別紙２

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（案）

令和２年３月

目次

1. 本ガイドラインの基本方針 1
1.1. 本ガイドライン策定の経緯 1
1.1.1. 医療情報に関する法整備 1
1.1.2. 医療情報安全管理ガイドライン 2
1.1.3. 総務省・経済産業省ガイドライン 2
1.1.4. 状況の変化に対する改訂の必要性 3
1.2. 本ガイドラインの策定方針 3
1.3. 本ガイドラインの構成 4
2. 本ガイドラインの対象 6
2.1. 本ガイドラインが対象とする医療情報と事業者 6
2.2. 医療情報システムの代表的な提供形態 7
2.2.1. 1社で提供するケース 8
2.2.2. 複数の事業者が提供するケース 8
2.2.3. 医療機関等が複数社と契約するケース 10
3. 医療情報の安全管理に関する義務・責任 11
3.1. 法律関係 11
3.1.1. 安全管理義務 11
3.1.2. 対象事業者の説明義務 13
3.1.3. 事後責任 13
3.2. 医療情報システムのライフサイクルにおける義務と責任 14
3.2.1. 契約前の合意形成及び契約中の合意の維持 15
3.2.2. 通常時の義務 16
3.2.3. 危機管理対応時の義務及び責任 16
4. 対象事業者と医療機関等の合意形成 18
4.1. 医療機関等へ情報提供すべき項目 18
4.2. 医療機関等との役割分担の明確化 19
4.3. 医療情報システムの安全管理に係る評価 20
4.4. 第三者認証等の取得に係る要件 20
5. 安全管理のためのリスクマネジメントプロセス 21
5.1. リスクマネジメントの実践 22
5.1.1. リスク特定 22
5.1.2. リスク分析 24
5.1.3. リスク評価 24
5.1.4. リスク対応の選択肢の選定 25
5.1.5. リスク対応の実施手順 27
5.1.6. リスクコミュニケーション 30
5.1.7. 継続的なリスクマネジメントの実践 32
5.2. リスクアセスメント及びリスク対応の実施例 32
5.2.1. リスクアセスメント 33
5.2.2. リスク対応 42
6. 医療分野における制度上の要求事項 44
6.1. 医療分野の制度が求める安全管理の要求事項 44
6.2. 電子保存の要求事項 44
6.3. 法令で定められた記名・押印を電子署名で行うことについて 45
6.4. その他取扱いに注意を要する文書等について 45

6.5.　外部保存の要求事項..... 45
用語集..... 46

1. 本ガイドラインの基本方針

1.1. 本ガイドライン策定の経緯

1.1.1. 医療情報に関する法整備

医療情報については、古くから診療録等の保存義務が法令上規定されてきた（医師法 24 条、医療法 21 条 1 項 9 号、保険医療機関及び保険医療養担当規則 22 条等）。その条文の文言上、電子媒体による保存を明確に排除しておらず、また、保存場所についても特に明示的な規定を定めていない。平成 11 年 4 月の通知「診療録等の電子媒体による保存について[1]」及び平成 14 年 3 月の通知「診療録等の保存を行う場所について[2]（以下、「外部保存通知」という。）」によって、診療録等の電子保存及び保存場所に関する要件等の解釈が明確化された。それぞれの通知に対して、「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン[3]」及び「診療録等の外部保存に関するガイドライン[4]」が示された。

さらに、法令等で作成又は保存が義務付けられている書面を電子的に取り扱うことを可能とする「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成 16 年法律第 149 号。以下、「e-文書法」という。）が平成 16 年 11 月に成立した。医療情報について上述の通り、電子保存は排除されていなかったが、改めて e-文書法の適用対象と整理され、「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」（平成 17 年厚生労働省令第 44 号）が制定された。

また、平成 15 年に「個人情報の保護に関する法律」（平成 15 年法律第 57 号。以下、「個人情報保護法」という。）が成立し、安全管理措置を講ずる義務（個人情報保護法 20 条）、従業者・委託先の監督義務（同 21 条、22 条）が規定され、情報セキュリティ[5]に関する義務が明確になった。医療・介護分野においては、平成 16 年 12 月に「医療・介護関係事業者における個人情報の適切な取扱のためのガイドライン」が公表されている。

---

[1] 平成 11 年 4 月 22 日付け健政発第 517 号・医薬発第 587 号・保発第 82 号厚生省健康政策局長・医薬安全局長・保険局長連名通知。民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成 17 年 3 月 31 日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知）にて廃止

[2] 平成 14 年 3 月 29 日付け医政発 0329003 号・保発第 0329001 号厚生労働省医政局長・保険局長連名通知

[3] 平成 11 年 4 月 22 日付け健政発第 517 号・医薬発第 587 号・保発第 82 号厚生省健康政策局長・医薬安全局長・保険局長連名通知に添付

[4] 平成 14 年 5 月 31 日付け医政発第 0531005 号通知に添付

[5] 情報セキュリティとは「情報の機密性、完全性及び可用性を維持すること」（JIS Q 2700 2）と定義されている。機密性、完全性および可用性は、情報セキュリティの 3 要素とされ、頭文字をとって「CIA」と呼ばれる。3 要素のそれぞれの定義は、以下のとおり。

- 機密性（Confidentiality）：認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性
- 完全性（Integrity）：資産の正確さおよび完全さを保護する特性
- 可用性（Availability）：認可されたエンティティが要求したときに、アクセスおよび使用が可能である特性

その後、平成 29 年には、個人情報保護法が改正され、これに伴い医療･介護分野における個別の対応を記した、「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ダンス」が策定された。

1.1.2. 医療情報安全管理ガイドライン

平成 17 年 4 月における、e-文書法の施行、並びに、個人情報保護法の全面施行に対して、厚生労働省では、病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等（以下、「医療機関等」という。）を対象として、平成 17 年 3 月に「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、「医療情報安全管理ガイドライン」という。）を策定した。このガイドラインは、「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」及び「診療録等の外部保存に関するガイドライン」を見直し、さらに、個人情報保護に資する情報システムの運用管理に関わる指針と e-文書法への適切な対応を行うための指針を統合して作成されたものである。その後、医療情報安全管理ガイドラインは、情報システムに関する環境変化や、個人情報保護法の改正を踏まえて改定を重ね、平成 29 年 5 月には第 5 版が策定された。

また、外部保存通知については、平成 14 年の制定時には、外部保存の場所は医療機関が管理する場所に限定されていたが、順次要件が緩和され [6]、平成 22 年改正では民間事業者が設置するデータセンターに保存することが解禁された。これにより、後述する総務省及び経済産業省のガイドラインを遵守する限り、外部保存が許されることが明確化された。

このような一連の施策等により診療録等の情報を電子的に作成し保存することが許容された。また、医療情報安全管理ガイドラインは、国民健康保険法等に基づく健康保険制度の保険診療点数表において引用されており、保険医療機関としても遵守が求められている。

1.1.3. 総務省・経済産業省ガイドライン

総務省及び経済産業省では、医療情報を電子的に作成し保存する際の安全を確保するため、医療情報を取り扱う情報システムやサービス（以下、「医療情報システム」という）を提供する事業者に対して、ガイドラインをそれぞれ策定した。

具体的には、総務省では、ASP･SaaS 事業者を対象として、平成 20 年 1 月に「ASP･SaaS における情報セキュリティ対策ガイドライン」（以下、「ASP･SaaS セキュリティガイドライン」という。）を、平成 21 年 7 月に「ASP･SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（以下、「ASP･SaaS 事業者ガイドライン」という。）を策定した。

---

[6] 「「診療録等の保存を行う場所について」の一部改正について」（平成 17 年 3 月 31 日付け医政発第 0331010 号・保発第 0331006 号厚生労働省医政局長・厚生労働省保険局長通知）
「「診療録等の保存を行う場所について」の一部改正について」（平成 22 年 2 月 1 日付け医政発 0201 第 2 号・保発 0201 第 1 号厚生労働省医政局長・厚生労働省保険局長通知）

さらに、平成 30 年 7 月には、ASP･SaaS セキュリティガイドラインにおける医療情報に関する内容と ASP･SaaS 事業者ガイドラインの内容を 1 つのガイドラインに統合するとともに、ガイドラインの対象を ASP･SaaS 事業者だけではなく PaaS や IaaS 等のクラウドサービス事業者も対象とする形で、「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（以下、「クラウド事業者ガイドライン」という。）を策定した。

また、経済産業省では、情報処理事業者を対象として、平成 20 年 7 月に「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」（以下、「情報処理事業者ガイドライン」という。）を策定した。その後、情報処理事業者ガイドラインは、医療情報安全管理ガイドラインの改定や ASP･SaaS 事業者ガイドラインの策定等を踏まえて、それらと整合性をとる形で、平成 24 年 10 月に第 2 版が策定された。

このような経緯から、医療情報の安全管理については、厚生労働省が策定した医療情報安全管理ガイドライン、総務省が策定したクラウド事業者ガイドライン並びに経済産業省が策定した情報処理事業者ガイドラインからなる、いわゆる 3 省 3 ガイドラインにより、必要な対策等が規定されてきた。

1.1.4. 状況の変化に対する改訂の必要性

近年、医療情報の安全管理を取り巻く環境は大きく変化している。具体的には以下の 3 点の変化が挙げられる。

第一に、多くの情報サービスが医療情報の外部保存を含んだクラウドサービスとして提供されている。医療情報の外部保存をクラウドサービスとして提供する事業者は、クラウド事業者ガイドラインと情報処理事業者ガイドラインの両方を参照しなければならないが、これらのガイドラインは、対策等を記載する観点が異なっていたため、事業者にとって双方のガイドラインへの対応が大きな負担となってきている。

第二に、情報処理技術の普及やサイバー攻撃の高度化に伴い、情報セキュリティを確保するための要求は拡大するとともに多様化している。3 省のガイドラインが策定された当初は、詳細な要求事項を定めていたが、今日の環境では、一律に定めた要求事項の全てに対応することは困難になってきている。

第三に、ISO/IEC 27001、 ISO/IEC 27002、ISO/IEC 27005、ISO/IEC 27017、ISO/IEC 27018 等の情報セキュリティに関する規格や、クラウドサービス提供における情報セキュリティ対策ガイドライン（平成 30 年 7 月 総務省）等の情報セキュリティに関するガイドラインが整備され、事業者はそれらの規格・ガイドラインとの整合性の確保も留意しなければならなくなってきている。

1.2. 本ガイドラインの策定方針

以上の変化を踏まえ、クラウド事業者ガイドラインと情報処理事業者ガイドラインが求

める要件を以下の方針に従い整理・統合する。

- 他の規格・ガイドラインとの整合性の確保に留意しながら、過去のガイドラインの遵守と同等の安全管理水準が確保されるようにする
- 医療情報システムの特性に応じた必要十分な対策を設計するために、一律に要求事項を定めることはせず、リスクベースアプローチに基づいたリスクマネジメントプロセス[7]を定義する
- セキュリティ対策の妥当性と限界について正しい共通理解と明示的な合意[8]のもと医療情報システムを運用するために、リスクコミュニケーションを重視する
- 医療情報システムに関連する法令の求めに対して対策の抜け漏れを防止するために、医療情報の取扱いにおいて留意すべき点や制度上の要求事項を明らかにする

以上の方針に従ってガイドラインを理解しやすくすることにより、確実な対策の実施を図るとともに、医療情報の効果的・効率的な安全管理の実現を目指す。

1.3. 本ガイドラインの構成

本ガイドラインの全体構成は以下の通り。

第 1 章では、本ガイドラインの策定の経緯や目的、策定方針について記載した。

第 2 章では、本ガイドラインが対象とする事業者及び想定される主要な医療情報システムの提供形態について記載した。

第 3 章では、医療情報の安全管理に関する義務・責任として、事業者に求められる義務と責任の考え方について整理している。ここでは、医療情報システムのライフサイクルを整理し、想定される義務と責任について記載した。

第 4 章では、医療機関等への情報提供と合意形成の対象について記載している。事業者は自らのリスク分析結果に基づく対応策について、医療機関等に対して情報提供した上で、合意形成を行うことが求められる。本章では、この際の考え方について記載した。

第 5 章では、安全管理のためのリスクマネジメントプロセスとして、リスクマネジメントの実践による対策決定のための手順を記載している。また、医療情報システムの提供形態に応じたリスクアセスメントとリスク対応の実施例を記載した。

---

[7] 本ガイドラインにおけるリスクマネジメントのプロセスは JIS Q 31000:2019 や JIS Q 27001:2014 等のリスクマネジメントの標準的なプロセスを参考としている。

[8] 「共通理解（Common understanding)」と「明示的な合意（Explicit agreement)」については、変化に対応して情報システム・サービスを継続的に提供するための指針である Open System Dependability（OSD）の考えに基づく国際標準 IEC 62853 における用語を参考としている。

第 6 章では、医療分野における制度上の要求事項として、第 5 章にて記載したリスクマネジメントに基づく対応とは別に、法令等の制度上の要求事項への遵守の観点から、事業者に対して一律の対応を求める事項を記載した。

また、本ガイドラインでは、第 4 章に基づく医療機関等との情報提供と合意形成にあたって活用することを想定した「別紙 1 サービス仕様適合開示書及び SLA の参考例」（以下、「別紙 1」という。）及び第 5 章に基づくリスクマネジメントの実践において事業者が確認する内容として、「別紙 2 旧ガイドラインにおける対策項目一覧と医療情報安全管理ガイドラインの対応表」（以下、「別紙 2」という。）を用意している。

2. 本ガイドラインの対象

2.1. 本ガイドラインが対象とする医療情報と事業者

本ガイドラインが対象とする医療情報は、「医療に関する患者情報（個人識別情報）を含む情報」である。この定義は医療情報安全管理ガイドラインにおける定義と同一である。医療情報には、医療従事者が作成・記録した情報のほか、医療従事者の指示に基づき介護事業者が作成・記録した情報がある。これらの医療情報は、その情報を作成・記録した者が所属する医療機関等で保管される場合や、その医療機関等から他の医療機関等に提供される場合のほか、患者等（患者本人のほか、患者の家族等で、患者の医療情報を閲覧する権限を有する者を含む。以下同じ）に提供される場合が想定される。

本ガイドラインが対象とする事業者は、医療機関等との契約等に基づいて医療情報システムを提供する事業者（以下、「対象事業者」という）である[9]。ただし、医療機関等と直接的な契約関係になくても、医療機関等に提供する医療情報システムに必要な資源や役務を提供する事業者や、患者等の指示に基づいて医療機関等から医療情報を受領する事業者は本ガイドラインにおける対象事業者[10]となる。

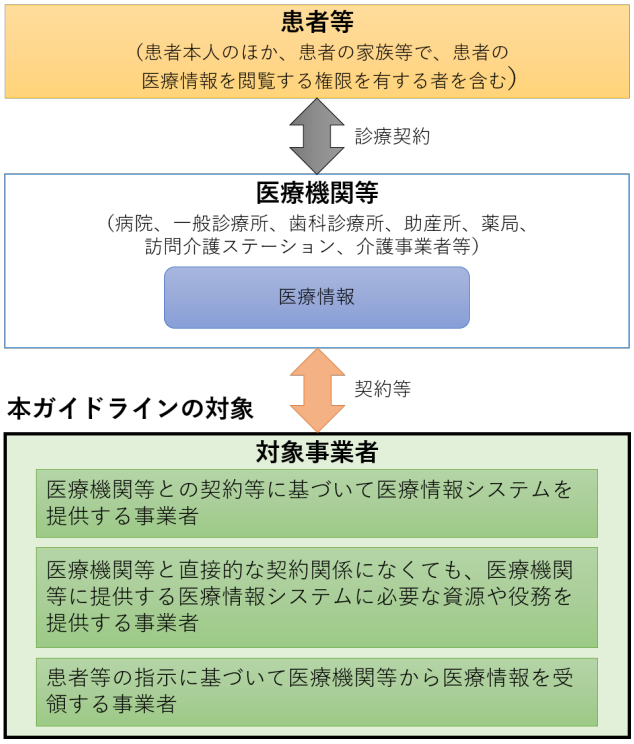

図 2-1　本ガイドラインの対象とする事業者

[9] クラウド事業者ガイドラインが対象としていた事業者及び情報処理事業者ガイドラインが対象としていた事業者は、引き続き対象範囲となる。
[10] 患者等から直接医療情報を受領する事業者は、本ガイドラインにおける対象事業者にはあたらない。

