝ 6
> 氏名または住所＋電話番号があるデータの本人特定容易度＝ 3
> 適切な対応ならば事後対応評価＝ 1
> 不適切な対応ならば事後対応評価＝ 2

これより医療機関が診療情報を漏えいしたと仮定した場合の、想定損害賠償額は 1 件あたり、以下のようになります。

①本人特定にコストを要するデータで適切な事後対応の場合　⇒　**303,000 円**

②本人特定にコストを要するデータで不適切な事後対応、あるいは容易な本人特定データで適切な事後対応の場合　⇒　**606,000 円**

③本人特定の容易なデータで、かつ不適切な事後対応の場合　⇒　**1,212,000 円**

仮に、漏えい情報が 1000 件とすると、データ内容・事後対応次第ですが、**約 3 億円～ 12 億円**になります。

執筆者（H 18 年度監査証跡検討委員会）

山本　隆一	東京大学大学院　情報学環
安藤　裕	放射線医学総合研究所　重粒子医科学センター病院　医療情報課
今井　功	三菱電機株式会社　情報技術総合研究所
冨高　政治	富士通株式会社　ソフトウェア事業本部
茗原　秀幸	保健医療福祉情報システム工業会（ＪＡＨＩＳ）
深尾　卓司	保健医療福祉情報システム工業会（ＪＡＨＩＳ）
岡田　康	保健医療福祉情報システム工業会（ＪＡＨＩＳ）
吉村　仁	社団法人日本画像医療システム工業会（ＪＩＲＡ）
西田　慎一郎	社団法人日本画像医療システム工業会（ＪＩＲＡ）
野津　勤	社団法人日本画像医療システム工業会（ＪＩＲＡ）

（事務局）

山田　恒夫	財団法人医療情報システム開発センター
町田　悦郎	財団法人医療情報システム開発センター
岡本　克郎	財団法人医療情報システム開発センター

発行日　平成 19 年 3 月
発行者　財団法人医療情報システム開発センター
住　所　東京都文京区西片 1 丁目 17 番 8 号（KS ビル 3 階）
電　話　03-5805-8203

この報告書は、平成 18 年度経済産業省医療情報システムにおける相互運用性の実証事業（運営支援団体：日本システムサイエンス株式会社）の一環としてとりまとめたものです。

URL: http://www.medis.or.jp