参考資料３-６

医療情報システムの契約における当事者間の役割分担等に関する確認表

令和６年６月

総務省

厚生労働省

経済産業省

１．本確認表の背景・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（SLA）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・運用するに当たり、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。さらに、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」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、事業者向けの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、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、「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」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て、確認表として取りまとめることとした。

○　なお、本確認表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、以下の項目について議論した。

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．本確認表の使い方

○　本確認表の主な対象は、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、厚労省ガイドライン別添小規模医療機関向けガイダンスを参考にして、必要な内容を定めることが重要である。

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、本確認表に掲げる項目は、最低限確認すべき項目も多いため、本確認表を自施設の状況等に応じて改変する等した上で、用いることも可能である。

○　本確認表の使い方としては、以下のとおりである。

①　まず、医療機関において、契約前に本確認表の 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医療機関を支援することも想定される。このため、Part１・Part２の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　協議の過程では、別添の「医療情報システムの契約における当事者間の役割分担等に関する確認表 -推奨される対応例-」を用いて、医療機関と事業者で、この「推奨される対応例」等も確認しながら、両者での役割分担等について協議する（※）。

（※）　本確認表では、「初回確認」欄及び「完了日」欄を設けており、「初回確認」欄においては、事業者と初回に協議した日の確認結果を記載する。（確認ができている項目については「はい」、確認ができていない項目については「いいえ」に印をつける。）「初回確認」欄において、「いいえ」になった項目については「完了日」欄を使用し、確認が完了した日付を記載することを想定する。

本確認表等で用いている用語のうち、＊が付けられている用語については、別添の「用語の解説」を適宜参照する。

また、「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」に関連する契約上重要な項目については、参考として、推奨される対応の具体例等を示しており、適宜参照する。

さらに、医療機関と事業者が共同で実施するPart２については、医療機関と事業者が共通認識を持つための「想定されるリスク」を示しており、適宜参照する。

④　最終的には、医療機関と事業者との間で協議した結果を、できるだけ具体的な文言で合意形成文書に落とし込むことを想定する。

なお、本確認表は、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たものではない。

○　本確認表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　本確認表は、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、本確認表を利用して、契約の締結等を行うに当たっては、その前提として、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　医療機関と事業者で協議を行う際には、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当事者間の役割分担等に関する確認表の利用イメージ」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　本確認表は、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といった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　本確認表における「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

○　「医療情報システムの安全管理に関するガイドライン」（厚労省ガイドライン）
（https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html）

○　厚労省ガイドライン別添小規模医療機関向けガイダンス
（https://www.mhlw.go.jp/content/10808000/001102587.pdf）

○　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
（https://www.mhlw.go.jp/content/10808000/001139055.pdf）

○　「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」（２省ガイドライン）
（https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html）

○　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
（https://www.ipa.go.jp/digital/model/model20201222.html）

謝辞

本確認表の作成に当たり、「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、ご議論をいただきました委員の皆様とともに、確認表の草案の作成等にご協力をいただきましたブレークモア法律事務所の皆様に、厚く御礼を申し上げます。

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
委員等名簿（敬称略・五十音順）

（座長）

山本　隆一 一般財団法人医療情報システム開発センター　理事長

（委員）

岩田　恵一 一般社団法人日本クラウド産業協会　執行役員

甲賀　啓介 公益社団法人全日本病院協会　常任理事

佐原　博之 公益社団法人日本医師会　常任理事

高倉　弘喜 国立情報学研究所　アーキテクチャ科学研究系　教授

野津　勤　 一般社団法人日本画像医療システム工業会　セキュリティ委員会副委員長

宮田　剛　 公益社団法人全国自治体病院協議会　常務理事

茗原　秀幸 一般社団法人保健医療福祉情報システム工業会　セキュリティ委員会委員長

山下　博之 独立行政法人情報処理推進機構　専門委員

渡辺　宗彦 ブレークモア法律事務所　弁護士

医療情報システムの契約における当事者間の役割分担等に関する確認表

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）

＊が付けられている用語については、別添の「用語の解説」を適宜参照すること。

項番	項目	内容	初回確認 （　/　）	完了日 （日付）	備考欄
A	**事業者選定・事業者管理**				
1	事業者からの開示資料の確認	事業者から開示を受けたサービス仕様適合開示書[*1]等（MDS/SDS[*2]、MDS2[*3]等）を確認しているか。	はい・いいえ	（　/　）	
2	事業者管理	①事業者との契約・協働体制を把握・管理できているか。	はい・いいえ	（　/　）	
		②医療情報を第三者提供する場合の管理体制が整備されているか。	はい・いいえ	（　/　）	
B	**医療機関の内部体制**				
1	「医療情報システムの安全管理に関するガイドライン」の確認	「医療情報システムの安全管理に関するガイドライン」を確認したか。	はい・いいえ	（　/　）	
2	「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」に基づく契約時での現状把握及び対応	「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」を用いて、契約時に医療情報システムの現状把握及び対応を実施しているか。	はい・いいえ	（　/　）	
3	安全管理のための人的管理	① 医療情報を取り扱う職員に関して人的安全管理対策を実施しているか。	はい・いいえ	（　/　）	
		② 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施し、教育・訓練の実施状況について定期的に経営層に報告しているか。	はい・いいえ	（　/　）	
4	通常時における管理責任	医療情報システムの管理や運用を適切に行っているか。	はい・いいえ	（　/　）	
5	通常時における説明責任	① 医療情報システムの機能や運用につき、医療機関として状況を適切に把握し、必要に応じて患者等に説明ができるようになっているか。	はい・いいえ	（　/　）	
		② システム構築等を実施する際に、医療機関として状況を適切に把握し、必要に応じて事業者に説明ができるようになっているか。	はい・いいえ	（　/　）	
6	物理的リスクの対応	① 機器や記憶媒体を持ち出す際の紛失・盗難リスクの対応を行っているか。	はい・いいえ	（　/　）	
		② 施設への物理的侵入リスクの対応を行っているか。	はい・いいえ	（　/　）	
C	**規程類の整備**				
1	医療情報システムの運用ルール及び規程類の策定	医療情報システムの運用ルールを定め、明文化された規程類を整備しているか。必要に応じて規程類の見直しを行っているか。	はい・いいえ	（　/　）	
2	通常時における定期的な見直し、改善責任	医療情報システムの運用につき、適宜事業者からの情報提供を受け、定期的に見直し、必要な改善を行えるようになっているか。	はい・いいえ	（　/　）	
3	インシデント発生に備えた対応	BCP[*4]（事業継続計画）について、定期的な見直しや従業員への訓練・周知等を行っているか。	はい・いいえ	（　/　）	

