

医療情報システム監査のご案内

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版に基づくシステム管理態勢のアセスメント

背景と目的

近年では、医療ICT技術の進展により、医療現場においては、電子カルテシステムやオーダエントリーシステム等の医療情報システムを用いた業務運営が一般的となっております。現在では、病院情報システムの機能と業務運用が不可分の関係にあり、病院機能を安心・安全に安定的に維持するためには、病院情報システムの管理が適正に整備・運用されている必要があります。

昨今、病院の情報システムが関連する情報漏えいや外部進入の脅威等が取りざたされており、多くの個人情報を預かる医療機関として、常に十分な管理態勢を確保する必要があります。ここで要請される医療情報システム管理態勢とは、単に規則として管理体制が整備されるのみならず、それが実際に適切に運用されることにより実現される、動的なPDCAサイクルにより管理されている状態を表します。

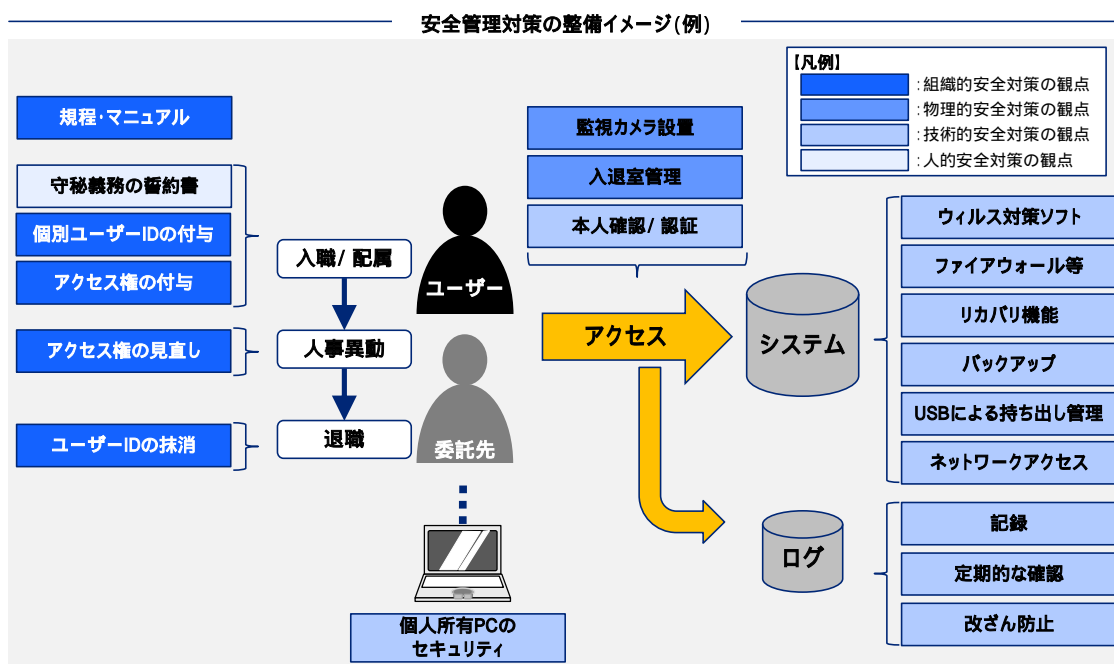
院内に内部監査部門等の医療情報システム管理態勢を適時に監査できる部門があればよいのですが、必ずしも内部監査部門が整備されていなかったり、また、外部委

託先(ITベンダー)に頼りきってしまっているケースも見受けられます。そこで、デロイト トーマツでは、医療情報システムを対象とする監査を実施し、医療情報システム管理態勢の整備状況の評価をご支援いたします。

監査基準

現時点では、厚生労働省が公表する「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」が一般的に用いられる監査基準となります。「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、医療情報システムの関連法令の要求事項に対して、対策を示すことを目的に公表されており、当該要求事項を満たすために、医療機関が実施する事項が明記されています。特に、ガイドライン中、「C. 最低限のガイドライン」として記載されている事項については、医療機関は必ず要求事項を満たさなければならないと定められています。

その他、必要に応じて関連法令等や他業界の先進事例等の視点も加味します。



* 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」より

実施アプローチ

・対象範囲

対象となる医療情報システム（Healthcare Information System : HIS）は、電子カルテシステム、オーダエントリシステム、医事会計システムの主要3システムの他に、重要な部門システムが数多くあります。医療情報の保護のためには、すべてのシステムの監査の実施が必要ですが、まずは、主要3システムを先行して実施することが考えられます。その後、各部門の情報システム管理態勢の整備状況を見ながら、放射線部門、臨床検査部門、薬剤部門の各システムを第2グループとして、その他の部門システムを第3グループとして、順次段階的に実施することが現実的と考えられます。

