**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（第１回）**

**議事要旨**

| | |
|---|---|
| 実 施 日 時 | 2023 年 11 月 15 日（水）14 時 00 分～16 時 00 分 |
| 実 施 場 所 | オンライン開催 |
| 参加構成員<br>（敬称略・<br>五十音順） | 岩田　恵一　　一般社団法人日本クラウド産業協会　執行役員<br>甲賀　啓介　　公益社団法人全日本病院協会　常任理事<br>佐原　博之　　公益社団法人日本医師会　常任理事<br>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<br>宮田　剛　　公益社団法人全国自治体病院協議会　常務理事<br>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<br>山下　博之　　独立行政法人情報処理推進機構　専門委員<br>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<br>渡辺　宗彦　　ブレークモア法律事務所　弁護士 |
| 事　務　局 | 株式会社エヌ・ティ・ティ・データ経営研究所 |
| 事務局管理 | 総務省　情報流通行政局　地域通信振興課デジタル経済推進室<br>厚生労働省　医政局　特定医薬品開発支援・医療情報担当参事官室<br>経済産業省　商務・サービスグループ　ヘルスケア産業課 |
| 資　　料 | 資料１　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　開催要綱（案）<br>資料２　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<br>資料３　医療情報システムの契約に関するチェックリスト　コンセプトペーパー（案）<br>資料４　医療情報システムの契約に関するチェックリスト（案）<br>資料５　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改定に向けた検討状況<br>参考資料１　医療情報システムの安全管理に関するガイドライン　第 6.0 版<br>参考資料２　医療情報システムの安全管理に関するガイドライン　別添医療機関等におけるサイバーセキュリティ対策チェックリスト<br>参考資料３　医療情報システムの安全管理に関するガイドライン　第 6.0 版　別添小規模医療機関等向けガイダンス<br>参考資料４　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　第 1.1 版<br>参考資料５　モデル取引・契約書見直し検討部会　民法改正対応モデル契約見直し検討ＷＧ　情報システム・モデル取引・契約書追補版　セキュリティチェックシート |

【議事】

1. 開催要綱等について
2. 座長の選出について
3. 医療情報システムの契約に関するチェックリスト（案）について

【議事要旨】

1. 開催要綱等において、事務局より資料１、資料２について説明が行われた。

2. 座長の選出において、山本座長が選出された。

３．医療情報システムの契約に関するチェックリスト（案）について、厚労省より資料３及び資料４について、事務局より資料５について説明が行われた。その後の質疑応答は、以下のとおり。

- 今回のチェックリストは中小規模およびそれに満たない医療機関であっても利用できるようにするという趣旨との説明があったが、そうであれば診療所もこれに含まれるという理解であるか。レセコンやオンライン資格確認システムに係る契約に関しても今回のチェックリストに含まれるのであれば、事実上ほぼすべての診療所が含まれることになると考えている。
  - 今回のチェックリストには、診療所が参照する内容としては少しオーバースペックなものも含まれていると思うが、そうした内容については読み飛ばしていただけばよいと考えている。
  - 今回のチェックリストは主として病院を読み手として想定しているため、すべての内容が診療所に適用されるとは考えていない。（厚労省）
  - 今回のチェックリストを診療所にどのように適用するかという点は、今後議論されるのか。
  - まずは中小規模の病院向けという建付けで今回のチェックリストを完成させ、実際に想定したとおりに現場での活用が行われるようにした上で、これを診療所においてどのように活用できるようにするかということについては、必要に応じて検討していきたい。（厚労省）
  - 承知した。そうであれば、今回のチェックリストは中小規模の病院向けであって、診療所向けのものは別途作成する旨を、どこかに明記していただきたい。診療所も、オンライン資格確認システム導入を契機として、サイバーセキュリティに対して敏感になっているところが多いと思われる。ベンダとの間で契約上定める責任分界について、どのようなことに留意しなければならないのか、診療所向けにも明示できるようになれば良いと考えている。
- 今回のチェックリストの公表に際しては、資料３も公表資料に含まれるのか。
  - 含まれる。資料３のコンセプトペーパーは、今回のチェックリストの前文として位置付けられる。
- パート１とパート２の位置付けについて、パート１では医療機関が実施する項目の一部が例示されているものと理解して良いか。
  - パート１は、体制・規程類の整備といったように、医療機関が決定主体となって決定せざるを得ない、ベンダのみで実施することは困難な取組項目を挙げている。コンセプトペーパーの「【医療機関が実施する項目】」という書きぶりからは、依然「医療機関だけが実施する項目」であるかのような印象を与えてしまうように思うので、修正する必要があるのかもしれないと考えている。（厚労省）
  - 本来、システムの導入等の契約の場面では、医療機関において、どのようなシステムを開発・納入するのかといった内容を定義し、これをベンダに示す必要がある。そのことを踏まえれば、パート１は、本来医療機関が実施すべきであるが、システムに関して分からないことが多いため、必要に応じてベンダの協力を得て実施すべき取組項目が挙げられていると理解している。
  - 実状として、システム設計の段階で、医療機関がベンダに細かく要件を指示するといったことはまずない。基本的に、医療機関はベンダが用意しているパッケージ製品を選択・導入することになる。パート１に挙げられているのは、どの製品を選択したとしても実施しなければならない取組項目である。

