参考資料９

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

令和２年８月

目次

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い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 27000）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、情報を使用させず、また、開示しない特性
- 完全性（Integrity）：正確さ及び完全さの特性
- 可用性（Availability）：認可されたエンティティが要求したときに、アクセス及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、及び、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、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、「医療情報システム等」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及び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、総務省「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 26 年 4 月、第 2 版平成 30 年 7 月）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と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。
- 医療情報システム等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等を運用するために、リスクコミュニケーションを重視する。
- 医療情報システム等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等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、医療情報システム等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

[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(ISO 31000:2018)や JIS Q 27001:2014（ISO/IEC 27001:2013)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 Systems 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。

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、医療情報システム等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。

第 6 章では、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等を提供する事業者（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等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。

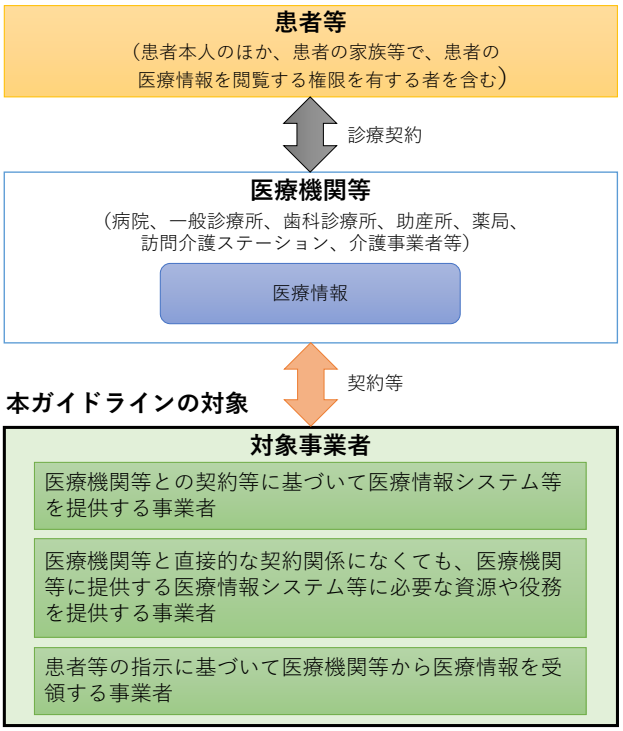

図 2-1 本ガイドラインの対象とする事業者

[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等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等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契約元の対象事業者に報告すること。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. 医療情報システム等の代表的な提供形態

本節では医療情報システム等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。

医療情報システム等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、医療情報システム等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。

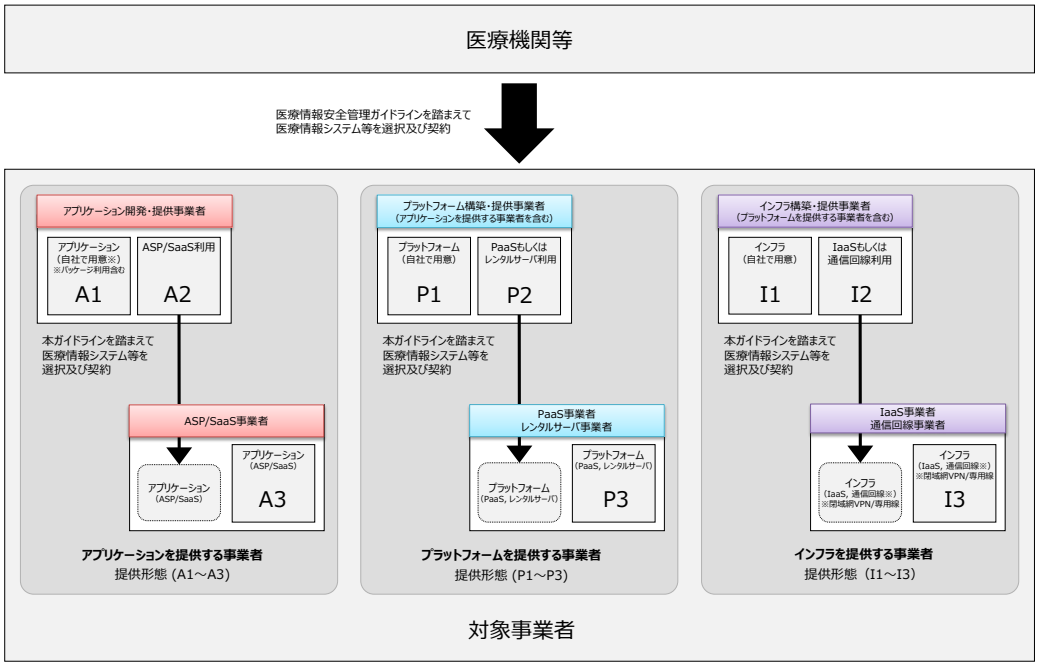

図 2-2　医療情報システム等の構成要素の類型

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等を提供するケース（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等について、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。

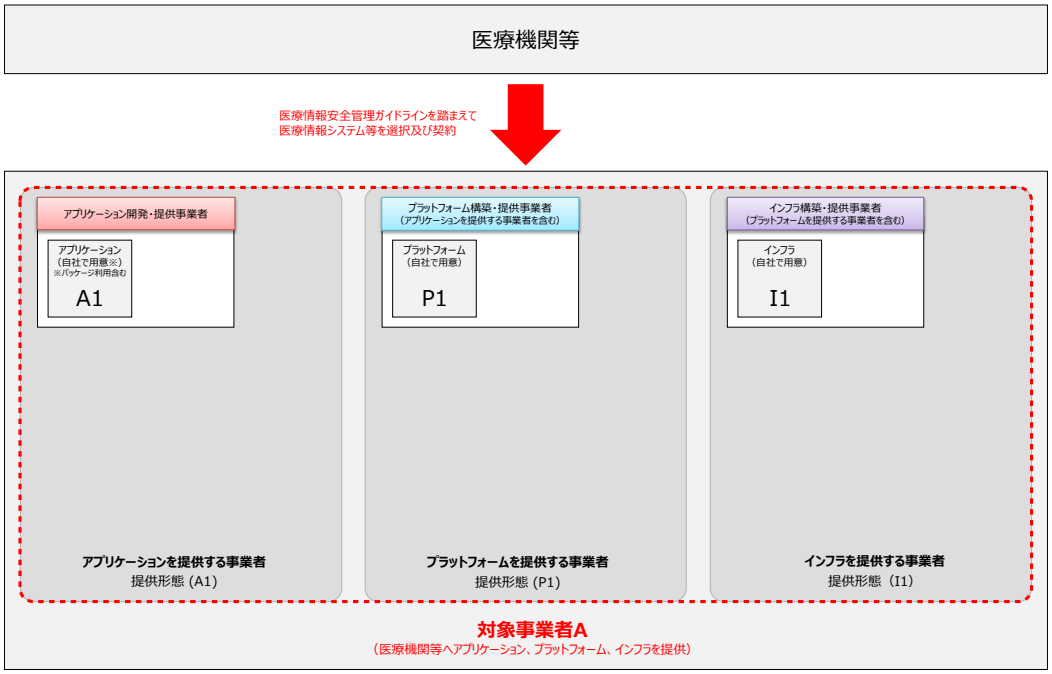

図 2-3　1 社で提供するケース（A1＋P1＋I1）

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）

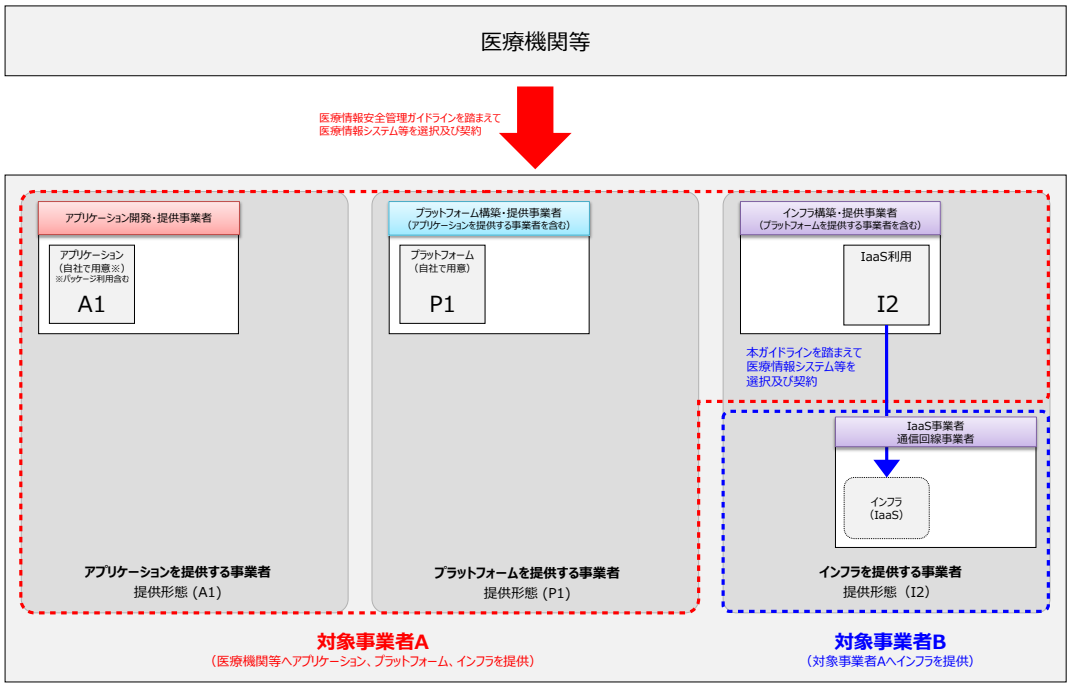

図 2-4　2 社で提供するケース（A1＋P1＋I2）

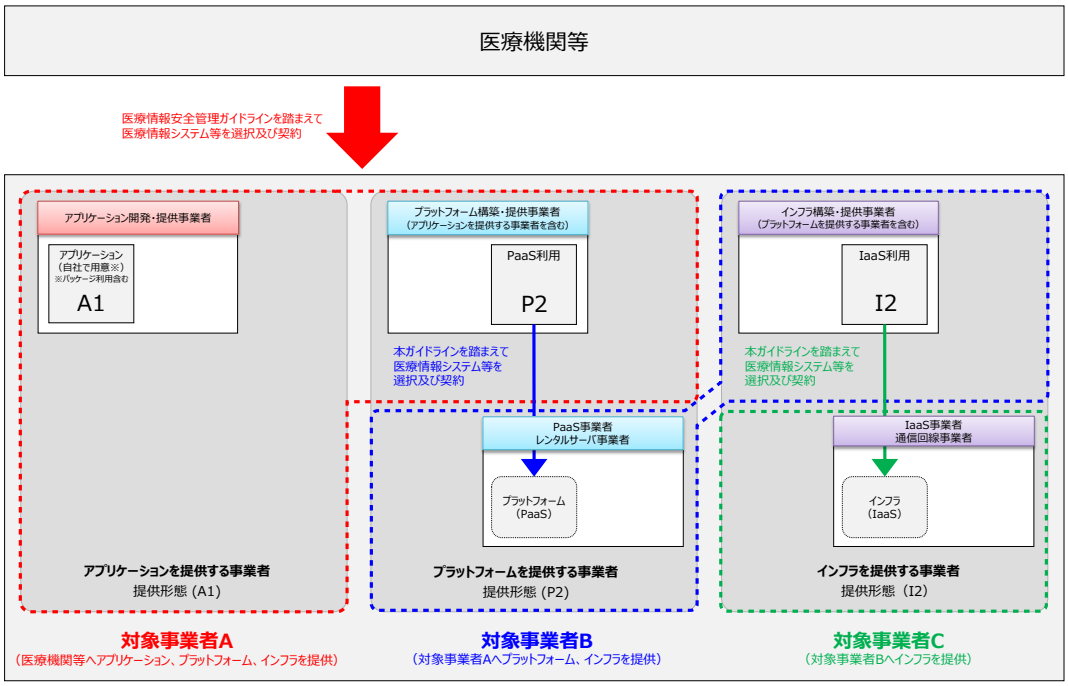

図 2-5　3 社で提供するケース（A1＋P2＋I2）

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等について、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等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等を提供すること。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。

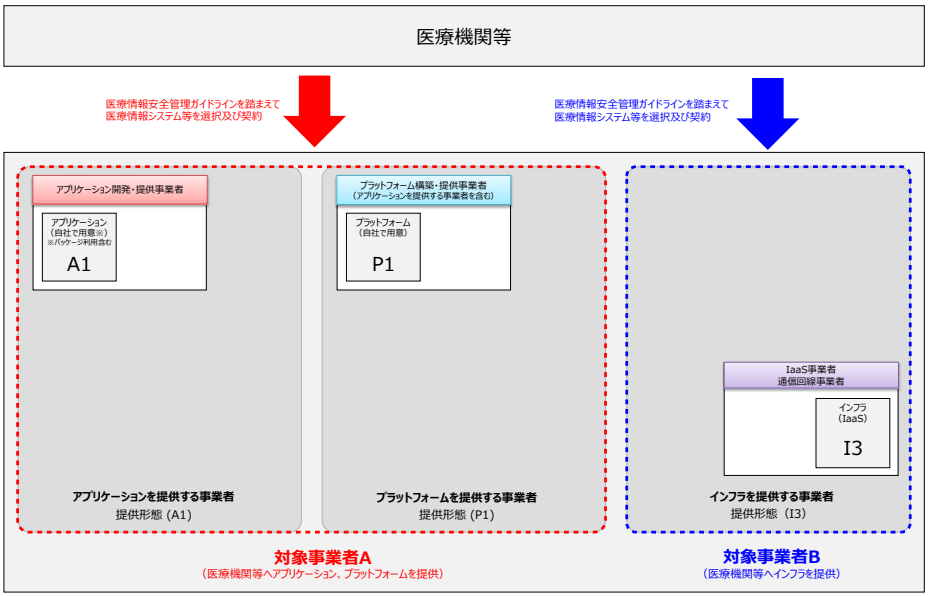

図 2-6　医療機関等が複数社と契約するケース（A1＋P1＋I3）

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、医療情報システム等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（えい）だけではなく、過失による情報開示・漏洩（えい）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。

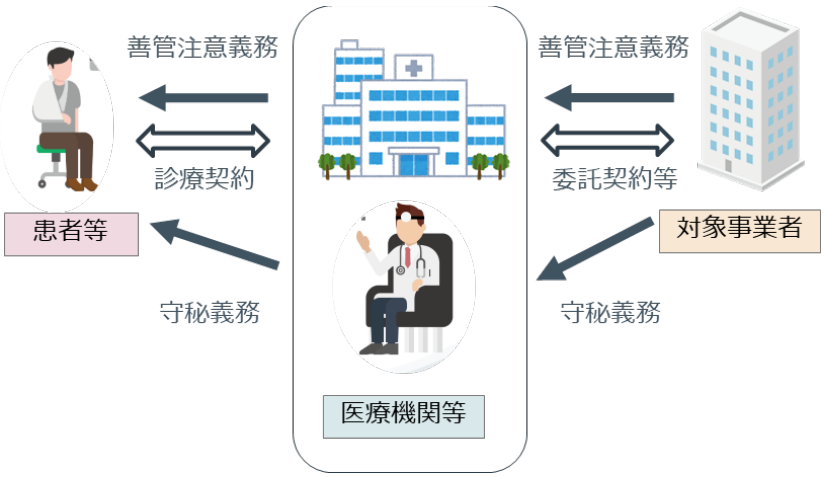

図 3-1 善管注意義務と守秘義務について

(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]。

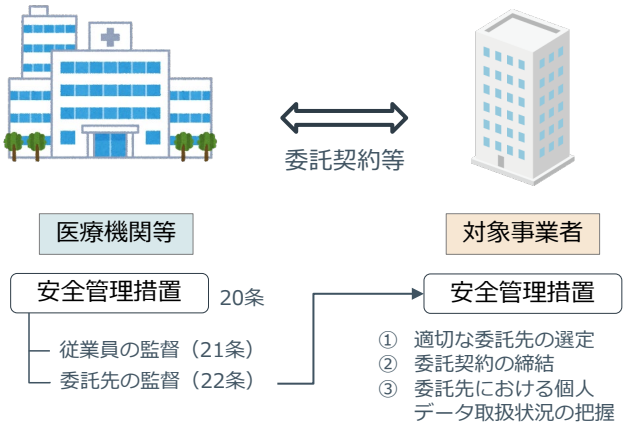

図 3-2 安全管理措置を講じる義務について

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。

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）」

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等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. 情報セキュリティ事故等発生時における義務と責任

(1) 危機対応義務

「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（えい）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、独立行政法人情報処理推進機構(IPA)より改正民法に対応した「情報システム・モデル取引・契約書」も公表されているため、参考とすること。

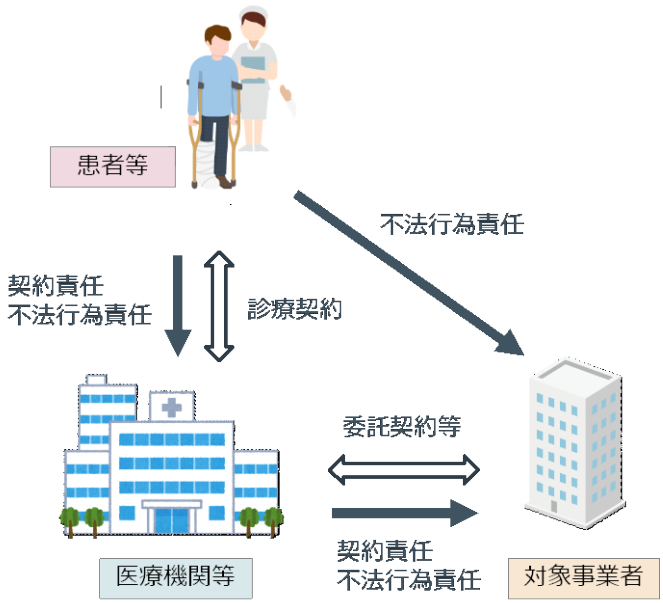

図 3-3 事後の対応における民事責任について

3.2. 医療情報システム等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等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等を対象とし、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等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. 情報セキュリティ事故等 発生時における義務と責任	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。

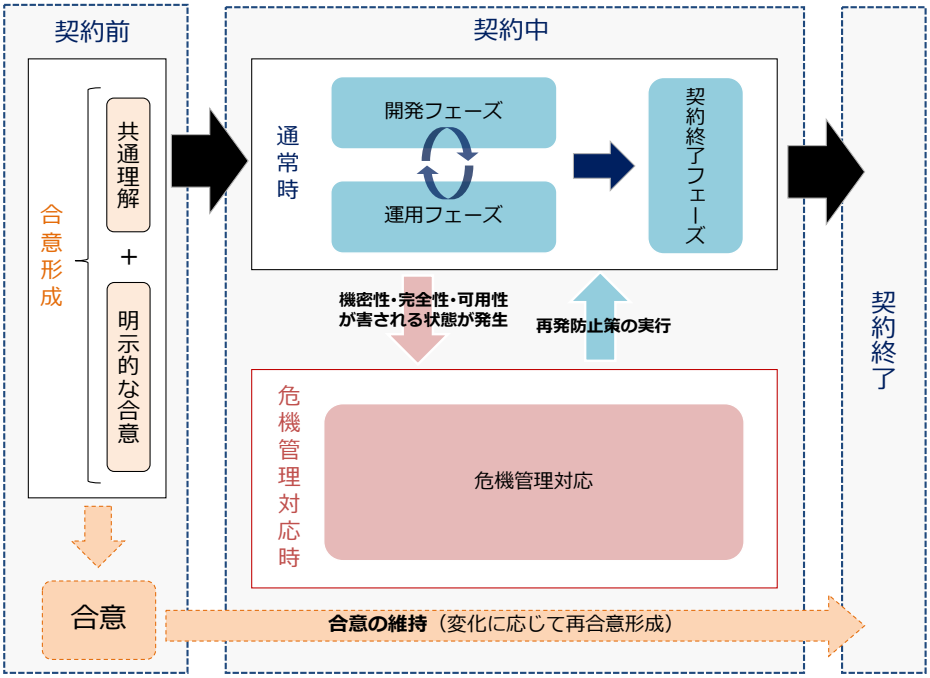

図 3-4 医療情報システム等のライフサイクル

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、情報セキュリティ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等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等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）や各医療機関等での初期設定といった、運用フェーズの前段階も広く含むものとする。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や、運用中に開発フェーズが並行発生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等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、医療情報システム等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等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、医療情報システム等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

医療情報システム等の提供に際しては、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、医療情報の漏洩（えい）や改竄（ざん）、医療情報システム等の停止等の情報セキュリティ事故が生じる可能性がある。本ガイドラインでは、このような情報セキュリティ事故が生じ、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、何らかの情報セキュリティ事故が発生した場合、発生した情報セキュリティ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

報セキュリティ事故の原因・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、発生した情報セキュリティ事故について、速やかに善後策を講じなければならない[13]。さらに、発生した情報セキュリティ事故自体に対応するための施策を講じるに留まらず、同様の情報セキュリティ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。

[13] 医療情報安全管理ガイドラインでは、情報セキュリティ事故発生時に厚生労働省への連絡を実施することが求められている。

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、医療情報システム等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。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[14]。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。

[14] 情報提供を行う際の文書例として別紙 1 に示すサービス仕様適合開示書等の参考例がある。本参考例の作成・提供は必須ではないが、本参考例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、一般社団法人日本画像医療システム工業会(JIRA)および一般社団法人保健医療福祉情報システム工業会（JAHIS）による「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等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、一般社団法人 ASP・SaaS・AI・IoT クラウド産業協会が運営する「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

目的		情報提供すべき項目
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		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
		医療情報等の安全管理に係る実施体制の整備状況
		実績等に基づく個人データ安全管理に関する信用度
		財務諸表等に基づく経営の健全性
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	医療機関等との役割分担の明確化（4.2 参照）	医療機関等の運用管理規程に定める必要がある事項
	医療情報システム等の安全管理に係る評価（4.3 参照）	医療情報システム等の安全管理に係る評価の結果
	リスクアセスメントの成果物（5.1.1、5.2.1 参照）	医療情報システム等の全体構成図
	リスク対応の成果物（5.1.5、5.2.2 参照）	リスク対応一覧
	運用管理規程に含める事項（5.1.6 参照）	医療情報システム等の安全管理に係る基本方針
		医療情報システム等の提供に係る体制
		契約書・マニュアル等の文書の管理方法
		機器等を用いる場合の機器等の管理方法
		リスク対応策の運用方法
		事故発生時の対応方法及び医療機関等への報告方法
		医療情報を格納する記憶媒体の管理方法
		医療情報の外部保存に係る患者等への説明方法
		医療情報システム等に対する監査の実施方針
		医療機関等の管理者からの問い合わせ窓口
	制度上の要求事項への対応の成果物（第 6 章参照）	制度上の要求事項への対応

4.2. 医療機関等との役割分担の明確化

医療情報システム等の安全管理には、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、医療情報システム等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. 医療情報システム等の安全管理に係る評価

対象事業者は、医療情報システム等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、医療情報システム等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、医療情報システム等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[15]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[16]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または ISMS 認証の取得が強く求められる。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[17]があり、対象事業者は、プライバシーマーク認定及び 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 。

---

15 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。

16 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。

17 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、医療情報システム等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、本章に従い、医療情報システム等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 はリスクマネジメントのプロセスを示している。