対象事業者は本ガイドラインに基づくリスクマネジメント及び制度上の要求事項への対応が求められ、医療機関等に提供する医療情報システムに必要な資源や役務の提供に係るサプライチェーン全体について、本ガイドラインで記載するリスクマネジメント及び制度上の要求事項に対応すること。

ただし、医療機関等と直接的な契約関係はなく、医療機関等に提供する医療情報システムに必要な資源や役務を提供する事業者は、契約元の対象事業者（一次請けだけでなく二次請け以降の場合もある）の求めに応じて、リスクマネジメント及び制度上の要求事項への対応状況を報告すること。また、患者等の指示に基づいて医療機関等から医療情報を受領する事業者は、医療機関等の求めに応じて、リスクマネジメント及び制度上の要求事項への対応状況を報告すること。

2.2. 医療情報システムの代表的な提供形態

本節では医療情報システムの代表的な提供形態を示し、対象事業者に求められる対応について記載する。

医療情報システムの構成要素をアプリケーション、プラットフォーム、インフラの 3 種類に分類した。その上で、各構成要素毎の提供形態を A1～A3、P1～P3、I1～I3 に類型化した（図 2-2）。次節以降において、医療情報システムの代表的な提供形態を構成要素の類型の組み合わせとして取り上げる。

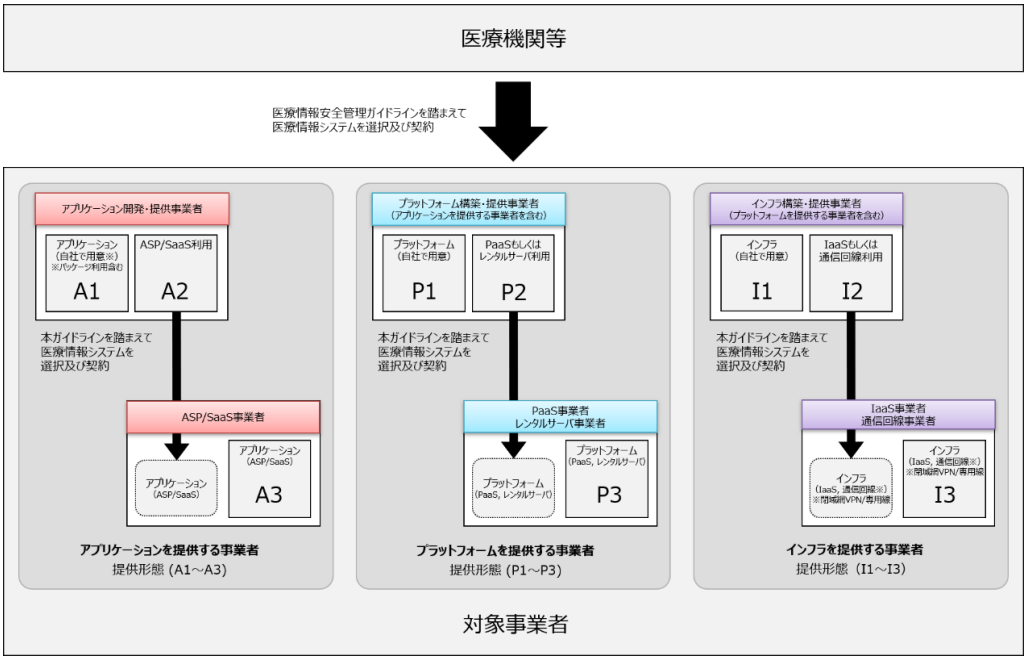

図 2-2　医療情報システムの構成要素の類型

2.2.1.　1 社で提供するケース

対象事業者 A が 1 社で医療情報システムを提供するケース（図 2-3）。

医療機関等との直接的な契約関係にある対象事業者 A は、自社の医療情報システムについて、本ガイドラインに基づきリスクマネジメント及び制度上の要求事項への対応を行うこと。

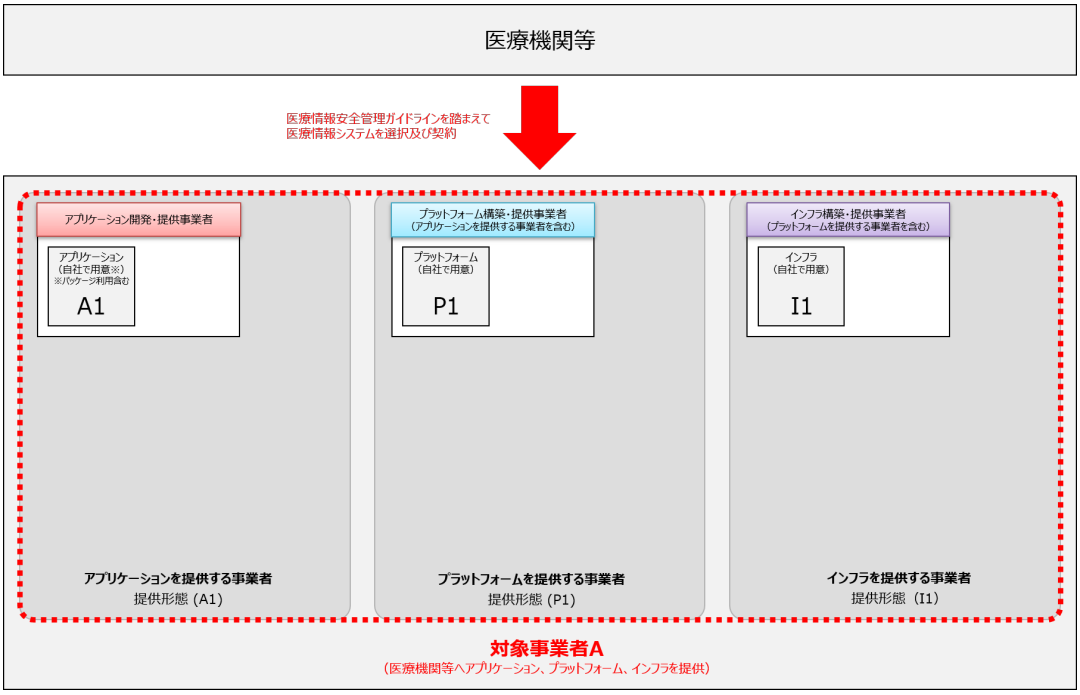

図 2-3　1 社で提供するケース（A1＋P1＋I1）

2.2.2.　複数の事業者が提供するケース

例えば、以下 2 つのケースが想定される。

【ケース 1】

対象事業者 A が対象事業者 B のインフラを調達するケース（図 2-4）

【ケース 2】

対象事業者 A が対象事業者 B のプラットフォーム及びインフラを調達し、さらに対象事業者 B が対象事業者 C のインフラを調達するケース（図 2-5）

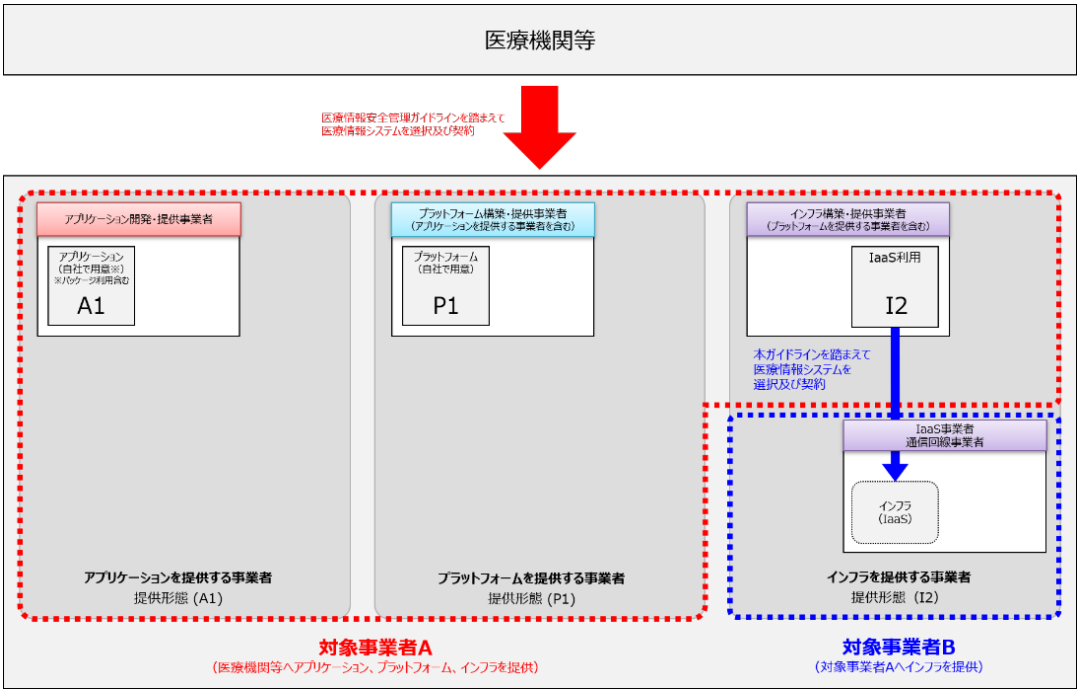

図 2-4　2 社で提供するケース（A1＋P1＋I2）

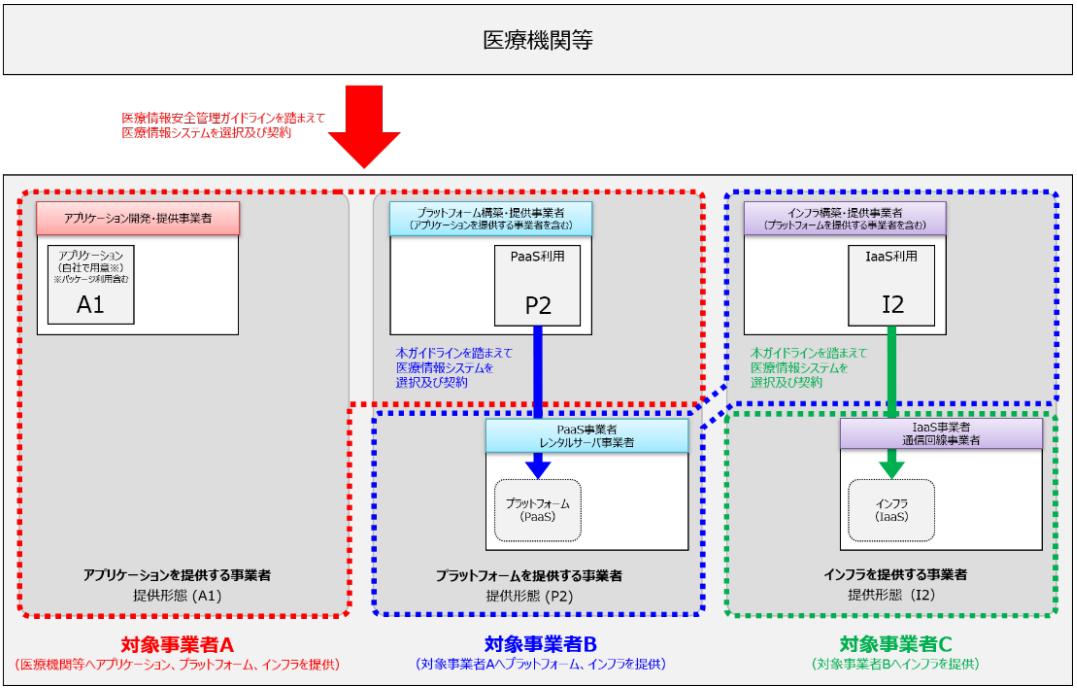

図 2-5　3 社で提供するケース（A1＋P2＋I2）

ケース 1、ケース 2 いずれにおいても、対象事業者 A は、医療機関等との直接的な契約関係にあるため、自社の医療情報システムについて、本ガイドラインに基づきリスクマネジメント及び制度上の要求事項への対応を行うこと。加えて、他の対象事業者 B、対象事業者 C から調達する構成要素に対しても、本ガイドラインに基づきリスクマネジメントを実施し、制度上の要求事項に対応すること。

このうち、ケース 1 では、対象事業者 A は、対象事業者 B の選定を行うとともに、対象事業者 B から調達する構成要素を含めてリスクマネジメント及び制度上の要求事項に対応すること。これに対して、ケース 2 では、対象事業者 A は対象事業者 B の選定を行うとともに、対象事業者 B 及び対象事業者 C から調達する構成要素を含めてリスクマネジメント及び制度上の要求事項に対応すること。

対象事業者 B は対象事業者 A に、対象事業者 C は対象事業者 B に対して、リスクマネジメントの実施状況と制度上の要求事項への対応状況を報告すること。

2.2.3. 医療機関等が複数社と契約するケース

対象事業者 A、対象事業者 B はそれぞれ独立して自社の医療情報システムについて本ガイドラインに基づくリスクマネジメント及び制度上の要求事項への対応を行い、医療機関等へ医療情報システムを提供すること。また、本ケースにおいては、対象事業者 A は、対象事業者 B の選定と管理について義務を負わないが、本ガイドラインが求める対応の対象範囲に、対象事業者 B が提供する構成要素を含めること。

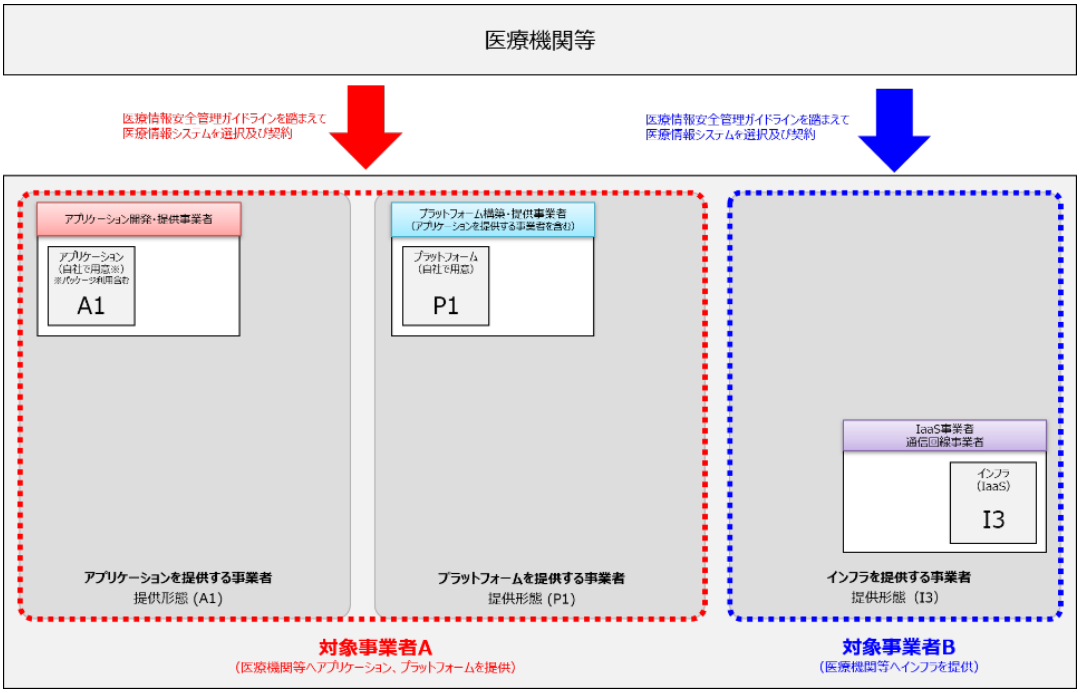

図 2-6　医療機関等が複数社と契約するケース（A1＋P1＋I3）

3. 医療情報の安全管理に関する義務・責任

本章では、医療機関等及び対象事業者がそれぞれ負う義務と責任を法律に基づいて整理する。また、医療情報システムのライフサイクルを構成する要素ごとに義務と責任を説明する。

3.1. 法律関係

3.1.1. 安全管理義務

(1) 善管注意義務と守秘義務

患者と医療機関等は、診療契約を締結し、医療機関等は診療契約（準委任契約）上の善管注意義務を負う。患者は、診療契約に基づいて、医療機関等に自己の医療情報を委ねているといえるため、医療機関等は、善管注意義務の一内容として、情報を適切に取り扱う義務を負っている。

また、医師等の医療従事者は、患者に対し、刑事上の守秘義務（刑法 134 条等）を負っている。医療機関等も、患者に対し守秘義務を負っていると解釈されている。この医療従事者及び医療機関等の患者に対する守秘義務は、故意による情報開示・漏洩だけではなく、過失による情報開示・漏洩も対象としていると解される。