- 実状がそうであるのは理解している。ただ、本来的には医療機関がどのようなシステム・サービスの提供を受けたいのか、きちんと決定してベンダに提示すべきであり、その決定に対して最終的に責任を負うのは医療機関であるというニュアンスをはっきりさせておく必要があると思う。これはチェックリストの内容にも関わると考えている。
- 医療機関がどの製品を選択したのかという点に関しては、医療機関が責任を負うことになるが、一旦製品を選択した後の、構築・導入・運用に関して契約を取り交わす場合に、そこで定められる責任は必ずしも医療機関のみならず、医療機関とベンダの両者に属し得るものであって、これを定める上でパート１やパート２の一部の内容を参照することが想定される。
- どのようなシステム・サービスを利用したいかということを主体的に決めるのが医療機関であるとしても、そのことが、システム・サービスの要件定義等に係る責任を医療機関がすべて負うべきということには繋がらない上、今回の検討の趣旨にも反する。医療機関とベンダとの間で、インシデントが発生した場合にその結果に対する責任の分界点を定めるため、事前に話し合いが行われるようにするのが今回の検討の趣旨である。（厚労省）
- パート１は本来医療機関がきちんと定義すべきであるが、それが難しい場合はベンダの協力を得て行う、ただし最終的な責任は医療機関が負うべきものであり、パート２は医療機関とベンダの間で、どちらが最終的な責任を負うべきか協議の上決定すべきものと理解している。
- パート１とパート２の位置付けに関しては、おっしゃるとおりである。

■ 資料３の「１．本チェックリストの背景・目的」でなされているパート１の説明は、当初契約時・契約前に医療機関が実施すべき項目とされていたが、そのように位置付けると、インシデント発生時の損害賠償責任を医療機関側が負うべき根拠資料として、賠償請求時に利用されてしまうおそれがあるため、厳格に医療機関だけが責任を負うものとするのではなく、幅を持たせた形でベンダの協力を得るべき旨を記載している。

- 損害賠償請求訴訟上、今回のチェックリストが、法律上の効果を発生させる書面として取り扱われることはなく、法律上の効果を発生させるのはあくまで当事者間で行われた契約であると理解しているが、その理解は正しいか。
- その理解で問題ない。ただ、パート２の内容は契約で盛り込まれる項目である一方で、パート１の内容は契約に盛り込まれることはなく、また、パート１の取組項目については主に医療機関が責任を負う、といった旨が契約において明示されることもないと思われる。その前提で、インシデントが発生し損害賠償請求訴訟が提起された場合、パート１の取組項目については医療機関が一義的な責任を負うことの証拠として、ベンダが裁判所に今回のチェックリストを提出するといった使われ方をされるおそれがある。具体的には、例えば、パート１のＢの４で上げられている病院職員の教育・研修に関しては、勿論病院の責任において実施すべきであるが、病院だけでは完結せず、ベンダから情報提供や研修への参画といった協力のもとに実施されることが自然であるように思う。そのような観点も踏まえ、パート１の位置付けを考えていく必要がある。

■ 実際に発生しているインシデントの事例をみると、医療機関側としての全体的な対応を統括する窓口が置かれていなかったことが課題として多く挙げられている。そのような観点で今回のチェックリストをみると、パート１のＢの１や２において、はじめから安全管理のための体制としてぶつ切りの体制構築が推奨されているような印象を受ける。安全管理の前に、システム保守契約をきちんと締結する、あるいは、クラウドの設定を一元的に引き受けてくれるようなマネージドサービス事業者を活用するといったことを医療機関に促す項目があるとありが

たい。

- 今回のチェックリストは契約時の協議事項や留意事項を示すものであるため、コメントいただいたような項目はないが、厚労省の安全管理ガイドラインで明示的に記載されているので、そちらを参照いただきたいと思う。

■ 契約時におけるチェックリストの実際的な使われ方として、パート１の内容は、ベンダから医療機関の責任において実施すべき旨の認識が医療機関にあるかを問い、これに対して医療機関が認識している旨を書面にて回答するといったやり取りが想像できる。今回のチェックリストが責任分界点を見極めるためのものであるならば、本来事業者の責任において実施すべき取組項目を挙げるパート３を設け、当事者を入れ替えた形で上記のやり取りを行うこととし、パート２の内容は必要最小限として、医療機関とベンダとの間の責任分界点を明快に示していただきたい。