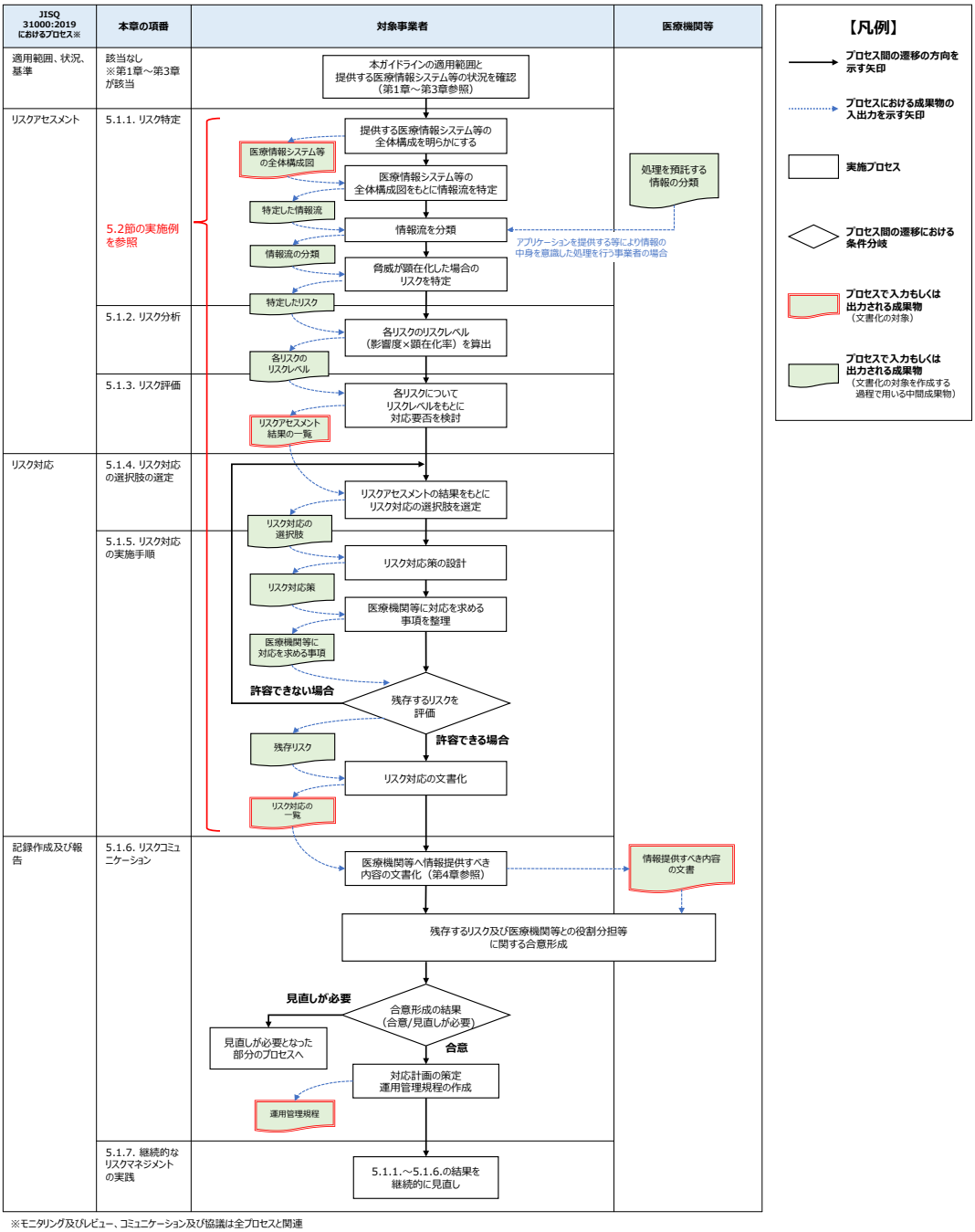

図 5-1 リスクマネジメントのプロセス

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等の全体構成図を作成することで、医療情報システム等の全体構成を明らかにすること。その上で、医療情報システム等の全体構成図をもとに、医療情報システム等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、医療情報システム等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 [18]全体を含めること。特に、医療情報システム等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「医療情報システム等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

[18] 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。

るものではない。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等の構成に応じて検討し、リスクを特定すること。

表 5-1 医療情報システム等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、医療情報システム等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	ネットワーク上を流れるデータの盗聴等により、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[19]	標的型メール等によって医療情報システム等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・漏洩	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。
情報の改竄・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。
医療情報システム等の停止	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、医療情報システム等が停止する。
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等に混入する。
機器や記憶媒体の持ち出し時の紛失・盗難	医療情報システム等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、医療情報システム等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、医療情報システム等に関連する機器や端末等が物理的に破損する等して、医療情報システム等の提供に支障をきたす。

[19] 閉域網内に構成される医療情報システム等においても、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、「医療情報システム等への影響の度合い」（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、「顕在化率」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等への機密性、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化率を特定すること。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、顕在化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、顕在化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、影響度と顕在化率をもとに、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

			顕在化率					リスクレベル（ランク）	影響度×顕在化率
			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（顕在化率及び影響度）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、医療情報システム等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 に影響度と顕在化率に応じた選択肢の考え方を示す。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。

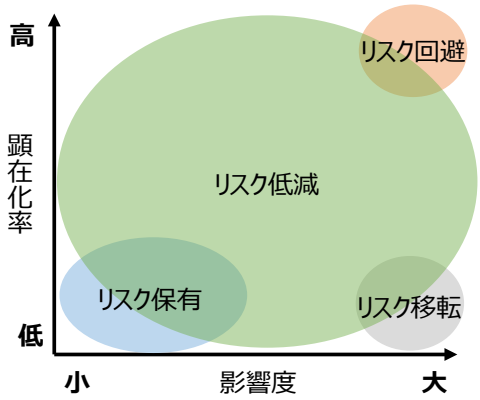

図 5-2 影響度と顕在化率に応じた選択肢の考え方

(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、影響度及び顕在化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洩（えい）リスクの影響度及び顕在化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

リスク低減を行った結果、顕在化率の低減は可能だが影響度の低減は困難なリスクについては、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、情報セキュリティ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. リスク対応策の設計・評価

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等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対応していることを確認をすることは、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[20]。

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)医療情報システム等特有の考慮事項

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

[20] 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等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 [21]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考慮事項

対象事業者は、提供するサービスに応じ、クローズドネットワークを含むネットワーク経路を適切に選択することが必要である。また、医療情報の機密性の高さや攻撃手法の高度化に鑑みた上で、様々な攻撃を想定し、適切な暗号化手法 [22]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

---

[21] 医療情報安全管理ガイドラインでは、第 5 版の公表（平成 29 年 5 月）から約 10 年後を目途に、2 要素認証の採用を「C.最低限のガイドライン」とすることが想定されている。

[22] 医療情報安全管理ガイドラインでは、専用線、公衆網、閉域 IP 通信網、IPsec を用いた VPN、HTTPS による暗号化等が例示されている。そこでは、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、SSL-VPN を原則として利用せず、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、そして、IPsec を用いる場合は、IKE を組み合わせる等して、確実にその安全性を確保するように求めている。

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。

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等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程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[23]。

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・規程の作成

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)医療情報システム等の安全管理に係る基本方針

対象事業者は、医療情報システム等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

[23] 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開示し、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）医療情報システム等の提供に係る体制

対象事業者は、医療情報システム等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[24]を有する責任者（システム管理者）、医療情報システム等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定め、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については、必要に応じて速やかに内容を確認できるようにすること。また、文書の不正な閲覧・操作をアクセス制限等により防止することを運用管理規程に含め、第三者による不正な閲覧・操作を防止すること。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、情報セキュリティ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。

---

[24] 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)医療情報システム等に対する監査の実施方針

対象事業者は、医療情報システム等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等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等提供にあたり、他社が提供する医療情報システム等を利用する場合は、他社が提供する医療情報システム等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、医療情報システム等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[25]。

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等の例を用いて、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

[25] 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。

節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。

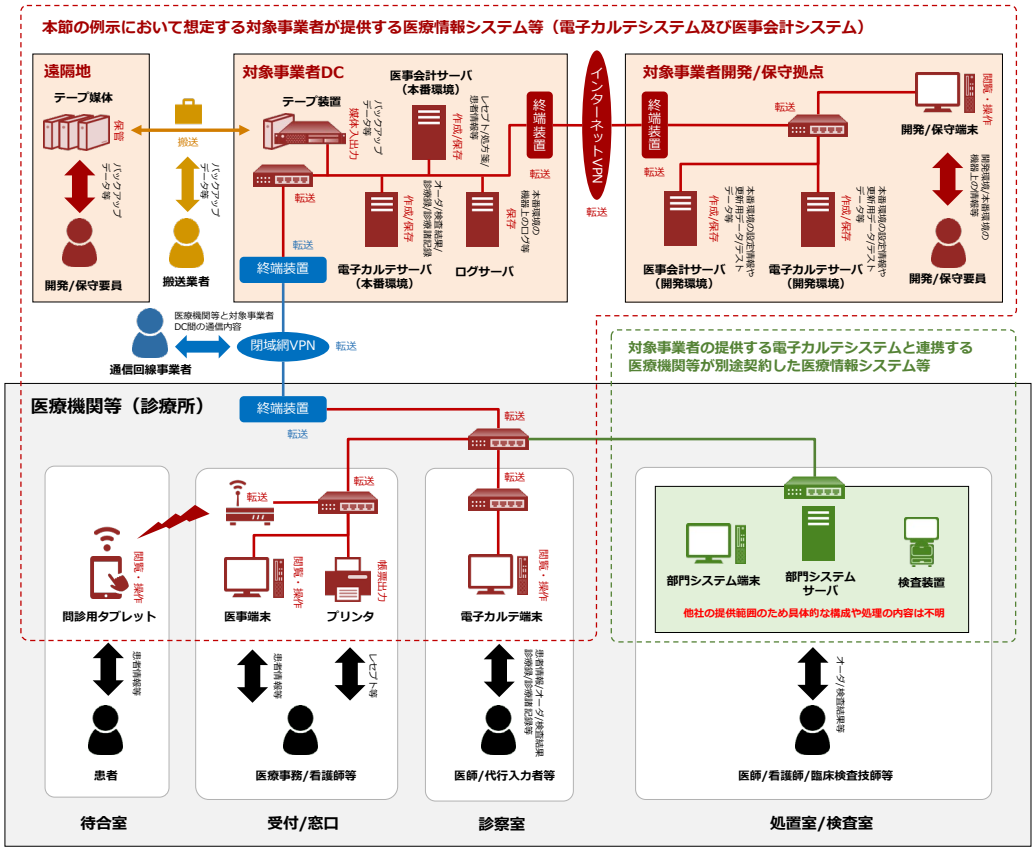

図 5-3 本節の例示に用いる医療情報システム等の全体構成図

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等の全体構成図の作成

医療情報システム等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等についても、自社が提供する医療情報システム等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[26]や記憶媒体があるかを可能な限り明らかにする（図 5-4）。

[26] クラウドサービス等における仮想マシンを含む。

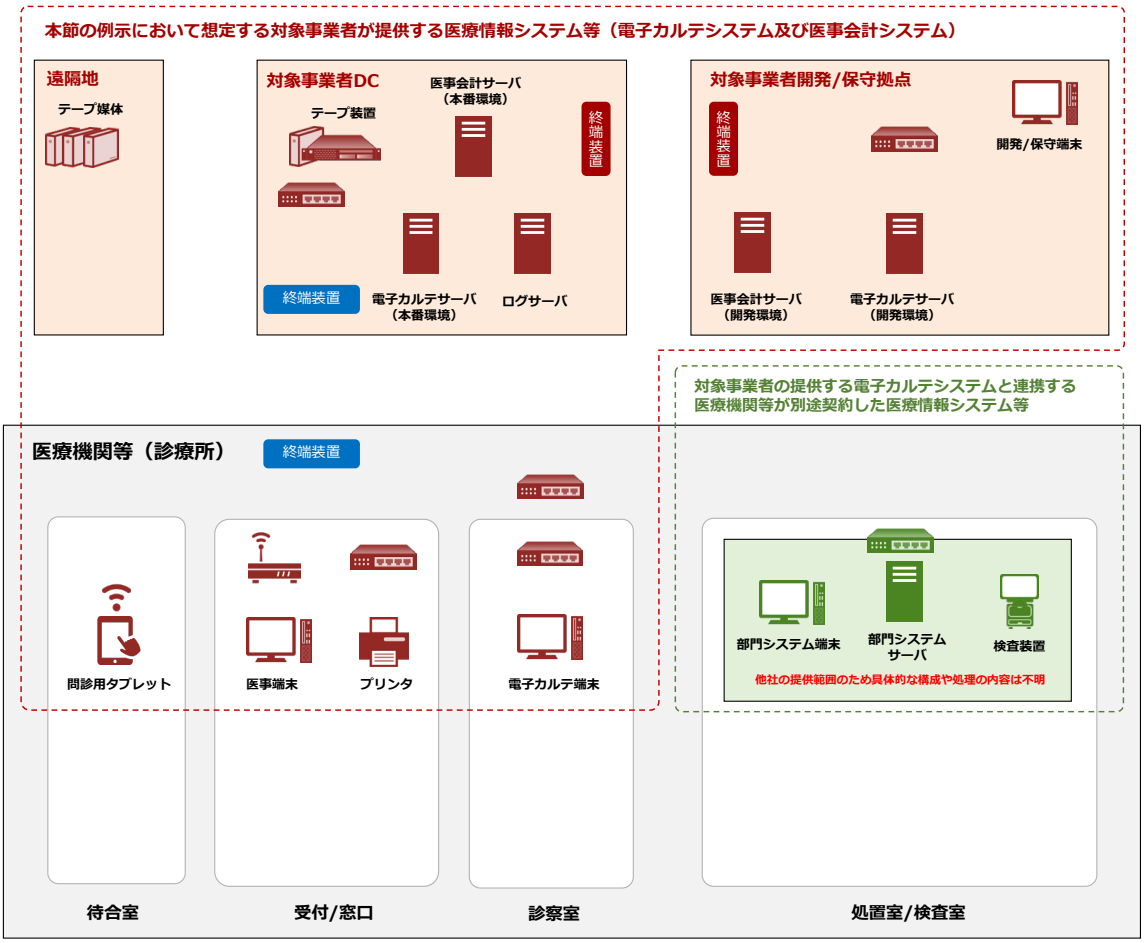

図 5-4 医療情報システム等の全体構成図の作成例（手順 1）

【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。

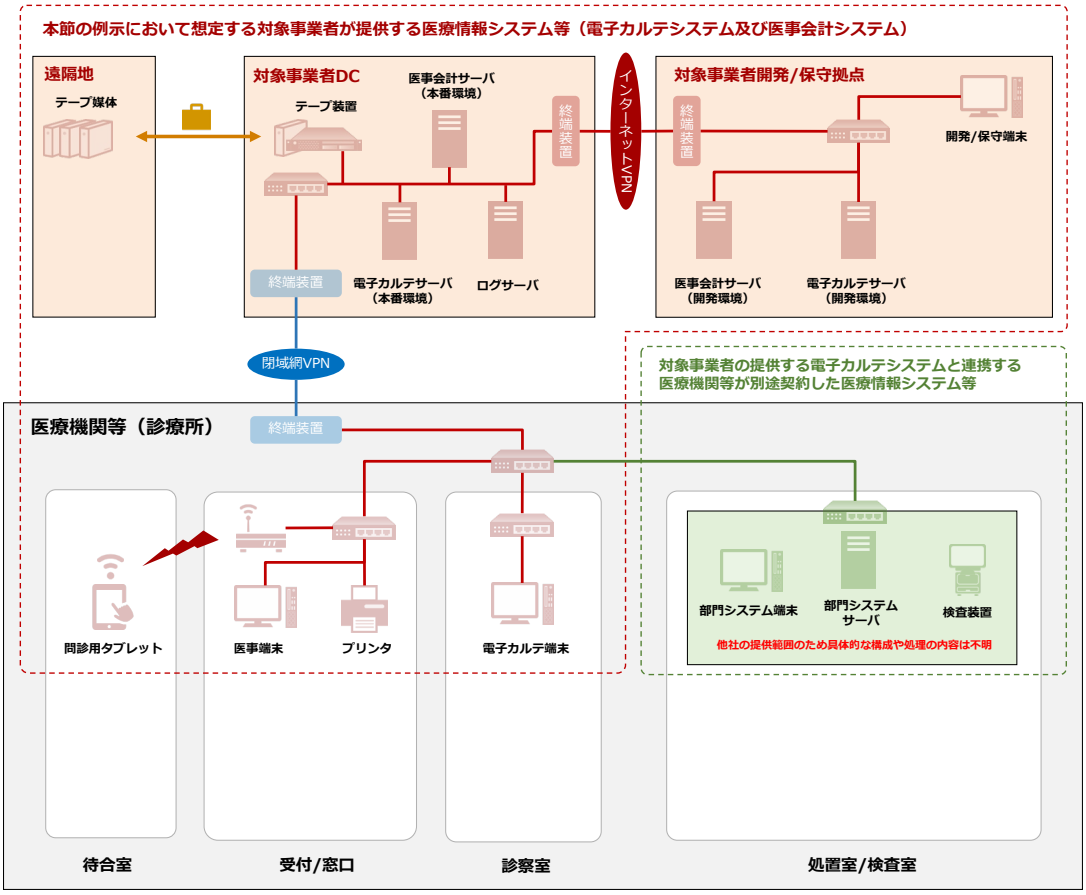

図 5-5 医療情報システム等の全体構成図の作成例（手順 2）

【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[27]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、対象事業者データセンター（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。

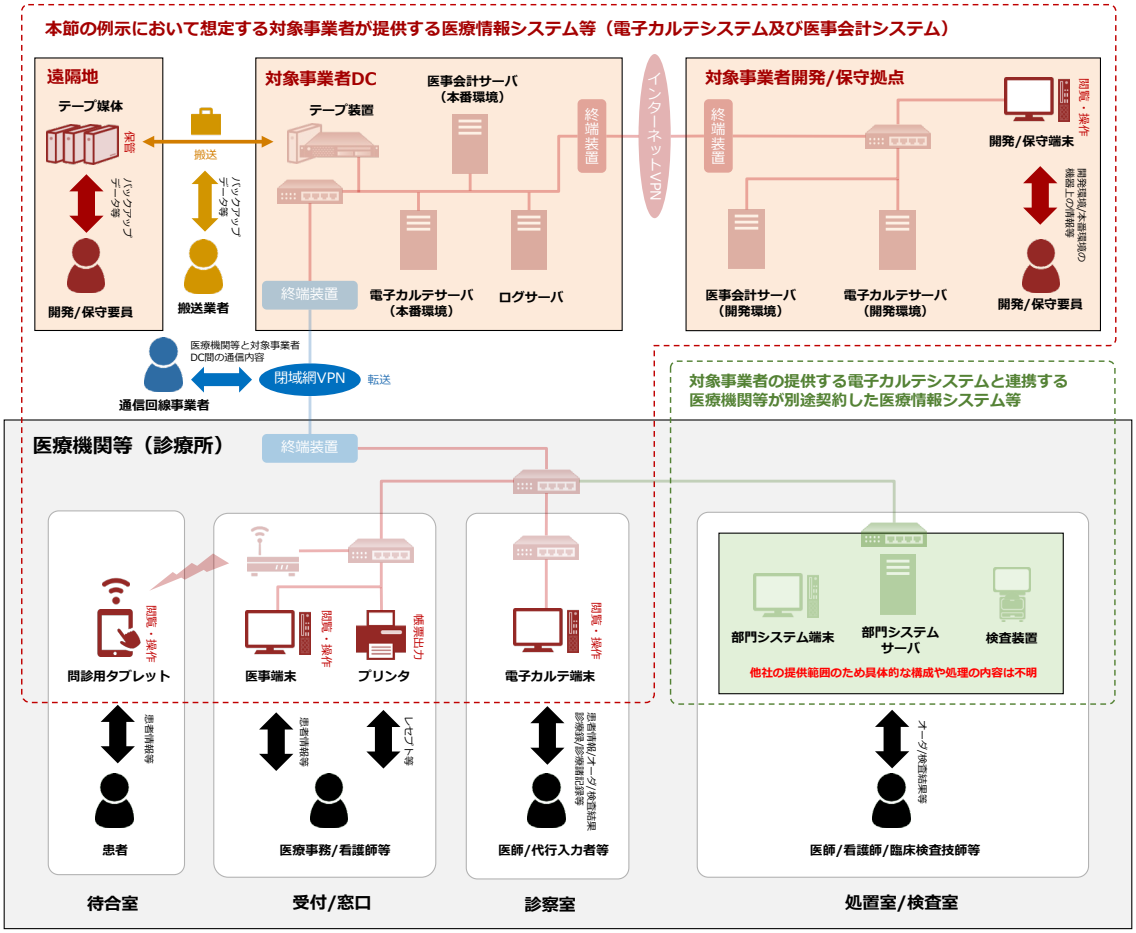

図 5-6 医療情報システム等の全体構成図の作成例（手順 3）

[27] 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

- 対象事業者データセンター（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。

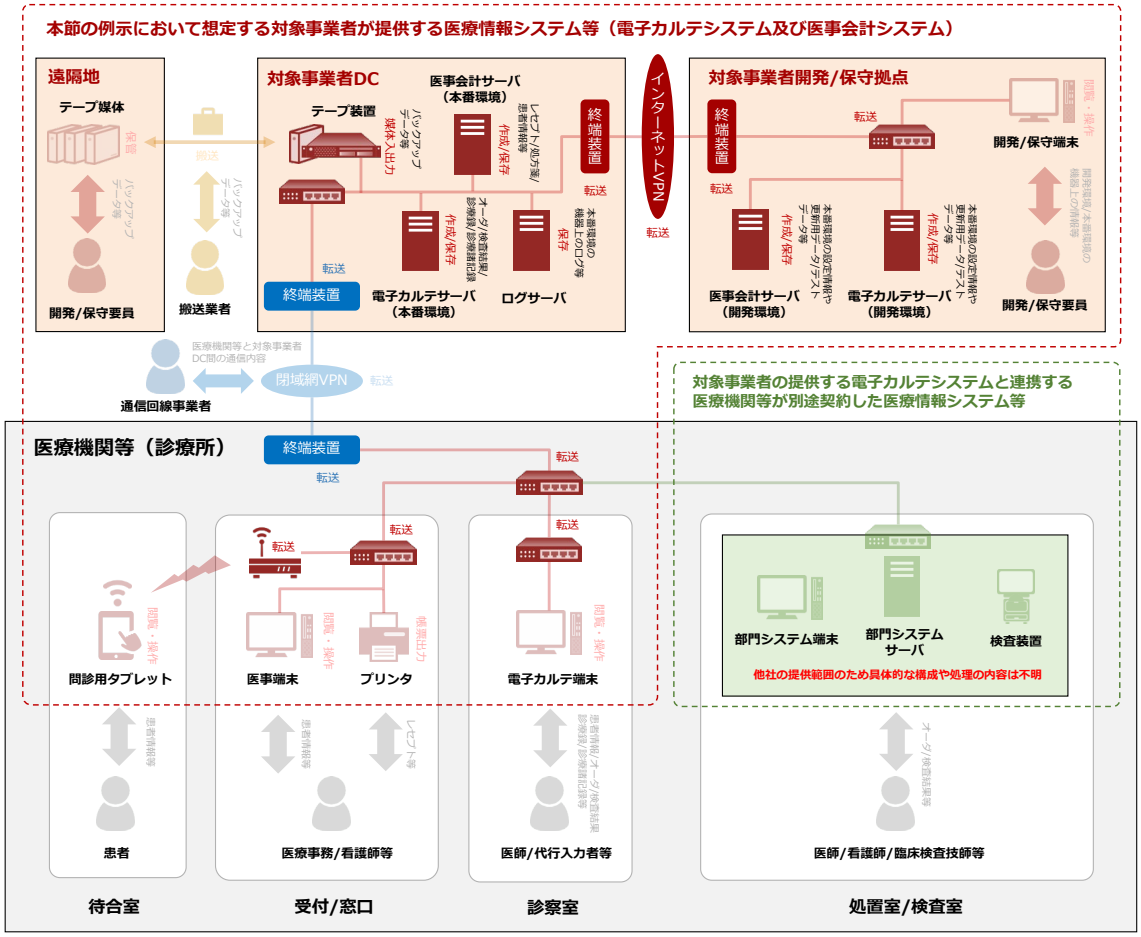

図 5-7 医療情報システム等の全体構成図の作成例（手順 4）

(2) リスク特定における情報流の特定

医療情報システム等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等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やサーバ機器で	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や端末で		
		有線LAN上のネットワーク機器や端末で		

