資料１

医療情報システムの契約に関するチェックリストについて

総務省
厚生労働省
経済産業省

１．本チェックリストの背景・目的

○　医療情報システムの導入・運用においては、本来、医療機関の経営や医療関連業務等の観点から医療等関連情報の内容及びそれらの情報化の必要性に応じて、医療機関がシステム化する業務・情報などの要件の明確化及びその構築・運用に係る規定や体制などの整備を実施ものである。他方、医療機関がシステムの導入・運用するにあたり、医療情報システム・サービス事業者（以下「事業者」という。）は、情報システム及びセキュリティに関する専門的な知識等を有することから、医療機関に対し、委託契約又は信義則に基づく付随義務として、適時適切に必要な情報を提供する義務を負うものである。

○　医療情報の安全管理に関しては、「医療情報システムの安全管理に関するガイドライン」（以下「厚労省ガイドライン」という。）及び「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（以下「２省ガイドライン」という。）に必要な対策が規定されているものの、近年の医療機関における情報セキュリティインシデントの発生で明らかになった課題を踏まえれば、医療情報システムに関する契約の際に、医療機関と事業者との責任分界が適切に協議されていなかったことが課題の一つとして考えられる。

○　また、契約上は責任分界が曖昧な点について、事業者が対応をした場合に責任の所在が問題となる等のケースがあることから、可能な限り、事前に双方の役割分担について取り決め、有事の際に即座に対応できるよう、合意形成文書に落とし込むことが重要であり、医療機関と事業者は、そのような姿勢で契約の締結等に向けて取り組むことが望まれる。役割分担を事前に取り決め、情報システム全体を漏れなく俯瞰的にとらえることで、セキュリティインシデントの予防にもつながるものと考えられる。

○　この点、厚労省ガイドラインでは、契約時に事業者と責任分界を取り決める際の考慮事項や、契約形態に応じた責任分界の取り決め方等は示されているが、具体的な協議事項は示されていない。

○　２省ガイドラインでは、契約時に、事業者から医療機関へ情報提供すべき内容は示されているが、事業者向けガイドラインであるため、医療機関に求める具体的な対応は示されていない。

○　こうしたことから、本チェックリストでは、「医療情報システムの契約のあり方等に関する有識者委員会」における議論を踏まえ、

Part１　【医療機関が主に実施する項目】

：事業者のみでの実施が難しく、契約を締結する上で医療機関が主体となって、必要に応じてシステム関連業者の協力を得ながら実施することが望ましい項目の例（医療機関が主体的

に実施する項目ではあるが、システム関連事業者は医療機関が意思決定を行う上で適切に情報提供等を行う必要がある場合があり、システム関連事業者においても一定の責任が生じうる。）

Part２　【医療機関と事業者が共同で実施する項目】

：技術的な対策等医療機関だけでは実施することが困難な事項で、責任分界を明確にしておくことが望ましい項目の例

の具体化を行うことを目的とする。

２．本チェックリストの使い方

○　本チェックリストの主な対象は、マルチベンダー型契約により責任分界が複雑であるものの、法務、IT に精通した担当者が不在である中小規模の病院を想定している。小規模な診療所等では対象外となるような項目が含まれているが、適切に選択すれば有用と考えられる。また大規模で法務、IT に精通した担当者が存在する場合でもこのリストに存在する項目は最低限チェックすべき項目も多いために、このリストを参考にして、自施設の状況に合わせて改変・拡張して用いられることが期待される。

○　医療機関においては、契約前に本チェックリスト Part１を用いて、医療機関自身が主体となって実施するセキュリティ対策を確認する。契約にあたって、Part1 についても必要に応じて事業者が支援することも想定されるため、Part1・Part2 ともにそれぞれの項目の役割分担・責任分界について、医療機関と事業者間の両者で共通理解と明示的な合意が得られるように協議を行う。Part1 のチェックリストは病院の責任を一義的に定めることを目的として作られるものではない。

最終的には、事業者との間で合意形成文書（契約書や SLA）に落とし込むことを想定する。

○　協議を実施する際は、厚労省ガイドラインや２省ガイドライン等の該当節を両者で確認することが望ましい。

○　Part1、Part２ともに、契約締結時のみならず、契約更新時やシステムの追加構築等を実施する際の適切なタイミングにおいて、現行の契約の確認に活用されることが望ましい。また、本チェックリストは責任分界の観点から作成したものであり、厚労省ガイドライン及び２省ガイドラインの内容を網羅しているものではないため、本チェックリストを利用して、契約の締結等を行うに当たっては、前提として、医療機関においては厚労省ガイドラインを、事業者においては厚労省ガイドラインに加え２省ガイドラインの内容を理解していることが求められる。

○　なお、本チェックリストにおける「医療情報システム」とは、厚労省ガイドラインと同様、医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般を想定する。これには、事業者により提供されるシステムだけでなく、医療機関等において自ら開発・構築されたシステムが含まれる。

３．参考資料

○　厚労省ガイドライン、同ガイドライン別添小規模医療機関向けガイダンス、同ガイドライン「医療機関のサイバーセキュリティ対策チェックリスト」等

○２省ガイドライン、IPA・経済産業省「情報システム・モデル取引・契約書（パッケージ、SaaS/ASP 活用、保守・運用）＜民法改正を踏まえた、追補版の見直し整理反映版＞」チェックリスト等