・監査手続

監査手続は、監査観点、スケジュール、業務への影響、作業工数等を勘案して、より合理的な手続を選択適用いたします。資料閲覧、視察、インタビュー等のほか、ヒアリング、作業証跡等の確認、日々の業務実施への立会い等の現場部門の方のご協力も必要になります。

・システム監査の事前準備

医療情報システム管理態勢の整備がまだ不十分であると認識されている場合、中長期的なロードマップを意識して、初年度はシステムに係る監査の準備段階と位置づけ、「予備調査」を実施し、医療情報システム管理態勢の整備

に注力することもあります。その後、医療情報システム管理態勢を改善し、翌年以降のシステム監査に望むこととなります。

また、システム監査の実施初期では、「医療情報システムの安全管理アウェアネス(意識付け)トレーニング」を実施することもあります。

・プロジェクト監査(スポット実施)

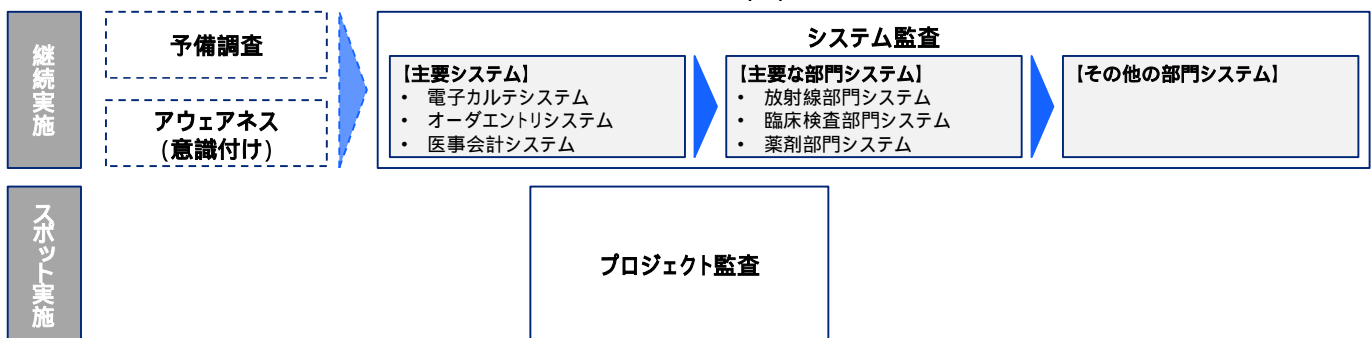
医療情報システム全体ではなく、特定のシステムについて、例えば電子カルテシステムの更改など、大規模な開発プロジェクトがある場合は、プロジェクトに特化して監査を実施することがあります。通常は、開発プロジェクトの計画段階から各フェーズ毎にプロジェクトの推進状況の監査を実施することになり、最終的なシステム移行(稼動)判定の判断材料の一つになります。

デロイトトーマツの支援体制

デロイトトーマツでは、医療機関に造詣の深いヘルスケア部門と、システム監査の経験豊富なアドバイザリー部門とのクロスファンクションチームでご支援を実施いたします。医療業界特有の事情を踏まえた上で、他業界での先進事例も参考にシステム監査を実施いたしますので、より具体的なシステム監査が実施できます。

主要メンバーには、医療情報技師、診療情報管理士、医療情報システム監査人補、看護師等の資格保有者がおり、医療現場とシステム現場の視点から、ご支援いたします。

展開アプローチ(例)



デロイトトーマツグループは日本におけるデロイトトウシュトーマツ リミテッド(英国の法令に基づく保証有限責任会社)のメンバーファームおよびそのグループ法人(有限責任監査法人 トーマツ、デロイトトーマツ コンサルティング合同会社、デロイトトーマツ ファイナンシャルアドバイザリー合同会社、税理士法人トーマツおよびDTI弁護士法人を含む)の総称です。デロイトトーマツグループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査、税務、法務、コンサルティング、ファイナンシャルアドバイザリー等を提供しています。また、国内約40都市に約7,900名の専門家(公認会計士、税理士、弁護士、弁護士、コンサルタントなど)を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイトトーマツグループWebサイト(www.deloitte.com/jp)をご覧ください。

Deloitte(デロイト)は、監査、コンサルティング、ファイナンシャル アドバイザリーサービス、リスクマネジメント、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約210,000名を超える人材は、“standard of excellence”となることを目指しています。

Deloitte(デロイト)とは、英国の法令に基づく保証有限責任会社であるデロイトトウシュトーマツ リミテッド(“DTTL”)ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL(または“Deloitte Global”)はクライアントへのサービス提供を行いません。DTTLおよびそのメンバーファームについての詳細はwww.deloitte.com/jp/aboutをご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性があります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。