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やサーバ機器で	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	有線LAN上のネットワーク機器やサーバ機器で		
		開発保守端末で		
	医療機関内の	無線LAN上のネットワーク機器や端末で		
		有線LAN上のネットワーク機器や端末で		
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、脅威の顕在化を想定して特定したリスク、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	顕在化率	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
				・・・				
		情報の改竄・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竄・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洩・改竄・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	顕在化率	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洩・改竄・破壊が生じる	5	3	A	要
				・・・				
		情報の改竄・破壊		アプリケーション提供に係る情報の改竄・破壊が生じる	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洩・改竄・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	顕在化率	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	顕在化率	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竄・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	顕在化率	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洩・改竄・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。	ー			
				・・・					
			物理的対策	ー					
			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・漏洩が生じる	低減	人的・組織的対策	ー	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	ー					
			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	顕在化率	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。	ー	ー			
				・・・					
			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。	ー	ー			
				・・・					
			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. 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洩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等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」の一部改正について」（平成 28 年 3 月 31 日付け医政発 0331 第 30 号・薬生発 0331 第 10 号・保発 0331 第 26 号・政社発 0331 第 1 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 [28]が求められている。

対象事業者は、e-文書法省令や施行通知で定められた医療関係文書等については、真正

[28] 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。

性、見読性、保存性を確保すること。

6.3. 法令で定められた記名・押印を電子署名に代える場合の要求事項

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等で作成する場合においては、上述の要件、要求事項を満たす電子署名を採用すること。

6.4. 取扱いに注意を要する文書等の要求事項

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。
ICT サプライチェーン	情報通信技術(ICT)に関わるシステム・サービス等の企画・設計・製造・流通・運用等の各プロセス。または当該プロセスを構成するシステム・組織等のこと。
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 Systems 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、サービス及びサービス目標を特定した、サービス提供者と顧客との間の合意

	文書(JIS Q 20000-1:2012)。
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。
医療情報システム等	医療情報を取り扱う情報システムやサービス
改竄（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 27000 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	正確さ及び完全さの特性。（JIS Q 27000 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、情報を使用させず、また、開示しない特性。（JIS Q 27000 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。
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。
顕在化率	リスクが顕在化する可能性。
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。
情報セキュリティ事故	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。
情報流	提供される医療情報システム等における、電子的又は物理的な情報の流れ。
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。
セキュリティタ	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

ーゲット	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等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	日本産業規格「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	目的に対する不確かさの影響。事象の結果とその起こりやすさ(発生確率)との組み合わせ。
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）
リスクコミュニケーション	リスクマネジメントの実効性を高めるために、医療機関等と対象事業者の双方によって実施される活動のこと。対象事業者から医療機関等への情報提供等の一方向的な活動だけでなく、医療機関等の疑問や要求に応えながら、共通理解を得る双方向的な活動が重要視される。
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）
リスクベースアプローチ	一律の要求事項を定めるのではなく、顕在化しうるリスクの内容に応じた対応方法の選択を実施する手法のこと。

略語集

50 音順

医療情報安全管理ガイドライン	医療情報システムの安全管理に関するガイドライン
クラウド事業者ガイドライン	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
情報処理事業者ガイドライン	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

参考文献

- 情報セキュリティマネジメントシステム要求事項（JIS Q 27001:2014）
  2014 年 3 月　日本工業標準調査会審議（日本規格協会発行）
- 情報セキュリティ管理策の実践のための規範（JIS Q 27002:2014）
  2014 年 3 月　日本工業標準調査会審議（日本規格協会発行）
- 情報セキュリティリスクマネジメント（ISO/IEC 27005:2018）
  2018 年 7 月　国際標準化機構及び国際電気標準会議
- JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範（JIS Q 27017:2016）
  2016 年 12 月　日本工業標準調査会審議（日本規格協会発行）
- PII プロセッサとして作動するパブリッククラウドにおける個人識別情報(PII)の保護のための実施基準（ISO/IEC 27018:2019）
  2019 年 1 月　国際標準化機構及び国際電気標準会議
- Open Systems Dependability（IEC 62853:2018）
  2018 年 6 月　国際電気標準会議
- SSL/TLS 暗号設定ガイドライン（第 2.0 版）
  2018 年 5 月　独立行政法人情報処理推進機構
- 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）
  2017 年 2 月　個人情報保護委員会
- 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
  2017 年 7 月　一般社団法人保健医療福祉情報システム工業会
- 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
  2017 年 3 月　総務省

別紙１

ガイドラインに基づくサービス仕様適合開示書及び

サービス・レベル合意書（SLA）参考例

令和２年８月

内容

本参考例の利用法について

１．　本参考例の目的

本参考例は、「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」（以下、「提供事業者ガイドライン」という）に基づいて、対象事業者が医療機関等に対してサービスの提供を行う際に求められる合意事項等を整理し、サービス仕様適合開示書[1]及びサービス・レベル合意書（SLA）参考例という形でまとめたものである。

２．サービス仕様適合開示書について

対象事業者と医療機関等が容易に合意形成することができるよう、情報提供すべき内容として記載すべき項目の参考例であり、対象事業者はサービス仕様適合開示書を医療機関等に提供し、医療機関等はこれに基づいて医療情報システム等の選択を行い、両者はその内容を踏まえた形でサービス内容の合意を図ることを想定している。なお、本開示書はその一つの例示であり、本開示書の作成・提供は必須ではないが、対象事業者は、このような開示書等を用いて、医療機関等に対して対応状況を開示・説明した上で、合意形成を図ることが求められる。

３．SLA 参考例について利用方法及び利用上の留意点

SLA は、医療情報システム等において、提供するサービスの具体的なサービスの内容、水準、免責内容などに関して、対象事業者と医療機関等の顧客の間で合意するものである。

本 SLA 参考例では、医療情報システム等において合意すべき具体的な内容を、提供事業者ガイドラインに則して、診療所向け診療録の作成・保存等の処理を行うクラウドサービスを想定したひとつのサンプルとして条項案を提示している。従って、提供するサービスの内容や医療機関等と対象事業者との役割分担の範囲、又は契約当事者間の交渉等により、この参考例の内容を変更、削除、追加する必要があることに留意されたい。また、対象事業者が提供するサービスの形態によっては、必要な条項についてのみ提供することも想定される。

本参考例の SLA では、各項目において「【本項を定める上での考え方】」を記述した。これは本参考例を記述する際に想定した内容や、本参考例を変更・加除する際に

[1]「医療情報システム等仕様における『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』への適合性の開示書」（以下「サービス仕様適合開示書」という）

念頭に置くべき考え方を概説するものである。本参考例を踏まえて、実際にSLA等を作成する際には、「【本項を定める上での考え方】」の内容を理解の上、利用されたい。

また２．で示すように、サービス仕様適合開示書に記載されている内容を以って、提供サービス内容として合意するために、サービス仕様適合開示書を添付し、SLAの内容とすることも想定される。

I.参考例編（サービス仕様適合開示書）

１．サービス仕様適合開示書参考例

（１） 医療機関等が医療情報安全管理ガイドラインに基づき、医療情報を取り扱う情報システム・サービスの事業者の選定にあたり最低限確認する必要がある内容

① 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

上記文書の整備状況	開示方法･条件･範囲

※本項目については、提供事業者ガイドラインの 5.1.6(2)(ア)参照

② 医療情報等の安全管理に係る実施体制の整備状況

情報セキュリティに関する役職	役職及び氏名	役割
管理責任者		
システム管理者		
運用管理責任者		
個人情報保護責任者		

※本項目については、提供事業者ガイドラインの 5.1.6(2)(イ)参照

③ 実績等に基づく個人データ安全管理に関する信用度

個人情報の流出事故がない旨の実績
受託情報の目的外利用、不当利用等を行っていないことに対する実績

④ 財務諸表等に基づく経営の健全性

上記内容を示す文書名	開示方法･条件･範囲

（2） 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内容

① 医療機関等の運用管理規程に定める必要がある事項

医療機関等の運用管理規程に定める必要がある事項

② 医療情報システム等の安全管理に係る点検や評価の結果

点検や評価の内容	点検や評価の実施者	点検や評価の結果の開示方法・条件・範囲

③ 医療情報システム等の全体構成図

上記内容を定めた文書名	開示方法・条件・範囲
・本サービスの全体構成図（例※）	

※当該資料の具体的な作成イメージについては、提供事業者ガイドラインの 5.2 節参照

④ リスク対応一覧

上記内容を定めた文書名	開示方法・条件・範囲
・リスク対応一覧（例※）	

※当該資料の具体的な作成イメージについては、提供事業者ガイドラインの 5.2 節参照

⑤ 医療情報システム等の安全管理に係る基本方針

上記内容を定めた文書名	開示方法・条件・範囲

※本項目については、提供事業者ガイドラインの 5.1.6(2)(ア)参照

⑥ 医療情報システム等の提供に係る体制

(a) サービス提供体制

部門	役割
電子カルテ事業部（例）	*本サービス提供を行う責任部門（例）*
コールセンター事業部（例）	*顧客問い合わせ対応部門（例）*

※本項目については、提供事業者ガイドラインの 5. 1. 6(2)(イ)参照

※緊急時には上記のほか、電子カルテ事業部を管轄する取締役の指揮管理に基づく。（例）

(b) サービス提供に係る再委託の状況

再委託事業者の有無(ある場合には事業者名)	再委託事業者がある場合には、再委託業務内容
○×株式会社(例)	*サービス提供用システム保守(例)*
・・・・・	

⑦ 契約書・マニュアル等の文書の管理方法

上記内容を定めた文書名	開示方法・条件・範囲

※本項目については、提供事業者ガイドラインの 5. 1. 6(2)(ウ)参照

⑧ 機器等を用いる場合の機器等の管理方法

上記内容を定めた文書名	開示方法・条件・範囲

※本項目については、提供事業者ガイドラインの 5. 1. 6(2)(エ)参照

⑨ リスク対応策の運用方法

上記内容を定めた文書名	開示方法・条件・範囲

※本項目については、提供事業者ガイドラインの 5. 1. 6(2)(オ)参照

⑩ 事故発生時の対応方法及び医療機関等への報告方法

事故発生時の対応方法及び医療機関等への報告方法
・受託する医療情報が漏洩した場合には、弊社危機管理本部により、原因の究明、被害拡大の防止、所管官庁への報告及び指示への対応、その他お客様の情報の安全性の確保に必要な対応を行います。(例) *・受託する医療情報が漏洩した場合には、漏洩状況について弊社ホームページ並びにお客様管理者へお電話にてご連絡いたします。(例)* *・受託する医療情報が漏洩した場合には、その原因が明確になるまで、サービスの一部又は全部の提供を停止することがあります。(例)*

※本項目については、提供事業者ガイドラインの 5. 1. 6(2)(カ)参照

⑪ 医療情報を格納する記憶媒体の管理方法

上記内容を定めた文書名	開示方法・条件・範囲

※本項目については、提供事業者ガイドラインの 5. 1. 6(2)(キ)参照

⑫ 医療情報の外部保存に係る患者等への説明方法

医療情報の外部保存に係る患者等への説明方法
本サービスの利用に係る患者等への説明については、第一次的にはお客様において対応して頂くこととし、弊社においては必要な資料等の提供等の範囲で対応させていただきます。 *お客様において受託する情報を分析し、あるいは第三者に提供するために必要な加工を施す際に求められる患者等への説明と同意に関しても同様といたします。(例)*

※本項目については、提供事業者ガイドラインの 5. 1. 6(2)(ク)参照

⑬ 医療情報システム等に対する監査の実施方針

監査の実施方針	監査結果の概要に関する開示の有無	開示する場合の開示方法・条件・範囲

※本項目については、提供事業者ガイドラインの 5. 1. 6(2)(ケ)参照

⑭ 医療機関等の管理者からの問い合わせ窓口

医療機関等の管理者からの問い合わせ窓口
【サポートセンター】 連絡先 03-++++-++++(例) *受付対応時間* *平日・土曜日 午前 7 時～午後 10 時(例)* *日曜日・祝日 午前 9 時～午後 5 時(例)*

※本項目については、提供事業者ガイドラインの 5. 1. 6(2) (コ)参照

⑮ 制度上の要求事項への対応

(a) 医療分野の制度が求める安全管理の要求事項

サービス提供に際して遵守している個人情報に係る法令、ガイドライン・ガイダンス
・個人情報保護法及び同施行令、施行規則 (例) *・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、外国にある第三者への提供編、第三者提供時の確認・記録義務編) 【個人情報保護委員会】 (例)* *※ なお、下記のガイドライン、ガイダンスについても、事業者として対応しております。* *・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【個人情報保護委員会・厚生労働省】 (例)* *・医療情報システムの安全管理に関するガイドライン第 5 版【厚生労働省】(例)*
医療情報システム等及び医療情報に対する国内法の適用状況

※本項目については、提供事業者ガイドラインの 5. 1. 6(2) (ア)参照

(b) 電子保存の要求事項

サービスに提供に際して処理を行う e-文書法の対象範囲となる医療関係文書

(ア) 真正性の確保

医療機関等に保存する場合の要求事項への対応	
対応項目	対応内容
医療情報安全管理ガイドライン 7.1 C.最低限のガイドライン	
(1) 入力者及び確定者の識別及び認証	

(2) 記録の確定手順の確立と、識別情報の記録	
(3) 更新履歴の保存	
(4) 代行入力の承認機能	
(5) 機器・ソフトウェアの品質管理	
ネットワークを通じて医療機関等の外部に保存する場合の要求事項への対応	
対応項目	対応内容
医療情報安全管理ガイドライン 7.1 C.最低限のガイドライン	
(1) 通信の相手先が正当であることを認識するための相互認証を行うこと	
(2) ネットワーク上で「改竄(ざん)」されていないことを保証すること	
(3) リモートログイン機能を制限すること	

(イ) 見読性の確保

保存する場所について共通する要求事項への対応	
対応項目	対応内容
医療情報安全管理ガイドライン 7.2 C.最低限のガイドライン	
(1) 情報の所在管理	
(2) 見読化手段の管理	
(3) 見読目的に応じた応答時間	
(4) システム障害対策としての冗長性の確保	
医療機関等に保存する場合の要求事項への対応	
対応項目	対応内容
医療情報安全管理ガイドライン 7.2 D.推奨されるガイドライン	
(1) バックアップサーバ	

(2) 見読性確保のための外部出力	
(3) 遠隔地のデータバックアップを使用した見読機能	
ネットワークを通じて医療機関等の外部に保存する場合の要求事項への対応	
対応項目	対応内容
医療情報安全管理ガイドライン 7.2 D.推奨されるガイドライン	
(1) 緊急に必要になることが予測される診療録等の見読性の確保	
(2) 緊急に必要になるとまではいえない診療録等の見読性の確保	

(ウ) 保存性の確保

医療機関等に保存する場合の要求事項への対応	
対応項目	対応内容
医療情報安全管理ガイドライン 7.3 C.最低限のガイドライン	
(1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止	
(2) 不適切な保管・取扱いによる情報の滅失、破壊の防止	
(3) 記録媒体、設備の劣化による読み取り不能又は不完全な読み取りの防止	
(4) 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止	
医療情報安全管理ガイドライン 7.3 D.推奨されるガイドライン	
(1) 不適切な保管・取扱いによる情報の滅失、破壊の防止	
(2) 記録媒体、設備の劣化	

による読み取り不能又は不完全な読み取りの防止	

(c) 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

サービスの提供に際して法令で定められた記名・押印を電子署名で行う文書

要求事項への対応	
対応項目	対応内容
医療情報安全管理ガイドライン 6.12 C.最低限のガイドライン	
(1) 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局又は認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと	
(2) 電子署名を含む文書全体にタイムスタンプを付与すること	
(3) 上記タイムスタンプを付与する時点で有効な電子証明書を用いること	

(d) その他取扱いに注意を要する文書等の取扱い

サービスの提供に際して処理するその他取扱いに注意を要する文書等

(e) 外部保存の要求事項

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及び個人情報保護法への準拠状況

１．本サービスの目的と対象

１．１ 本サービスの目的

【サービス名】（以下、「本サービス」という）の目的及び対象は下記のとおりである。

(1) 本サービスの目的

本サービス（サービス名）は、××株式会社【対象事業者名】（以下、「乙」という）が●●クリニック【医療機関等名】（以下、「甲」という）に対して、クラウドサービスにより診療録の作成、その保存、及びそれに伴うサービスを提供することを目的とする。なお、ここで言う診療録とは、医師法第 24 条 1 項に定めのあるものを指し、当然に保存義務を含めた医師法、医療法等の要件を満たすものである。

(2) 本サービスの対象

本サービスの対象は、診療所とする。

【本項を定める上での考え方】

・本項では、SLA により提供されるサービスの目的を明示する。
・本例では、サービスの目的を、診療所向け診療録の作成・保存等のサービスを想定して提供することを明示している。
・クラウドサービスの提供目的等により、医療機関等及び対象事業者双方の想定されるリスクが異なり、これに応じて提供すべきサービスのレベル等にも大きく影響することから、SLA の前提の一つとしてサービス提供の目的を明確にすることが重要である。
・対象事業者が提供するサービスを、医療機関の業務との関係でどのような目的で利用するのかを明示することにより、SLA の各項目の内容の妥当性を判断することに寄与するものである。
・また、SLA で記述されていない項目についての実施内容の妥当性を判断する際に、その判断基準ともなりうることからも、可能な限り明確にすることが、対象事業者、医療機関等の両当事者にとって重要である。

１．２ 本サービスの提供範囲

本サービスの提供範囲は下記のとおりである。なお、詳細は「別紙１サービス提供システム概要」、「別紙２　提供サービス全体構成図」を参照のこと。

(1) クラウドサービス

本サービスでは、乙は、１．１に示す目的で利用するアプリケーションをクラウドサービスとして甲に提供する。また甲の本サービスの利用に係る技術的なサポート、運用に関わる報告等も本サービスの提供範囲とする。

(2) ネットワークサービス

甲が本サービスの利用に際して必要となるネットワークサービス（ネットワーク回線サービス及びVPNサービス）は、本サービスには含まない。

(3) 使用機器等

甲が本サービスの利用に際して必要となる端末（PC）、ネットワーク機器等の提供及びこれらに係る技術的サポートは、本サービスに含まない。

(4) 本サービスの利用に供するソフトウェア

甲が本サービスの利用に際して必要となるソフトウェア（OS及びブラウザー）の提供及びセットアップ等は、本サービスには含まない。技術的なサポートについては、本サービスの利用に必要な範囲で、本サービスの提供範囲とする。

【本項を定める上での考え方】

・本項では、SLAにより提供されるサービスの提供範囲を明示する（本書では「別紙１」及び「別紙２」に該当するものは添付していない）。
・本例では、クラウドサービスのみを提供し、機器、ソフトウェア、ネットワークサービス等を含まない事例を想定している。専用ブラウザ等が必要なクラウドサービスの場合には、提供するソフトウェア等を明示する必要がある。
・クラウドサービスでは、対象事業者が利用者の使用機器の調達、設定、ネットワークサービスの提供まで含む一元的なサービスを提供するケースから、クラウドサービスの利用のみをサービスとするケースまで多様なサービス展開が考えられる。サービスの提供範囲は後述の責任分界とも密接に関わる。
・サービス提供範囲は、提供サービスのコストと関連するが、利用者側に十分サービス範囲を理解してもらわないままにすることにより、医療情報の取り扱いに際して、不測のトラブルの発生要因にもなりうる。

・サービス提供範囲については、必要に応じて図表等も含める等、できるだけ相手方の理解を深められるようにすることが重要である。

１．３ 本サービスの提供時間

本サービスは、７．１(2)の「事前に合意された事由」に基づく停止を除き、24 時間提供する。

本サービスの提供に当たり、乙の通常業務時間は以下のとおりである。

【平日・土曜日】 8:00～21:00

【日曜・祝日】 8:00～17:00

【本項を定める上での考え方】

・本項では、本サービスの提供時間を明示する。
・サービス提供時間は、対象事業者が提供するサービスの「量」に当たるものである。SLA との関係では、サービス稼働率などの算定の根拠にもなる。またサポートなどの周辺業務の対応時間等にも関連する部分でもあり、全体的には、サービス費用に影響しやすい項目である。
・本例で示すサービス提供時間は、定期保守等による停止以外の 24 時間とし、その中でサポートなどを行う対象事業者の通常業務時間を別途定義している。実際には医療機関等における業務の必要性により、決定する内容である。対象事業者と医療機関等において、十分協議の上、定めることが望ましい。
・本例で示すサービス提供時間は、あくまでも例示であるので、対象事業者のサービス内容や、医療機関等の要請を勘案して変更されることを想定している。

２．本 SLA について

２．１ 本サービスにおけるサービスレベル合意書の意義

本サービスにおけるサービスレベル合意書（以下、「本 SLA」という。）の意義は下記のとおりである

(1) クラウドサービスを利用する際の医療情報の安全性の確保を図る

本 SLA においてサービス内容及びレベルを明確にすることにより、甲が本サービスを利用して医療情報を取り扱うに際して、各種法令、ガイドラインを満たすものであることを確認することが可能となる。結果、甲が医療情報の取り扱いの安全性を確保することができる。

この趣旨に鑑みて、乙は、本サービスを利用する際に、甲が甲の医療情報が安全かつ適切に管理されていることを確認できることを支援しなくてはならない。同時に、甲に提供するアプリケーション及びシステム運用に変更が生じた場合の影響範囲を分析、把握し、主体的に必要な対応を取ることによって、サービス品質の確保に努めることが求められる。

(2) 医療業務等への影響の把握

本 SLA により、アプリケーションの機能変更やシステム運用に変更等がなされた場合においても、サービス品質の低下を避けるため、あらかじめ合意された客観的指標を用いての評価が可能となる。

(3) サービス品質とコストの妥当性を図る

本サービスのサービスレベルを本 SLA で明確化することにより、必要な品質のサービスを妥当なコストで安定的に提供することが可能となる。

(4) 各役割分担の明確化を図る

本 SLA で、甲と乙との役割分担を明確にすることにより、サービス提供に際しての不明瞭な部分を排除することが可能となる。また甲において別途契約する事業者（ネットワーク事業者、機器提供事業者等）との役割分担・対応も含めて明確にすることにより、不測の事態が生じた際にも速やかに対応を図ることが可能となる。

【本項を定める上での考え方】

・本項では、本サービスのサービスレベルに合意する意義を明示する。
・通常のサービスレベルの合意では、対象事業者と利用者の間でサービス品質と価格の妥当性を明確にすること、役割分担を明らかにすることで各種リスクを回避すること等を内容とすることが多いが、医療情報を取り扱う場合は、サービス内容を明らかにすることが、サービス利用時の安全性の確保に資することにつながる。
・サービスレベル合意書において、サービス内容を明確にする際には、このような視点も含めて項目を整理することが重要である。

２．２ 本サービスにおけるサービスレベル適用の考え方

本サービスにおけるサービスレベル適用の考え方については、下記のとおりである。

(1) 電子カルテの利用に鑑みたサービスレベルの適用

本サービスは、甲が診療行為を行う際に必要な情報の作成、表示、保存等を目的とするものである。サービスの提供に当たっては、診療行為の重要性・重大性に鑑みたサービス品質の確保を考えることが必要である。具体的には、

