

医療機関に情報セキュリティが必要な背景、その必要性

情報技術の進展に伴い「情報」が個人や組織が活動するための貴重なものとなり、安全に管理する事の重要性が益々高まっています。情報がコンピュータで取り扱われるものだけではなく紙ベースや会話などいろいろな形で扱われています。これらの情報を安全に管理する事は、医療機関に限ったことではなく社会的な責務となっています。個人情報保護と安全性確保は、全ての個人、企業、研究機関、政府において重要ですが、医療分野でのセキュリティ要件(機密性、完全性、可用性)は特に高い分野です。なぜなら医療機関は、医療提供の必要性から個人的情報(家系や宗教、思想信条など)に触れることもありえますので、個人医療情報は全ての個人情報の中でもっとも機密性があると見なされており、その機密性を保護することは患者のプライバシーを守る為には基本的なことです。

この管理を怠った場合、その被害は自らに及ぶのみならず、他者にも及ぶことが考えられます。個人の医療情報漏洩の事件はその一例です。多数の関係者が情報に関与する医療機関で、安全な情報セキュリティ管理をするためには、組織として行う必要があります。例えば医療情報の完全性を確保するために、その情報の取得から保存、更新、提供、廃棄までの完全なライフサイクル管理が行われなければなりません。完全性の確保のみならず、医療情報の可用性の確保も、効果的な医療提供のためには必要になってきます。セキュリティ管理に重きを置き過ぎる余り、医療行為に支障が出るような事態となってしまう本末転倒です。医療情報システムはまた、自然災害やシステム故障時に当たっても運用性が確保されることが必要不可欠な要請となっています。したがって、医療情報の機密性、完全性、とりわけ可用性を保持することは、医療分野では大きな特徴と言えます。

医療分野で情報セキュリティマネジメントが必要な要因のひとつに、医療提供においてインターネット技術や無線通信などの技術が、どんどん使われてきていることの現実があります。これらの技術は適切に扱われないと医療情報の機密性、完全性、可用性のアンバランス、危険な状態を増やします。医療行為は、大学病院もあれば、個人経営の診療所あるいは小規模診療所で提供される場合もあります。小規模診療所ではセキュリティを管理するための体制が不十分になりがちです。医療施設の規模、場所、医療提供形態に関係なく、全ての医療機関は医療情報の保護のために厳重な管理をしなければなりません。従って、医療機関は組織的に情報セキュリティマネジメントシステムを構築し、必要な管理策の選択と実装が急務となっています。

医療機関の関係者

医療機関には多数の関係者が存在します。資格で区分すると、医師、歯科医師、薬剤師、臨床検査技師、診療放射線技師、看護師、などが挙げられます。「JIS Q 9000:2000」の定義を医療機関に当てはめると、「組織」とは各種形態の医療機関、上記の資格者、その他の医療機関で働く人々と言えます。「顧客」とは言うまでも無く患者、患者団体および家族です。「供給者」とは、医療機関への物品、サービスの提供業者です。「利害関係者」とは前記全ての他に、医療機関の設立組織、保険者、薬局、資格者の団体が含まれます。これら関係者の情報への関与の仕方を明確にする事が重要となります。

医療情報の形態

医療情報は様々な形態で存在します。言語や数字で表現されたものだけでなく、写真、図、ビデオ、医療画像の形態をとるものもあります。また保管形態も、紙、フィルムや電子的媒体があります。また、伝送する方法には、手渡し、FAX、郵便、コンピュータネットワーク等が利用されます。医療情報がどんな形態を取り、どんな媒体、手段で転送や保管されたとしても、適切に保護されなければなりません。

取扱いする医療情報の把握

情報システムで扱う医療情報をすべてリストアップし、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持する必要があります。このリストは情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理されなければなりません。安全管理上の重要度は、安全性が損なわれた場合の影響の大きさに応じて決めます。少なくとも患者等の視点からの影響の大きさと、継続した業