このように、医療機関等は、患者に対して善管注意義務及び守秘義務を負っており、その内容は重なりあう。そして、いずれも適切なセキュリティ体制を構築、維持、運用する義務（以下、「安全管理義務」という。）を含む。

また、対象事業者は、医療機関等と委託契約を締結しているが、これが準委任契約である場合は、医療機関等に対し善管注意義務を負う（民法 644 条）。契約の形式が準委任契約でない場合（請負契約等）においても、医療情報の取扱いを委託する以上、当該委託契約には他人の事務の処理の委託関係という準委任契約の要素が含まれており、対象事業者は、善管注意義務又はこれと実質的に類似の義務を負う。また、契約上、守秘義務が規定されるのが一般的である。このような善管注意義務及び守秘義務には、契約内容及びその解釈によって定まる一定の事項についての安全管理義務が含まれる。

したがって、対象事業者は、医療機関等に対し、一定の事項についての安全管理義務を負っており、患者との関係では、医療機関等の患者に対する安全管理義務（の一部）の履行補助者の地位に立っている。

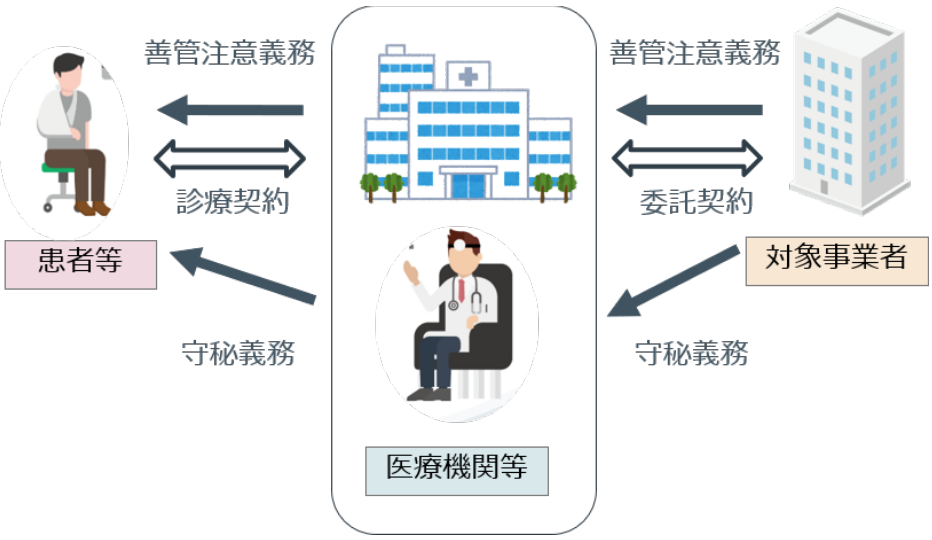

図 3-1 善管注意義務と守秘義務について

(2) 安全管理措置を講じる義務

個人情報保護法では、委託元である医療機関等と委託先である対象事業者が、それぞれ安全管理措置を講じる義務を負う。そして、委託元には、委託先を監督する義務（以下、「監督義務」という。）があると規定されている（個人情報保護法 22 条）。

監督義務の内容としては、①適切な委託先の選定、②委託契約の締結、③委託先における個人データ取扱状況の把握という 3 点が挙げられている[11]。

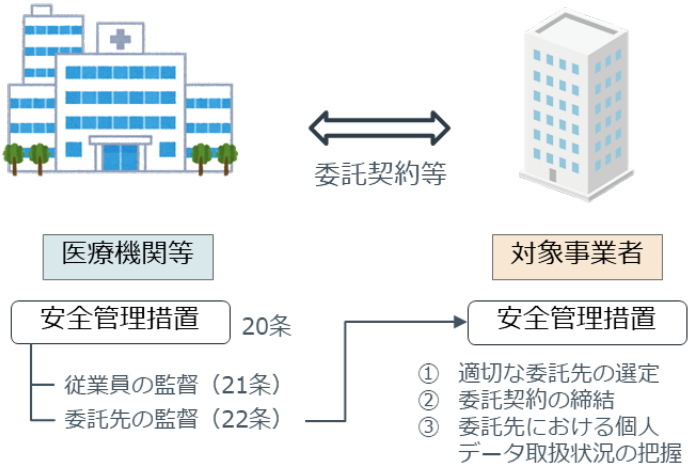

図 3-2 安全管理措置を講じる義務について

[11] 「個人情報の保護に関する法律についてのガイドライン（通則編）」

これらは、行政法規である個人情報保護法等に定められた安全管理義務であり、民事上の安全管理義務を補完するものである。

3.1.2. 対象事業者の説明義務

医療機関等は、上記①～③のために適切に情報を取得する必要がある。しかし、医療機関等は医療の専門機関であって、セキュリティについての専門性は乏しいことが十分に想定される。これに対し、対象事業者は、医療機関等に対し専門的な医療情報システムを提供する事業者であり、セキュリティに関する専門的な知識・経験・人材を擁しているべきである。

このような専門性の格差に鑑みて、対象事業者は、医療機関等に対し、委託契約又は信義則に基づく付随義務として、医療機関等が患者に対する安全管理義務を履行するために必要な情報を適時適切に提供する義務（以下、「説明義務」という。）を負う[12]。

3.1.3. 事後責任

(1) 危機対応義務

個人情報保護法に規定はないが、「個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第 1 号）」を参考に、必要な対策を講ずることが望まれる。

(2) 民事責任

情報漏洩等のセキュリティ事故が発生し、患者等に被害が生じると、患者等は医療機関等に対し、契約責任または不法行為責任に基づき損害賠償を請求することがある。また、患者等は、直接の契約関係がない対象事業者に対しても、不法行為責任に基づき損害賠償を請求する可能性がある。

契約責任の場合、事業者がいかなる債務を負っていたのかという、委託契約（サービス提供契約、開発委託契約等）の解釈問題となる。また、不法行為責任の場合、事業者の過失の存否（すなわち、いかなる注意義務を負っていたか）として判断される。

[12] 2020 年民法（債権法）改正に伴い、請負契約における瑕疵担保責任（瑕疵があった場合は、引き渡しから 1 年間の修補、解除、損害賠償）が、契約不適合責任（知った時から 1 年以内に通知、5 年以内に追完、代金減額、解除、損害賠償、消滅時効 10 年）となった。対象事業者は、医療機関等と請負契約を締結する際には、本改正を踏まえた上でセキュリティ条項等について医療機関等と合意形成を図ることが求められる。なお、民法改正を踏まえたセキュリティ条項を含むモデル契約については、別途独立行政法人情報処理推進機構(IPA)より公表予定であり、その報告書を参考とすること。

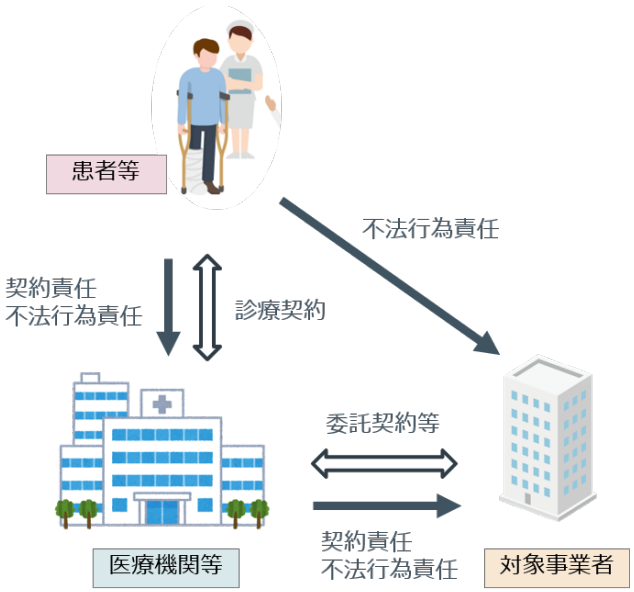

図 3-3 事後の対応における民事責任について

3.2. 医療情報システムのライフサイクルにおける義務と責任

対象事業者が前節で記載した義務や責任に対応するにあたって、全ての医療情報システムに共通な一律の要求事項を定めることは難しい。そのため、対象事業者は自らが提供する医療情報システムを対象とし、リスクマネジメントのプロセスとリスクベースアプローチに基づいて対策をとりまとめ、医療機関等との間で合意を形成することとする。

本節では、一般的に想定される医療情報システムのライフサイクルにおいて対象事業者に求められる義務や責任への対応方法を示す。なお、前節で記載した義務や責任と、本節にて示す内容との対応関係は表 3-1 の通りである。

表 3-1 「3.1. 法律関係」記載内容と本節記載内容の対応関係

「3.1. 法律関係」記載内容	本節記載内容
3.1.1. 安全管理義務	3.2.2. 通常時の義務
3.1.2. 対象事業者の説明義務	3.2.1. 契約前の合意形成及び契約中の合意の維持
3.1.3. 事後責任	3.2.3. 危機管理対応時の義務及び責任

また、本ガイドラインで想定する基本的なライフサイクルの全体像について図 3-4 に示す。

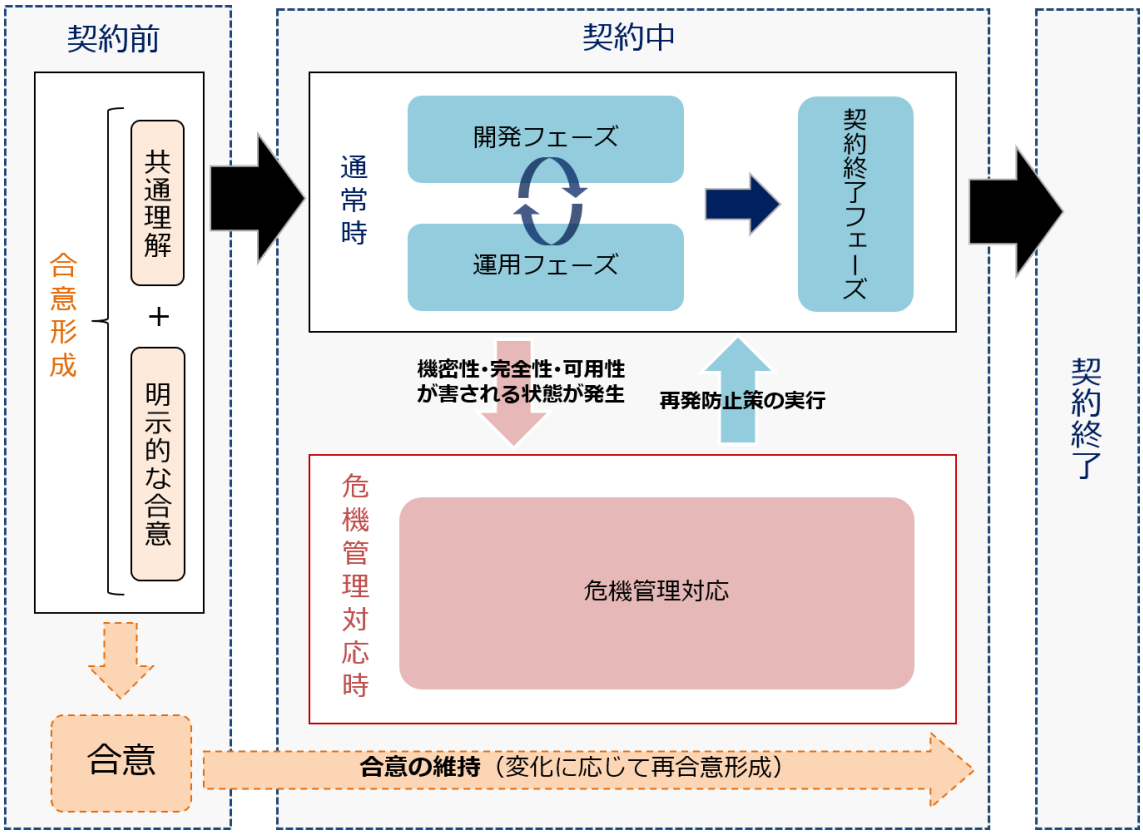

図 3-4 医療情報システムのライフサイクル

3.2.1. 契約前の合意形成及び契約中の合意の維持

対象事業者は説明義務を果たすために、医療機関等との間で「共通理解」と「明示的な合意」の形成を行うこと。

契約前の合意形成において、対象事業者は、4.1 にて示す「医療機関等へ情報提供すべき項目」について、医療機関等と共通理解を形成すること。このとき、対象事業者は、医療機関等との間で適切な共通理解が形成されるよう、ICT やセキュリティに係る専門知識の差異があることを踏まえ、用語集や解説を加える等の工夫に努めること。なお、本ガイドラインにおける「共通理解」とは、契約書や SLA 等の契約上の文書による明示的な合意とは別に、共通の理解を形成することであり、その取組みの記録として議事メモや作業記録等の文書等に残すことは重要である。対象事業者は、医療機関等との共通理解の上で、契約書や SLA 等の契約上の文書を作成し、医療機関等と明示的な合意を形成すること。合意形成にあたって情報提供すべき内容については、4.1 に示す。

また、契約中においても、医療機関等からの要求内容や環境に変化が生じた場合や、情

報事故発生により開発・運用内容等を見直す必要が生じた場合等には、共通理解や明示的な合意に基づく合意形成を改めて実施し、合意を維持すること。

3.2.2. 通常時の義務

通常時の医療情報システムのライフサイクルは「開発フェーズ」「運用フェーズ」「契約終了フェーズ」に分けられる。したがって、対象事業者が必要な対応を抜け漏れなく洗い出すにあたっても、これら 3 フェーズに分け、当該フェーズでの実施内容を踏まえた上で、想定されるリスクや対応方針について整理することが有効である。

「開発フェーズ」は、対象事業者が医療機関等との契約中に、医療機関等に提供する医療情報システムの開発を実施するフェーズである。「開発フェーズ」には新規の開発（新規開発）だけでなく、機器・端末のアップデートや機能更新に伴う開発（保守開発）も含むものとする。したがって、開発フェーズは 1 度のみ発生するとは限らず、運用フェーズから再度開発フェーズに移行することも考えられる。対象事業者は、安全管理義務へ対応するために医療機関等との合意に基づいて医療情報システムの開発と情報の取扱いを行わなくてはならない。

「運用フェーズ」は、対象事業者が医療機関等との契約中に、医療情報システムの運用作業を実施するフェーズである。対象事業者は、安全管理義務へ対応するために、自らが提供する医療情報システムの運用状況等について医療機関等に対して定期的な報告を実施するとともに、実施しているセキュリティ対策に関しては定期的に自己点検し、その結果の報告を必要に応じて実施しなければならない。

「契約終了フェーズ」は、対象事業者が医療機関等との契約中に、医療情報システムに関する契約を終了する際のフェーズである。対象事業者は、安全管理義務へ対応するために、予め医療機関等と合意した手順に則って情報（プログラム等も含む）の返却・移管・破棄を実施しなければならない。また、当該手順に則って情報の返却・移管・破棄を適切に実施したことの証跡を取得しておくことも必要である。

なお、対象事業者が各フェーズで実施する具体的な対応事項については、後述の通り、第 5 章で記載するリスクマネジメントの実践手順に従って洗い出し、医療機関等への情報提供と合意形成を行うこととしている。

3.2.3. 危機管理対応時の義務及び責任

医療情報システムの提供に際しては、特段の問題が発生しないことが本来期待されているが、上述の各フェーズにおける脅威が顕在化した場合、医療情報の漏えいや改ざん、医療情報システムの停止等の情報事故が生じる可能性がある。本ガイドラインでは、このような情報事故が生じ、当該問題への対処が必要となる場合を、危機管理対応時と定義する。

対象事業者は、何らかの情報事故が発生した場合、発生した情報事故に関する詳細な情

報を医療機関等へ提供することとなるが、この際、発生した情報事故の原因・範囲等、医療機関等の管理者が個々の患者、行政機関や社会へ説明・公表するために必要となる情報の収集をサポートできるよう、できる限り詳細な情報を提供するべきである。

また、対象事業者は、発生した情報事故について、速やかに善後策を講じなければならない。さらに、発生した情報事故自体に対応するための施策を講じるに留まらず、同様の情報事故が以降発生しないように再発防止策を医療機関等に提案すること。提案した内容については、医療機関等と適切に合意（再合意）形成を行った上で実行すること。