・診療録の作成、表示、保存において改竄（ざん）等のリスクを最小化すること
・診療行為を行う時間帯において、利用が不能となるリスクを最小化すること
・サービスの提供に重大な障害が生じた際には、速やかに復旧を可能にするための、回復措置又は代替措置を講じること

等を念頭に置いたサービスレベルの設定や適用が求められる。

(2) 情報システムに関する管理業務についてのサービスレベル

甲が本サービスを用いて医療情報を取り扱うに際し、その安全性の確保を、専門的な技術を有する乙において支援することが求められる。本サービスにおける運用管理及び報告に関するサービスの内容も、このような視点が求められる。

【本項を定める上での考え方】

・本項では、本サービスにおけるサービスレベル適用の考え方を明示する。
・サービスレベルの適用においては、１．１(1)で記述した目的等を踏まえて、具体的なレベルの設定やこれに基づくサービスの提供を行う必要があるが、その際にサービス特性（提供するアプリケーションの内容、形態、提供するサービスの範囲等）等を踏まえて行うことが必要となる。このような観点を整理して記述する。

２．３ 本 SLA の適用期間

本 SLA の適用期間は、下記のとおりとする。なお、本 SLA は、乙において管理するシステムの外部・内部の環境変化に応じて、必要に応じて都度、改定が行われるものとし、改定の度に適用期間を定めるものとする。

版数	適用開始日	適用終了日
第 1.0 版	平成 30 年 4 月 1 日（契約開始日）	平成 31 年 3 月 31 日（契約終了日）

本項で明示する適用期間を越えて本サービス利用契約が継続する場合には、適用期間経過後も引き続き、本 SLA が適用されるものとする。

【本項を定める上での考え方】

・本項では、本サービスにおけるサービスレベル適用期間を明示する。
・サービスレベルの適用期間は、通常は利用契約に連動して設定されるが、クラウドサービスの場合には、利用期間を定めない契約も多い。その場合には、一般的には 1 年以上の期間の適用期間を定めるか、契約期間終了までを適用期間として定める。
・本例では、SLA の適用期間が経過しているにもかかわらず、利用契約自体が継続している場合の考え方について、一般的な継続的契約に関する考え方を採用し、医療機関等側、対象事業者側で新たな取り決めがあるまでは、サービス内容も維持されるものとしている。

２．４ 本 SLA の改定

(1) 改定の契機

本 SLA は、必要に応じて見直しを実施し、改定する。改定時は、改版履歴に改定内容を明記する。改定の契機は、下記のとおりとする。

・ 双方の合意事項に明確な変更があった場合
・ その他、双方責任者が必要と認めた場合

(2) 変更の手続き

本 SLA の改定が必要となった場合は都度、双方で協議の上、サービスレベル変更の内容を合意する。

・サービスレベル変更の必要が生じた場合、乙が改定案を作成する。
・改定案を甲に提出し、双方で協議する。
・双方で合意承認を得た後、乙は改定版として発行し、双方で保管する。

【本項を定める上での考え方】

・本項では、本 SLA の改定手続について示す。
・SLA の改定は定期的に実施する方法と、改定期間を示さずに必要に応じて実施する方法がある。本例では後者の方法を記述している。
・改定を定期的に実施する方式では、例えば、改定時期を毎年 4 月等に定めて実施することが想定される。
・「双方の合意事項に明確な変更があった場合」の例としては、例えば新たなサービスをクラウドサービスとして提供することになった場合等の環境やリスクの変化により対策の見直しが必要となった場合等が挙げられる。また「双方責任者が必要と認めた場合」については、例えば、法令、ガイドライン等の変更により、別途対応措置が必要となるような場合等が挙げられる。

３．前提条件

３．１ リスクマネジメント

本サービスの提供において、乙は、乙が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に準拠したリスクマネジメントに基づいて受託情報の管理を行う。

本サービスの提供に係るリスクマネジメントは、乙は年次及び乙が必要と認める場合に妥当性や有効性の評価と見直しを実施する。

本項で示す乙の行うリスクマネジメントに関する情報については、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、サービス提供の前提として、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に準拠したリスクマネジメントを実施して行う旨を示す。

・この観点からサービス提供の前提条件として、対象事業者においてリスクマネジメントを実施したうえで対策を講じており、その資料については、医療機関等の求めに応じて提供する旨を、SLA として定めた例を示している。

・なお、「Ⅰ.参考例編（サービス仕様適合開示書)」の（２）③及び④では、サービス選択をするのに必要な範囲での、リスクマネジメントの結果を開示するための成果物を示している。これらの成果物は、セキュリティ情報でもあることから、サービス仕様適合開示書により一般的な開示が難しいものについては、本項にあるように、６．６(3)(運用状況に係る情報提供について)により、提供することになる。

３．２ サービス利用環境

乙は、本サービスで提供するアプリケーションについて、別紙「サービス利用環境」に示す利用環境における稼動を保証する。

別紙の内容は、予告の上、適宜変更を行う。

最新のサービス利用環境については、【http://+++.****.jp/----/（乙の用意するWeb 上のページ)】にて公開する。

【本項を定める上での考え方】

・本項では、アプリケーションを利用するための利用者側の環境を示す。具体的な環境については、別紙に規定する方式を採用している（本書では「別紙」に該当するものは添付していない。各対象事業者が、提供サービスに応じて作成することを想定している。)。

・クラウドサービスの場合、多くはWebブラウザ等が使用されるが、動作の正確性や表示の正確性を確保する観点から、利用に供されるOSやブラウザの製品名、バージョン情報、アプリケーションによってはセキュリティパッチへの対応の有無等が動作保証の条件とされる場合がある。また、使用するPCに関する仕様や、ネットワーク回線の仕様等も動作保証条件、又は推奨環境等の形で明示されることがある。

・本項では、提供する医療情報システム等の利用環境を明示することにより、利用環境に関する医療機関等側、対象事業者側の責任の範囲を明らかにすることにもなるため、可能な限り具体的にする。そのほか、必要に応じて都度更新し、正確な内容をサービス利用者に伝えることが必要である。

３．３ サービス提供環境・運用に係る前提条件

本サービスの提供に係る受託情報、プログラム等の保存、及びこれらに関するサーバ等の機器類の設置については、乙が委託する【委託先データセンター会社名】データセンターにて行う。ただし本サービス提供に係る運用をリモートアクセスで行う範囲で、乙所定の場所に、乙は運用に供する機器を設置する。

乙は本サービスの提供に係る受託情報、プログラム等の保存、及びこれらに関するサーバ等の機器類は、日本国の法令の適用が及ぶ場所に設置する。

乙は、本サービス運営上、データセンター等での機器や通信回線の増強、運用に係るプログラムの改善等を目的とし、必要最小限の範囲で、受託された情報の利用状況（例えばハードディスク容量、データへのアクセス状況、回線のトラフィック等）に関する統計データの取得を行う。

乙は、本サービス提供に際し、個別の障害対応等に際して、受託された医療情報を、甲との事前の合意に基づき参照することがある。また、セキュリティ対応上、必要と考えられる受託情報へのアクセス状況やシステム負荷の状況等を統計化することがある。

本項で示すサービス提供環境・運用に関する乙の対策内容、実施状況等の情報については、６．６(2)、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、対象事業者のサービス提供環境・運用に係る前提条件について示す。
・具体的な内容として本項では、サービス提供に係る機器等の所在、データセンターの所在、運用管理に必要な受託情報等の利用等を前提条件として示す。
・サービス提供に係る機器等の所在につき、本例では委託先データセンターに格納する旨を示す。データの所在については、データセンターかそれ以外（例えば自社サーバルーム）か、データセンターが自社のものか委託先のものかを明示することが求められる。また委託先の場合、委託先会社名も併記することが求められる。
・運用等により、リモートアクセスを行う場合には、その有無を明記する必要がある。再委託事業者による場合も同様である。これらの所在については、再委託事業者の項（４．３）、運用組織の項（６．１(1)）において、明確にすることが望ましい。なお、「Ⅰ.参考例編（サービス仕様適合開示書)」では、(2) ⑮（ｂ）(ア)でリモートログイン機能の制限に係る実施状況を示している。
・医療情報を取り扱う医療情報システム等に供する機器等については、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により、国内法の執行が及ぶ場所に設置することが求められる（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 6.1)。本例の第 2 段落はこの内容を示すものである。

・本例の第 3 段落では、サービスの運用上不可欠なハードウェアや回線の利用状況の把握について記載している。
・本例の第 4 段落では、サービス提供上生じた個別の障害対応等に際して、受託する医療情報をやむを得ず参照する場合や、セキュリティ対応上、必要と考えられる受託情報へのアクセス状況やシステム負荷の状況等を例として示している。なお、「Ⅰ.参考例編（サービス仕様適合開示書)」では、(2) ⑮（ｂ）（ア）で実施している機器・ソフトウェア等の品質管理を示している。
・本例の第 5 段落では、対象事業者が行うこれらの対応内容や状況について、医療機関等の求めに応じて情報提供を行う旨について、示している。

３．４ 機器・ソフトウェアの品質

乙は、下記に示す事項を実施し、本サービスの提供に係るソフトウェア及びサーバ等の機器類の品質管理を行う。

・ サービス提供に供するハードウェア及びソフトウェア等の仕様の明確化
・ ハードウェア及びソフトウェア等の導入の妥当性を示すプロセス、及び改定履歴等の文書化の実施
・ サービス提供に供する機器、ソフトウェアの品質管理の手順の策定及びその実施。
・ サービス提供に供するシステム構成やソフトウェアの動作状況に関する内部監査の実施

本項で示す品質管理に関する乙の対策内容、実施状況等の情報については、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、対象事業者に課せられる機器・ソフトウェアの品質管理を示す。なお、「Ⅰ.参考例編（サービス仕様適合開示書)」では、(2) ⑮（ｂ）（ア）で実施している機器・ソフトウェア等の品質管理を示している。
・品質管理については、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においても、仕様や導入プロセスの明確化や品質管理に係る文書化、内部監査等の実施が示されている。
・本例では、同ガイドラインの記述内容に準じた対応を対象事業者が行うことを SLA で明記することとしている。
・品質管理に関しては、医療機関等の求めに応じて、実施状況等の資料を提出することを本例では示している。対象事業者によっては、ISO 9001 及び/又は ISO 20000 等の認証を取得している場合には、これを取得していることをもって、資料提出に代える等も想定される。

３．５ 準拠する法令・ガイドライン等

本サービスの提供に当たり、乙は、下記に示す法令及びガイドラインを遵守する。

・個人情報の保護に関する法律（平成 15 年法律第 57 号）
・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（総務省、経済産業省　令和〇年〇月）

なお、上記ガイドラインの遵守は、下記のガイダンス及びガイドラインに記述された趣旨を理解した上で、実施する。

・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（個人情報保護委員会、厚生労働省 平成 29 年 4 月 14 日）
・医療情報システムの安全管理に関するガイドライン　第 5 版（厚生労働省　平成 29 年 5 月）

乙は、甲から受託する医療情報につき、その内容及び件数等が、「個人情報の保護に関する法律」の対象とならない場合（例えば死者に関する情報）等であっても、医療情報の重要性から同法における運用に準じて取り扱う。

【本項を定める上での考え方】

・本項では、対象事業者が遵守している法令及びガイドラインについて明示する。
・対象事業者が遵守すべきガイドラインとしては、本項で記述したガイドラインが挙げられる。また、それらのガイドラインに対応する医療機関等が遵守すべきガイダンス、ガイドラインの 2 つについても、その中で示されている医療機関等の情報システムの管理責任者が追うべき責務を理解することが望ましい。
・個人情報保護法及び施行令では、死者の情報については、個人情報には当たらないとされている。しかし医療情報の重要性、機微性に鑑みると、死亡した患者に関する情報についても、生存する者の情報と同様に取り扱う必要があり、また、取り扱う個人情報の件数によって安全管理対策を講じる必要性は変わらない。

３．６ 守秘義務等

乙は、本サービスの提供に当たり、業務上知り得た情報に対する守秘義務を全うするため、下記の対応を行う。

・ 乙は、従業員に対し、業務上知り得た秘密（個人情報を含む）に関する守秘義務を課すること。
・ 乙は、個人情報の取り扱いに関する業務に従事させることを予定して採用する従業員に対し、守秘義務を課して雇用契約を締結すること。
・ 乙は、従業員が退職した後も、その従業員が在職中に業務上知り得た秘密（個人情報を含む）を保護するための守秘義務規定を個人情報保護規程等で文書化すること。
・４．３に示す再委託事業者又はサービス提供に際して用いる他の事業者が提供するサービス（連携クラウドサービス）を提供する事業者（連携対象事業者）が、業務上の必要により診療録の個人情報にアクセスする際に知り得た個人情報につき、乙は、上記事業者に守秘義務を課すとともに、これに違反した場合の罰則等の措置を講じることを内容とする契約を締結すること。

【本項を定める上での考え方】

・本項では、対象事業者の負うべき守秘義務に関して、対象事業者が使用する従業員や再委託事業者、連携対象事業者に対する具体的な守秘義務について明示する。
・対象事業者は、医療機関等から医療情報を受託する場合に、業務上知り得た情報に対して守秘義務が課せられるのは当然であるが、これを対象事業者が使用する従業員や再委託事業者、連携する対象事業者に対する具体的な守秘義務として課することにより、医療情報の保護を徹底する趣旨である。上記内容は、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においても示されており、本項はその内容を明示するものである。

３．７ 監査

乙は、本サービスの提供に関するサービス仕様及び運用状況等につき、年次で内部監査を実施し、その結果を甲に対して報告する。

乙が実施する内部監査については、乙において定める規程に基づいて実施する。その規程等の具体的な内容、及び監査結果についての詳細な実施状況等の情報については、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、対象事業者が実施する監査について明示する。なお、「Ⅰ.参考例編（サービス仕様適合開示書)」では、（２）⑬で実施するシステム監査の概要を示している。
・医療情報安全管理ガイドライン、医療機関等に対して運用管理規程に監査に関する規定を盛り込むこととしているほか（6.3 C)、各対策項目において内部監査を求めている（例えば、7.1 C)。
・本例では、本 SLA で定めるサービス仕様に関する内容及び運用状況について、対象事業者が内部監査を年次で実施し、その結果を医療機関等に報告する旨を明示している。
・また、クラウドサービスの特殊性から、報告方法については、本 SLA 参考例６．５(1)②にしたがって実施することを想定し、医療機関等が個別により詳細な実施状況の資料等を求める場合には、別途資料提供を行うという形式としている。
・対象事業者において、例えば、ISO27001 等の第三者認証制度を取得している場合には、当該認証に係る検査の結果をもって監査結果に代える等も想定される。

４．役割分担

４．１ システム構成上の役割分担と責任（各ベンダー間等の役割分担）

(1) 本サービス提供に対する責任

乙は、提供するアプリケーションが正常に稼動し、甲が利用できることについての責任を有する。サービスの提供に係るアプリケーションに障害等が発生し、それによってサービスレベルが低下した場合、その対応の責任を負う。

【本項を定める上での考え方】

・本項では、本サービス提供に対する責任について明示する。
・クラウドサービスでは、サービスの提供は、1 事業者がアプリケーションに関する機能を提供する場合のほか、複数の事業者がそれぞれのサービス（ネットワークや通信サービス、PC 等の端末の提供・管理サービス等）を提供した上で、当該クラウドサービスを活用する場合等がある。
・本項では対象事業者が、自己が提供するサービスについて責任を負う範囲について明示する。

(2) 本サービスの甲における利用環境に係る具体的な役割分担と責任

① 利用環境に関する役割分担と責任

甲における本サービスの利用環境において、甲が利用する機器等に関する役割分担及び責任については、下記のとおりとする。

・甲が本サービスの利用に関して設置する PC 等の端末については、甲が必要な設定及びセキュリティ対策を実施するとともに、それを適正に管理する責任を有する。乙は、甲が必要とする情報収集の支援を行う。
・甲が本サービスの利用に関して設置するネットワークサービスを利用するための通信機器等については、甲が必要な設定及びセキュリティ対策を実施するとともに、それを適正に管理する責任を有する。乙は、甲が必要とする情報収集の支援を行う。
・本サービスの利用に関して、甲がその管理する施設において設置する LAN（無線 LAN を含む）については、甲が必要なセキュリティ対策を実施するとともに、その管理責任を有する。乙は、甲が必要とする情報収集の支援を行う。
・甲が設置する本サービスの利用に連携した臨床検査システムや医用画像ファイリングシステム等については、甲が必要な設定及びセキュリティ対策を実施するとともに、それを適正に管理する責任を有する。乙は、甲が必要とする情報収集の支援を行う。

本サービスの甲における利用環境につき、甲が利用するサービス等に関する役割分担及び責任については、下記のとおりとする。

・本サービスの利用に関して、甲が外部から利用するために必要となるネットワークに対する不正侵入の防止措置については、甲が必要なセキュリティ対策を実施するとともに、それを適正に管理する責任を有する。乙は、甲が必要とする情報収集の支援を行う。
・本サービスの利用と連携するため、甲が導入する他のクラウドサービス等のサービス、アプリケーション、及びその他のシステム等については、甲が必要な設定及びセキュリティ対策を実施するとともに、それを適正に管理する責任を有する。乙は、甲が必要とする情報収集の支援を行う。

乙が行う上記に関する甲への情報収集の支援に際し、乙において郵送費、出張費用等の実費等が生じる場合には、甲の負担とする。

【本項を定める上での考え方】
・本項では、利用者側の役割分担について明示する。

・クラウドサービスでは、事業者側が後述のように一定のサービス仕様に基づくサービスを提供し、そのために必要な運用を行うが、医療機関等においてもサービスを利用するために一定の役割を果たすことが求められる。
・本例では、本サービスの利用に当たり、利用者側で用意すべき機器やサービス（ネットワーク等）についての役割分担のほか、外部からの当該クラウドサービスの利用や、当該対象事業者が関与しないクラウドサービスの利用に伴う設定についての役割分担を例示している。
・本項で示す内容は、あくまでも例であり、具体的な内容については、対象事業者と医療機関等により協議することが求められる。その際、対象事業者は、専門的な知見からの協力を行うことが望ましい。

② 障害一般に関する役割分担と責任

本サービスにおいて、利用上の障害が発生した場合の役割分担及び責任については、下記の場合には、乙は、その責任において対応を行う。

・本サービスの提供に際して障害等が生じた場合に、乙は、甲の連絡又は自己の判断に基づき、その原因の調査を行い、報告する（第一次対応）。
・第一次対応の結果、障害の要因が乙の管理する、機器、アプリケーション等のシステム、ネットワーク、又はこれに関連するサービス等に起因するものであることが判明した場合には、乙の責任として速やかに対応を行う。

下記の場合には、乙は、本サービスの利用に関して甲が利用するベンダー等と復旧に必要な対応をとるための協議を行う。これに関して、甲は乙が必要とする対応を行う。

・第一次対応の結果、障害の要因が甲の管理する、機器、アプリケーション等のシステム、ネットワーク、又はこれに関連するサービス等に起因するものであることが判明した場合には、甲の責任とし、乙は、復旧に対して必要な情報提供等の支援に努める。
・第一次対応の結果、障害の要因が甲乙いずれの管理に帰する事由に起因するものでないことが判明した場合には、甲乙協議の上、対応を行う。

【本項を定める上での考え方】

・本項では、障害一般に関する役割分担と責任について明示する。
・本例では、クラウドサービスの提供において発生した障害につき、第一次対応については、対象事業者が行うとした上で、障害の原因の帰属先によって、責任と役割分担、対応等を示している。
・本項で示す内容は、あくまでも例であり、具体的な内容については、対象事業者と医療機関等により協議することが求められる。その際、対象事業者は、専門的な知見からの協力を行うことが望ましい。

③ 甲が行う他の利用機関等との情報交換に関する障害についての役割分担と責任

本サービスに関連して、甲が他の医療機関等と情報交換する際に利用上の障害が発生した場合、下記については、②に準じて役割分担及び責任を定める。また、下記の場合以外については、甲乙協議の上、対応する。

・甲が受信した保存情報を、正しく本サービスにおいて利用できなかった場合
・甲が本サービスを通じて出力した情報が、送信先医療機関等において正しく利用できなかった場合

【本項を定める上での考え方】

・本項では、医療機関等が他の医療機関等と医療情報の交換を行う際に生じた障害に関する役割分担と責任について明示する。
・医療情報安全管理ガイドラインでは、医療機関等が他の医療機関等と医療情報の交換を行う際に生じた障害に関する責任分界について、事前に切り分けることを求めている（6.11 C)。
・本例では、本サービスを利用する医療機関等が、情報交換を行うデータを受信したにもかかわらず、対象事業者が提供するサービスにおいて利用できない場合、又は逆に対象事業者が提供するサービスを通じて出力した情報が、送信先医療機関等において利用できない場合について、通常の障害と同様の責任分担の切り分けをする旨を示している。それ以外の情報交換における障害については、対象事業者と医療機関等において、協議により決める旨を示している。
・本項で示す内容は、あくまでも例であり、具体的な内容については、対象事業者と医療機関等により協議することが求められる。その際、対象事業者は専門的な知見からの協力を行うことが望ましい。

４．２ 甲の業務上の役割分担と責任

(1) 甲のサービス利用に関する業務上の役割分担

本サービスの提供において、下記の業務については、甲は、その責任において実施するものとする。

・甲における利用者の ID の発行、変更、削除、初期パスワード発行等に関する申請業務
・本サービスに係る甲における各利用者の権限設定

上記に関し、乙は、甲に対して必要な情報提供等を行い、支援を行う。

(2) サービス利用開始及び利用終了における情報内容の確認

本サービスの利用開始及び利用終了に当たり、下記の事項については、甲は、その責任において実施するものとする。

・甲が本サービスの利用以前に作成したデータを、甲が本サービスにおいても利用する場合、当該データが、本サービスにおいて提供するアプリケーションにおいて正しく反映されていることの確認
・甲が本サービスの利用を終了する際に、６．２(4)にしたがって乙から甲に対して受託情報のデータが返却される場合に、当該データの内容が、正しいものになっていることの確認

(3) 甲が患者に対して行う情報提供に関する業務上の役割分担

本サービスに関連して、甲が患者等に対して行う情報提供につき、乙は、下記の事項に関する資料等の提供、及びこれに係る支援を行う。

・甲から受託する患者情報に関する管理状況等
・本サービスに係る乙が実施する各種対策の状況
・本サービスに係る乙の運用状況

上記につき、６．６(2)、６．６(3)に基づいて、乙は、甲に資料提供等を行う。

【本項を定める上での考え方】

・本項では、サービス提供上発生する手続等の業務について、医療機関等と対象事業者との役割分担と責任について明示する。

・本例では、医療機関等における利用者の ID 発行及び権限設定と、医療情報の内容の確認、患者に対する説明責任についての役割分担等を例示している。

・本例では、サービス利用に係る利用者の ID 及び初期パスワードについては、医療機関等が対象事業者に対して申請して、発行する形を想定している。対象事業者によっては、サービス提供に際して、ID 及びパスワードを郵送する等により対応する等も想定される。

・利用者側の権限設定については、本例では医療機関等自らが各利用者の情報へのアクセス権限や業務処理権限を設定することを想定している。対象事業者のサービスによっては、対象事業者が設定することも想定される。なお、いずれの場合においても、医療機関等において権限設定等の作業を行うことを想定する場合には、対象事業者は、必要な情報及び支援を医療機関等に行い、誤った権限設定がなされないようにする対応をとることが求められる。

・データ内容の確認については、サービスの開始時や終了時の返却が生じる際の、データ内容の確認を医療機関等側において実施する旨を示している。

・本例では、対象事業者の個人情報の管理状況や対策、運用状況等についての情報提供、及びこれに係る支援等について示している。本例では、患者に対する情報提供を行う条件等（例えば、情報漏洩（えい）が発生した等）を明記していないが、説明を行う趣旨等によっては、これらを明記した上で、対応する期間等（例えば、医療機関等による要請後、1 週間以内等）を明確にする等の方式も想定される。