- 個人的には、今回のチェックリストでは、コメントいただいたようなパート３は存在し得ないと考えている。
- 今回のチェックリストは、パート１が専ら医療機関において責任を負うべき取組項目、パート２が医療機関とベンダの両者において責任を負うことが考えられる取組項目、として、章の区切りを責任分界点と見立てているのではない。あくまでもパート１、パート２において、医療機関とベンダの間で協議の上、責任分界点を決めていただく必要がある項目を挙げているものである。パート１とパート２の違いについては、現行案では分かりにくい部分があるため、今後整理する。（厚労省）

■ 資料３の p.2 で責任分界の「界」の字が「解」となっているので修正が必要。

- ご指摘のとおり修正する。

■ 責任分界を定めるためのチェックリストであれば、項目はより具体的な記載とするのが好ましいが、パート１が有事の際に医療機関側の責任を法的に根拠付ける資料として使われ得るという事態は心配である。

- パート１がそのような使われ方をされるとは考えにくい。
- このチェックリストの項目によって、医療機関の責任が法的に根拠付けられることはない。ただ、そのような心配をされないためにも、書きぶりに関しては注意を払うようにしたい。（厚労省）

■ 例えば、医療機関と直接契約関係にあるベンダとそうでないベンダとの間、あるいは、既に医療機関にシステム・サービスを提供しているベンダと新規に提供を行うベンダとの間においても、責任分界を定めることが必要である以上、ベンダ間の責任分界を定めるためのパート３を設ける必要があるのではないか。

- ベンダ間で責任分界がきちんと定められているかについては、２省ガイドラインの中で、ベンダにおいて実施すべき内容として記載しており、医療機関としては、いわゆるプライムのベンダにその実施状況を確認するほかなく、責任範囲に関して細かいところまで把握することはできないと思われる。
- パート２ではベンダ間でも責任分界を定めるべき旨の項目がないが、必要ではないか。
- パート２の A の１において、プライムのベンダがいる場合に、当該ベンダと関係する他のベンダとの間で責任分界を取り決めるべき旨を記載している。（厚労省）
- プライムの定義とは何か。医療機関としては、ベンダ間で責任分界に関して話し合い、取り決めた結果の報告を受ける必要があるのではないか。特に、異なるベンダから小さいシステムを多数導入している医療機関においては、その必要性が高いと思われる。例えば、新規に医療機関にシステム・サービスを提供するベンダは、既に提供を行っているベンダに対して一度はコンタクトを取り、相互に責任分界を定めた上で、その結果を踏まえて、医療機関が新規に参入するベンダを利用するか決めるといった工程を踏むことが重要ではないか。

- プライムのベンダとは、複数事業者を取りまとめる事業者である想定している。（厚労省）
- プライムのベンダがどこであるかを決めるのは医療機関の責任であり、新規のベンダに対して、既存のベンダと協議するよう指示するのも医療機関の役割である。現実問題として、医療機関がそれを決めるのは難しいと思うが、そうであるからといって、知らないベンダ同士が医療機関のあずかり知らぬところで勝手に話し合うと、むしろ医療機関にとって不利益な結果を招くことになる。
- ベンダが相互に話し合い、その結果責任分界をきちんと取り決めたという状況でなければ、医療機関は安心して新規のベンダを利用することができないと思う。
- 工夫するが、ベンダが実施すべき内容として位置付けるのは難しいのではないかと考えている。

■ 中小規模の医療機関が恐れているのは、近年発生しているサイバーインシデントの発生によって大きな損害を被った際、ベンダにも一部損害を補填してもらえるのかといった、損害賠償に関する具体的なところである。どのようなケースであればベンダに責任が認められるのかといった、具体的なシチュエーションを盛り込んでほしいという意見が医療機関から挙げられている。

- 損害賠償に関する議論は、今回のチェックリストの検討趣旨と少しずれる。
- 損害の発生時に、ベンダと医療機関のどちらに賠償責任が認められるかはケースバイケースであり、例示として示すのは難しい。今回のチェックリストの検討趣旨から外れるものである。（厚労省）

■ 今回のチェックリストは、あくまでトラブルの発生を予防するために意識すべき項目を挙げる趣旨であるというのは理解できるが、実際にこのチェックリストが最も活きるのは、損害の発生時における金銭的補償範囲の画定時であり、責任分界という言葉が使われている以上、そのような用途で扱われる可能性が高い。

■ 厚労省としては、今回のチェックリストの項目を一つずつ、医療機関とベンダとの間で確認していくという使われ方ではなく、事前に両者間でチェックリストを確認した旨を確認し合い、その後契約に至るという使われ方を想定しているのではないか。