4. 対象事業者と医療機関等の合意形成

本章では、対象事業者が医療機関等と適切な合意形成を行うにあたり、医療機関等へ情報提供すべき項目、医療機関等との役割分担の明確化、医療情報システムの安全管理に係る評価及び、第三者認証等の取得に係る要件について示す。

4.1. 医療機関等へ情報提供すべき項目

対象事業者と医療機関等の合意形成においては、対象事業者から医療機関等への適切な情報提供が必要である。本節では、合意形成のために提供すべき情報とは何であるかを表4-1 に示す[13]。対象事業者は、これら項目に係る情報提供にあたっては、医療機関等が容易に理解可能となるよう努め、適切に共通理解を得ること。

[13] 情報提供を行う際の文書例として「サービス仕様適合開示書」を別紙 1 に示す。本開示書の作成・提供は必須ではないが、本開示書等と同等の内容について情報提供した上で、適切な共通理解に基づく合意形成を図ることを求める。なお、本節で示す情報提供すべき内容を作成するにあたっては、例えば、保健医療福祉情報システム工業会（JAHIS）が策定する「製造業者による医療情報セキュリティ開示書チェックリスト」があり、当該チェックリストが対象とする医療情報システムを提供する対象事業者においては、当該チェックリストを参考とすることが有効である。また、クラウドサービス情報開示認定機関（特定非営利活動法人 ASP・SaaS・IoT クラウド コンソーシアム）が運営する「医療情報 ASP・SaaS 情報開示認定制度」よる認定を受け、総務省が定める「ASP･SaaS（医療情報取扱いサービス）の安全･信頼性に係る情報開示指針（平成 29 年 3 月 31 日）」を満たした情報提供を行うことも有効である。

表 4-1 医療機関等へ情報提供すべき項目

<table>
<tr><th colspan="2">目的</th><th>情報提供すべき項目</th></tr>
<tr><td colspan="2" rowspan="4">医療機関等が医療情報安全管理ガイドラインに基づき「外部保存を受託する事業者の選定基準」として少なくとも確認する必要がある項目</td><td>医療情報等の安全管理に係る基本方針・取扱規程等の整備状況</td></tr>
<tr><td>医療情報等の安全管理に係る実施体制の整備状況</td></tr>
<tr><td>実績等に基づく個人データ安全管理に関する信用度</td></tr>
<tr><td>財務諸表等に基づく経営の健全性</td></tr>
<tr><td rowspan="13">医療機関等との共通理解を形成するために情報提供すべき項目</td><td>医療機関等との役割分担の明確化（4.2 参照）</td><td>医療機関等の運用管理規程に定める必要がある事項</td></tr>
<tr><td>医療情報システムの安全管理に係る評価（4.3 参照）</td><td>医療情報システムの安全管理に係る評価の結果</td></tr>
<tr><td>リスクアセスメントの成果物（5.1.1、5.2.1 参照）</td><td>医療情報システムの全体構成図</td></tr>
<tr><td>リスク対応の成果物（5.1.5、5.2.2 参照）</td><td>リスク対応一覧</td></tr>
<tr><td rowspan="9">運用管理規程に含める事項（5.1.6 参照）</td><td>医療情報システムの安全管理に係る基本方針</td></tr>
<tr><td>医療情報システムの提供に係る体制</td></tr>
<tr><td>契約書・マニュアル等の文書の管理方法</td></tr>
<tr><td>機器等を用いる場合の機器等の管理方法</td></tr>
<tr><td>リスク対応策の運用方法</td></tr>
<tr><td>事故発生時の対応方法及び医療機関等への報告方法</td></tr>
<tr><td>医療情報を格納する記憶媒体の管理方法</td></tr>
<tr><td>医療情報の外部保存に係る患者等への説明方法</td></tr>
<tr><td>医療情報システムに対する監査の実施方針</td></tr>
<tr><td>医療機関等の管理者からの問い合わせ窓口</td></tr>
<tr><td>制度上の要求事項への対応の成果物（第 6 章参照）</td><td>制度上の要求事項への対応</td></tr>
</table>

4.2. 医療機関等との役割分担の明確化

医療情報システムの安全管理には、対象事業者と医療機関等の双方における適切な運用管理を行うこと。例えば、医療情報システムが堅牢なアクセス制御機能を持っていたとしても、医療機関側の利用者がパスワードを利用端末に貼っていたり、アカウントを複数で共有していたりすれば、医療情報を守ることはできない。

したがって、対象事業者は、合意形成にあたり、医療機関等における運用管理も踏まえた形で、役割分担を定めること。具体的には、4.1 で示した医療機関等の運用管理規程に定める必要がある事項として、医療機関等へ対応を求める内容を含めること。

4.3. 医療情報システムの安全管理に係る評価

対象事業者は、医療情報システムの安全管理の妥当性について、医療機関等と適切な共通理解を得るため、医療情報システムの安全管理に係る評価を行い、評価結果を医療機関等へ情報提供すること。このとき、医療情報システム関連業務に関与する担当者自らが評価を行うと、信頼性及び客観性が低下するため、対象事業者内部の独立した監査部門や第三者機関[14]が評価を行うことが望ましい。

4.4. 第三者認証等の取得に係る要件

医療情報の機微性に鑑み、対象事業者は、医療情報を取り扱う事業者として、最低限の適格性を医療機関等へ示すため、情報セキュリティに係る公的な第三者認証として、プライバシーマーク認定または ISMS 認証[15]を取得すること。なお、医療情報を直接取り扱わない対象事業者の場合においても、プライバシーマーク認定の取得を強く求めるほか、ISMS 認証の取得も望ましい。また、これら以外の公正な第三者の認証等として、セキュリティ管理に係る内部統制保証報告書[16]があり、対象事業者は、プライバシー認定及び ISMS 認証の取得と併せて当該報告書による保証を受けることも望ましい。ただし、これら認証の取得をもって、本ガイドラインが求める安全管理水準を満たすわけではないことに留意すること。

なお、対象事業者が ISMS 認証を取得する場合、その適用範囲（スコープ）は、処理を受託する医療情報の入口から出口まで包括的に設定することが望ましい。また、適用宣言書の開示についても、医療機関等が委託先事業者を選定する際に確認できるよう、医療機関等への開示を前提として記載に配慮するとともに、医療情報を取り扱うために特別に配慮している管理策等を明確にすることが望ましい。

また、対象事業者がプライバシーマーク認定を取得する場合は「保健医療福祉分野のプライバシーマーク認定指針（第 4 版） 」を参照し、遵守に努めることが望ましい 。

---

[14] 第三者機関による評価として、例えば、一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）による、医療情報に関する IT サービスに関するガイドラインへの適合性評価が挙げられる。

[15] ISMS に関する一般的な基準である JIS Q 27001:2014 (ISO/IEC 27001:2013) に基づく認証のほか、クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針である JIS Q 27017:2016 (ISO/IEC 27017:2015)やパブリッククラウドにおける個人情報保護に関する指針である ISO/IEC 27018:2014 に基づく認証等がある。

[16] 日本では公認会計士協会が実務指針を公開した IT 委員会実務指針第 7 号「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持及びプライバシーに係る内部統制の保証報告書」、海外では、米国で実務指針が策定された、サービス・オーガニゼーション・コントロール報告書（「SOC2」）等がある。

5. 安全管理のためのリスクマネジメントプロセス

本章では、医療情報システム特有のリスクに応じて適切な対応を行うためのリスクマネジメントのプロセスを定める。対象事業者は、図 5-1 のプロセスに従い、医療情報システムを提供する際に想定されるリスクを洗い出し、必要な対策をとりまとめること。

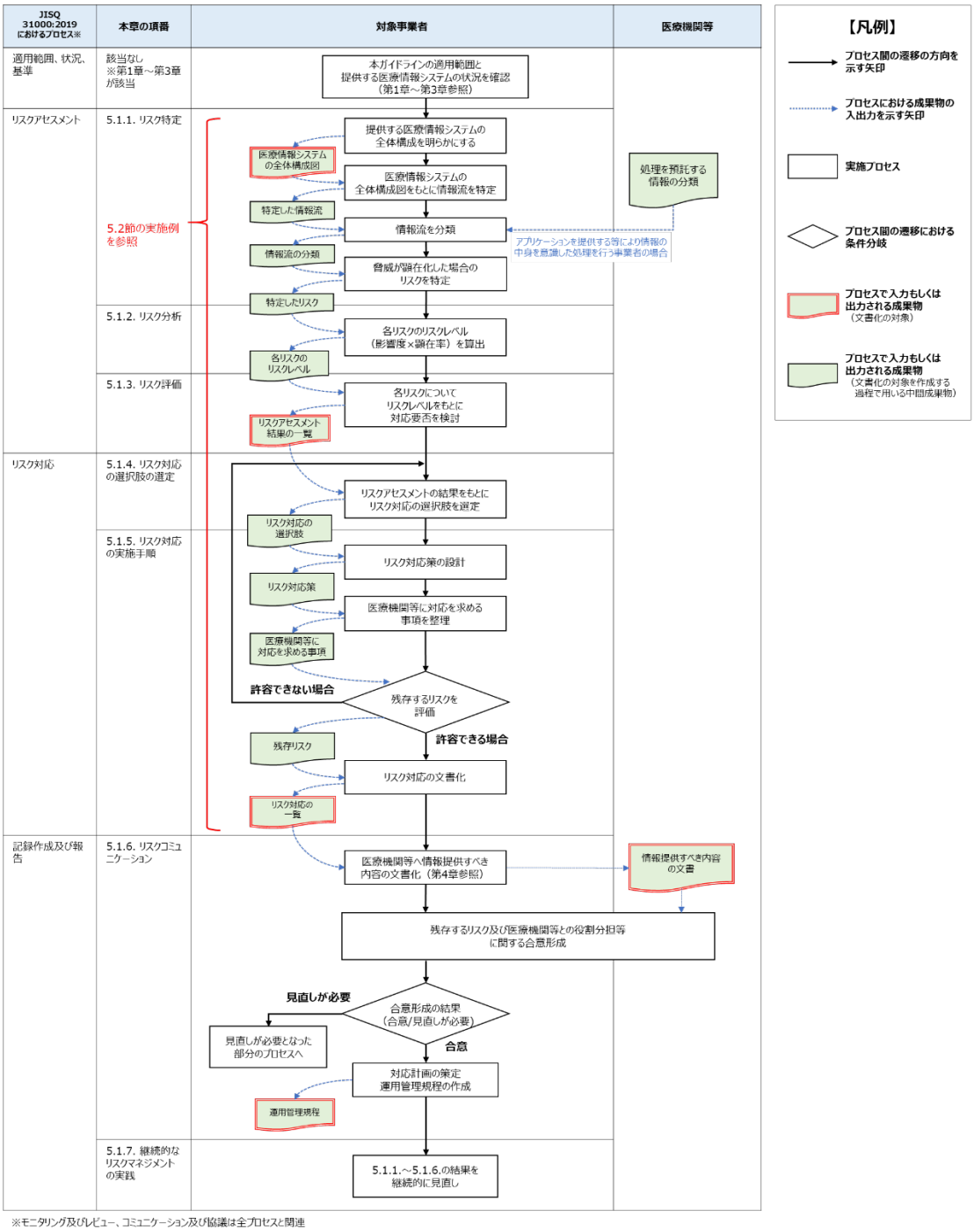

図 5-1 リスクマネジメントのプロセス

5.1. リスクマネジメントの実践

本節では、対象事業者が実施すべきリスクマネジメントのプロセスとして「リスク特定、リスク評価、リスク分析」（以下、「リスクアセスメント」という。）や「リスク対応」、「リスクコミュニケーション」等の各プロセスで実施する内容について定義する。また、対象事業者は 5.1.1～5.1.5 のプロセスの実施にあたり、詳細な実施方法については 5.2 に記載する実施例を参考にし、抜け漏れなく対策をとりまとめること。

5.1.1. リスク特定

対象事業者は、自らが提供する医療情報システムの全体構成図を作成することで、医療情報システムの全体構成を明らかにすること。その上で、医療情報システムの全体構成図をもとに、医療情報システムのライフサイクルにおけるフェーズ毎の情報流を特定すること。本ガイドラインでは、医療情報システムの提供に関わる情報の流れを「情報流」と定義する。情報流にはネットワークを介した電子的な情報の流れだけでなく、記憶媒体の搬送により発生する情報の移動も含まれる。全体構成図をもとに情報の作成及び参照、更新、保存、移送、廃棄等の処理を洗い出すと、構成要素間で情報がどのように流れるのかが明らかになるため、結果として情報流が特定される。このとき、情報流を洗い出す範囲には、ICT サプライチェーン [17]全体を含めること。特に、医療情報システムをクラウドサービスとして提供するケースにおいては、ASP・SaaS と PaaS、IaaS をそれぞれ別の事業者が提供する等、ICT サプライチェーンが複雑となる傾向にあるため、抜け漏れがないよう十分留意すること。

次に、対象事業者は、洗い出した情報流について、当該情報流で処理を行う対象の情報の安全管理上の重要度に応じて分類すること。例えば、診療録や診療諸記録、処方箋、レセプト情報等は、「患者個人情報」等として分類し、「アプリケーションの設定情報」や「テストデータ」等とは区別した分類とすること。このとき、アプリケーションを提供する等により、情報の中身を意識した情報の処理を行う対象事業者においては、医療機関等が医療情報安全管理ガイドラインに基づき実施する情報の分類の結果について、医療機関等へ情報提供を求め、分類の参考とすることが望ましい。逆に、プラットフォームやインフラのみを提供する等により、処理する詳細な情報の中身が不明な場合「アプリケーション提供に係る情報（医療情報を含む可能性のある情報）」とそれ以外の情報（機器や OS/ミドルウェアの設定情報等）を最低限区別した分類とすること。

さらに、対象事業者は、洗い出した情報流に対して、表 5-1 に示す「医療情報システム提供上の代表的な脅威」（以下、「代表的な脅威」という。）をあてはめ、当該情報流に対してそれぞれの脅威が顕在化した場合に生じ得るリスクを特定すること。ただし、代表的な脅威については、ISO /IEC 27005:2018 の附属書 C「典型的な脅威の例」を参考に、本ガイドラインにて独自に整理したものであり、医療情報に関する全ての脅威を網羅している

[17] ICT サプライチェーンの考え方については、ISO/IEC 27017:2015 及び JIS Q 27017:2016 で示されているため、対象事業者は、本ガイドラインと併せてこれら規格を参照することが望ましい。

ものではない。したがって、対象事業者は、代表的な脅威以外の脅威についても、提供する医療情報システムの構成に応じて検討し、リスクを特定すること。

表 5-1 医療情報システム提供上の代表的な脅威

脅威	脅威の具体例
不正な閲覧・操作	正当な権限を持たない者（組織の内外を問わない）が、医療情報、認証情報等を盗み見る。または、医療情報システムに関連する端末等を不適切に操作する。
ネットワーク上の盗聴・なりすまし	スニッフィング等によって、ネットワーク上を流れる認証情報等を入手する。または、入手した認証情報等を用いて正当な権限を持つ者になりすます。
高度サイバー攻撃[18]	標的型メール等によって医療情報システムや関連する端末等をマルウェアに感染させる。
情報の窃取・漏えい	物理的あるいは電子的方法を用いて、医療情報等を盗み出す。または、故意/過失に依らず、医療情報等を不適切に組織外へ流出させる。
情報の改ざん・破壊	故意/過失に依らず、医療情報等を物理的あるいは電子的に不正に書き換える、もしくは破壊する。
医療情報システムの停止	悪意を持った者による攻撃、あるいは過失による設定ミスや誤操作等により、医療情報システムが停止する。
技術的脆弱性の混入	故意/過失に依らず、OS やミドルウェア・アプリケーション等のソフトウェアの脆弱性や、IoT 機器やルータ等のネットワーク機器の脆弱性が医療情報システムに混入する。
機器や記憶媒体の持ち出し時の紛失・盗難	医療情報システムに関連する機器や記憶媒体を業務上の理由で施設等の外へ持ち出す際、機器や記憶媒体を誤って紛失する、あるいは第三者に盗難される。
施設への物理的侵入	正当な権限を持たない者（組織の内外を問わない）が、執務エリアやデータセンター等、医療情報システムに関連する機器や記憶媒体が設置されている施設に侵入する。
災害等	自然災害や社会インフラの損失等により、医療情報システムに関連する機器や端末等が物理的に破損する等して、医療情報システムの提供に支障をきたす。