・本項で示す内容は、あくまでも例であり、具体的な内容については、対象事業者と医療機関等により協議することが求められる。その際、対象事業者は専門的な知見からの協力を行うことが望ましい。

４．３ 再委託事業者・連携対象事業者等

(1) 業務の再委託

① データセンター業務

本サービスの提供において、乙は、下記の業務の一部再委託を行う。

【株式会社××データセンター】(以下、丙とする)

・乙の管理する受託情報を含むシステムに関する物理的安全管理対策の管理業務

・乙の管理する受託情報を含むシステムに関する運用業務

② 保守業務

本サービスの提供において、乙は、下記の業務の一部再委託を行う。

【株式会社××情報サービス】(以下、丁とする)

・乙の管理する受託情報を含むシステムに関する保守業務

(2) 連携対象事業者

本サービスの提供において、乙は、その管理に基づく対象事業者と連携したサービスの提供は行わない。

(3) 再委託先・連携対象事業者に対する管理責任等

本サービスの提供において、本項で定める事業者が行う上記業務につき、乙は、管理責任を有する。

本サービスの提供に関する上記業務の再委託において、乙が運用業務を実施する際に甲に対して負う義務と同じ内容の義務を、乙は、本項で定める事業者に対して課するものとする。

(4) 再委託先・連携対象事業者に関する情報提供

本項で示す再委託事業者及び連携対象事業者に関する情報については、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項ではサービス提供に際して、対象事業者が行う業務に関する再委託及び連携対象事業者について明示する。なお、「I.参考例編（サービス仕様適合開示書)」では、（２）⑥(b)で再委託先の状況について示している。

・クラウドサービスの提供においては、単一の事業者がすべての業務を完全に行うほか、一部業務を他の事業者に業務の再委託を行うことも想定される。これは、他の事業者に再委託することにより、より質の高いサービスをより効率的に利用者に提供する観点から行われる。なお、自らクラウドサービスの提供を行わず、自らは契約主体

となるだけで、クラウドサービスの提供を専ら連携対象事業者に委ねた場合でも、対象事業者としての第一次的な責任を負うものと考える。

・業務の再委託に関しては、利用者側においても再委託されている事実について認識することが必要であり、対象事業者においては、その情報を提供することが求められる。特に医療情報の場合には、高度な安全管理対策が求められることから、利用者である医療機関等においても、再委託先の安全管理対策について十分に考慮する必要がある。したがって、再委託の事実だけではなく、再委託先の安全管理対策の内容についても明示することが求められる。また、同様の観点から、再委託される業務の内容についても明示し、再委託が合理的な範囲であることを判断できるように配慮することが求められる。

・本例では、データセンター業務と保守業務の一部を対象事業者が再委託した場合を例示している。再委託業務については、例えば、ヘルプデスク業務等の業務を行う場合も想定される。これらは、対象事業者が再委託業務の内容にしたがって変更することが求められる。

・対象事業者間の連携は、他の事業者が提供するクラウドサービスを併せて提供することで、より効率的かつ利便性の高いサービスを利用者に提供することを目的とするものである。この場合でも、対象事業者は上記の再委託事業者に関する情報と同様の内容を利用者に明示することが求められる。なお、データセンターについては、明示の対象は事業者までとし、セキュリティ上の対応としてデータセンターの所在地等までは明示しないのが一般的であると考えられる。

・本例では、対象事業者が他の対象事業者と連携を行わない場合を想定している。連携する事業者がある場合には、連携対象事業者名のほか、提供されるサービス名等について明示することが求められる。

・再委託事業者及び連携対象事業者を用いる場合、それらの事業者の実施した業務の結果については、すべて対象事業者が責任を有する。本例では、このことを明示しているほか、再委託事業者及び連携対象事業者に対して、対象事業者が医療機関等に対して契約上課せられる義務を課することを示している。これは、医療情報の重要性に鑑み、単に業務の結果責任だけではなく、業務を実施する際に高度の注意義務を課する趣旨である。

・再委託事業者及び連携対象事業者を用いる場合、それらの事業者の情報についても、対象事業者は医療機関等に提供する旨を本例では示している。

・本項で示す内容は、あくまでも例であり、具体的な内容については、対象事業者と医療機関等により協議することが求められる。その際、対象事業者は専門的な知見からの協力を行うことが望ましい。

４．４ 連絡体制

(1) 通常時の連絡体制

本サービスの提供に係る甲乙の担当責任者は、下記のとおりである。

甲： 【医療機関等側管理責任者】

乙： 【対象事業者側管理責任者】

本サービスの提供に係る乙側の問合せ先は、下記のとおりである。

【対象事業者側ヘルプデスク窓口】（通常業務時間）

【対象事業者側メール問合せ先】

【本項を定める上での考え方】

・本項では、医療機関等と対象事業者との連絡体制について明示する。なお、「I. 参考例編（サービス仕様適合開示書)」では、（２）⑥（a）で組織体制を示している。
・本例では、医療機関等側の責任者と対象事業者側の責任者のほか、ヘルプデスク窓口の連絡先を明示している。なお、「I. 参考例編（サービス仕様適合開示書)」では、（２）⑭で問い合わせ窓口について示している。
・対象事業者が提供するサービスにおいて、連携対象事業者等が含まれる場合でも、医療機関等側と直接契約をしている対象事業者を直接の連絡先とすることが求められる。

(2) 障害時・非常時の連絡体制・告知方法

本サービスの提供において、障害時・非常時の乙の連絡体制については、下記のとおりである。

通常業務時間　　【連絡先】

上記以外の時間　　【連絡先】

なお、障害時、非常時における対応状況、及びサービス復旧の見込み等については、下記の場所において告知する。

・【http://+++.****.jp/----/（乙の用意する Web 上のページ)】

【本項を定める上での考え方】

・本項では、障害時・非常時の対象事業者の連絡体制を明示する。
・本例では、通常業務時間（１．３参照）及びそれ以外の連絡先を明示している。
・対象事業者の用意する問合せ先については、電話による連絡先が通常である。しかし、日中等以外の時間帯における問合せ先としては、メール等による連絡の場合も想定される。ただし、医療機関等の業務によっては、障害時・非常時等のようなケースで、即時性や双方向性等が求められることもある。サービスを供する業務の性格や、必要性等に鑑みて合意することが求められる。

５．サービス仕様

５．１ ネットワークセキュリティに関するサービス仕様

(1) ネットワーク経路の安全管理対策（暗号化、盗聴対策、使用機器等）

本サービスの提供に際して乙が使用するネットワーク及びこれに関する機器につき、乙は「サービス仕様適合開示書」に示す事項を実施することにより、ネットワーク経路の安全管理対策を実施する。

本項で示すネットワーク経路の安全管理対策に関する乙の対策内容、実施状況等については、６．６(2)、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、ネットワーク経路の安全管理対策（暗号化、盗聴対策、使用機器等）について明示する。
・医療機関等においては、医療情報安全管理ガイドラインによりネットワーク経路の安全管理対策の実施が求められる（例えば、6.11 C 等）。
・そこで、本 SLA では、上記の趣旨を反映した運用内容を「ネットワーク経路上の安全管理対策」に示し、対象事業者は、これを運用管理規程に含めることとし、本例ではこれに基づいてネットワーク経路の安全管理対策の実施を行う旨を明示している。
・また、対象事業者の実施するネットワーク経路の安全管理対策の状況等につき、医療機関等からの要請があった場合に、対象事業者は、一定の条件で資料提供を行う旨を明示している。

(2) 外部からの不正アクセス対策（不正アクセス防止、なりすまし防止等）

本サービスの提供に際して乙が使用するネットワーク及びこれに関する機器につき、乙は別添「サービス仕様適合開示書」に示す事項を実施することにより、不正アクセス対策を実施する。

本項で示す外部からの不正アクセス対策に関する乙の対策内容、実施状況等については、６．６(2)、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、外部からの不正アクセス対策（不正アクセス防止、なりすまし防止等）について明示する。
・医療機関等においては、医療情報安全管理ガイドラインにより不正アクセス対策の実施が求められる（例えば、6.11 C、7.1 C 等）。
・そこで本 SLA では、上記の趣旨を反映した運用内容を「不正アクセス対策」に示し、これを対象事業者は運用管理規程に含めることとし、本例ではこれに基づいて不正アクセス対策の実施を行う旨を明示している。
・また、対象事業者の実施する不正アクセス対策の状況等につき、医療機関等からの要請があった場合に、対象事業者は一定の条件で資料提供を行う旨を明示している。

５．２ 受託情報に関するサービス仕様

(1) 真正性に関するサービス仕様

① 利用者認証（利用者資格認証、電子署名等）

甲が本サービスを利用する際に必要となる利用者認証については、ID･パスワードによる認証と IC カードを用いた認証の組み合わせにより行う。

本サービスの提供に際して、乙は別添「サービス仕様適合開示書」に示す事項を実施することにより、利用者認証の安全性を確保する。

本項で示す利用者認証の安全性に関する乙の対策内容、実施状況等については、６．６(2)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、利用者認証（利用者資格認証、電子署名等）について明示する。
・医療機関等においては、医療情報安全管理ガイドラインによりアクセス制御の実施が求められる（例えば、6.5 C、7.1 C 等)。
・そこで本 SLA では、上記の趣旨を反映した運用内容を「アクセス制御」に示し、これを対象事業者は運用管理規程に含めることとし、本例では、これに基づいて、アクセス制御の実施を行う旨を明示している。
・本例では ID･パスワードによる認証と IC カードを用いた認証の組み合わせによる利用者認証を採用している例を示している。実際の SLA では対象事業者が採用する認証方法（パスワード等の記憶要素、ハードウェアトークン又は IC カード等の物理媒体要素、指紋・顔などの生体情報(バイオメトリクス)要素等）を記載する。
・また、対象事業者の実施する利用者認証の状況等につき、医療機関等からの要請があった場合に、対象事業者は、一定の条件で資料提供を行う旨を明示している。

② 職種等に基づくアクセス制御

甲が本サービスを利用する際に必要となる利用者認証については、下記の機能を含む。

・甲が利用する利用者 ID において、複数の担当業務又は職種毎にアクセス権限を設定できること。
・甲が利用する、複数の担当業務又は職種に関するアクセス権限のある利用者 ID において、職種別等のアクセス管理機能があること。
・対象情報ごとに入力者の職種や所属等の必要な区分に基づいた権限管理（アクセスコントロール）が定められること。
・権限のある利用者以外による作成、追記、変更、削除を防止する機能を有すること。

本項で示すアクセス権限の設定は、４．２に基づいて実施する。

本項で示す利用者認証におけるアクセス制御に関する乙の対策内容、実施状況等については、６．６(2)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、職種等に基づくアクセス制御について明示する。
・医療情報を作成する場合、法令による職種等の身分要件や管理者等の役職要件が求められるものがある。特に本 SLA で想定する電子カルテについては、医師による作成が義務付けられている。
・このような観点から、法的保存義務のある文書を電子的に作成するために用いるクラウドサービスにおいては、サービス仕様として職種等に基づくアクセス制御が必要とされる。
・そこで、本例では上記の趣旨を反映し、職種等に基づくアクセス制御の機能をサービスに備える旨を明示している。
・本例で示す項目に関しては、システム機能として実装できない場合でも、運用方法により代替することによって同程度の安全性を確保できる場合には、その内容を記述することが想定される。
・また、本サービスに係る職種等に基づくアクセス制御の状況等につき、医療機関等からの要請があった場合に、対象事業者は、一定の条件で資料提供を行う旨を明示している。

③ 電子署名

本サービスにおいて、甲と乙は協議の結果、PKI による電子署名を採用することができる。

本サービスの提供において、乙が使用する電子署名については下表の内容を満たす。

【電子署名に係る要求事項】

仕様	保健医療福祉分野 PKI 認証局の仕様に準じた電子署名
発行者等	・保健医療福祉分野 PKI 認証局が発行する電子証明書、又は電子署名法に基づく認定認証事業者が発行する電子証明書によるものである。
タイムスタンプ	・「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの 安全な長期保存のために－」（総務省、平成 16 年 11 月）等で示されている時刻認証業務の基準に準拠していること ・一般財団法人日本データ通信協会が認定した時刻認証事業者のものであること。 ・第三者がタイムスタンプを検証することが可能であること ・検証可能なタイムスタンプを含む

本項で示す電子署名に関する仕様等に関する情報は、６．６(2)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、電子署名を採用する場合の仕様等について明示する。なお、「I.参考例編（サービス仕様適合開示書)」では（２）⑮（ｃ）（ア）で、実施している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の安全管理対策を示している。

・「電子署名及び認証業務に関する法律」（電子署名法）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、法令で署名又は記名・押印が義務付けられた文書等を含む医療情報を取り扱うシステムにおいて、長期保存を考慮した電子署名によることが求められている（6.12 C)。

・本サービスで電子署名を採用する場合、その仕様等の情報については、医療機関等からの要請があった場合に、対象事業者は、一定の条件で資料提供を行う旨を明示している。

④ 診療記録の確定（本人による確定、代行確定等）

本サービスにおける診療記録を確定する機能について、下記の機能を含む。

・診療録等として作成・保存するデータについて、甲の作成責任者が特定できること
・記録の入力後、確定処理を行う機能を有すること
・入力された内容を確定する前に、入力内容の確認画面等の表示により甲の作成責任者が確認できる措置を講じていること
・甲における代行操作の権限付与が設定できること
・代行操作により記録された診療録等に対して、甲の作成責任者による「確定操作（承認）」を行えること
・臨床検査システム、医用画像ファイリングシステム等から情報を取り込み、本サービスにおいて記録を作成した場合、出力結果の取り込みを行った者及びその職種等が特定できること

本項で示す代行操作に関する権限の設定は、４．２に基づいて実施する。

本項で示す診療記録の確定の仕様に関する情報、乙の対策状況等については、６．６(2)、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、診療記録の確定（本人による確定、代行確定等）の仕様等について明示する。なお、「I.参考例編（サービス仕様適合開示書）」では（２）⑮(ｂ)で、ｅ-文書法の対象となる医療情報を含む文書等の作成を目的とするサービスにおける機能を示している。
・記録の確定は、作成責任者による入力の完了、検査・測定機器による出力結果の取り込みの完了によってなされる。
・作成責任者による入力の完了については、作成責任者本人による入力とその確定のほか、代行操作者による入力と作成責任者による記録の確定が挙げられる。本例では、代行操作による入力を認める場合を想定した事例を明示している。
・検査、測定機器による出力結果の取り込みの完了については、機器からの出力結果を取り込む際に、作成責任者又は代行取込者がこれを行うことを想定した事例を明示している。
・本サービスにおける記録確定に関する仕様等の情報については、医療機関等からの要請があった場合に、対象事業者は、一定の条件で資料提供を行う旨を明示している。

⑤ データの更新履歴管理

本サービスにおいて、記録されたデータの更新履歴を管理する機能について、下記の機能を含む。

・記録された診療情報の更新の前後を確認できること
・同じ診療録等に対して更新が複数回行われた場合に、更新順序の識別が可能であること
・記録された診療情報に複数回の更新が行われた場合に、更新の前後を確認できること

本サービスにおいて、乙は確定された記録が、第三者による故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じるとともに、万が一このような事態が発生した場合には、乙は、甲と協議の上、必要な対応を行う。

本項で示す記録されたデータの更新履歴を管理する機能に関する情報については、６．６(2)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、診療記録のデータの更新履歴管理の仕様等について明示する。なお、「I. 参考例編（サービス仕様適合開示書)」では（２）⑮(ｂ)で、ｅ-文書法の対象となる医療情報を含む文書等の作成を目的とするサービスにおける機能を示している。
・診療録の作成等を電磁的記録により行う場合には、医療情報安全管理ガイドラインでは作成責任者本人の作成･更新・削除に限定し、不正若しくは過誤による書き換えや消去、混同等を防止する対策が求められている(7.1 C)。そしてこれを担保するための手段として、更新記録の管理ができる機能を求めている。
・本例では、上記趣旨に鑑みて、更新記録の管理に必要な機能等をサービス仕様に含む旨を明示している。
・本項で定める機能等を実現するためには、サービスで提供するアプリケーションにおける機能の実装のほか、対象事業者による運用上での対応も想定される。
・第２段落では、本項で定める機能の実装等により防止対策を講じたにもかかわらず、確定された記録が第三者により不正な書き換えや消去等がなされた場合に必要な対応をとることについて例示している。具体的な対応の内容としては、被害状況の把握、被害拡大防止、原因の究明、警察等への通報、データの回復措置等が想定される。
・本サービスにおける診療記録のデータの更新履歴管理に関する仕様、対応等の情報については、医療機関等からの要請があった場合に、対象事業者は、一定の条件で資料提供を行う旨を明示している。

(2) 見読性に関するサービス仕様

① 表示仕様

本サービスにおいては３．２において示す利用環境下において、正常に表示されることを保証する。

本サービスで提供するアプリケーションにおける入力及び確定画面の表示仕様は、乙が甲に対して提供する【利用マニュアル】に示す。

本項で定める画面について、何かしらの事情で変更する場合、乙は、予告の上、適宜これを行う。変更に際して、乙は、入力結果が誤って確定されない設計となることに努める。

② 応答時間

本サービスで提供するアプリケーションにおける入力及び確定、検索画面の結果の表示につき著しい遅延が生じる場合には、乙は、甲からの連絡又は自己の判断に基づき、調査し、甲への報告を行う。

調査の結果、上記遅延の要因が、乙の責めに帰する事由によるものであることが判明した場合には、乙は、障害として速やかに対応を行う。

上記遅延の要因につき、乙の責めに帰すべからざる事由によるものであることが判明した場合には、４．１(2)、４．２に基づき、甲乙協議の上、対応を行う。

③ 冗長性

乙は、本サービスのアプリケーションサービスに供するサーバ類につき、RAID-1 又は RAID-6 相当以上のディスク構成を採用し、障害対策を講じる。

本サービスの提供に関し、乙が採用する冗長性を確保するための仕様等（外部ファイル出力機能、印刷機能等）の情報につき、乙は、６．６(2)に基づいて提供する。

【本項を定める上での考え方】

・本項では、見読性に関するサービス仕様等について明示する。なお、「I.参考例編（サービス仕様適合開示書)」では、応答時間の状況及び冗長性については（２）⑮（ｂ）（イ）で示している。
・電磁的記録による場合には、「民間事業者等が行う書面の保存等における情報通信技術の利用に関する法律」(「e-文書法」）等により見読性の確保が求められる。すなわち電磁的記録においても、紙媒体による場合と同様の内容が完全に再現できることを確保することが求められる。
・医療情報安全管理ガイドラインでは、これに加えて、「診療」、「患者への説明」、「監査」、「訴訟」等の利用目的に鑑みて支障のない応答性等も求めている。
・本例では、上記趣旨に鑑みて、見読性に関するサービス仕様に上記要求事項を含む旨を明示している。
・また、本例では表示仕様について、正常な再現性を保証する環境を示すとともに、表示画面を別途マニュアルにて示すこととしている。ただし、表示については、業務に影響を与えない範囲で利用者側の同意なくして変更されることを想定している。
・応答時間との関係では、クラウドサービスの場合には、ネットワークのトラフィックの状況等により、応答速度にバラつきが生じることがある。そして責任分界等との関係においては、スループットタイムを保証するか等が論点となる。本 SLA では対象事業者がネットワークサービスを提供しないことを前提としているため、本例ではスループットタイムを保証しない形式を採用している。その上で、サービス提供上、表示の遅延が認められた場合の対応について示している。
・冗長性については、サービス提供に係る完全性の確保の観点から、対象事業者のシステムにおける冗長性の例として、RAID による対応を示している。
・また、障害発生時の代替的な措置を医療機関等において講じることができるようにする観点から、出力機能やデータダウンロード機能を実装していることを想定した例示としている。個別の内容については、対象事業者のサービス内容にしたがって記述することが求められる。電子カルテ等の重要システムにおいて、障害回復時間等をサービス内容として明確にしない場合には、医療機関等において障害発生時の代替的措置を講じることができるようにすることが望ましい。
・本サービスにおける見読性に関する仕様、対応等の情報については、医療機関等からの要請があった場合に、対象事業者は一定の条件で資料提供を行う旨を明示している。

(3) 保存性に関するサービス仕様

① データの破壊防止対策（ウイルス等による攻撃対策等）

本サービスの運用に供する乙の施設において、乙は、別添「サービス仕様適合開示書」に示す内容を実施することにより、本サービスの運用におけるウイルス等によるデータの破壊防止対策を行う。

本サービスの提供において、乙は、セキュリティ対応策を下記のインターバルで実施する。

・ウイルス対策のためのパターンファイルの更新、並びにOS及びミドルウェア等のセキュリティパッチについては、概ね１日以内に実施する。ただし乙において、本サービスの提供に係るシステムへの影響が大きいと判断した場合には、必要な措置を速やかに適用する。

本項で示すウイルス等によるデータの破壊防止対策に関する乙の対策内容、実施状況等については、６．６(2)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、データの破壊防止対策について明示する。
・医療情報安全管理ガイドラインでは、保存性に対する脅威の一つとして、ウイルスや不適切なソフトウェア等による情報の破壊を挙げている（7.3 B)。
・本例ではこれに基づいて、対象事業者は、ウイルス等によるデータの破壊防止の対策について明示している。
・また、併せて本例では、主にウイルス対策用ソフトウェアのパターンファイルの更新頻度、及びOS等の主にセキュリティ上の脆弱性に対するパッチファイル（いわゆるセキュリティパッチ）の適用の対応等について明示している。なお、本例で示した数値は、あくまでも例示であり、対象事業者において必要とされる頻度等について、変更することが想定される。
・本サービスにおける保存性に関する仕様、対応等の情報については、医療機関等からの要請があった場合に、対象事業者は、一定の条件で資料提供を行う旨を明示している。

② データの劣化、滅失対策

本サービスに供する乙の施設において、本サービスの運用におけるデータの劣化、滅失対策に必要なモニタリングを行う。

乙は、本サービスの提供に係る運用において、下記を実施することにより、データの劣化、滅失対策を行う。

・データ保存する際に用いるデータ形式及び転送プロトコルを変更する際に、変更前の方式との互換性を確保すること。
・障害により甲から乙の管理する機器へのデータ転送が正常に完了しなかった場合に、乙へのデータ転送が完了しなかったことを甲が確認できるようにする機能を有すること。

本項で示すデータの劣化、滅失対策に関する乙の対策内容、実施状況等については、６．６(2)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、データの劣化、滅失対策について明示する。なお、「I.参考例編（サービス仕様適合開示書)」では、データの劣化対策については（２）⑮(ｂ)（ウ）で示している。
・医療情報安全管理ガイドラインでは保存性に対する脅威の一つとして、データの劣化、滅失による情報の破壊を挙げている（7.3 B)。
・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では、電子保存の要求事項を示している(6.2)。本例では、これに基づいて、対象事業者はデータの劣化、滅失等によるデータの破壊防止の対策について明示している。
・併せて、本例では主にデータ形式や転送プロトコルの変更やバージョンアップが生じる場合には、旧方式のものとの互換性を確保することについて明示している。
・また、医療機関等がサービス利用中に、何らかの障害が発生し、データの転送が医療機関等から対象事業者に対してデータの転送が完了していなかった場合に、その旨を表示する機能を実装する例を示している。本項では、データ転送中のトラブルへの対応方法について、各対象事業者において講じている内容を規定することを想定している。
・本サービスにおけるデータの劣化、滅失対策及びその実施状況については、医療機関等からの要請があった場合に、対象事業者は、一定の条件で資料提供を行う旨を明示している。

③ データ仕様について

本サービスの提供に供するデータベースのデータ仕様の採用に際し、乙は、「医療情報システムの安全管理に関するガイドライン　第5版」の「5情報の相互運用性と標準化について」に従って実施する。