務を行う視点からの影響の大きさを考慮する必要があります。この他に医療機関等の経営上の視点や、人事管理上の視点等の必要な視点を加えて重要度を分類します。個人識別可能な医療に係る情報の安全性に問題が生じた場合、患者等にきわめて深刻な影響を与える可能性があり、医療に係る情報は最も重要度の高い情報として分類されます。

医療機関における情報セキュリティのリスク分析

分類された情報毎に、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤などによる脅威を列挙します。医療機関等では一般に他の職員等への信頼を元に業務を進めているために、同僚等の悪意や過誤を想定することに抵抗があります。しかし、情報の安全管理を達成して説明責任を果たすためには、たとえ起こりえる可能性は低くても、万が一に備えて対策を準備する必要があります。また説明責任を果たすためには、これらのリスク分析の結果は文書化して管理する必要があります。この分析の結果、得られた脅威に対して、リスク値に応じてリスク対応方針にそった管理策を適用し対策を実施していきます。特に安全管理や、個人情報保護法で原則禁止されている目的外利用の防止はシステム機能だけでは決して達成できないことに留意しなければなりません。システムとして可能なことは、人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保障することであり、これが限界です。従って、人の行為も含めた脅威を想定し、運用管理規程を含めた対策を講じることが重要です。医療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データに関してだけでなく、入出力の際に露見等の脅威にさらされる恐れのある個人情報保護するための方策を考える必要があります。以下にさまざまな状況で想定される脅威を列挙します。

- 1.医療情報システムに格納されている電子データ（不正アクセス、改ざん、き損、滅失、漏えいなど）
 - 2.入力の際に用いたメモ・原稿・検査データ等（メモ・原稿・検査データ等の覗き見、持ち出し、コピー、不適切な廃棄など）
 - 3.個人情報等のデータを格納したノートパソコン等の情報端末（持ち出し、不正アクセス、改ざん、き損、滅失、漏えいなど）
 - 4.データを格納した可搬媒体等（持ち出し、コピー、不適切な廃棄、盗難、紛失など）
 - 5.参照表示した端末画面等（覗き見など）
 - 6.データを印刷した紙やフィルム等（覗き見、持ち出し、コピー、不適切な廃棄など）
 - 7.医療情報システム自身（IT障害、不正侵入、改ざん、不正コマンド実行、情報かく乱、ウイルス感染、サービス不能など）
 - 8.非意図的要因によるIT障害（システムの仕様やプログラム上の欠陥（バグ）、操作ミス、故障、情報漏えいなど）
 - 9.地震、水害、落雷、火災などの災害によるIT障害（電力供給の途絶、通信の途絶、コンピュータ施設の損壊等、IT機能不全など）
- これらの脅威に対し、適切な管理策を実施することにより、発生の可能性を低減し、リスクを實際上、問題のないレベルにまで小さくすることが必要になります。

医療情報システムの安全管理に関するガイドライン

近年の医療の情報化の進展に伴い、個人自らが医療情報を閲覧・収集・提示することによって、自らの健康増進へ役立てることが期待されています。これを受けて医療情報ネットワーク基盤検討会が、各所より医療情報に関するガイドラインの整合を図る検討しまとめたものが、「医療情報システムの安全管理に関するガイドライン」です。

「医療情報システムの安全管理に関するガイドライン」は、病院、診療所、薬局、助産所等（以下「医療機関等」という。）における診療録等の電子保存に係る責任者を対象とし、理解のしやすさを考慮して、現状で選択可能な技術にも具体的に言及しています。ガイドラインは技術的な記載の陳腐化を避けるために定期的に内容を見直すことになっています。現在、改訂を重ね第4版が最新版となっています。

このガイドラインは「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」と対になるもので、個人情報保護は情報システムに関わる対策だけで達成されません。従って、本ガイドラインを使用する場合、情報システムだけの担当者であっても、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」を十分理解し、情報システムにかかわらない部分でも個人情報保護に関する対策が達成されていることを確認することが必要であるとされています。