[18] 閉域網内に構成される医療情報システムにおいても、高度サイバー攻撃の脅威は生じ得る前提でリスクについて特定することが重要である。

5.1.2. リスク分析

対象事業者は、特定したリスクについて、「医療情報システムへの影響の度合い」（以下、「影響度」という。）と「当該リスクが顕在化する可能性」（以下、「顕在率」という。）をもとに、「リスクの大きさの度合い」（以下、「リスクレベル」という。）を算出すること。

リスク分析の手順として、まず、対象事業者は、特定したリスクについて、リスクを洗い出す際のもととなった情報流の分類を参考に、当該リスクが顕在化した場合の医療情報システムへの機密性、完全性、可用性への影響度合いを総合的に判断し、リスクの影響度を特定すること。例えば、リスクを洗い出す際のもととなった情報流の分類が「患者個人情報等」であり、当該情報が頻繁かつ大量に処理されるような場合は、リスクの影響度は極めて大きいと考えられる。

次に、対象事業者は、被害が発生する際の前提条件等をもとにリスクの顕在率を特定すること。例えば、サイバー攻撃においては、インターネット経由で直接的な攻撃が可能である場合や、認証を要求していない場合、既に攻撃手法が知られており被害が発生している場合等は、顕在率は高いと考えられる。一方、施設へ物理的な侵入を行わないと攻撃ができない場合や、多要素認証を要求している場合、攻撃手法が知られておらず攻撃難易度が高い場合等は、顕在率が低いと考えられる。

本ガイドラインでは、リスク分析手法の実践例として、影響度と顕在率をもとに、5 段階のリスクレベルに分類する例を表 5-2 に示す。対象事業者は ISO/IEC 27005:2018 の規格等も参考に自ら適切なリスク分析手法を選択し適用すること。

表 5-2 リスクレベルの分類例

			顕在率					リスクレベル（ランク）	影響度×顕在率
			きわめて低い（ほとんど起こらない）	低い（まず起こらない）	中程度（起こる可能性がある）	高い（起こる可能性が高い）	きわめて高い（頻繁に起こる）		
			1	2	3	4	5		
影響度	きわめて小さい	1	1	2	3	4	5	S	20～25
	小さい	2	2	4	6	8	10	A	10～16
	中程度	3	3	6	9	12	15	B	5～9
	大きい	4	4	8	12	16	20	C	2～4
	きわめて大きい	5	5	10	15	20	25	D	1

5.1.3. リスク評価

対象事業者は、各リスクについて、リスクレベルをもとに対応要否を検討し、リスクアセスメント結果一覧を作成する。この際、リスクレベルに応じた対応基準（以降、「リスク基準」という。）を定めておくのも一案である。例えば、表 5-2 のように S ランク～D ラ

ンクにリスクレベルを分類した場合のリスク基準の例として、S ランクについては複数の対策による対応を必須、A ランクは対応を必須、B～C ランクはリスクレベルの高いものを優先しつつも個別事情も勘案した上で対応の要否を検討、D ランクは対応を不要とする等のリスク基準が考えられる。

5.1.4. リスク対応の選択肢の選定

対象事業者は、5.1.1～5.1.3 に係るリスクアセスメントの結果を踏まえ、リスク対応の選択肢を選定すること。このとき、リスク対応の選択肢としては、表 5-3 に示す「リスク低減」、「リスク回避」、「リスク移転」、「リスク保有」の 4 種類に分類される。

表 5-3 リスク対応の選択肢

選択肢	概要
リスク低減	リスクへの対策を行うことで、リスクレベル（顕在率及び影響度）を低減させる。
リスク回避	リスクを生じさせる情報流を廃止したり、別の情報流に変更する。
リスク移転（リスク共有ともいう）	保険への加入により金銭面での損失に備えたり、医療情報システムの運用を外部に委託することで専門的な業者の管理下に置いたりする。
リスク保有（リスク受容ともいう）	意思決定に基づき、残存するリスクの顕在化により生じ得る被害や金銭面での損失を受容する。

図 5-2 にリスクレベルに応じたリスク対応の例を示す。対象事業者は、リスク低減を中心としつつ、費用対効果を念頭に置いた上で最適なリスク対応の組み合わせを検討すること。このとき、それぞれのリスク対応において、対象事業者に求める事項を次の(1)～(4)に記載する。

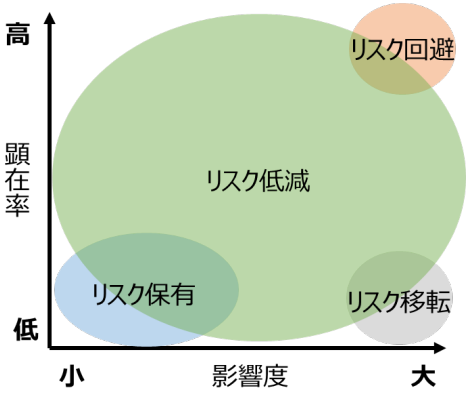

図 5-2 影響度と顕在率に応じた選択肢の考え方

(1) リスク低減

対象事業者は、リスクへの対応を要としたリスクについては、原則として、リスク低減について検討すること。このとき、対策については、費用対効果を踏まえつつ、過剰とならない範囲で複数組み合わせることによる多層防御（多重防御ともいう）を講じることが望ましい。

(2) リスク回避

対象事業者は、影響度及び顕在率ともに極めて高いリスクについては、リスク回避を検討すること。例えば、「外部と大量の個人情報の電子メールによる受け渡し」が頻繁に発生する場合、誤送信による情報漏えいリスクの影響度及び顕在率は極めて高いと判断することができる。こういったケースでは、教育や誤送信対策システムの導入等によるリスク低減策よりも、別の手段により個人情報を受け渡すリスク回避策のほうが有効となることもあり得る。

(3) リスク移転

リスク低減をしたとしても、顕在率の低減は可能だが、影響度の低減は困難であるリスクについては、リスク移転を検討することが有効である。例えば、情報流の一部を他社に委託することにより、サイバー攻撃で被害を受けたとしても、契約等により被害に対する損害賠償責任の一部を委託先に移転することができる。また、リスクが顕在化し損害賠償を求められた時に備えて、サイバー保険等により金銭的な損失を補填することができる。ただし、サイバー保険等によるリスク移転は、あくまでも金銭面での損失にのみ有効な対応であり、情報事故発生時の被害や、医療機関等の信用失墜を防ぐものではない。このため、リスク移転はリスク低減を行った上で残存するリスクに対して適用を検討すべきである。

(4) リスク保有

対象事業者は、リスクアセスメントの結果、リスク低減等のリスク対応を検討した上で、残存するリスクについては、当該リスクを認識した上でリスク保有を検討すること。

5.1.5. リスク対応の実施手順

対象事業者は、リスク対応の選択肢を選定した後、以下の(1)～(4)に示す手順を実施すること。

(1) リスク対応策の設計

対象事業者は、リスク対応策について、次に示す基本的な考え方と医療情報システム特有の考慮事項を踏まえて設計すること。

(ア)基本的な考え方

対象事業者は、対策の設計にあたっては、医療機関等が医療情報安全管理ガイドラインを遵守できるような設計となっていることについて、3.1.2 で述べた説明義務を有していることに留意しなければならない。ここで、対策の設計や、設計した対策の妥当性を判断するにあたっては、高度な専門性が要求されるが、従前の情報処理事業者ガイドライン及びクラウド事業者ガイドラインの要求事項を医療情報安全管理ガイドライン（第 5 版）との対応関係を踏まえ対策項目として整理・統合した別紙 2 を用い、その全ての対策項目についての確認をすることは、対象事業者による対策の設計や妥当性の判断、説明義務への対応において必須である。また、リスク対応策を取りまとめる際には、「人的・組織的」、「物理的」、「技術的」の 3 つの対策の観点について、特定の観点の対策に依らず、複数観点を組み合わせた対策の設計が重要である[19]。

さらに、対策を設計する際に、別紙 2 に書かれている「対策項目で対応できるリスクシナリオ（例）」を参考にすることも有効である。ただし、当該リスクシナリオ例はあくまで参考例であり、関連するリスクと対策が他にも存在しないかを対策の設計を行う際に確認すること。

(イ)医療情報システム特有の考慮事項

対象事業者は、対策の設計にあたっては上記で示す基本的な考え方に加え、以下に記載

[19] 例えば、不正な閲覧・操作を防止するための技術的対策として、利用者認証を講じるような場合は、併せて人的・組織的対策として利用者の教育を行い、利用者認証に用いる IC カードやパスワード等の認証情報の適切な管理を求める必要があると考えられる。また、IC カードと静脈認証等により特定の 1 人のみを入室可能とする物理的対策を講じた区画においては、技術的対策としてパスワード等による認証は不要と判断することも考えられる。

する医療情報システム特有の考慮事項を参照し、必要な対策を設計すること。

① 利用者認証における考慮事項

医療情報の機密性の高さや攻撃手法の高度化に鑑み、多要素認証（知識認証、物理認証、生体認証のうち異なる 2 つ以上の要素を用いる認証方式）を可能な限り早期[20]に採用すべきである。

② ログの保存期間における考慮事項

取り扱う医療情報に法定保存年限が設けられている場合は、当該医療情報に関するアクセスを記録したログについて、法定保存年限以上の保存期間を設けること。

③ ネットワーク経路における暗号化における考慮事項

医療情報の機密性の高さや攻撃手法の高度化に鑑み、オープンなネットワークを介して接続を行う際は、様々な攻撃を想定した上で、適切な暗号化手法[21]を選択すべきである。

④ 無線 LAN の端末接続制限における考慮事項

無線 LAN の端末接続制限に係る対策として、MAC アドレスを用いた端末接続制限が一般的に知られているが、MAC アドレスは容易になりすまし可能であるため、医療情報の機密性の高さや攻撃手法の高度化に鑑み、MAC アドレスを用いた端末接続制限に加えて IEEE 802.1X と電子証明書を組み合わせる等のより安全な方法を採用すべきである。

⑤ 小型半導体メモリの利用における考慮事項

記憶媒体のうち、小型で記憶容量が大きい小型半導体メモリは、衣服等のわずかな隙間にも隠すことができるため、不正な情報の持ち出しを企図するものにとっても有益なものといえる。対象事業者は、原則として医療情報を格納する記憶媒体として小型半導体メモリの使用を行うことができないよう配慮することが望ましい。

---

[20] 医療情報安全管理ガイドライン第 5 版の公表（平成 29 年 5 月）から約 10 年後に医療情報安全管理ガイドラインの「C.最低限のガイドライン」となることが想定されている。

[21] HTTPS 接続においては、TLS の設定はサーバ/クライアントともに CRYPTREC が定める「SSL/TLS 暗号設定ガイドライン（第 2.0 版）平成 30 年 5 月 8 日（以下、「SSL/TLS 暗号設定ガイドライン」という。）」に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行うこと。また、医療情報安全管理ガイドラインは、SSL-VPN を原則として利用しないよう求めている。やむを得ず SSL-VPN を利用する場合は、SSL/TLS 暗号設定ガイドラインに基づき、「クライアント型」での SSL-VPN とすること。

⑥　事業継続計画の策定における考慮事項

事業継続計画の策定において、対象事業者は、「災害等によりシステムが停止した場合」だけでなく、システムが正常であったとしても「災害等により多数の傷病者が医療サービスを求める状態となり、通常の手段では著しい不都合が生じる場合」や「一定期間停止したシステムを復旧して運用を再開する際に、情報の一部欠損の発生や情報の連続性が担保されないことにより不都合が生じる場合」についても考慮すること。

(2) 医療機関等へ対応を求める事項の整理

対象事業者は、設計したリスク対応策のうち、医療機関等による対応が必要となる内容について、医療機関等へ対応を求める事項として整理すること。

(3) 残存するリスクの評価

対象事業者は、医療機関等へ対応を求める事項を整理した上で、それでも残存するリスクについて改めてリスク評価（5.1.3）を実施すること。リスク評価の結果、残存するリスクの評価結果が対象事業者として許容できないと判断する場合は、リスク対応方法について再度検討すること。

(4) リスク対応の文書化

対象事業者は、リスク対応の選択肢についての選定結果及び、選定結果に基づき設計した対応策を「リスク対応一覧」として文書化すること。

5.1.6. リスクコミュニケーション

(1) 医療機関等とのリスクコミュニケーションの実施

対象事業者は、自らが提供する医療情報システムの安全管理に係る説明義務を果たし、医療機関との共通理解を形成するために、医療機関等に対して第 4 章で情報提供すべき内容として示した事項を含む必要な情報を文書化して提供すること。具体的には、5.1.5 で作成した「リスク対応一覧」や後述の運用管理規定に定められた事項に係る情報提供を通して、医療機関等との役割分担、対象事業者として受容したリスクの内容等について、医療機関等と合意形成を図ること。なお、その際には、対象事業者は、医療機関等が容易に理解可能となるよう内容を工夫する等、適切に共通理解を得ること[22]。

なお、医療機関等と合意に至らなかった場合は、対象事業者はリスク対応事項の見直し結果に基づく再協議、残存するリスクの共通理解に向けた再協議等、医療機関等と再度合意形成を図ること。

(2) 文書・規定の作成

対象事業者は、医療機関等と合意したリスクへの対応を踏まえ、リスクに対する対応計画を策定すること。また、対象事業者が安全管理義務を果たすために、医療機関等と合意形成した結果を文書化し、以下の(ア)～(コ)を含む運用管理規程を定めること。

(ア) 医療情報システムの安全管理に係る基本方針

対象事業者は、医療情報システムの安全管理に係る基本方針として、以下の事項を運用管理規程に含めること。

- 本ガイドライン及び医療情報安全管理ガイドラインの遵守
- 個人情報保護法やその他最新の関連法令等の遵守
- 個人情報に関して他の情報と区別した適切な管理
- 個人情報保護委員会及び厚生労働省が定める「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ダンス（平成 29 年 4 月 14 日）」に基づき、患者等が死亡した後においても、当該患者等の情報を保存している場合には、死者に係る情報であっても、個人情報と同等の安全管理措置の実施
- 情報セキュリティに関する基本方針等の情報セキュリティポリシーの策定

[22] 医療機関等との共通理解を得るプロセスは、JIS Q 31000:2019 におけるリスクコミュニケーションに該当する。リスクコミュニケーションは、リスクアセスメントやリスク対応の内容を医療機関等に情報提供するといった限定的なものではなく、リスクマネジメントのあらゆるプロセスにおいて、その実効性を高めるために実施される活動である点に留意すること。そのため、対象事業者は、医療機関等の十分な理解を得るために、リスク対応を行った最終段階だけでなく、その分析途中についても情報を公開し、医療機関等の疑問や要求に応えながら、共通理解を得ることが重要である。

- 情報セキュリティポリシーの遵守を担保する組織体制の構築

（イ）医療情報システムの提供に係る体制

対象事業者は、医療情報システムの提供に係る体制として、最終的な管理責任者や、十分な技術的能力及び経験[23]を有する責任者（システム管理者）、医療情報システムの運用に関する事務を統括する責任者、個人情報保護に係る責任者をこれら責任者の役割や任命・解任等のルール、緊急時の対応と併せて運用管理規程に含めること。また、再委託を行う場合は、再委託先の体制に関する情報も運用管理規程に含めること。

（ウ）契約書・マニュアル等の文書の管理方法

対象事業者は、契約書や運用管理規程を含むマニュアル等の管理方法として、必要に応じて速やかに内容を確認できるようにするほか、アクセス制限により第三者によるこれら文書の不正な閲覧・操作を防止することを運用管理規程に含めること。なお、アクセス制限を侵害する行為については、検出・記録できるような仕組みが実装されていることが望ましい。

（エ）機器等を用いる場合の機器等の管理方法

対象事業者は、機器等を用いる場合、機器等の管理方法について台帳管理等による所在確認を行う旨を運用管理規程に含めること。

（オ）リスク対応策の運用方法

対象事業者は、リスクへの対応策の運用方法として、リスク対応にて決定したリスクへの対策のうち、対象事業者による運用が必要となる事項についての運用手順を運用管理規程に含めること。

（カ）事故発生時の対応方法及び医療機関等への報告方法

対象事業者は、事故発生時の対応方法及び医療機関等への報告方法として、情報事故が発生した場合の被害拡大防止のための対応方法や緊急時の代替手段、原因調査のためのログ等の記録の保全及び医療機関等への報告タイミングや報告フローを運用管理規程に含めること。

---

[23] 十分な技術的能力及び経験には、例えば情報処理安全確保支援士等の情報セキュリティに関する資格を有し、情報セキュリティに係る技術的対策の実務を一定年数以上経験していること等が想定される。