本項で示すデータ仕様等の情報については、６．６(2)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、データ仕様について明示する。
・医療情報安全管理ガイドラインでは、媒体・機器･ソフトウェアの不整合による情報の復元不能を回避するため、診療録のデータ項目について標準仕様のあるものについては、原則としてこれを採用することを求めている（7.3 C)。
・本例では、対象事業者が採用するデータ仕様について、医療情報安全管理ガイドラインにおける「5情報の相互運用性と標準化について」に従うことを明示している。対象事業者が採用するデータ仕様について、標準仕様を採用することが困難な項目も想定される。この場合には、標準仕様を採用できないデータ項目について、容易に入出力が可能となるような機能又は手順を講じる等が想定される。
・本サービスにおける対象事業者が採用するデータ仕様については、医療機関等からの要請があった場合に、対象事業者は一定の条件で資料提供を行う旨を明示している。

６．運用内容

６．１ 運用組織・規程等

(1) 運用組織・体制

本サービスの提供に係る乙のサービス提供体制を、下記に示す。

【乙体制図】

【本項を定める上での考え方】

・本項では、対象事業者の運用体制を明示する。なお、「I.参考例編（サービス仕様適合開示書)」では、（２）⑥（ａ）でサービス提供体制を示している。
・本例では、対象事業者の運用体制図を示す形をとっている。
・医療情報を情報システムで取り扱う場合、医療機関等には、組織体制を含む運用管理規程の整備等が求められる（医療情報安全管理ガイドライン 6.3 B)。この観点から、医療機関等の管理責任者が把握できる形で、対象事業者の運用管理体制を明示することが求められる。
・対象事業者の運用体制については、
  ✓自社内の体制（担当する部署等が複数ある場合には、それらを明記する）
  ✓データセンター事業者や、保守等の目的で再委託事業者を利用する場合には、その事業者
  ✓連携対象事業者がある場合には、その事業者

と、それぞれの役割を明示することが求められる。

(2) 運用に関する規程

① 本サービス提供上、根拠とする運用管理規程等

乙が甲に対して本サービスを提供する際の運用管理規程等については、下記のルールを適用する。

・甲において、情報セキュリティポリシー、医療情報を取り扱う情報システムに関する運用管理規程等が存在しない場合、乙は、自社の情報セキュリティポリシー、情報システム管理規程、運用管理規程等（以下「乙規程等」）が、３．５に掲げる法令、ガイドライン等に準拠することを確認した上で、乙規程等に基づいて、本サービス提供に係る運用を行うものとする。

・甲において、情報セキュリティポリシー、医療情報を取り扱う情報システムに関する運用管理規程等が存在する場合、乙規程等との相違点等を確認した上で、それらが３．５に掲げる法令、ガイドライン等に準拠することを確認した上で、甲乙協議の上、採用する規程類、条項等を決するものとする。相違点がない条項等については、乙規程等に基づいて運用を行う。

【本項を定める上での考え方】

・本項では、本サービス提供上、根拠とする運用管理規程等の考え方を明示する。
・医療情報安全管理ガイドラインでは、安全管理の観点から運用管理規程を設けることとされている（6.3 B)。また、対象事業者においても、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 5.1.6 にもとづく文書化が求められる。そこで、これらの規程間の整合を図る必要が生じる。
・本例では、下記のルールに基づいて、規程類を適用する例を示している（ただし、いずれの事項についても対象事業者の規程で定める内容が、３．５に定める法令・ガイドラインの内容を満たすものであることを前提とする)。
  ✓医療機関等の運用管理規程において存在しない事項がある場合には、当該事項につき、対象事業者の運用管理規程等に定める内容を適用する
  ✓医療機関等の運用管理規程において規定が存在する場合で、対象事業者の運用管理規程等と内容が異ならない部分は、対象事業者の運用管理規程等に定める内容を適用する
  ✓医療機関等の運用管理規程において規程が存在する場合で、対象事業者の運用管理規程等と内容が異なる部分は、医療機関等と対象事業者で都度協議し、どちらの規程の条項を採用するか決める
・特に小規模医療機関等においては、必ずしも情報システムに関する明確な規程が存在しない場合もある。この場合には、原則として SLA の内容と対象事業者の運用管理規程等が、医療機関等の運用管理規程を代替することになるため、対象事業者は、必要に応じて運用管理規程等の情報開示が求められる。

② 運用の方針となる規程

乙規程等においては、下記に定めるシステム運用に係る前提となる方針を含んでおり、これに基づいて、本サービスに係る運用を実施する。

・アクセス制御方針
・個人情報保護指針等
・運用管理における理念（基本方針と管理目的）

③ 運用管理を構成する規程・要領・手順等

乙規程等には、下記に定める規程・要領・手順等が含まれる。

乙規程等は、乙の定める手続に基づき、必要に応じて改訂される。なお、サービス提供上、大きな影響を及ぼすと考えられる変更が生じた場合には、乙は、甲に対して報告するものとする。

・運用管理規程
・サービスサポート実施要領
・サービスデリバリ実施要領
・サポートデスク実施要領

④ 本項で示す運用管理規程類等の提供

本項で示す乙規程等については、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、対象事業者が本サービス提供上、根拠とする運用管理規程等について明示する。
・一般的には運用管理規程の上位規程として、情報管理方針やアクセス制御方針、個人情報保護指針等の方針等が定められ、これを具体化するために運用管理規程等が整備され、さらに個別の運用手順等が整備される。
・本例で示す規程類の名称は、事例に過ぎない。実際には各対象事業者がサービス提供において整備している名称等を記述する。
・運用管理規程等については、各対象事業者のセキュリティ対策等に関係する内容も含まれていることから、一般的には公開には馴染まない。ただし６．１(1)に示すように医療機関等の運用管理規程に代替するものとして取り扱われることも想定されることから、一定の条件等に基づいて、医療機関等に対して提供する旨を、本例では明示している。

(3) 運用における遵守事項

本サービスの提供に際して甲から受託する情報を乙が使用する範囲につき、乙は、下記の内容を遵守する。

・乙は、受託した医療情報を、匿名化されたものを含めて、分析、解析等を実施しない。
・なお、甲乙協議の上、本サービス利用契約とは別の契約を締結の上、甲の依頼内容に限った分析等を実施することは妨げない。ただし、その場合であっても、患者等の同意取得方法に関して十分な検討をする。
・乙は、受託した医療情報を、許可無く第三者に提供しない。
・乙は、甲の依頼がある場合であっても、代行操作等は実施しない。

【本項を定める上での考え方】

・本項では、対象事業者がサービス提供上の禁止事項を明示する。
・受託した医療情報は、個人情報の中でも特にセンシティブな内容を含む。また医療業務においては、診療録の作成のように、作成者の身分が求められる業務も含まれる。本例ではこれらの観点から、特に対象事業者において禁止されるべき内容を明記している。
・診療録の作成、保存等のサービスの機能の一つとして、記録後、何らかの理由で確定が行われない場合、一定時間経過後に、自動的に記録を確定する機能を有する場合がある。このような機能を有するサービスを提供する場合、対象事業者は医療機関等に対して必要な説明を行う。

６．２ 受託情報の取り扱い

(1) 受託情報の取り扱い範囲

本サービスで、受託情報を乙が取り扱える範囲につき、乙は、下記の内容を遵守する。

・乙は原則として、受託した医療情報を参照しない。
・乙においての参照は、サービス提供の運用業務に支障が生じる、保守等の実施でやむを得ない場合に限ることとして、その場合も必要不可欠な範囲を超えて参照しない。
・上記の場合に、乙における本サービス提供に係る運用者等が保有する ID で受託した医療情報を参照する場合の権限は必要最小限に限定する。

本項で示す受託情報の取り扱い範囲の制限に関する乙の対策内容については、６．６(3)に基づいて、乙は、甲に提供する。また受託した医療情報の取り扱い状況については、６．５(1)①に基づいて報告する。

【本項を定める上での考え方】

・本項では、対象事業者がサービス提供上、受託情報を取り扱う際の範囲等につき、明示する。
・受託した医療情報は、個人情報の中でも特にセンシティブな内容を含むことから、原則として対象事業者は参照不能であると解するべきである。その上で、
  ✓サービス提供上やむをえない場合には、必要最小限の範囲での参照のみ認める
  ✓ただし対象事業者において受託した医療情報の内容を参照できる者を限定し、その範囲でのみ参照権限を付与する
  ✓受託した医療情報を参照する場合には、原則として委託元の医療機関等に事前告知及び事後報告する。サービスの提供上、緊急性があり、事前連絡が困難な場合でも、参照後に委託元の医療機関等へ速やかに報告を行う

等の対応が求められる。本例は、上記内容について、例示しているものである。

(2) 受託情報の管理

本サービスで乙が甲より受託する情報につき、乙は本項で示す受託情報の管理に関する乙の対策内容、実施状況等については、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、サービス提供に際して、対象事業者の実施する受託情報の管理について明示する。
・本 SLA では、対象事業者が行うべき受託情報の管理について、「受託情報の管理」に示す内容を運用管理規程等で規定することとしている。本例では、これに基づいて、対象事業者は受託情報を管理する旨を明示している。
・医療機関等においては、医療情報安全管理ガイドラインにより医療情報の管理状況を把握することが求められる（例えば、6.7 C、6.9 C 等)。そのため医療機関等は対象事業者の受託情報の管理につき、具体的な対応内容や実施状況を把握する必要が生じうる。そこで本例では、医療機関等からの要請があった場合に、対象事業者は一定の条件で受託情報の管理状況についての資料提供を行う旨を明示している。

(3) 受託情報の提供

甲が乙に対し、受託情報の提供を求めた場合、甲乙は、協議により、下記の内容を決定する。

・提供する受託情報の範囲、件数
・提供する受託情報のフォーマット
・受託情報の提供方法

甲が乙に対し、あらかじめ定められた範囲を超えて受託情報の提供を求めた場合、甲乙は、協議により、下記の内容を決定する。

・受託情報の提供に要する費用

本項につき、乙は、受託情報を甲に提供する際、下記の事項を実施する。

・「医療情報システムの安全管理に関するガイドライン　第５版」の「5 情報の相互運用性と標準化について」に従った実施
・提供される情報に、標準仕様に該当しない項目等の内容が含まれている場合には、甲において正確なデータの確認が可能となるために必要な説明又はこれに代わる資料の提出

【本項を定める上での考え方】

・本項では、サービス提供に際して、医療機関等から対象事業者に対して、寄託している医療情報等の提供を求められた場合の対応について明示する。
・対象事業者が提供するサービスによっては、アプリケーションに、寄託している医療情報等をダウンロードできる機能を有している場合も想定されるが、本例では、このような機能が実装されていないサービスの場合で、医療機関等から寄託している情報を電子媒体等で求められる場合の手続等を明示している。
・対象事業者から医療機関等に対して、受託情報を電子媒体等により提供する場合、提供されたデータ項目の内容等が明確であることが重要である。この観点から、本例では、医療情報安全管理ガイドラインの「5 情報の相互運用性と標準化について」に準拠する内容で提供するべき旨を明示している。また、仮に標準的なデータ項目による提供ができないものが含まれる場合には、医療機関等側で提供された情報の内容を正確に把握できる資料の提出等を明示している。

(4) 受託情報の返却等

本サービスの提供の終了に際し、甲乙は、協議により、下記の内容を決定する。

・受託情報の返却の要否
・受託情報の抹消の方法及びその実施期日
・契約終了後の受託情報抹消の報告

本サービスの提供の終了に際し、乙が受託情報を甲に返却する場合、甲乙は、協議により、下記の内容を決定する。

・返却する受託情報の範囲、件数
・返却する受託情報のフォーマット
・受託情報の返却方法
・受託情報の返却期日

受託情報の返却に際し、甲が乙に対し、あらかじめ定められた範囲を超えて情報の提供を求めた場合、甲乙は、協議により、下記の内容を決定する。

・受託情報の返却に要する費用

本項につき、乙は、受託情報の返却に際し、下記の事項を実施する。

・「医療情報システムの安全管理に関するガイドライン　第5版」の「5情報の相互運用性と標準化について」に従った実施
・ 提供される情報に、標準仕様に該当しない項目等の内容が含まれている場合には、甲において正確なデータの確認が可能となるために必要な説明又はこれに代わる資料の提出
・甲において返却された情報の内容の正確性を、確認できるような形での資料提供を行うこと。

【本項を定める上での考え方】

・本項では、サービス提供契約終了に際して、対象事業者が行う受託情報の返却等の対応について明示する。
・サービス提供契約終了に際して、医療機関等と対象事業者は、医療情報等の寄託情報の返還の要否や、寄託情報の消去の方法等に関して協議することが求められる。
・本例では、寄託情報の返却を要する場合には、返却する情報の範囲のほか、返却方法やフォーマット等に関して、医療機関等と対象事業者で協議して決める旨を明記している。対象事業者によっては、費用の有無及びその金額等をあらかじめサービス契約で明示していることも想定される。

・本項は、サービス提供契約終了を念頭に置いた項目であり、契約終了時のトラブルを未然に防ぐ意味からも明確な記載が必要である。
・契約の終了においても、前項同様、対象事業者から医療機関等に対して、受託情報を電子媒体等により返却する場合、提供されたデータ項目の内容等が明確であることが重要であり、同様の規定により明示している。

６．３ 運用仕様及びその指標

(1) 機密性

① 物理的セキュリティ

本サービスの運用に供する乙の施設において、本サービスの運用における物理的セキュリティを確保する。

本項で示す物理的安全管理対策について、サービス仕様適合開示書に記載している内容以外の乙の対策内容、実施状況等については、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、対象事業者が運用において講じる物理的セキュリティについて明示する。
・医療機関等においては、医療情報安全管理ガイドラインにより物理的安全管理対策の実施が求められる（例えば、6.4 C 等）。
・そこで本 SLA では、対象事業者は物理的セキュリティに関する事項を運用管理規程に含めることとし、本例ではこれに基づいて物理的セキュリティの実施を行う旨を明示している。
・また対象事業者が実施する物理的安全管理対策のうち、サービス仕様適合開示書に記載されている内容以外の対策状況等につき、医療機関等からの要請があった場合に、対象事業者は一定の条件で受託情報の管理状況についての資料提供を行う旨を明示している。

② セキュリティ管理

本サービスの運用につき、運用の機密性等を確保するため、乙は、下記の措置を講じる。

・乙の管理下にあるネットワーク及びサービス提供に係るシステムにおいてセキュリティが確保されていることの監視
・乙の管理下にあるネットワーク及びシステムの稼動状況（特に、通信容量とトラフィック変動が重要）の監視
・乙の管理するネットワーク及びシステム等に対するサイバー攻撃に対するネットワーク等に関する定期的な監視
・業務上、受託情報を外部に持ち出す際の適切なウイルス対策等の実施
・業務上受託情報の参照等を行う場合の覗き見予防措置の実施
・バックアップデータにつき、その内容の改竄（ざん）を防ぐためのデータ管理

本項で示すセキュリティ管理に関する乙の対策内容、実施状況等については、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、対象事業者が運用において講じるセキュリティ管理について明示する
・本例では、対象事業者が実施すべき運用上のセキュリティの管理について明示している。
・サービスの仕様に関わるセキュリティ対策については、５.「サービス仕様」で明示しており、本例ではそれ以外の対象事業者の運用業務において必要と考えられる事項を挙げている。
・セキュリティ管理については、６．１、６．２に記述している事項の実施を前提とした上で、さらに対象事業者に運用上求められるセキュリティ確保のための事項が記述される。
・また対象事業者の実施するセキュリティ管理の状況等につき、医療機関等からの要請があった場合に、対象事業者は一定の条件で受託情報の管理状況についての資料提供を行う旨を明示している。

(2) 可用性

本サービスの運用の可用性を確保するために、乙は、下記の措置を講じる。

・サービス稼働率については、以下の目標値を設定する。

通常業務時間帯　99.95%

その他の時間帯　99.5%

なお、サービス稼働率は、以下により算出するものとする。

サービス稼働率＝（サービス提供時間－サービス提供停止時間）／サービス提供時間

サービス停止時間は、１．１「本サービスの目的」に定めるサービスの提供が停止する時間を指す（サービス機能の一部が停止している場合でも、甲の業務に重大な支障を及ぼさない場合は除く）。

サービス提供停止時間は、サービス停止時間のうち、７．１(2)「サービスレベル算定除外事項」に示す事由による停止時間を除いたものを指す。

・甲の業務に継続な支障をきたす程度の機器、ソフトウェア等のシステム障害等、及びサービス利用における応答速度の低下については、４．４(2)に示す通常業務時間内において、乙による感知又は甲からの連絡があった時刻から、●時間以内に第一次対応（４．１②参照）をする。

・機器、ソフトウェア等のシステム障害等、及びサービス利用における応答速度の低下の感知、サービス応答速度等のサービスパフォーマンスの正常性の把握等のために行う検知の場所、検知のインターバル、画面の表示チェック等の検知方法については、乙が運用に際して定める方式に基づいて実施する。

本項で示す可用性確保のための措置に関する乙の対策内容、実施状況等については６．６(2)、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、本サービスの可用性について明示する。

・本例では、サービス稼働率、及び障害等発生からの対応時間等について明示している。

・クラウドサービスにおける可用性は、正常なサービスを利用するための信頼性と密接に関係する。これを具体的に図る指標としては、サービス稼働率や、応答時間、復旧時間、原因解明時間、原因解明率、死活監視間隔等、いくつかのものが挙げられる。

・本例では、診療録の作成、保存等のサービスを想定して、対象事業者が保証するサービス稼働率を例示している。稼働率の例については、対象事業者に起因するサービスが障害により停止した場合に、サービス提供時間において、最大半日程度以内には回復できることを想定して設定している。

・本例で示した報告項目及び数値は、あくまでも例示であり、サービス稼働率、問題管理対応時間等及び問題検出のための手法（例えば、死活監視間隔やロードアベレージの検出等）について挙げている。実際の SLA においては、サービスの内容に応じて対象事業者がサービス提供上必要とされる可用性の確保に必要な項目や指標について、追記することが想定される。なお、乙による感知又は甲からの連絡があった時刻から第一次対応を行うまでの時間については、医療機関等と対象事業者の合意にしたがって記入されることを予定している。
・また、本例では、ネットワークに起因するサービスレベルの低下については明示していない。本例の想定では、対象事業者がネットワークサービスの提供を行っていないことから、これに起因するサービス応答時間の遅延等は、SLA により保証されるサービスとしていないためである。対象事業者がネットワークサービスも含めて包括的にサービス提供をしている場合には、ネットワークの障害やトラフィックに起因する可用性に係る事項等も含めることが求められる。
・対象事業者が実施する可用性の維持及びそのための対策の状況等につき、医療機関等からの要請があった場合に、対象事業者は、一定の条件で受託情報の管理状況についての資料提供を行う旨を明示している。

(3) 完全性

本サービスの運用の完全性を確保するために、乙は、サービス提供及び運用に係る下記の記録を収集し、管理を行う。

・利用者における個人情報へのアクセス状況（利用者の ID、アクセス対象、日時等）
・メンテナンスにおける個人情報へのアクセス状況（作業者の ID、アクセス対象、日時等）

上記の記録につき、乙は法定保存年限経過後 5 年間保存する。

本項で示す運用に関する記録に関する情報については、６．６(2)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、運用の完全性について明示する。
・本例では、運用の完全性を担保する観点から、対象事業者が利用者及び運用者の受託情報へのアクセス状況を記録し、保存することを明示している。
・アクセス記録の保存期間として本例では法定保存年限経過後 5 年間としている。
・アクセス記録については、取得対象とするシステムや方法によって記録容量等が大きくなることも想定される。そのため、記録方法や保管形態、保管方法によりサービスコストの上昇につながりうる。またアクセス記録に対するレビュー等をサービス内容とする場合にも、サービスコストに大きく影響が生じる。対象事業者はその旨も含めて、医療機関等の理解を得た上で合意を行うことが求められる。
・本例で示した報告項目及び数値は、あくまでも例示であり、アクセス記録対象及び記録保存期間について、追記等することが想定される。
・また本例の想定では、対象事業者がネットワークサービスの提供を行っていないことから、ネットワークに関するアクセス記録については明示していない。対象事業者がネットワークサービスも含めて包括的にサービス提供をしている場合には、ネットワークへのアクセス記録等も含めることも想定される。
・対象事業者が実施するアクセス状況の記録に関する情報及びその記録内容につき、医療機関等からの要請があった場合に、対象事業者は一定の条件で受託情報の管理状況についての資料提供を行う旨を明示している。

６．４ 非常時の対応

災害、長時間の停電、ネットワーク網の障害、サイバーテロ等の発生により、乙においてサービス提供が困難となった場合において、乙は本サービスの運用における非常時対応行う。また必要に応じて、乙は、甲に対するサービス停止を行う。

非常時におけるサービス停止の判断は、乙において行う。サービス停止が発生している旨について及びその対応状況については、下記の場所において告知するほか、４．４(2)に示す連絡先において、情報提供を行う。

・【https://+++.****.jp/----/（乙の用意する Web 上のページ)】

本項で示す非常時対応に関する手続・手順等については、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、非常時の対応について明示する。
・本例では、災害、長時間の停電、ネットワーク網の障害、サイバーテロ等に起因するサービス提供の停止を非常時と位置づけて、その対応手続等を事前に対象事業者が定めて、これに従い対応を行うことを示している。
・災害、長時間の停電、ネットワーク網の障害に起因するサービス提供の不能は、大きく分けて、対象事業者側の所在する地域で発生した災害等に伴う場合と、医療機関等が所在する地域において発生した災害等やネットワーク等の広範囲な障害等に伴う、多数の利用者における場合の２つの場合が想定される。対象事業者は、それぞれに対応した手順等を事前に文書化し、対応することが求められる。
・本例では、非常時の対応をとる旨についての判断は、障害の発生の判断に準じて、対象事業者が行うものとして示している。
・対象事業者が非常時の対応として実施する対策やそのための手順等につき、医療機関等からの要請があった場合に、対象事業者は、一定の条件で資料提供を行う旨を明示している。

６．５ 報告事項・事前連絡

(1) 報告事項と頻度

① 月次報告事項

本サービスの提供に係る運用に関し、乙は、下記の事項につき、月次で甲に対して報告を行う

・乙が甲より受託する受託情報件数

・甲の本サービスの利用状況（利用主体別アクセス状況、利用時間等）

・７．１(1)に示す管理指標

【本項を定める上での考え方】

・本項では、対象事業者が医療機関等に行う報告につき、月次報告の内容について明示する。

・対象事業者から医療機関等に対してなされる報告は、医療機関等が医療情報安全管理ガイドラインに基づき課せられている管理義務を果たすために必須のものである。医療機関等の情報システム管理責任者は、必ずしも情報システムについて詳細な知見を持ち合わせているわけではない。そのため医療機関等が寄託している医療情報が、不正に使用されていないこと等を確認するための資料等の提出が求められる。

・本例で示した報告項目は、あくまでも例示であり、最低限の内容である。したがって対象事業者において上記観点から必要とされる項目について、月次の報告とすることが想定される。

・月次の報告については、本例では、特に報告時期については定めていない。必要があれば、対象事業者において、月次報告を行う時期（例えば、毎月第一週目の火曜日等）等を定めることも想定される。

② 年次報告事項

本サービスの提供に係る運用に関し、乙は、下記の事項につき、年次で甲に対して報告を行う

・乙における３．５に掲げる法令・ガイドライン等の遵守状況
・乙における実績等に基づく個人データ安全管理に関する信用度
・３．７により実施した本サービス提供に係る監査結果
・巻末の「要員教育」に示す項目を実施している旨、及びその概要、結果等
・乙における経営状況等を示す資料（財務状況等）

