資料１

医療情報システムの契約における関係者間の役割分担等に関するチェックリストについて

令和●年●月●日
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

○　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、医療機関と医療情報システム・サービス事業者（以下「事業者」という。）との役割分担等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、契約上は役割分担等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を踏まえれば、可能な限り、事前に双方の役割分担等について取り決め、有事の際に即座に対応できるよう、契約の段階で合意形成文書（契約書やサービス・レベル合意書等）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。役割分担等を事前に取り決め、医療情報システム全体を漏れなく俯瞰的にとらえることは、情報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。

○　医療情報システムの導入・運用においては、本来は、医療機関が、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、システム化する業務・情報等の要件の明確化及びその構築・運用に係る規程や体制等の整備を実施すべきものである。他方、医療機関が医療情報システムを導入・運用するにあたり、事業者は、医療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。

○　こうした中で、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。

○　また、厚生労働省においては、令和５年４月から、医療法に基づく医療機関に対する立入検査の項目に、サイバーセキュリティ対策の項目を位置付けた。また、立入検査の際に確認する項目について、「厚労省ガイドライン」から特に取り組むべき重要な項目を抽出し、「医療機関におけるサイバーセキュリティ対策チェックリスト」（以下「立入検査用チェックリスト」とい

う。）を公表した。こうした「特に取り組むべき重要な項目」についても、医療機関において適切な対応が行われるためには、契約の段階から医療機関と事業者が役割分担等を協議しておくことが重要である。

○　しかしながら、現状、厚労省ガイドラインでは、契約時に事業者と役割分担等を取り決める際の考慮事項や、契約形態に応じた役割分担等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。

○　また、２省ガイドラインにおいても、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、近年の情報セキュリティインシデントで明らかになった課題を踏まえつつ、また、立入検査用チェックリストの項目も参考に、医療情報システムの契約において、医療機関と事業者が役割分担等を協議する上で必要な項目について、具体化を図ることを目的とした。また、本チェックリストの作成に当たっては、「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」において、以下の項目に関して議論した。

Part１　【主に医療機関が実施する項目】
：契約を締結する上で医療機関が主体となって、必要に応じて事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、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、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、役割分担等を明確にしておくことが望ましい項目の例

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役割分担等が複雑であるものの、法務や 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（※）。

（※）例えば、小規模な診療所等では、担当する業務ごとに区分された組織（部署）がなく、組織運営のための計画等がない場合がある。このような場合は、情報セキュリティ対策に係る詳細な計画や規程類を策定したとしても、実効性が伴わず、医療機関の負担のみが増大してしまう可能性があるため、こうした規程類の策定に当たっては、医療機関等の組織や規模等に鑑みてリスク評価を行い、その上で必要な内容を定めることが必要である。

また、大規模な病院等で法務や IT に精通した担当者が存在する場合でも、本チェックリストに掲げる項目は最低限チェックすべき項目も多いため、本チェックリストを自施設の状況等に応じて改変等を行った上で、用いることも可能である。

○　本チェックリストの使い方としては、以下のとおりである。

①　まず、医療機関において、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情報セキュリティ対策を確認する。
②　次に、契約に当たっては、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。このため、Part１・Part２ともに、それぞれの項目の役割分担等について、医療機関と事業者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。
③　最終的には、事業者との間で合意形成文書に落とし込むことを想定する。

なお、本チェックリストは医療機関や事業者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。

○　本チェックリストの使用に当たっての留意事項としては、以下のとおりである。

①　本チェックリストは、役割分担等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。このため、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。

②　協議を実施する際には、別添の「新規システムの導入に際しての医療情報システムの契約における関係者間の役割分担等に関するチェックリスト　利用イメージ」も参考となる。こうした利用イメージや医療機関の情報セキュリティ対応上の課題を踏まえ、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。

③　本チェックリストは、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等の適切なタイミングにおいて、現行の契約の確認にも活用されることが望ましい。

④　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、立入検査用チェックリスト等

○　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