- 前者の使われ方を想定している。一つ一つの項目について、医療機関とベンダがそれぞれにどこまで担保できるのかを協議いただきたいという趣旨である。（厚労省）

■ 現実問題として、医療機関とベンダとの間で発生しているようなサイバー攻撃によって発生した損害の補償に関する問題は、２省ガイドラインの改定検討において議論するのが適当ではないか。

- ご指摘のとおり、少なくとも今回のチェックリストの議論の射程からは外れるものと考えている。そもそも、悪意ある攻撃によって損害が発生した場合、医療機関やベンダにおいて重大な瑕疵・過失が認められない限り、損害賠償責任を負うのは本来攻撃者であって、医療機関やベンダはいずれも被害者であることから、被害者間でどちらが責任を負うかを協議するというシーンは想定していない。

■ 医療機関において管理すべき情報を保管するためのシステムについては、その選定・管理・運用に関して責任を負うのが医療機関であることは勿論であるが、医療機関のリソースが限られている場合には、これらの一部を外部に委託することも想定されるため、その場合、委託範囲の画定やベンダ間の調整等に関しても医療機関が責任を負うことになると考えている。

■ IPA が一般の情報システム構築・運用に関するモデル契約書を公表しているが、このモデル契約書が想定しているシーンでは、セキュリティに関して、利用者とベンダとの間で議論し、セキュリティ仕様書という形で合意をまとめることとしており、その作成に必要な取組事項として、公的なガイドを参照したり、利用者においてリスク評価を行ったり、ベンダにおいてコスト等の試算を行ったりといったことを具体的に、細かく提示している。これと同様に、今回のチェックリストでもより細かく取組事項を記載した方が良いのではないか。例えば、パート１の A の

１にベンダの選定に関する項目があるが、これを読んだ医療機関が具体的にどのように選定すべきか分かりづらい。既存の実践的なガイドに参照を飛ばすなど、より使い勝手を良くするための工夫をしていただきたい。

- いただいたご意見はそのとおりであると考えている。ご意見を踏まえ、どのように修正できるか検討したい。（厚労省）

■ パート１の内容は医療機関がチェックし、念のためベンダに対して、これで良いかと確認し、ベンダが確認するという使われ方、パート２の内容は医療機関とベンダが相互に確認し、すべて確認完了した上で契約するという使われ方というイメージで良いか。そのイメージを、より具体的な形でどこかに明示して欲しい。

■ 各項目について、具体的にどのように取り組めば良いのかを示していただけるとありがたい。医療機関もベンダも慣れていない同士では、具体の例示がないと話が進まない。

■ パート２のＡの４は削除した方が良いかもしれない。パート２のＡの４では、ベンダが医療機関にサービス仕様適合開示書を提示し、これを参照して医療機関がベンダを選定し、契約を結ぶという流れが想定されているが、パート１のＡの１においても部分的に同趣旨のことが記載されている。そもそも医療機関によるベンダの選定は、契約上の責任分界を取り決める時点よりも前の話であって、特定のベンダが主体になり得ないことから、パート１に集約するのが適切と考える。

- パート２ではベンダにおいてサービス仕様適合開示書や SDS・MDS を作成することを定め、パート１ではそれを受けて医療機関においてベンダを選定するということで、重複している部分はないと思う。
- パート１とパート２で挙げられている文書に重複・不足があるため、その点は、並びを取る形で修正する。（厚労省）

■ 中小規模の医療機関にはシステムに詳しくない職員が多いため、チェックリストではなるべく平易な言葉を使用して欲しい。

■ 今回のチェックリストは項目が多岐にわたる。細かく規定するほど安全ではあるが、その分対応できない医療機関が増えることから、その点の配慮もお願いしたい。

- チェックリスト・コンセプトペーパーの両者ともに、平易な言葉を使う形にしたい。

■ 資料５では、２省ガイドラインも並行して改定検討を進めているとの説明があった。今回のチェックリストは２省ガイドラインを参照しているが、改定のタイミングはいつになるのか。

- 経産省・総務省との間では、今年度改定が行うのは難しいのではないかという見立てをしている。少なくとも、現行の２省ガイドラインに適合する形で今回のチェックリストを作成する。（事務局）
- 今回のチェックリストの内容を必要に応じて見直すこととするというのは、２省ガイドラインの改定に対応してという趣旨か。
- 少なくとも、２省ガイドラインの附属資料である SLA 参考例は今年度改定するので、これは今回のチェックリストにも反映させる予定である。その他、チェックリストに影響を与え得るようなガイドラインの改定があった場合には、適宜チェックリストにも反映させる。

以上

＜お問い合わせ先＞
商務・サービスグループ　ヘルスケア産業課
電話：03-3501-1790