【本項を定める上での考え方】

・本項では、対象事業者が医療機関等に行う報告につき、年次報告の内容について明示する。
・医療機関等は、適切な委託先と契約をしていること、また、継続して委託してよいか確認する必要があることから、対象事業者は、自身の運用状態に係る情報や、経営等に係る情報等についても定期的に報告をすることが望ましい。特に医療情報安全管理ガイドラインでは、契約開始段階で一定の条件を満たした事業者が外部保存を行うサービスを提供することを条件としており（8.1 3(c)）、契約の継続等を進める上でも、定期的に条件を満たしていることを確認する必要がある。
・上記の観点から、本例では、対象事業者の運用に関する信用に係る情報や、経営等に係る情報について、年次で報告すべき項目を例示している。
・本例で示した報告項目は、あくまでも例示であり、対象事業者において上記観点から必要とされる項目については、年次の報告とすることが想定される。
・年次の報告については、本例では特に報告時期については定めていない。必要があれば、対象事業者において、年次報告を行う時期（例えば、毎年契約更新時等）等を定めることも想定される。

③ 発生の都度に報告する事項

本サービスの提供に係る運用に関し、乙は、下記の事項につき、発生の都度、甲に対して報告を行う。

・本サービスに係る業務体制、管理体制、保守体制等の変更
・システムの動作確認において、乙が受託する医療情報を参照した際の作業結果
・リモートメンテナンスによる甲のシステム改造、保守作業の実施結果
・乙が業務上、受託情報を組織外に持出し、あるいは、再委託事業者へ保存した結果
・ウイルス混入や不正なメッセージの混入等による改竄（ざん）、パスワード盗聴、本文盗聴が生じた際の経緯・顛末
・障害等に伴うサービスの停止に関する経緯、顛末
・保守等に伴うシステムの変更の結果

【本項を定める上での考え方】

・本項では、運用上、不定期で発生する事項に関して、対象事業者が医療機関等に報告すべき内容について明示する。
・報告対象となる運用上、不定期で発生する事項は、障害等のサービス提供上の問題や、セキュリティ事故、あるいは、原則禁止とされている事項で、例外的に対象事業者において運用上実施する必要がある事項等、サービス利用者である医療機関等に対して周知する必要性が高い内容である。
・本例で示した報告項目は、あくまでも例示であり、対象事業者において上記観点から必要とされる項目については、追記することが想定される。
・不定期で発生する事項については、定期報告とは異なる機会に報告することが求められる。次項(2)に示すように、報告内容が医療機関等を特定するものでない場合には、Web 上や、同報発信によるメールにより報告することも想定される。報告内容が特定の医療機関等に対するものである場合、メール又は書面により直接、報告対象となる医療機関等に対して報告することが想定される。

(2) 報告方法

(1)に示す事項につき、乙は、下記に示す方法により、甲に対して報告を行う。

個人情報を含む報告については、書面又は暗号化が施された電子メールによるものに限定する。

① 書面又は電子メールにより報告を要する項目

・乙が甲より受託する受託情報件数

・甲の本サービスの利用状況（利用主体別アクセス状況、利用時間等）

・システムの動作確認において、乙が受託する医療情報を参照した際の作業結果

② 書面又は電子メールによるほか、乙において管理する乙の名義における Web 上で公開による報告が可能な項目

(1)に示す事項のうち、(1)①以外の事項。

【本項を定める上での考え方】

・本項では、報告事項に関する報告方法について明示する。

・本例では、報告内容が医療機関等を特定するものでない場合には、Web 上や、同報発信によるメールにより報告することとしている。報告内容が特定の医療機関等に対するものである場合、メール又は書面により直接、報告対象となる医療機関等に対して報告することとしている。

・報告内容において個人情報を含む場合には、当然のことながら、医療機関等に直接報告する方法である書面又は暗号化を施した電子メールに限定することを明示している。

・本項で示した内容は、あくまでも例示であり、対象事業者において上記観点から必要とされる項目については、追記することが想定される。

(3) 事前連絡及び承認等

① 保守業務に伴うサービスの停止の告知

本サービスを提供するシステムの保守業務の実施のため、提供するサービスを停止する場合には、乙は、1 週間以上前に、甲に対して告知を行う。ただし障害等に伴い、緊急で行うサービスの停止については、この限りではない。

サービス停止中は、サービス停止中である旨の表示をサービス利用画面において行う。

【本項を定める上での考え方】

・本項では、保守業務に伴うサービスの停止の告知が必要とされる場合の手続きについて明示する。
・第 1 段落では、保守業務に伴いサービスを停止する際の事前告知について明示している。本例では事前に予定されている保守作業によりサービスを停止する場合には、1 週間以上前の時点から、利用者である医療機関等にサービス停止する旨を告知することとしている。これは、サービス停止を事前告知することにより、利用者側での業務の調整の機会を与え、仮に業務に影響が出ることが予想される場合に、利用者からの連絡により対応措置を講じること等により、利用者の業務への影響を最小限にすることを目的としている。
・したがって、この場合には、できるだけ利用者に周知することが重要であり、事前告知については Web 上だけではなく、電子メール等による連絡等も併せて行うことが望ましい。
・なお、本例では、事前告知のタイミングを 1 週間以上前としているが、この期間については上記趣旨を満たす間隔であれば、変更されることを想定している。
・第 1 段落但し書は、障害等により、予定しないサービス停止の場合の告知について、明示している。
・障害等が発生して、その保守のためにサービス停止を余儀なくされる場合、速やかに正常復帰することが最も重要であることから、この場合には事前告知なく、サービス停止を行い、保守対応をすることが求められる。
・ただし、この場合でも可能であれば、例えば、「1 時間後に緊急保守業務のためサービス停止を行う」等の告知を、電話、メール、サービス利用画面等で行うことが望ましい。
・第 2 段落は、サービス停止中にサービス停止中である旨の表示を行うことを明示している。
・非常時にサービス停止を行う場合はもちろん、事前に予定されたサービス停止を行う場合でも、サービス停止状態にあることを知らないまま、利用者が利用画面にアクセスすることが想定される。これに伴う混乱を回避するため、本例ではサービス停止中である旨の表示を行うことを定めている。

② 受託情報等に関する保守業務の事前連絡・承認

本サービスを提供するに当たり、乙は、下記の対応を実施する前に、必ず甲に対して連絡し、承認を受ける。ただし、甲への事前連絡及びその承認を得られないことが、乙の責めに帰すべからざる事由によるものであり、下記の対応を行うことに緊急性が認められる場合には、この限りではない。

・システムの動作確認において、受託した個人情報の参照をする場合
・リモートメンテナンスによる甲側のシステム改造、保守作業を実施する場合
・乙が受託した情報を組織外に持出し、又は再委託事業者へ保存する場合

上記事項については、実施後、乙は、速やかに甲にその内容を報告し、承認を受ける。

【本項を定める上での考え方】

・本項では、受託情報等に関する保守業務の事前連絡・承認が必要とされる事項について明示する。
・第1段落では、保守業務を実施する上で、受託情報を参照したり、外部に持出したり、あるいは、医療機関等の管理するシステム（例えば、利用端末）をリモートメンテナンスする場合等について、事前の連絡と承認を受ける旨を明示している。
・受託する医療情報は、特に取扱いに注意を要する個人情報であることから、原則として受託する対象事業者の外部に持出したり、システムの動作確認等に用いたりすべきではない。しかしながら保守業務の関係で、例外的に実施せざるを得ない場合には、委託元である医療機関等に対して事前連絡を行った上で、承諾を得ることが求められる。
・また対象事業者のサービス内容によっては、医療機関等がクラウドサービスの利用端末等の環境を保守する場合も想定される。この場合でも、利用者側の混乱や不測の影響を回避する観点から、事前連絡と承認が求められる。
・第1段落但し書きは、前段の原則に対する例外を明示している。
・対象事業者が繰り返し事前連絡を行ったにもかかわらず、医療機関等側から合理的な理由がないまま承認がない、等の医療機関等の帰責事由によって承認が得られない状況が生じ、かつ保守業務との関係で速やかに受託情報を参照しなければならない等の要請がある場合の例外的な対応について明示している。
・第2段落では、事前連絡及び承認に基づいて、本項で定める保守業務を実施した場合に、事後の報告と承認を得る旨を明示している。
・本例で定めている事前連絡・承認の対象となる事項は、例示であり、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において示される内容である。上記の観点から、対象事業者において必要と考える事項を追記する等も想定している。

③ 保守業務に関する事前連絡等

本サービスを提供に供するシステムの保守業務につき、乙は、甲に対して下記の事前及び事後の対応を行う。

実施内容	事前・事後の対応
ア）ウイルスのパターンファイルへの対応 乙が管理する機器のファームウェアの更新	実施後、【http://+++.****.jp/----/（乙の用意するWeb上のページ）】にて報告
イ）OS等へのセキュリティパッチ等の適用	実施前に事前告知を行い、適用し、実施後、【http://+++.****.jp/----/（乙の用意するWeb上のページ）】にて報告 （ただし提供ベンダーにより、適用することについて緊急性及び重要性が高い旨の評価がある場合には、ア）に準じる）
ウ）その他のシステム上のプログラムの改変等	事前に実施内容につき甲に連絡をした上で、甲の承諾を得て実施。実施後、乙の管理する乙名義のWeb等にて報告 （ただし契約時において、包括的事前承諾を得ている保守対象となる事項については、イ）に準じる）

【本項を定める上での考え方】

・本項では、保守業務に関する事前連絡等が必要とされる事項について明示する。
・医療情報安全管理ガイドラインは、システムの保守業務等に関して、医療機関等の管理者に事前承認と事後承認を行う旨を明示している（6.8 C）。
・一方でクラウドサービスは、多数の利用者に対して同時にアプリケーションを利用できる環境を提供するサービスという性格を有している。そのため、すべての利用者が保守業務に対して事前承認を行わなければ着手できないとすると、かえって安全な利用環境の提供ができなくなる場合が生じることが懸念される。
・本例では、保守業務の内容により、ア)事後報告のみを要する保守内容、イ)事前告知及び事後報告を要する保守内容、ウ)事前承認及び事後報告要する保守内容に分けている。これにより、医療機関が行うべき、医療情報に供するシステムの安全性の確保のための手続きと、クラウドサービスの特性から生じる要請を満たすことを目的としている。
・なお、本例では、上表ウ）に当たる実施内容においても、契約時に包括的事前承認を得ている保守業務については、例外として扱う旨を明示している。

・包括的事前承認の対象となる保守業務は、機能の追加や削除等ではなく、専ら従来の機能に対して利用者の利便性を改善するための措置等が想定される。例えば、法令の改正に伴いテーブルに設定されるデータに変更が生じた場合等が挙げられる。

６．６ サポート

(1) 利用者に対するサポート

① サポート内容

本サービスの利用に関し、乙は、甲から下記の問い合わせを受け付け、サポート対応をする。

・本サービスで提供するアプリケーションの使用方法等に関する内容
・本サービスの利用環境及びその設定に関する確認（OS、Web ブラウザ等。ただし、以下は含まない。本サービスで提供するアプリケーション以外のアプリケーション等の使用方法等、乙が管理しないパソコンの機器の使用方法等に関する内容）
・本サービスの利用上の障害に関する内容
・本サービスの利用に起因する甲のシステムの障害に関する内容

【本項を定める上での考え方】

・本項では、サポート内容を明示する。
・対象事業者は、一般に利用者からの問合せに対する問合せ受付を用意する。その際、どの範囲の内容を受け付けるのかをあらかじめ合意する必要がある。
・クラウドサービスの利用では、その前提として利用者側の OS やネットワークに関する設定、Web ブラウザ等の設定等が正しくなされていることが求められる。一方で利用者によっては、OS やブラウザの利用方法自体に精通していない場合も多く想定される。
・サポートセンターの受付内容として、利用者の幅広い問い合わせを受け付ける場合には、一般的にはそのための人員や受付時間のための負担が多くなり、サービスコストの上昇が余儀なくされる。そのため、受付内容の範囲を明確にし、利用者の利便性とサービスコストとのバランスを図ることが求められる。
・本例で示した報告項目は、あくまでも例示であり、対象事業者において上記観点から必要とされる項目については、追記することが想定される。また受付方法や応答時間との関係で、受付内容の範囲を区分することも想定される（急を要しない内容については受付内容の範囲を広くする等）。

② サポート対応時間

本サービス提供に関し、乙は、甲からの問い合わせを受けるため、下記において受付対応を行う。

【乙サポートセンター】　連絡先　（受付対応時間、曜日）

【本項を定める上での考え方】

・本項では、サポート対応時間等を明示する。なお、「I.参考例編（サービス仕様適合開示書)」では、問合せ対応について（2）⑭で示している。

・サポート対応時間は、通常電話によるものが想定されるが、例えば、時間外や、急を要しない照会内容等は、メールによる受付を行う対象事業者もある。このような場合には、本項で問合せ用の Web ページ等を併せて明示する。

(2) 技術情報提供について

本サービス提供上、乙が採用するセキュリティ対策等につき、採用する技術仕様等に関する情報、対策実施に関する技術情報について甲から提供の要請があった場合に、下記に従い、乙は提供する。乙において情報の開示が困難である場合には、乙は、困難である理由を提示し、安全性を示すための代替する説明資料の提供を行う。

・甲と乙において別途、機密保持契約を締結した上で提供する。
・提供範囲、方法については、別途甲乙協議の上、決定する。
・提供に係る費用については、本サービス提供に係る基本サービス料金とは別途発生するものとし、甲乙協議の上、決定する。

【本項を定める上での考え方】

・本項では、技術情報提供について明示する。なお、「I.参考例編（サービス仕様適合開示書)」ではそれぞれの項目で、技術情報を含む情報の開示方法・条件・範囲等を示している。
・本 SLA では、対象事業者が講じるべき安全管理対策のうち、技術的な対応については、個別の対応措置の内容や方式、仕様等を明記せず、各項目において３．５に示す法令・ガイドラインの該当箇所を満たす対応を実施する、という規程振りを採用している。その上で、個別の対応措置の内容や方式、仕様等については、医療機関等の求めに応じて対象事業者が必要な対応を講じていることの根拠となる資料を提供する、という記述方法を採用している。
・これは、個別の対応措置の内容や方式、仕様等を明記すること自体がセキュリティ対策等との関係で好ましくないこと、技術の進展等により、採用すべき仕様等も変更される可能性が高いことから、あえてそれらを明記せず、変更の都度に資料の提供を求める形の方が、柔軟な対応を講じやすいこと等を想定しているためである。
・上述の観点から本例では、
  ✓原則として、対象事業者は、医療機関等の求めに応じて資料を提供する
  ✓提供に際しては、一定の条件が必要な場合には、その調整を行う
  ✓対象事業者は、医療機関等の求めに応じて資料を提供することが困難な場合には、その理由を明らかにするとともに、要求事項に対して必要な措置を講じていることを示す代替資料を提出する

  というような記載にしている。
・なお、技術資料の提出については、資料の内容等によっては、別途費用を要することも想定されることから、対象事業者はその旨も含めて、医療機関等の理解を得た上で合意を行うことが求められる。

(3) 運用状況に係る情報提供について

本サービス提供上、乙が行う運用に関し、乙が実施する本 SLA の各項の運用の状況を示す情報について、甲から提供の要請があった場合に、下記に従い、乙は、提供する。乙において情報の開示が困難である場合には、乙は困難である理由を提示し、運用の完全性を示すための代替する説明資料の提供を行う。

・甲と乙において別途、機密保持契約を締結した上で提供する。
・提供範囲、方法については、別途甲乙協議の上、決定する。
・提供に係る費用については、本サービス提供に係る基本サービス料金とは別途発生するものとし、甲乙協議の上、決定する。

【本項を定める上での考え方】

・本項では、運用状況に係る情報提供について明示する。なお、「I.参考例編（サービス仕様適合開示書)」ではそれぞれの項目で、運用状況を含む情報の開示情報や条件・範囲等を示している。
・本例では、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に記述する各項目について、対象事業者は運用管理規程で文書化を行った上で、これに基づき実施し、必要な記録を残す、という形を採用している。
・本項では、この運用状況を示す記録等に関する資料提供について、明示する。本例では、
  ✓原則として対象事業者は医療機関等の求めに応じて資料を提供する
  ✓提供に際しては、一定の条件が必要な場合にはその調整を行う
  ✓対象事業者は医療機関等の求めに応じて資料を提供することが困難な場合には、その理由を明らかにするとともに、運用管理規程に基づいて運用していることを示す代替資料を提出する
  というような記載にしている。
・なお、運用状況の記録の中には、例えば、利用者のアクセス記録等、資料の内容等によっては、別途費用を要することも想定されることから、対象事業者は、その旨も含めて、医療機関等の理解を得た上で合意を行うことが求められる。

７．サービスレベルに関する合意事項

７．１ サービスレベルの評価方法

(1) 管理指標及び評価方法

① 管理指標

本サービスの提供につき、乙は、下記に示す管理指標を甲に報告し、共同で評価を行う。

・サービス稼働率
・障害対応時間
・ウイルス対策のためのパターンファイル並びに、OS 及びミドルウェア等のセキュリティパッチの対応状況
・巻末に示す事項の実施状況

本項の評価を行うのに必要な限りで、乙は、甲に対して情報の提供を行う。

【本項を定める上での考え方】

・本項では、サービスレベルの管理指標について明示する。
・SLA を示す契約においては、SLA で記載された内容の実施状況を定期的に対象事業者が利用者に対して報告し、サービス品質の管理が行われる。実施状況を示す指標として管理指標が定期的に対象事業者から利用者に対して報告される。
・本例では、６．３において示す事項のうち、指標化が可能な内容、ウイルス対策等の実施状況及び実施率を管理指標とすることを示している。また、SLA の評価を行うのに必要な限りでの、情報の提供を行うことを示している。
・本例は、あくまでも事例であり、どのような指標を採用するかについては、対象事業者の提供するサービス内容や、SLA の内容等によって異なってくる。対象事業者と医療機関等との協議の結果、変更されることを想定している。

② 評価方法

サービスレベルの評価は、年次ごとに実施する。ただし甲乙協議の上、必要に応じて、別途、評価を行うことができる。

本 SLA の評価は、①で示す指標につき、以下のように評価する。

■　未達成件数の計算

SLA の未達成についての計算方法を、以下に示す。

項目	計算方法
・サービス稼働率	評価期間中の数値が６．３(2)に示す数値に満たない場合、未達成とする。
・障害対応時間 ・ウイルス対策のためのパターンファイル並びに、OS 及びミドルウェア等のセキュリティパッチの対応状況	発生都度において、本 SLA で示す数値を満たさない場合には、都度未達成 1 件として計算する。

■ SLA の評価

年次の評価期間における未達成件数から、本 SLA の達成度を以下のように評価する。

未達成件数	評価
0	A
1-10	B
11-20	C
21-	D

【本項を定める上での考え方】

・本項では、サービスレベルの評価方法について明示する。

・SLA による契約の場合、SLA の評価指標に対して、一定の方法に基づいて SLA の評価を行うことが求められる。評価方法については、サービスの内容や特質等を勘案して当事者間により決められる。

・本例では、各種ガイドラインの遵守に重点を置く観点から、本 SLA の実施項目自体の未達成を重視した評価方法としている。本例では、各項目について特に軽重を置かない形を例示しているが、例えば情報漏洩事故に強く関係する要求事項の不達成を重視して評価を定めるなどの考え方もある。

・本例は、あくまでも事例であり、どのような評価方法を採用するかについては、対象事業者の提供するサービス内容や、SLA の内容等によって異なってくる。対象事業者と医療機関等との協議の結果、変更されることを想定している。

(2) サービスレベル算定除外事項

前項のサービスレベルの評価に関し、下記については算定除外事項とする。

事前に合意された事由	・定期保守のための停止 ・機器の導入やシステムの構成変更作業のための停止 ・データベース再編成等業務上必要な停止
制御できない事由	・電力供給業者の障害 ・通信回線業者の障害 ・自然災害等の不可抗力 ・その他の企業・団体が提供する機器やサービスに起因する障害
甲の責任に帰する事由	・甲の作為又は不作為 ・甲の管理する機器、ソフトウェア等の障害に起因する事由 ・本合意に定める甲の不履行 ・甲の誤った作業依頼、指示等
その他、乙の責めに帰すべからざる事由	・性能要件【定義必要】を超える負荷 ・乙が保証したシステム環境以外での使用 ・その他、甲と乙の協議により定めたもの

【本項を定める上での考え方】

・本項では、サービスレベルの評価に際しての除外項目について明示する。

・SLA の評価に当たっては、対象事業者の責めに帰すべからざる事由により発生した未達成となる事項については、当事者の公平の観点から SLA の評価対象となる事案からはずすことが求められる。

・この場合に問題となるのは、対象事業者、医療機関等の両当事者の責めに帰すべからざる事由により生じた未達成となる事項についてである。クラウドサービスの場合、複数のサービスを合わせることで利用される場合（例えば、通信サービスとクラウドサービス等）等が挙げられる。この点は、責任分界とも密接に関係する部分である。

・本例では、対象事業者が管理しない事象により発生した事項については、SLA の評価対象外とすることを示している。

・本例は、あくまでも事例であり、どのような項目を算定除外項目にするかについては、対象事業者の提供するサービス内容や、サービスの提供形態、責任分界の考え方によって異なってくる。対象事業者と医療機関等との協議の結果、変更されることを想定している。

７．２ サービスレベルマネジメント

本サービスにおけるサービスレベルを維持するために、下記のサービスレベルマネジメントを実施する。

・乙が甲に行う月次の報告において、本 SLA で定めるサービス内容に達しないとする内容があった場合には、乙は、甲に対してその事由を報告するとともに、改善策を提示する。
・前項で本 SLA が定めるサービス内容に達しないとされた項目について、1 年以上改善が見られない場合には、甲は、乙に対して損害賠償の請求、契約の解除を申し入れることができる。
・SLA の評価の結果、C と評価された場合で、続く 1 回の評価において改善しない場合には、甲は、乙に対して契約に基づいて、損害賠償の請求、契約の解除を申し入れることができる。
・評価が D になった場合には、甲は、乙に対して契約に基づいて、損害賠償の請求、契約の解除を申し入れることができる。
・巻末に示す事項について遵守されていないことが判明した場合に、甲は、乙に対して相当の期間を定めて改善を図る旨を要請する。相当期間経過後、改善が見られない場合には、甲は、乙に対して損害賠償の請求、契約の解除を申し入れることができる。
・その他、サービスレベルの維持を行うため、甲乙は、必要に応じて協議を行う。

【本項を定める上での考え方】

・本項では、サービスレベルマネジメントについて明示する。
・SLA の評価の結果、サービスレベルを維持するためにどのような対応をとるのかがサービスレベルマネジメントである。
・本例では、SLA の評価等により、サービスレベルの達成状況に問題がある場合の対応について示している。本例で示す対応のほか、対象事業者の運用体制の変更を申し入れる等、サービス内容や実施体制等により、異なる対応により追記･変更することを想定している。また医療情報を取り扱う診療録の作成、保存等のサービスを想定していることから、評価についても著しく低い評価となった場合には、サービス契約の解除も含む内容となっている。
・本例ではサービスレベルの達成状況による対応を例示するが、例えば情報漏洩事故等が生じた場合の対応などについては、別途、契約書などで明記することが想定される。
・本例は、あくまでも事例であり、どのような評価方法を採用するかについては、対象事業者の提供するサービス内容や、SLA の内容等によって異なってくる。対象事業者と医療機関等との協議の結果、変更されることを想定している。

「別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインとの対応表」の見方

項目名		解説
対策項目	大項目	対策項目例に関連する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、「人的・組織的」・「物理的」・「技術的」の３つの対策の観点毎に整理・統合した内容。 主な実施主体として、対象事業者を想定する。
	小項目	
	No.	
	内容	
	区分	◎：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における遵守事項に該当 ○：従前の情報処理事業者ガイドラインにおける推奨事項に該当
対策項目により対策可能なリスクシナリオ例		対策項目により対策可能となる、代表的なリスクシナリオを例示
関連する医療情報安全管理ガイドラインの要求事項	項番	関連する医療情報安全管理ガイドラインの要求事項。 主な実施主体として、医療機関等を想定する。
	区分	
	内容	