医療情報システムの契約における当事者間の役割分担等に関する確認表

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）

＊が付けられている用語については、別添の「用語の解説」を適宜参照すること。

項番	項目	内容	初回確認 （　/　）	完了日 （日付）	備考欄
A	共通				
1	「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」の確認	事業者は「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」を確認する。	はい・いいえ	（　/　）	
2	複数事業者間の役割分担	医療機関が複数事業者と契約する場合における、事業者間の役割分担及び抜け漏れがないことを確認する。	はい・いいえ	（　/　）	
3	「医療情報システムの安全管理に関するガイドライン」の遵守	下記「B.システム導入」「C.システム運用・保守契約」で例として示すもの以外にも、事業者が提供する医療情報システムやサービスが「医療情報システムの安全管理に関するガイドライン」の遵守事項を満たす上で必要な仕様や運用となっていることを確認する。	はい・いいえ	（　/　）	
4	継続的なリスクマネジメントプロセスの実施	「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」5.1に示されたリスク特定、リスク分析、リスク評価、リスク対応の選択肢の選定、リスク対応策の設計・評価、リスクコミュニケーションのプロセスを継続的に実施する。	はい・いいえ	（　/　）	
5	開示されたサービス仕様等の事後的な変更	契約締結前に事業者から提示された医療情報システム関連情報について、変更があった場合に情報提供する。	はい・いいえ	（　/　）	
6	サービス・レベル合意書（SLA）*5 の締結	事業者が提供するサービスの保証範囲を合意するため、サービス・レベル合意書（SLA）*5 を締結する。	はい・いいえ	（　/　）	
7	事業者の責任と秘密保持義務	医療情報システムに関わる事業者に対して、医療機関の職員と同様の責任や秘密保持義務を課す。	はい・いいえ	（　/　）	
8	個人情報の管理	個人情報の適切な取り扱いについて取り決める。	はい・いいえ	（　/　）	
9	医療情報の外部保存	診療録及び診療諸記録等の機密情報や個人情報について事業者が提供するサービスを用いた外部保存を行う場合に満たすべき要件（特にクラウドサービス*6 を利用する場合）を遵守する。	はい・いいえ	（　/　）	
10	再委託先の選定・管理	医療情報システムに関する業務を事業者が再委託する場合に、再委託先の選定・管理について医療機関が関与する。	はい・いいえ	（　/　）	
11	医療情報システムのセキュリティに関する情報提供義務	事業者が医療機関に対して、医療機関が患者に対する安全管理義務を履行するために必要なセキュリティに関する情報を適時適切に提供する義務（説明義務）の具体的内容・範囲について定める。	はい・いいえ	（　/　）	
12	セキュリティ対策の見直し提案	情報セキュリティを巡る情勢に鑑み、事業者から自発的に対策の見直しを提案する。	はい・いいえ	（　/　）	
B	システム導入契約				
1	利用者認証	医療情報システムへのアクセスを正当な利用者のみに限定するため、利用者の識別・認証機能を設定する。	はい・いいえ	（　/　）	
2	通信相手の認証	医療情報システムにおいて通信しようとする相手方が、通信目的に適った正当な相手かどうか認証する。	はい・いいえ	（　/　）	
3	通信経路に対する安全対策の確保	通信経路に対する安全対策を確保する。	はい・いいえ	（　/　）	
4	暗号化	通信及び保存情報の暗号化を実施する。	はい・いいえ	（　/　）	
5	ネットワーク構成	診療等に必要なネットワークを適切に構築する。	はい・いいえ	（　/　）	
6	品質確保の状況	医療情報システムの品質管理方法等について両者で確認するための情報提供を行う。	はい・いいえ	（　/　）	

項番	項目	内容	初回確認 （　/　）	完了日 （日付）	備考欄
C	システム保守・運用契約				
1	ネットワークのトラフィック*7監視	ネットワークのトラフィック*7の監視及び異常発生時の対応を確認する。	はい・いいえ	（　/　）	
2	機器運用監視	サーバ、ネットワーク機器の稼働監視を行う。	はい・いいえ	（　/　）	
3	運用委託先によるシステムの管理状況の報告	医療情報システムの運用を委託する場合において、医療機関が管理状況を把握し、安全管理がなされていることを確認できるような体制を構築する。	はい・いいえ	（　/　）	
4	事故発生時の報告	事故発生時の対応方法及び医療機関への報告について取り決める。	はい・いいえ	（　/　）	
5	事故発生時の原因究明・対策	事故発生時の原因究明、善後策の策定・実施、再発防止策の策定・実施に係る役割分担を行う。	はい・いいえ	（　/　）	