このガイドラインの6章では、「6.1 方針の制定と公表」において JIS Q 15001:2006 の引用によって公表すべき基本方針の項目を明示し、JIS Q 27001:2006 の引用によって安全管理方針を具体的に説明した上で「C 最低限のガイドライン」を新設されています。同様に、「6.2 医療機関における情報セキュリティマネジメントシステム (ISMS) の実践」においても「C 最低限のガイドライン」及び「D 推奨されるガイドライン」を新設しています。「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」においては、B 項及び D 項に従業者による外部からのアクセスに関する事項を追加しています。

医療機関における情報セキュリティマネジメントシステム (ISMS) の実践

医療情報を取り扱う事業者は、「医療情報システムの安全管理に関するガイドライン」に沿って、医療機関における情報セキュリティマネジメントシステム (ISMS) の実践が求められています。その実現手段として ISO27001 認証取得をすることは、体系的なマネジメントシステムを短期間に合理的に構築するという面で非常に有効です。ISMS の構築は PDCA モデルによって行われます。JIS Q27001:2006 では PDCA の各ステップは下記のように規定しておりますので、合理的に構築を進めることができます。

- ・ P では ISMS 構築の骨格となる文書 (基本方針、運用管理規程等) と文書化された ISMS 構築手順を確立する。
- ・ D では P で準備した文書や手順を使って実際に ISMS を構築する。
- ・ C では構築した ISMS が適切に運用されているか、監視と見直しを行う。
- ・ A では改善すべき点が出た場合には是正処置や予防処置を検討し、ISMS を維持する。

上記のステップをより身近にイメージできるようにするために、医療行為における安全管理のステップがどのようにおこなわれているかについて JIPDEC (財団法人 日本情報処理開発協会) の「医療機関向け ISMS ユーザーズガイド」の例などを参照して進めていきます。

医療分野においては診察、診断、治療、看護等の手順が過去からの蓄積によってすでに確立されているため、あとは事故やミスを発見したときにその手順にそって分析していくことで、どこを改善すればよいかがおのずと判定できます。分析結果にもとづき必要な対策を実行することで、安全が高まる仕組みが出来上がっているためと言えます。反面、情報セキュリティでは IT 技術の目覚ましい発展により、過去の経験の蓄積だけでは想定できない新たなセキュリティ上の問題点や弱点が常に存在し得ます。そのため情報セキュリティ独自の管理方法が必要であり、ISMS はそのために考え出されました。ISMS は医療の安全管理と同様 PDCA サイクルで構築し、維持して行きます。逆に言えば、医療関係者にとって ISMS 構築は P のステップを適切に実践し、ISMS の骨格となる文書体系や手順等を確立すれば、あとは自然に ISMS が構築されていく土壤があると言えます。

ニーズで選べる支援内容

タテックス株式会社では、医療情報サービスを展開する企業の情報セキュリティマネジメントシステムのコンサルティング実績がございます。認証取得に関するご相談はお気軽にお問合わせください。

また、既にシステム運用をしていて、改善したいのだが。。。といった改善のご相談もお気軽にお問合わせください。実績豊富な ISO コンサルタント陣が ISO 取得に必要な工数をお客様のニーズで選べます。お問合わせください。

ISO27001 特別レポートを無料公開!

実績豊富な ISO コンサルタント陣が ISO9001, ISO14001, P マーク取得ノウハウをご提供。ISO 担当者だけでなく経営者も必見の情報です。まずは最新の無料レポートをご覧ください。ISO27001, ISO14001, ISO9001, P マーク取得に関するお悩み・ご相談を無料メール相談でお受けします。専門家のアドバイスを受けたい方、まずは無料サービスを活用ください。

御見積りは信頼と実績のタテックスまで[お問合せ](#)ください。

お問合せは、[ここをクリック](#) [お問合せ](#)