(キ)個人情報を格納する記憶媒体の管理方法

対象事業者は、個人情報を格納する記憶媒体の管理方法として、保管や取扱いの方法及び保管や取扱いに係る履歴の記録について運用管理規程に含めること。

(ク)医療情報の外部保存に係る患者等への説明方法

対象事業者は、医療情報の外部保存に係る患者等への説明方法として、医療機関等へ必要な資料の提供もしくは、医療機関等に代わり対象事業者が直接患者等へ説明する場合は、その方法について、運用管理規程に含めること。

(ケ)医療情報システムに対する監査の実施方針

対象事業者は、医療情報システムに対する監査の実施方針として、提供する医療情報システムの安全管理に係る監査の方針や内容のほか、監査の実施に係る記録についての保存・管理方法について運用管理規程に含めること。なお、医療機関等への医療情報システム提供にあたり、他社が提供する医療情報システムを利用する場合は、他社が提供する医療情報システムに対する監査の方針や内容もしくは、監査に代替する対応についても運用管理規程に含めること。

(コ)医療機関等の管理者からの問い合わせ窓口

対象事業者は、医療機関等の管理者からの問い合わせ窓口として、医療機関等の管理者からの一元的な問い合わせ窓口となる連絡先及び連絡方法のほか、問い合わせを受け付ける時間帯について運用管理規程に含めること。

5.1.7. 継続的なリスクマネジメントの実践

5.1.1～5.1.6 に示したプロセスは、一度だけ実施すれば良いというものではない。対象事業者は、医療情報システムにおける情報流や脅威の変化、想定外の事態の発生等に応じて、医療機関等との契約締結後も継続的に実施し、見直しを行うこと[24]。

5.2. リスクアセスメント及びリスク対応の実施例

本節では、図 5-3 に示す医療情報システムの例を用いて、5.1.1～5.1.5 の手順の実施例を示す。本節で記載する例はいずれも一部を簡略化して提示している。対象事業者は、本節

[24] このような継続的なリスクマネジメントの実践については、JIS Q 27001:2014 (ISO/IEC 27001:2013)として標準的なプロセスが規格化されている。

で記載する手順を参考とした上で、網羅的なリスクマネジメントを行うこと。

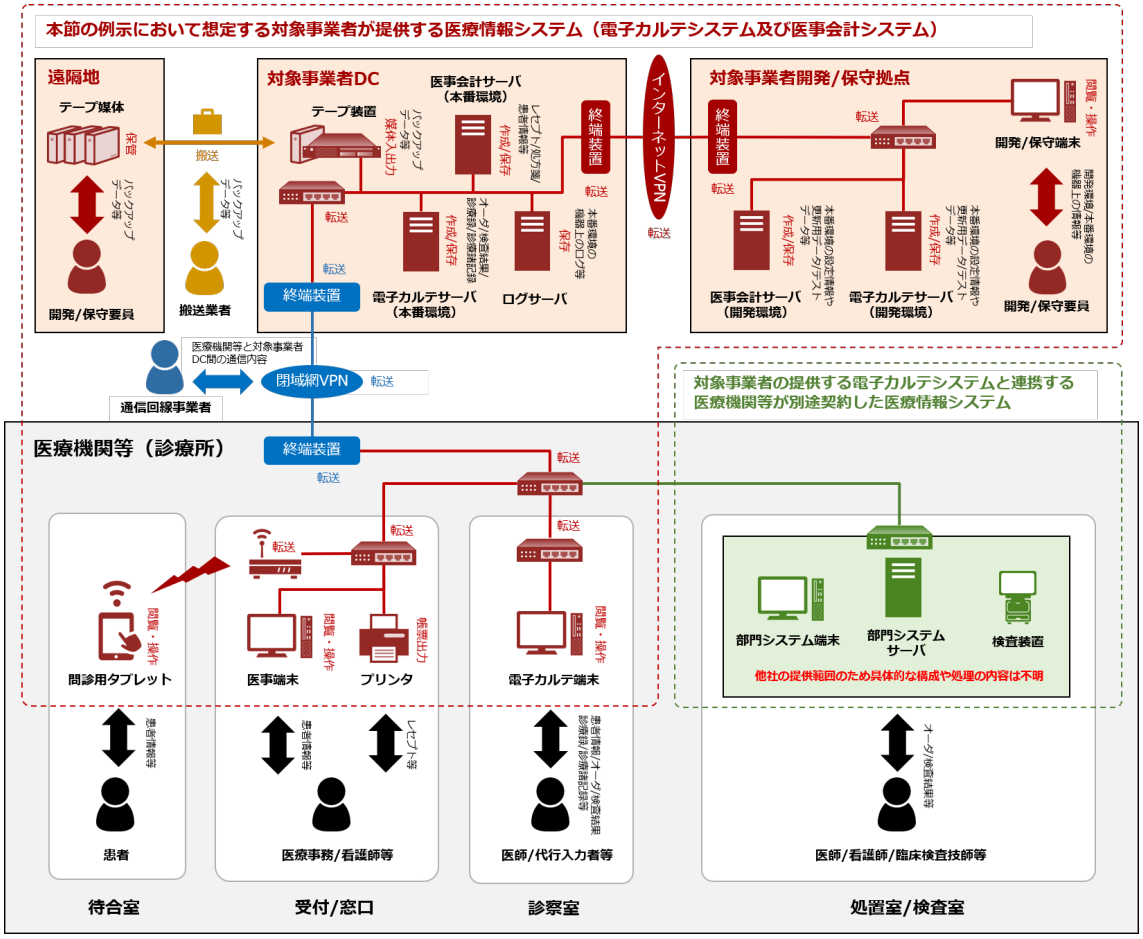

図 5-3 本節の例示に用いる医療情報システムの全体構成図

5.2.1. リスクアセスメント

(1) リスク特定における医療情報システムの全体構成図の作成

医療情報システムの全体構成図の作成においては、情報流及びリスクを網羅的に洗い出すことができるよう、複数の事業者間の ICT サプライチェーン全体を含め構成を明らかにする。また、自社と契約関係にない他社が提供する医療情報システムについても、自社が提供する医療情報システムと情報のやりとりが行われる場合は、他社システムとの連携に係る情報流が特定できるように構成を明らかにする。

【手順 1】どこにどのような機器や記憶媒体があるかを明らかにする

医療情報の処理に関連し、どこにどのような機器[25]や記憶媒体があるかを可能な限り明らかにする（図 5-4）。

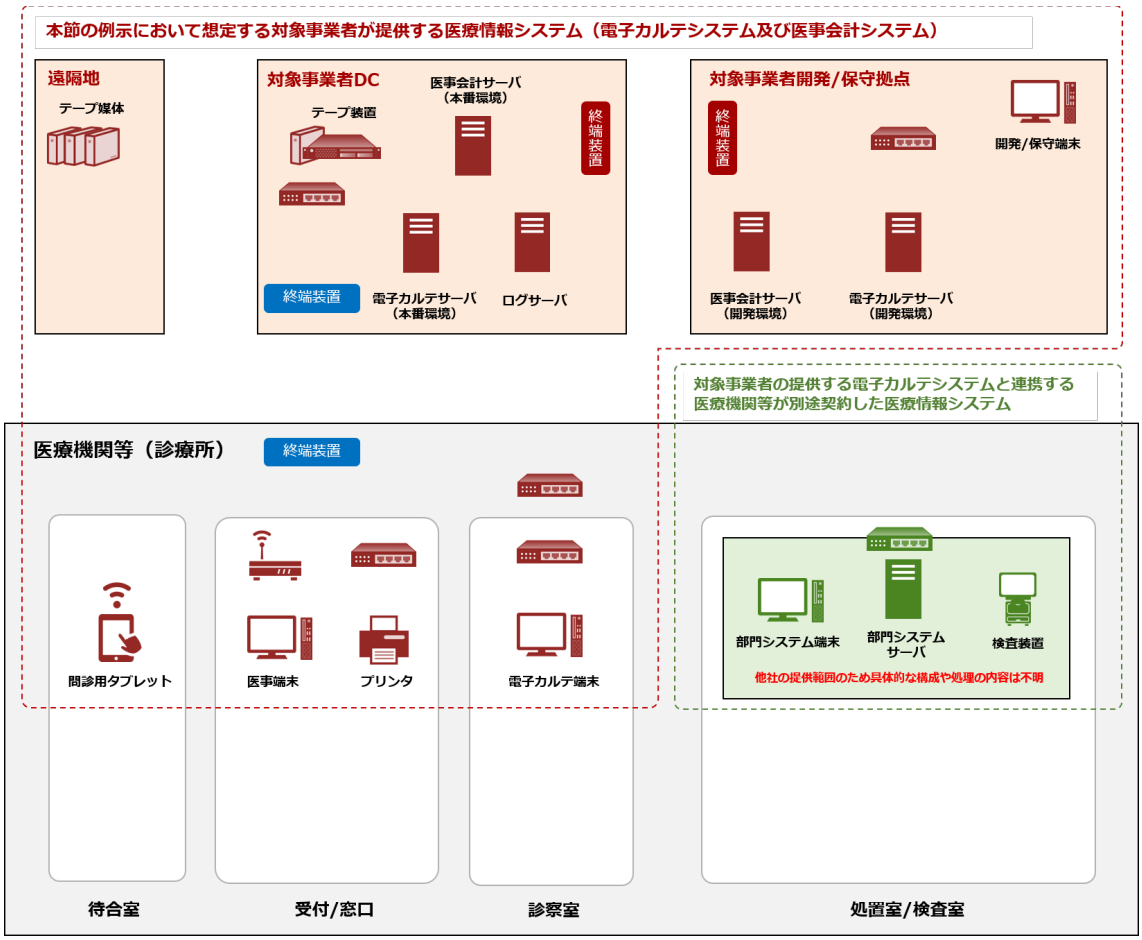

図 5-4 医療情報システムの全体構成図の作成過程（手順 1）

25 クラウドサービス等における仮想マシンを含む。

【手順 2】機器同士の接続や記憶媒体の搬送を明らかにする

機器間のネットワーク接続や、記憶媒体の搬送を可能な限り明らかにする（図 5-5）。このとき、機器や記憶媒体の物理的な所在を踏まえつつ、全ての機器同士の接続や記憶媒体の搬送による情報の流れを特定し、論理構成の全体像を明らかにすること。

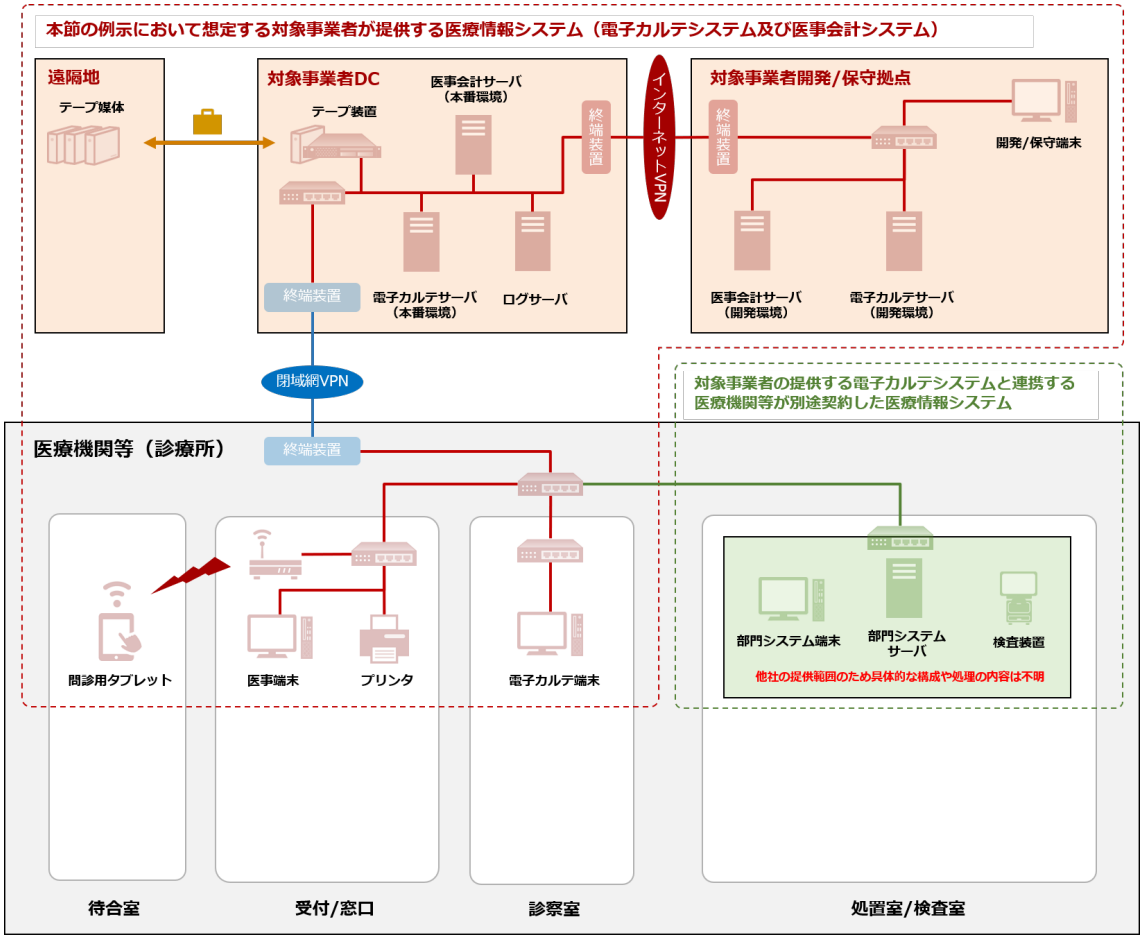

図 5-5 医療情報システムの全体構成図の作成過程（手順 2）

【手順 3】人が扱う機器や記憶媒体における情報の処理を明らかにする

人が扱う機器や記憶媒体における情報の処理を、「誰が」、「どこの」、「どの機器や記憶媒体で」、「何を」、「どうするか」の切り口で可能な限り明らかにする（

図 5-6）。人が扱う機器や記憶媒体としては、情報の閲覧・操作を行うための端末や、帳票出力のためのプリンタ、物理的なデータの搬送に用いる磁気テープやDVD 等の記憶媒体のほか、通信回線事業者が提供する閉域網 VPN[26]等が想定される。

手順 3 において明らかにする情報の処理の例

- 患者が、待合室の、問診用タブレットで、患者情報等を、閲覧・操作する
- 通信回線事業者が、対象事業者 DC と医療機関等の間の、閉域網 VPN で、アプリケーション提供に係る情報を転送する

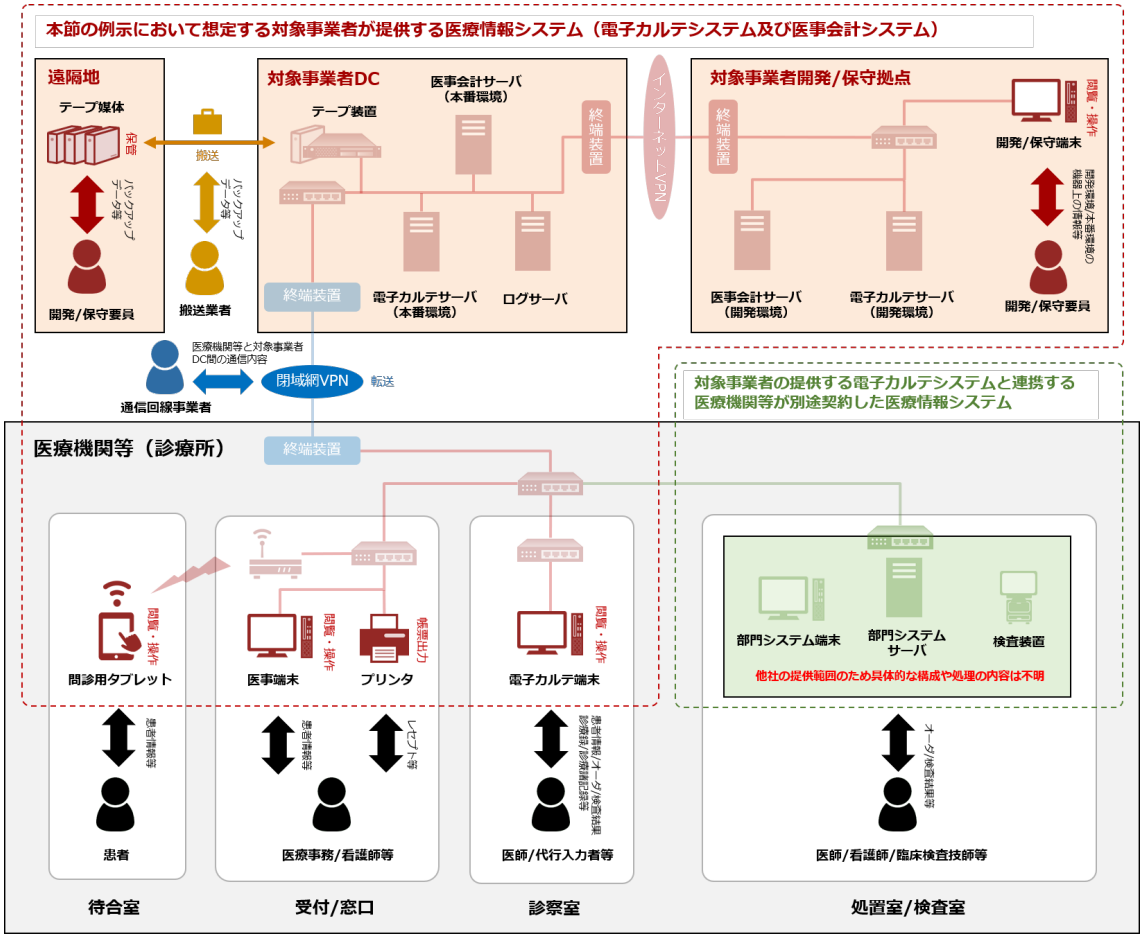

図 5-6 医療情報システムの全体構成図の作成過程（手順 3）

[26] 通信回線事業者が提供する閉域網 VPN 内の機器を含む。

【手順 4】人が直接扱わない機器における情報の処理を明らかにする

人が直接扱わない機器における情報の処理を「どこの」、「どの機器で」、「何が」、「どうされるか」の切り口で可能な限り明らかにする（図 5-7）。人が直接扱わない機器としては、サーバやネットワーク機器等が想定される。

手順 4 において明らかとする情報の処理の例

- 対象事業者 DC の、医事会計サーバ（本番環境）で、レセプト／処方箋／患者情報等が、作成／保存される
- 対象事業者開発拠点の、医事会計サーバ（開発環境）で、本番環境の設定情報や更新用データ／テストデータ等が、作成／保存される

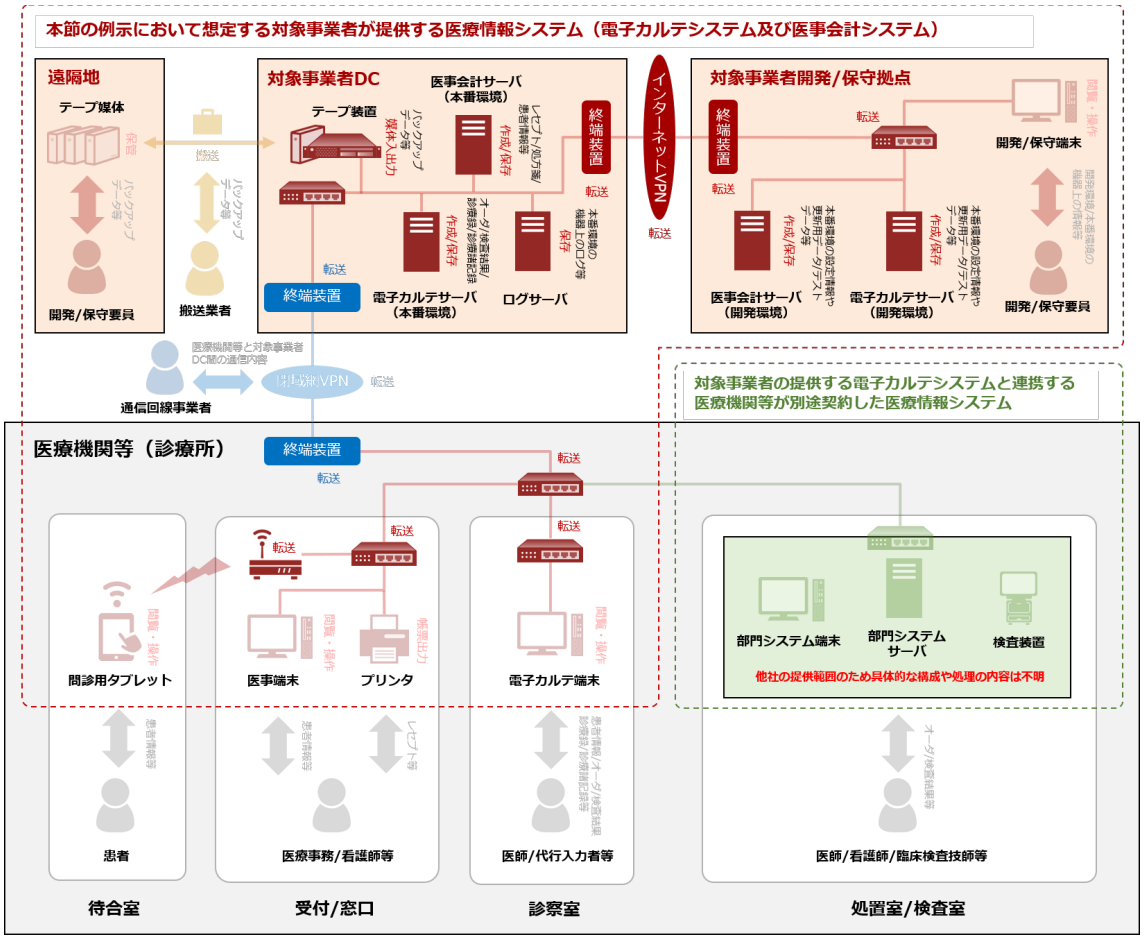

図 5-7 医療情報システムの全体構成図の作成過程（手順 4）

(2) リスク特定における情報流の特定

医療情報システムの全体構成図をもとに、情報流を明らかにする。なお、サービス提供形態によって情報流の特定の観点が異なるため、本節では、2.2 で整理した医療情報システムの代表的な提供形態として、アプリケーション、プラットフォーム、インフラそれぞれの提供における情報流の特定の観点について例示する。

【アプリケーション提供における情報流の特定例】

開発フェーズにおける情報流の特定例

開発フェーズにおける情報流は、本番環境だけではなく開発環境や試験環境を含め、アプリケーション上の情報の処理に着目して特定する。

Who（誰が）	Where（どこの/どこを）	Which（どの機器で/どの媒体で）	What（何を/何が）	How（どうするか/どうされるか）
開発/保守要員が	対象事業者DCの	開発保守端末で	本番環境のアプリケーションのプログラム/設定情報/テストデータ等を	閲覧・操作する
				媒体入出力する
	対象事業者開発拠点の			閲覧・操作する
				媒体入出力する
ー	対象事業者開発拠点の	電子カルテサーバ（開発環境）で	本番環境のアプリケーションのプログラム/設定情報/テストデータ等が	作成や保存される
		医事会計サーバ（開発環境）で		

運用フェーズにおける情報流の特定例

運用フェーズにおける情報流は、実際の業務におけるアプリケーションの活用に着目して特定する。

Who（誰が）	Where（どこの/どこを）	Which（どの機器で/どの媒体で）	What（何を/何が）	How（どうするか/どうされるか）
患者が	待合室の	問診用タブレットで	患者情報等を	閲覧・操作する
医療事務/看護師等が	受付/窓口の	医事端末で		
		プリンタで	レセプト等を	帳票出力する
医師/代行入力者等が	診察室の	電子カルテ端末で	患者情報/オーダ/検査結果/診療録/診療諸記録等を	閲覧・操作する
医師/看護師/臨床検査技師等が	処置室/検査室の	電子カルテシステムと連携する他社が提供するシステムで	オーダ/検査結果等を	処理する
ー	対象事業者DCの	電子カルテサーバ（本番環境）で	オーダ/検査結果/診療録/診療諸記録等が	作成や保存される
		医事会計サーバ（本番環境）で	レセプト/処方箋/患者情報等が	
		ログサーバで	アプリケーションのログが	保存される

契約終了フェーズにおける情報流の特定例

開発フェーズと運用フェーズにおいてアプリケーション上に保存される情報の廃棄や移管等の処理に着目して情報流を特定する。

Who（誰が）	Where（どこの/どこを）	Which（どの機器で/どの媒体で）	What（何を/何が）	How（どうするか/どうされるか）
ー	対象事業者DCの	電子カルテサーバ（本番環境）で	作成や保存されたオーダ/検査結果/診療録/診療諸記録等を	廃棄もしくは移管する
		医事会計サーバ（本番環境）で	作成や保存されたレセプト/処方箋/患者情報等を	
		ログサーバで	保存された本番環境のアプリケーションのログを	
	対象事業者開発拠点の	電子カルテサーバ（開発環境）で	作成や保存された本番環境のアプリケーションのプログラム/設定情報/テストデータ等を	
		医事会計サーバ（開発環境）で		

【プラットフォーム提供における情報流の特定例】

開発フェーズにおける情報流の特定例

開発フェーズにおける情報流は、本番環境だけでなく開発環境や試験環境を含め、プラットフォームに対する操作に着目して特定する。

Who（誰が）	Where（どこの/どこを）	Which（どの機器で/どの媒体で）	What（何を/何が）	How（どうする/どうされる）
開発/保守要員が	対象事業者DCの	開発保守端末で	本番環境のOS/ミドルウェア上の設定情報等を	閲覧・操作や媒体入出力する
	対象事業者開発拠点の			
ー	対象事業者開発拠点の	電子カルテサーバ（開発環境）で	本番環境のOS/ミドルウェア上の設定情報等が	作成や保存される
		医事会計サーバ（開発環境）で		

運用フェーズにおける情報流の特定例

運用フェーズにおいては、プラットフォームが提供する機能の利用に着目して情報流を特定する。

Who（誰が）	Where（どこの/どこを）	Which（どの機器で/どの媒体で）	What（何を/何が）	How（どうする/どうされる）
ー	待合室の	問診用タブレットで	アプリケーション提供に係る情報を	処理する
	受付/窓口の	医事端末で		
		プリンタで		
	診察室の	電子カルテ端末で		
	処置室/検査室の	電子カルテシステムと連携するシステムで		
	対象事業者DCの	電子カルテサーバ（本番環境）で		
		医事会計サーバ（本番環境）で		
		ログサーバで	OS/ミドルウェアのログが	保存される
搬送業者が	対象事業者DCと遠隔地間を	テープ媒体で	バックアップデータ等を	搬送する
開発/保守要員が	遠隔地の			保管する
ー	対象事業者DCの	テープ装置で	バックアップデータ等が	入出力される

契約終了フェーズにおける情報流の特定例

開発フェーズと運用フェーズにおいてプラットフォーム上に保存される情報の廃棄や移管等の処理に着目して情報流を特定する。

Who（誰が）	Where（どこの/どこを）	Which（どの機器で/どの媒体で）	What（何を/何が）	How（どうする/どうされる）
対象事業者が	対象事業者開発拠点の	開発保守端末で	OS/ミドルウェア上のデータを	廃棄もしくは移管する
		電子カルテサーバ（開発環境）で		
		医事会計サーバ（開発環境）で		
	待合室の	問診用タブレットで		
	受付/窓口の	医事端末で		
		プリンタで		
	診察室の	電子カルテ端末で		
	処置室/検査室の	電子カルテシステムと連携するシステムで		
	対象事業者DCの	電子カルテサーバ（本番環境）で		
		医事会計サーバ（本番環境）で		
		ログサーバで	OS/ミドルウェアのログを	
	遠隔地の	テープ媒体で	バックアップデータ等を	

【インフラ提供における情報流の特定例】

開発フェーズにおける情報流の特定例

開発フェーズにおける情報流は、本番環境だけでなく開発環境や試験環境を含め、インフラの構築や変更における設定や試験に着目して特定する。

Who（誰が）	Where（どこの/どこを）	Which（どの機器で/どの媒体で）	What（何を/何が）	How（どうする/どうされる）
開発/保守要員が	対象事業者開発拠点の	開発保守端末で	本番環境の機器の設定情報等を	閲覧・操作する
				媒体入出力する
	対象事業者DCと対象事業者開発拠点間の	インターネットVPNで	本番環境と開発環境の機器上の情報等を	転送する

運用フェーズにおける情報流の特定例

運用フェーズにおいては、管理者やオペレータによるインフラへの操作や、インフラの稼働状況の監視に着目して情報流を特定する。

Who（誰が）	Where（どこの/どこを）	Which（どの機器で/どの媒体で）	What（何を/何が）	How（どうする/どうされる）
通信回線事業者が	対象事業者DCと医療機関等の間の	閉域網VPNで	アプリケーション提供に係る情報を	転送する
ー	対象事業者DCの	有線LAN上のネットワーク機器で	アプリケーション提供に係る情報が	転送される
	対象事業者開発拠点の			
	医療機関内の	無線LAN上のネットワーク機器で		
		有線LAN上のネットワーク機器で		

契約終了フェーズにおける情報流の特定例

開発フェーズと運用フェーズにおいてインフラ上に保存される情報の廃棄や移管等に着目して情報流を特定する。

Who（誰が）	Where（どこで/どこを）	Which（どの機器で/どの媒体で）	What（何を/何が）	How（どうするか/どうされるか）
対象事業者が	対象事業者DCの	有線LAN上のネットワーク機器で	機器の設定情報を	廃棄もしくは移管する
	対象事業者開発拠点の			
	医療機関内の	無線LAN上のネットワーク機器で		
		有線LAN上のネットワーク機器で		
	対象事業者DCの	開発保守端末で		
	対象事業者開発拠点の			
通信回線事業者が	対象事業者DCと対象事業者開発拠点間の	閉域VPN網で	機器の設定情報を	

(3) リスク特定・リスク分析・リスク評価における成果物の作成

リスクアセスメント結果一覧の作成にあたっては、情報流に対し、情報流の分類、関連する脅威、脅威が顕在化した場合のリスクを特定し、リスクレベルと対応要否を次に示すような形で整理する。

【アプリケーション提供の情報流に係るリスクアセスメント結果一覧の作成例】

リスク特定					リスク分析			リスク評価
情報流	分類	関連する脅威	特定したリスク		影響度	顕在率	リスクレベル	対応要否
医療事務/看護師等が受付/窓口の医事端末で患者情報等を閲覧・操作する	患者個人情報	不正な閲覧・操作	受付/窓口の医事端末において	正当な者以外による患者個人情報の不正な閲覧や作成、更新が行われる	5	3	A	要
				・・・				
		情報の改ざん・破壊		故意又は過失による虚偽入力、書き換えにより患者個人情報の改ざん・破壊が行われる	5	3	A	要
				・・・				
		医療情報システムの停止		アプリケーション停止により、患者個人情報が見読不可となる	5	3	A	要
				・・・				
		技術的脆弱性の混入		アプリケーションに混入した脆弱性の悪用により患者個人情報の漏えい・改ざん・破壊が行われる	5	3	A	要
				・・・				
		・・・						
・・・								

【プラットフォーム提供の情報流に係るリスクアセスメント結果一覧の作成例】

リスク特定					リスク分析			リスク評価
情報流	分類	関連する脅威	特定したリスク		影響度	顕在率	リスクレベル	対応要否
診察室の電子カルテ端末でアプリケーション提供に係る情報を処理	アプリケーション提供に係る情報（医療情報を含む可能性あり）	不正な閲覧・操作	診察室の電子カルテ端末において	不正プログラムの実行により、アプリケーション提供に係る情報の漏えい・改ざん・破壊が生じる	5	3	A	要
				・・・				
		情報の改ざん・破壊		アプリケーション提供に係る情報を電子媒体へ不正に複製され、情報の窃取・漏えいが生じる	5	3	A	要
				・・・				
		医療情報システムの停止		OS/ミドルウェアの停止により、アプリケーション提供に係る情報の見読性が失われる	5	3	A	要
				・・・				
		技術的脆弱性の混入		OS/ミドルウェアに混入した脆弱性の悪用によりアプリケーション提供に係る情報の漏えい・改ざん・破壊が生じる	5	3	A	要
				・・・				
		・・・						
・・・								

【インフラ提供の情報流に係るリスクアセスメント結果一覧の作成例】

リスク特定					リスク分析			リスク評価
情報流	分類	関連する脅威	特定したリスク		影響度	顕在率	リスクレベル	対応要否
対象事業者DCの有線LAN上のネットワーク機器でアプリケーション提供に係る情報が転送される	アプリケーション提供に係る情報（医療情報を含む可能性あり）	ネットワーク上の盗聴・なりすまし	対象事業者DCの有線LAN上のネットワーク機器において	アプリケーション提供に係る情報の盗聴・なりすましが行われる	5	3	A	要
		医療情報システムの停止		障害に伴うアプリケーション提供に係る情報の滅失・破壊が生じ、見読性や保存性が失われる	5	3	A	要
		施設への物理的侵入		アプリケーション提供に係る情報に物理的にアクセスされる	5	3	A	要
		災害等		アプリケーション提供に係る情報の処理が地震、水害、落雷、火災等並びにそれに伴う停電等により、停止もしくは不具合が生じる	5	3	A	要
		・・・						
・・・								

5.2.2. リスク対応

リスク対応一覧の作成にあたっては、まず、対応するリスクに対し 5.1.4 のプロセスで決定したリスク対応の選択肢を記載する。次に、「人的・組織的」、「物理的」、「技術的」の複数の観点から決定した対策のうち、対象事業者が実施する対策について記載する。そして、リスク対応において医療機関等に対応を求める事項を明らかにした上で、残存するリスクを記載する。

【アプリケーション提供に係るリスクへの対応例】

リスク対応									
対応するリスク		対応	対策の観点	対象事業者が実施する対策	医療機関等へ対応を求める事項	残存するリスク	影響度	顕在率	リスクレベル
受付/窓口の医事端末において	正当な者以外による患者個人情報の不正な閲覧や作成、更新が行われる	低減	人的・組織的対策	―	医療機関等の職員への内部不正防止のための教育や、患者等による画面の覗き見防止のための医事端末のレイアウト調整については、医療機関等にて実施をお願いいたします。	―			
			物理的対策	―					
			技術的対策	医事端末のアプリケーション利用に際して、利用者を一意に識別するID/パスワード（8桁以上英数大文字小文字混合）による認証と静脈による多要素認証を実装する。					
				・・・					
	故意又は過失による虚偽入力、書き換えにより患者個人情報の改ざん・破壊が行われる	低減	人的・組織的対策	誤操作防止のための医療機関等の利用者向けマニュアルを提供する。	医療機関等の職員への内部不正や誤操作防止のための教育については、医療機関等にて実施をお願いいたします。	―			
				・・・					
			物理的対策	―					
			技術的対策	患者個人情報の更新や削除に係る履歴を、ログとして取得する。なお、法定保存期間が定められた情報に関しては当該期間の間ログを保存し、それ以外の情報については1年間ログを保存する。					
				・・・					
・・・									

【プラットフォーム提供に係るリスクへの対応例】

リスク対応									
対応するリスク		対応	対策の観点	対象事業者が実施する対策	医療機関等へ対応を求める事項	残存するリスク			
							影響度	顕在率	リスクレベル
受付/窓口の医事端末において	不正プログラムの実行により、アプリケーション提供に係る情報の漏えい・改ざん・破壊が生じる	低減	人的・組織的対策	医療機関等による定義ファイルやスキャンエンジンの自動アップデートのためのマニュアルを提供する。	長期間利用しない端末については、弊社が定めるマニュアルに従い、定義ファイルやスキャンエンジンの手動アップデートの実施をお願いいたします。	―			
				・・・					
			物理的対策	―					
			技術的対策	電子カルテ端末に不正プログラム対策ソフトウェアを導入し次の設定を行う。 ・ リアルタイムスキャン、定期スキャン ・ 電子媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャン ・ 定義ファイル、スキャンエンジンの自動アップデート ・ 管理者以外による設定変更やアンインストールの禁止					
				・・・					
	アプリケーション提供に係る情報を電子媒体へ不正に複製され、情報の窃取・漏えいが生じる	低減	人的・組織的対策	―	電子媒体の適切な管理について実施をお願いいたします。	媒体毎の個別許可・禁止設定ができない電子媒体（CD、DVD等）は自由に利用できてしまう。	3	2	B
			物理的対策	―					
			技術的対策	電子カルテ端末のUSBポートには、事前に登録した電子媒体のみ接続を許可するよう制御を行う。					
				・・・					
・・・									

【インフラ提供に係るリスクへの対応例】

リスク対応									
対応するリスク		対応	対策の観点	対象事業者が実施する対策	医療機関等へ対応を求める事項	残存するリスク			
							影響度	顕在率	リスクレベル
対象事業者DCの有線LAN上のネットワーク機器やサーバ機器において	アプリケーション提供に係る情報の盗聴・なりすましが行われる	低減	人的・組織的対策	機器の管理手順を策定し、機器の設置や保守に関わる作業者全員に対して、周知し、理解したことの確認を行う。	―	―			
				・・・					
			物理的対策	機器は、許可した者のみが入室可能となるようICカードと静脈認証による多要素認証を必須とするサーバルームに設置する。					
				・・・					
			技術的対策	アプリケーション提供における端末・サーバ間の通信についてTLS1.2による暗号化を実装する。					
				・・・					
	障害に伴うアプリケーション提供に係る情報の滅失・破壊が生じ、見読性や保存性が失われる	低減	人的・組織的対策	機器の障害に伴う交換や修理等の作業手順を定める。	―	―			
				・・・					
			物理的対策	電源系統の障害に備えた、電源系統の二重化及び、UPSや無給油で24時間稼働可能な自家発電装置による瞬断及びブラックアウトへの対策を行う。					
				・・・					
			技術的対策	ネットワーク機器やサーバ機器については、合意した稼働率を満たすよう、冗長化を行う。					
				・・・					
・・・									

6. 医療分野における制度上の要求事項

医療分野において法令等で作成・保存が義務付けられた医療情報の安全管理にあたり、全ての対象事業者に対し一律の対応を求める事項を記載する。

医療情報安全管理ガイドラインにおける制度上の要求事項への対応策について、対象事業者は医療機関等に対し別紙 2 を適宜参照する等して説明すべきである。

6.1. 医療分野の制度が求める安全管理の要求事項

医療情報は患者の身体・生命に関わるものであり、その作成や保存は、医療従事者の責務として、医師法及び歯科医師法、薬剤師法、医療法等の法令において規定されている。また、医療従事者に対する業務上知り得た秘密の漏えいに関する罰則が刑法等において規定されている。

医療法では適切な医療提供体制の確保の一環として、都道府県知事等は必要に応じて医療機関等に対し、構造設備や診療録、帳簿書類その他の物件等の提出等を命じることができるとされており、当該命令に適切に対応しなかった場合の罰則も規定されている。したがって、医療機関等は調査機関等の検査に対し、適切に対応できるようにしなければならない。

以上のような法令で定められた医療機関等に対する義務や行政手続の履行を確保するために、医療情報及び当該情報に係る医療情報システムが国内法の執行の及ぶ範囲にあることを確実とすること。

6.2. 電子保存の要求事項

e-文書法の対象範囲となる医療関係文書等として、e-文書法省令や「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成 28 年 3 月 31 日付け医政発 0331 第 31 号・薬生発 0331 第 11 号・保発 0331 第 27 号・政社発 0331 第２号厚生労働省医政局長、医薬・生活衛生局長、保険局長、政策統括官（社会保障担当）連名通知。以下、「施行通知」という。）で定められた文書等については、電子保存の要件として、真正性、見読性、保存性の確保[27]が求められている。

対象事業者は、e-文書法省令や施工通知で定められた医療関係文書等については、真正性、見読性、保存性を確保すること。

---

[27] 医療情報安全管理ガイドラインによれば、真正性とは「正当な権限において作成された記録に対し、虚偽入力、書き換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であること」、見読性とは「電子記憶媒体に保存された内容を、「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応じて、それぞれの目的に対し支障のない応答時間やスループット、操作方法で、肉眼で見読可能な状態にできること」、保存性とは、「保存性とは、記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されること」とされる。

6.3. 法令で定められた記名・押印を電子署名で行うことについて

電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）では、書面における署名に代えて一定の要件を満たした電子署名により、署名と同様の証拠力を認めている。また、医療情報安全管理ガイドラインでは、法令で署名または記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、法定保存期間等の長期にわたって信頼性を持って署名を検証できること等が要求事項として定められている。法令で署名または記名・押印が義務付けられた文書等を医療情報システムで作成する場合においては、上述の電子署名を採用すること。

6.4. その他取扱いに注意を要する文書等について

施行通知で定められた文書等のほか、個人情報の保護について留意しなければならない文書等として、医療情報安全管理ガイドラインでは以下の文書が示されている。

<u>個人情報の保護について留意しなければならない文書等</u>

- 施行通知には含まれていないものの、e-文書法の対象範囲で、かつ患者の個人情報が含まれている文書等（麻薬帳簿等）
- 法定保存年限を経過した文書等
- 診療の都度、診療録等に記載するために参考にした超音波画像等の生理学的検査の記録や画像
- 診療報酬の算定上必要とされる各種文書（薬局における薬剤服用歴の記録等）等

対象事業者は、これらの文書について、医療情報安全管理ガイドラインに従い取り扱うこと。

6.5. 外部保存の要求事項

診療録及び診療諸記録については、外部保存を行う際の基準が「「診療録等の保存を行う場所について」の一部改正について」（平成 25 年 3 月 25 日付け医政発 0325 第 15 号・薬食発 0325 第 9 号・保発 0325 第 5 号厚生労働省医政局長・医薬食品局長・保険局長連名通知。以下、「外部保存改正通知」という。）により定められている。

対象事業者は、診療録等の外部保存の受託にあたり、外部保存改正通知「第 2 1 電子媒体により外部保存を行う場合」の要求事項を満たすこと。なお、当該要求事項のうち、従前の情報処理事業者ガイドライン及びクラウド事業者ガイドラインへの遵守については、本ガイドラインの遵守により代替されるものである。

用語集

アルファベット順・50 音順

ASP･SaaS (Application Service Provider･Software as a Service)	アプリケーションの利用をサービスとして提供。
IaaS (Infrastructure as a Service)	CPU、メモリ、ストレージ、ネットワーク等のハードウェア資産をサービスとして提供するクラウドサービス。
IEC 62853:2018	Open Systems Dependability（開放系総合信頼性）の国際標準。 状況が変化してもシステムが継続してサービスを提供し続けるための要件を記載。 合意形成、説明責任遂行、変化対応、障害対応の４つの観点で構成。
IEEE 802.1x	LAN におけるユーザー認証の方式の規格。IEEE 802.1x は、無線 LAN だけでなく、有線も含んだユーザー認証の方式である。クライアントが接続を要求した場合には、認証サーバである Radius サーバが認証処理を行う。クライアントが認証された場合には、セッションごとに暗号鍵が与えられる。 なお、IEEE 802.1x では通常暗号化を行わないため、無線 LAN を利用する場合には暗号化する。
IoT	情報社会のために、既存もしくは開発中の相互運用可能な情報通信技術により、物理的もしくは仮想的なモノを接続し、高度なサービスを実現するグローバルインフラのこと。
ISMS (Information Security Management System)	個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること。
MAC アドレス	Media Access Control（メディア・アクセス・コントロール）アドレス。LAN カードの中で、イーサネット（特に普及している LAN 規格）を使って通信を行うカードに割り振られた一意の番号のこと。 インターネットでは、IP アドレス以外にも、この MAC アドレスを使用して通信を行っている。LAN カードは、製造会社が出荷製品に対して MAC アドレスを管理しているため、原則同一の MAC アドレスを持つ LAN カードが 2 つ以上存在することはない。
Open Sytems Dependability	期待されるサービスを要求されたときに要求されたように提供するために、目的、目標、環境及び実際のパフォーマンスの変化に対応し、説明責任を継続的に果たす能力 (IEC 62853:2018 による) 。 オープンで変化するシステムが継続してサービスを提供し続けるための能力とみなすことができる。
PaaS (Platform as a Service)	オペレーティングシステムや、アプリケーションの実行環境（開発環境を含む）をサービスとして提供するクラウドサービス。

SLA (Service Level Agreement)	書面にしたサービス提供者と顧客との合意であって、サービス及び合意したサービスレベルを記述したもの（JIS Q 20000-1:2007）。
VPN（仮想私設網、Virtual Private Network）	不特定事業者が接続されるネットワーク上に構築された、特定の事業者間のみを接続する仮想的な閉域網のこと。
アクセスポイント	通常は、無線 LAN アクセスポイントを指す。ノートパソコンやスマートフォン等の無線 LAN 接続機能を備えた端末を、相互に接続したり、有線 LAN 等、他のネットワークに接続するための機器。
医療機関等	病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等。
改ざん	情報を不正に書き換えることである。例えば、ホームページを不正に書き換えたり、伝送途中の情報を書き換えたりする行為が挙げられる。
可用性	認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。（JIS Q 27001 を基に定義）
患者等	患者本人のほか、患者の家族等で、患者の医療情報を閲覧する権限を有する者を含む。
完全性	資産の正確さ及び完全さを保護する特性。（JIS Q 27001 を基に定義）
機密性	認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性。（JIS Q 27001 を基に定義）
脅威	組織に損害や影響を与えるリスクを引き起こす要因。（JIS Q 27001 を基に定義）
クラウドサービス	提供形態から、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）及び SaaS（Software as a Service）に分ける。また、実現形態から、プライベートクラウド、パブリッククラウド及びハイブリッドクラウドに分けることができる。
見読性	電子記憶媒体に保存された内容を、権限保有者からの要求に基づき必要に応じて肉眼で見読可能な状態にできることである。
合意形成	システム、システムの目的、目標、環境、性能、ライフサイクル、及びこれらの変化に関する共通理解と明示的合意（契約等）を確立し維持すること(IEC 62853:2018 による)。
サービス仕様適合開示書	対象事業者が、自ら提供するサービスの仕様につき、本ガイドラインへの適合状況を医療機関等へ開示するために作成するための資料のこと。詳細は、本ガイドライン第 4 章及び別紙 1 にて示す。
情報事故	機密性、完全性又は可用性が害される状態が発生すること。
真正性	正当な人が記録･確認を行った情報について、第三者にとって作成の責任の所在が明確であり、かつ、故意又は過失による虚偽入力･書換え･消去･混同 が防止されていること。
脆弱性	脅威によって悪用される可能性がある欠陥や仕様上の問題。（JIS Q 27001 を基に定義）
セキュリティターゲット	情報処理製品や情報処理システムの、セキュリティ対策方針・セキュリティ機能等を記載した文書。情報処理製品や情報処理システムの開発や改善に際して利用されるものであり、評価対象を評価する際に必要なドキュメントでもある。

対象事業者	医療機関等から医療情報の加工や保存等の処理に関連する医療情報システム提供を受託する事業者のこと。
盗聴	ネットワークに特有の事象ではなく、広く第三者が意図的に会話の内容･情報を盗み聞くこと。ネットワークでは、一般的には何らかの手段で伝送中の情報（電気信号）を盗み取ることを指す。
なりすまし	本人ではない第三者が、本人のふりをしてネットワーク上で活動すること。例えば、情報を受け取る人のふりをして不正に情報を取得する行為や、他人の ID やパスワード等を盗み出して、本人しか確認することができない情報を閲覧する行為が挙げられる。
プライバシーマーク制度	「日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度のこと。
保存性	記録された情報が法令等で定められた期間にわたって真正性を保ち、見読性が確保された状態で保存されることをいう。
無線 LAN	無線でデータの送受信を行なう LAN のこと。特に、IEEE 802.11 諸規格に準拠した機器で構成されるネットワークのことを指すこともある。
リスク	事象の発生確率と事象の結果との組合せ（目的に対して不確かさが与える影響）。（JIS Q 27001 を基に定義）
リスクアセスメント	リスクアセスメントとは、リスク特定、リスク分析及びリスク評価を網羅するプロセス全体を指す。（JIS Q 31000 を基に定義）
リスク対応	リスクに対処するための選択肢を選定し、実施すること。
リスク特定	組織の目的の達成を助ける又は妨害する可能性のあるリスクを発見し、認識し、記述すること。（JIS Q 31000 を基に定義）
リスク評価	決定を裏付けること。どこに追加の行為をとるかを決定するために，リスク分析の結果と確立されたリスク基準との比較を含む。（JIS Q 31000 を基に定義）
リスク分析	必要に応じてリスクのレベルを含め、リスクの性質及び特徴を理解すること。（JIS Q 31000 を基に定義）