記載全般に係る注意事項

別紙2における「利用者」という表記については、従前のクラウド事業者ガイドラインと同様に、医療機関等においてサービスを利用する者のほか、医療情報システム等の運用もしくは開発に従事する者又は管理者権限を有する者も含めた位置づけとしている。対象事業者は関連する情報流やリスクによって利用者が異なることに留意すること。

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
1. 人的・組織的対策								
1.1. 規程・手順の策定	①アクセス管理規定の策定	①-1	医療情報システム等へのアクセス制限、記録、点検等を定めたアクセス管理規定を作成し、医療機関等の求めに応じて提出できる状態にしておく。	◎	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	6.3 組織的安全管理対策（体制、運用管理規程）	C.最低限のガイドライン	3.情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。
		①-2	アクセス管理規定には以下の内容を含める。 ・アクセス権限、アカウント管理における登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセス ・認証及びアクセス等に対する記録の収集と保存 ・認証及びアクセス等に対する記録の定期的なレビュー ・アクセス管理の運用状況に関する定期的なレビューの実施	◎				
	②持ち出した機器の外部のネットワークに接続する場合の対策の策定	②-1	持ち出した機器を外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改竄が生じないようにするための具体的な措置（不正プログラム対策、暗号化、ファイアウォール導入等））を運用管理規程に含める。	◎	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	6.5 技術的安全対策	C.最低限のガイドライン	10.システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
	③情報の廃棄対応	③-1	CD-R 等の廃棄手順について定める。	◎	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	6.7 情報の破棄	C.最低限のガイドライン	1.「6.1 方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。
		③-2	ハードディスク等の廃棄手順について定める。	◎				
		③-3	破棄手順に、不可逆的な破壊･抹消等により元のデータを復元できなくする措置を含める。	◎				
		③-4	ハードディスク等を医療情報システム等内の別の機器で再利用する場合には、再利用前に、複数回のデータ書き込みによる元データの消去等の確実な方法でデータを消去し、再利用前に情報が消去されていることを確認する。	◎		6.7 情報の破棄	C.最低限のガイドライン	2.情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること。
		③-5	サーバ等の BIOS パスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去する。	◎				
		③-6	ハードディスクを機器に接続する際には、再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証する。	◎				
		③-7	ハードディスクの廃棄については、再利用及びデータの読み出しが不可能となるよう、複数回のデータ書き込みによる元データの消去、強磁気によるデータ消去措置、物理的な破壊措置（高温による融解、裁断等）等を適用し、当該装置に実施した措置の概要の記録（対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等）について、医療機関等の求めに応じ、速やかに提出できるよう整備する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		③-8	物理的な破壊措置については受託事業者自身で行うことが望ましいが、外部の事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し外部委託の了承を得ておく。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておく。 なお、ハードディスクの廃棄方法としては、一定以上の強度を持つ磁力線を照射する方法、溶融処理等の物理的破壊措置が確実であるが、ランダムデータ及び固定パターンの複数回の書き込みを行うソフトウェア実行によるデータ消去方式（NSA 推奨方式、米国防総省準拠方式、NATO 方式、グートマン方式等）も良く利用されている。保存されている情報の重要性に合わせて適切な方式を選択し、医療機関等側に選択の合理的な理由を説明、合意を得た上で実施することが望ましい。	○				
		③-9	電子媒体を廃棄する場合には、物理的な破壊措置（高温による融解、裁断等）を適用し、情報の読み出しが不可能であることを確認する。	◎				
		③-10	運用管理規程に以下の内容を定める。 ・管理する個人情報又はこれを格納する媒体等について、医療情報システム等提供上の要否の確認を定期的に行うこと。 ・医療情報システム等提供上不要とされた個人情報及びこれを格納する媒体についての破棄手順。 ・医療情報システム等提供上不要とされた個人情報及びこれを格納する媒体の破棄に際して、医療機関等が不測の損害を被らないようにするための措置(事前に破棄の基準等を告知する等）。	◎		6.7 情報の破棄	C.最低限のガイドライン	4.運用管理規程において下記の内容を定めること。 (a) 不要になった個人情報を含む媒体の破棄を定める規程の作成
		③-11	情報の破棄手順について、医療機関等と合意する。	◎				
	④情報や機器の組織外への持出に対する対策	④-1	受託する個人情報を運用や保守に用いる端末に原則保存しない旨、自社の運用管理規程等に定める。	◎	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	6.8 情報システムの改造と保守	C.最低限のガイドライン	7.保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。
		④-2	医療情報を格納する機器等を、保守（例えば機器の修理等）の目的で、医療機関等又は受託事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、その手順を策定する。	◎				
		④-3	④-2で定める手順及び情報の提供条件について、医療機関等と合意する。	◎				
		④-4	持ち出した機器を再度設置するための適切な検証手順を策定する。	◎				
		④-5	保守点検で障害不良等が発見された際の対応作業等を行う際には受託事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにする。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去してから持ち出す。記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的な破壊を行ってからの廃棄を選択する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		④-6	持ち出し手順に含まれる事項には次のようなものが考えられる。 ・ 装置の持ち出し申請書のフォーマット（申請者情報、承認者情報、対象機器情報、持ち出し日時、返却予定日時、持ち出す場所の情報、持ち出す理由、機器に納められている情報の概要、持ち出しに伴うリスク評価の結果、機器が紛失・損傷した場合の対応策、等） ・ 申請承認プロセス ・ 返却確認プロセス、等。	◎		6.8 情報システムの改造と保守	D.推奨されるガイドライン	4.保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。
		④-7	返却時の検証手順に含まれる事項には次のようなものが考えられる。 ・ 装置の動作確認 ・ 盗聴装置等、情報の安全性を脅かす装置の有無 ・ 悪意のあるプログラムの検出作業 ・ 収められている情報の検証作業（不正な改竄等）、等。	◎				
	⑤持ち出した機器や媒体の管理手順の策定	⑤-1	サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（委託元からの持ち出しを含む）に関する方針及び規則等を、運用管理規程に定める。	◎	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	1.組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。
		⑤-2	⑤-1における「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。	◎				
		⑤-3	⑤-1で定める内容について、医療機関等と合意する。	◎				
		⑤-4	電子媒体について受託事業者施設外への不要な持ち出しを行わない。CD、DVD、MO 等の電子媒体については、追記のできない光学メディア（CD-R、DVD-R 等）を用い、情報交換作業終了後、電子媒体を確実に廃棄処分する。	◎		6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	2.運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。
		⑤-5	情報交換目的やバックアップ目的で MT、DAT、半導体記憶装置、ハードディスク等の大容量の電子媒体を用いる場合には、その管理を厳重に行う。これらの電子媒体に複数回の情報記録を行う場合には、単に上書きするのではなく、確実な情報消去等の情報漏洩対策を行う。	◎				
		⑤-6	全ての電子媒体には格納される情報の機密レベルを示すラベル付けを行う。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		⑤-7	記録媒体･記録機器に関し、以下の内容を運用管理規程に含める。 ・管理体制及び管理方法 ・記録媒体･記録機器の取扱い ・サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等 （「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。） ・サービスに関する情報を持ち出した場合で、当該情報を格納する機器･媒体等の盗難･紛失（持ち出し時の機器･媒体等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等（第三者による悪意の送信、従業者等における誤送信等を含む。））が起きた場合の対応	◎		6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	3.情報を格納した可搬媒体若しくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。
		⑤-8	⑤-7の内容に関する教育を従業員等に対して行う。	◎		6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	4.運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと。
		⑤-9	⑤-7の内容を含む運用管理規程については、再委託先に対しても遵守等を求める。	◎				
	⑥機器・ソフトウェアの品質管理に係る手順の策定	⑥-1	情報処理装置及びソフトウェアの適切な変更手順を策定する。原則、保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受ける。	◎	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	3.　機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。
		⑥-2	機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等に含める。	◎				
		⑥-3	機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う。	◎				
		⑥-4	医療情報システム等に係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。	◎				
		⑥-5	変更手順に含まれる事項には次のようなものが考えられる。 ・ 変更についての影響が及ぶ関係者への通知プロセス ・ 装置の変更申請書のフォーマット（申請者情報、承認者情報、対象機器情報、変更作業開始日時、変更作業期間、変更理由、機器に納められている情報の概要、変更に伴うリスク評価の結果、機器が損傷した場合の対応策、等）申請承認プロセス変更試験プロセス ・ 変更作業に支障が発生した場合の復旧手順変更終了確認プロセス ・ 変更に伴う影響を監視するプロセス、等。	○		7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	2.　機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスが規定されていること。

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
1.2. 個人情報を含まないテストデータの利用	①個人情報を含むデータの利用に対する対策	①-1	医療情報を開発及び試験用データとして直接利用しない。利用する場合には、個人を識別できる情報等の削除及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関等に示し、了解を得た上で利用する。	◎	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	6.5 技術的安全対策	C.最低限のガイドライン	5.動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。
1.3. 守秘義務に係る契約	①医療情報システム等提供に係る職員全てとの守秘義務に係る契約締結	①-1	医療情報を操作する可能性のある受託事業者の職員全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求める。派遣従業員については守秘義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求める。	◎	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	6.6 人的安全対策　（1）従業者に対する人的安全管理措置	C.最低限のガイドライン	1.法令上の守秘義務のある者以外を事務職員等として採用するに当たって、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。
		①-2	医療情報を操作する可能性のある受託事業者の職員（派遣従業員含む）については、守秘義務に関する内容を就業規則等に含める。	◎				
		①-3	医療情報を操作する受託事業者の職員（派遣従業員含む）が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておく。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求める。派遣従業員については、派遣契約解除時に同等の合意書への署名を求める。	◎		6.6 人的安全対策　（1）従業者に対する人的安全管理措置	C.最低限のガイドライン	3.従業者の退職後の個人情報保護規程を定めること。
		①-4	医療情報を操作する受託事業者の職員（派遣従業員含む）が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等に含める。	◎				
		①-5	上記に違反した受託事業者（派遣従業員含む）の職員に対して、適切な懲戒手続きを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。定めた懲戒手続きについては各職員に周知し、理解したことの確認を行う。	◎		6.6 人的安全対策　（2）事務取扱委託業者の監督及び守秘義務契約	C.最低限のガイドライン	1.医療機関等の事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。 ① 受託する事業者に対する包括的な罰則を定めた就業規則等で裏付けられた守秘契約を締結すること ② 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行うこと。 ③ 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。 ④ 委託事業者が再委託を行うか否かを明確にして、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。
		①-6	医療情報を操作する受託事業者の職員（派遣従業員含む）に対する教育･訓練の実施状況や、守秘義務等への対応状況等に関する資料の提供について、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	②医療機関等や再委託先との守秘義務を含めた契約の締結	②-1	医療情報システム等に係る情報及び受託した情報に関する守秘義務について、医療情報システム等提供に係る契約に含める。契約には、守秘義務に違反した受託事業者にはペナルティが課されること、及び委託した情報の取扱いに対する医療機関等による監督に関する内容を含める。	◎	医療情報システム等提供に係る事業者（再委託先も含む）による故意又は過失による情報漏洩が行われる。	6.6 人的安全対策　（2）事務取扱委託業者の監督及び守秘義務契約	C.最低限のガイドライン	2.プログラムの異常等で、保存データを救済する必要があるとき等、やむを得ない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行うこと。
						6.8 情報システムの改造と保守	C.最低限のガイドライン	6.保守会社と守秘義務契約を締結し、これを遵守させること。
						6.8 情報システムの改造と保守	D.推奨されるガイドライン	3.作業員各人と保守会社との守秘義務契約を求めること。
						8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準	C.最低限のガイドライン	3(ア) 医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取扱いに対して監督を行えること。
		②-2	医療情報システム等の動作確認に際し、受託した個人情報を含むデータをやむを得ず使用する場合には、守秘義務が課された要員･委託先等により動作確認を行う旨を含めた手順を定める。	◎		6.8 情報システムの改造と保守	C.最低限のガイドライン	1.動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めること。
		②-3	医療情報システム等の動作確認に際し、受託した個人情報をやむを得ず使用する場合について、医療機関等と合意する。	◎				
1.4. 教育訓練の実施	①医療情報システム等提供に係る教育訓練の実施	①-1	医療情報を操作する可能性のある受託事業者の職員の全てに個人情報保護及び情報セキュリティに関する教育を行い、一定水準の理解を得た職員だけを業務に従事させる。	◎	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生する。	6.6 人的安全対策　（1）従業者に対する人的安全管理措置	C.最低限のガイドライン	2.定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。
		①-2	派遣従業員に関しては、派遣元に対し、個人情報保護及び情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行う。	◎				
		①-3	この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行う。	◎				
		①-4	医療情報を操作する受託事業者の職員（派遣従業員含む）の退職時又は契約終了時以降の守秘義務について、教育･訓練に含める。	◎		6.6 人的安全対策　（1）従業者に対する人的安全管理措置	C.最低限のガイドライン	3.従業者の退職後の個人情報保護規程を定めること。
1.5. 運用状況のモニタリング	①医療情報システム等提供に係る閲覧・操作内容のモニタリング	①-1	受託事業者の職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改竄又は破壊等の行為が行われていないことを検証する。	◎	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	6.6 人的安全対策　（1）従業者に対する人的安全管理措置	D.推奨されるガイドライン	1.サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。
		①-2	医療情報システム等の保守業務を行う際には、原則として業務の事前及び事後に医療機関等の管理者に対して書面等による通知を行う。事前の了解を必要とする業務及びその業務について事前の了解を得ることができない場合の対応方法について、医療機関等と合意する。	◎		6.8 情報システムの改造と保守	C.最低限のガイドライン	5.保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。
		①-3	保守業務実施後には、医療機関等に対し報告等を行い、医療機関等の管理者の確認を得る。本手順の対応について、医療機関等と合意する。	◎				
		①-4	医療情報システム等の保守業務を医療機関等の施設内で行う際の対応について、医療機関等と合意する。	◎		6.8 情報システムの改造と保守	D.推奨されるガイドライン	2.保守作業時には医療機関等の関係者立会いの下で行うこと。

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	②機器や媒体の定期的な所在確認	②-1	電子媒体は台帳を作成して管理する。台帳と電子媒体を定期的に検証し、盗難、紛失の発生を検証する。台帳においては利用に関する記録を行い、電子媒体の廃棄後も一定期間にわたり記録を維持する。	◎	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	5.医療機関等や情報の管理者は、情報が格納された可搬媒体若しくは情報機器の所在について台帳を用いる等して把握すること。
		②-2	情報を格納する機器･媒体等については、台帳管理等を行い、定期的に所在確認を行う。	◎				
		②-3	個人情報が保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。	◎				
	③システム構成やソフトウェアの動作状況に関する内部監査の実施	③-1	システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等に含める。	◎	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	4.　システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施すること。
1.6. 物理的に情報を搬送する場合の対策	①組織外に持出する情報に対する暗号化等の対策	①-1	物理的に情報を搬送する際には以下の対策を実施する。 ・ 医療機関等が合意する基準にもとづいて信頼できる配送業者を選択する。 ・ 配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐ。 ・ 配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認する。 ・ 配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用する。 ・ 電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さない。 ・ 電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施す。	◎	搬送中の電子媒体内の情報が抜き取られることで、情報漏洩が生じる。	6.8 情報システムの改造と保守	C.最低限のガイドライン	7.保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。
1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-1	受託した医療情報を保守･運用を行うために閲覧するのは必要最小限とする。	◎	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	6.6 人的安全対策　（2）事務取扱委託業者の監督及び守秘義務契約 ----- 8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準	C.最低限のガイドライン ----- C.最低限のガイドライン D.最低限のガイドライン	1.医療機関等の事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。 ① 受託する事業者に対する包括的な罰則を定めた就業規則等で裏付けられた守秘契約を締結すること ② 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行うこと。 ③ 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。 ④ 委託事業者が再委託を行うか否かを明確にして、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。 ----- (C.最低限のガイドライン) ③ 医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合 (エ) 保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。なお保守に関しては、「6.8 情報システムの改造と保守」を遵守すること。 (オ) 外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること。 (カ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、誤った閲覧（異なる
		①-2	①-1の閲覧が必要な場合には、緊急時を除き、システム管理者の事前･事後の承認により実施する。	◎				
		①-3	受託した医療情報を緊急時に閲覧した場合には、閲覧した受託情報の範囲及び緊急で閲覧が必要な理由等を示して、システム管理者の承認を得る。	◎				
		①-4	①-1～①-3における閲覧に係る範囲、手順等について、医療機関等と合意する。また①-2、①-3により医療情報を閲覧した場合に、速やかに医療機関等にその旨の報告を行う。	◎				
		①-5	受託した医療情報の解析･分析は、医療情報システム等提供に係る契約とは独立した契約に基づいて医療機関等からの委託を受けた場合を除いて行わない。	◎				
		①-6	受託した医療情報を匿名加工した情報も、医療情報に準じて取り扱う。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-7	受託した医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わない。	◎				患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないようにさせること。 (D.推奨されるガイドライン) (ウ)「②行政機関等が開設したデータセンター等に保存する場合」及び「③医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」では、技術的な方法として、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保すること。 (エ) 外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつこと。具体的には、「暗号化を行う」、「情報を分散保管する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を併せ持つこと。
		①-8	①-7の内容を、医療情報システム等提供に係る契約に含める。	◎				
		①-9	医療機関等の指示に基づき、受託した医療情報の第三者提供（閲覧）を行う場合には、医療機関等が許諾した者以外が閲覧･取得できないように対応策を講じる。	◎				
		①-10	①-9により、第三者提供（閲覧）を行う場合には、閲覧･取得が可能な者のID及び利用権限について、医療機関等又はその委託を受けた者（医療情報連携ネットワーク等）の指示に基づき、速やかに変更･削除できる対応を行う。	◎				
		①-11	医療機関等の指示に基づいて受託した医療情報の第三者提供を行った場合には、医療機関等に対してその内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告を行う。	◎				
		①-12	①-7～①-11により第三者提供及びその報告を行うための条件、範囲等について、医療機関等と合意する。	◎				
1.8. 情報の破棄に係る記録の提出	①情報の破棄に係る実施記録の取得及び医療機関等への提出	①-1	情報の破棄を実施した場合に、医療機関等の求めに応じて、実施担当者及び情報の削除方法（電磁記録媒体の消磁･物理的破壊等）を含む実施内容を医療機関等に対して報告し、破棄記録等を提出する。	◎	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	6.7 情報の破棄	C.最低限のガイドライン	3.外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策 （2）事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。
		①-2	物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については受託事業者自身で行うことが望ましい。外部の専門事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し十分な理解を得る。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておく。	○				
		①-3	①-1で講じる措置及び資料を提供するのに必要な条件等について、医療機関等と合意する。	◎				
		①-4	医療情報システム等提供の停止又は医療機関等における医療情報システム等利用停止が生じた場合は、速やかに、記録の削除、媒体の廃棄等を行う。記録の削除、媒体の廃棄等を行った場合には、これを証明する資料を医療機関等に対して提出する。	◎				
		①-5	①-4に関して、医療機関等へのサポート（所管官庁への情報提供含む）等に関連して必要最低限の範囲で、記録を保持し続ける場合には、その目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等について、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-1	情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、合意を得る。また、当該再委託に係る契約において体制を明確にする。	◎	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生する。	6.8 情報システムの改造と保守	C.最低限のガイドライン	9.再委託が行われる場合は、再委託する事業者にも保守会社の責任で同等の義務を課すこと。
		①-2	再委託先には、自社と同等の個人情報保護指針等を遵守させる。	◎				
		①-3	再委託に係る契約に、委託業務に係る守秘義務を含める。	◎				
		①-4	再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。	◎				
		①-5	医療情報システム等の保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等及びその情報の提供に関する条件について、医療機関等と合意する。	◎				
		①-6	医療情報システム等の保守に関して、外部事業者にその一部又は全部を委託する場合には、自社において実施している運用管理規程及び安全管理措置等への対応を、当該外部事業者に対して求める。	◎				
		①-7	①-6の実施状況に関して、契約実施ごとに又は定期的に、外部事業者に対して報告を求め、確認する。	◎				
		①-8	再委託先により提供される医療情報システム等の安全管理策及びサービスレベルが十分であることを確認する。	◎				
		①-9	再委託先による医療情報システム等の実施、運用、維持について定期的に検証する。	◎				
		①-10	再委託先による医療情報システム等の実施、運用、維持について定期的サービス実施について事前、事後報告を義務づけ、報告内容を点検確認する。	◎				
		①-11	再委託先による医療情報システム等を実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れない。	◎				
		①-12	医療情報システム等の実施中に再委託先が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯する。	◎				
		①-13	再委託先による医療情報システム等の実施にともなう処理施設内への立ち入り手順に関しては、受託事業者の職員の入室、退室手順に準ずる。	◎				
		①-14	再委託先による医療情報システム等の変更時には、引き続き安全性が維持されていることについて適切な検証を行う。	◎				
		①-15	医療情報システム等の保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関するガイドライン第 5 版」6.8 章 C 項の管理策を実施する。	◎				
		①-16	外部事業者が医療情報システム等を実施する際は、受託事業者又は外部事業者の正規職員が管理している状況で作業を行うことが望ましい。	○				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
1.10. 非常時に備えた対応	①医療情報システム等の提供に係る事業影響度分析の実施	①-1	医療情報処理に関わる業務プロセス（プロセスを実施するための作業員を含む）、情報処理装置等について識別する。	◎	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	6.10 災害、サイバー攻撃等の非常時の対応	C.最低限のガイドライン	1.医療サービスを提供し続けるための BCP の一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。
		①-2	業務プロセス間の相互関係を評価する。	◎				
		①-3	事業を継続するための業務プロセスの優先順位を明確にする。	◎				
		①-4	医療情報システム等に発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別する。	◎				
		①-5	医療情報システム等に発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別する。	◎				
	②医療情報システム等の提供に係る事業継続のための計画策定と模擬試験等による検証	②-1	医療情報システム等の提供における業務プロセス及び医療情報システム等の優先順位にもとづいて、医療情報処理に関する事業継続計画を策定する。	◎	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	6.10 災害、サイバー攻撃等の非常時の対応	C.最低限のガイドライン	1.医療サービスを提供し続けるための BCP の一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。
		②-2	策定した事業継続計画について模擬試験を含めた適切な方法でレビューする。	◎				
		②-3	事業継続計画について定期的に見直しを行う。	◎				
		②-4	策定される事業継続計画には次のような事項を含むことが望ましい。 ・ 事前準備計画 ・ 「非常時」判断手順 ・ 関係者の召集、対応本部の設置 ・ 機器及び作業員の縮退措置及び代替施設の手配措置 ・バックアップ施設等、代替施設への切替え措置 ・ 代替施設運用中の考慮事項（非常時アカウントの運用手順、復帰後に医療情報を正常システムに同期するための配慮等） ・障害の拡大範囲に関する判断手順、基準 ・正常復帰の判断手順、基準 ・正常復帰後の医療情報システム等の点検手順（不正侵入、情報改竄、情報破損等の検出等） ・ 所管官庁への連絡体制、等	○				
		②-5	策定した事業継続計画に基づくサービス内容について、医療機関等と合意する。	◎				
	③医療情報システム等復旧後における整合性確保	③-1	非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定･検証方法の規定等）を講じる。	◎	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	6.10 災害、サイバー攻撃等の非常時の対応	C.最低限のガイドライン	2.正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること。
	④非常時用の利用者アカウントや機能の管理手順の策定	④-1	非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置について、医療機関等と合意する。	◎	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	6.10 災害、サイバー攻撃等の非常時の対応	C.最低限のガイドライン	3.非常時の情報システムの運用 ・「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。 ・ 非常時機能が定常時に不適切に利用されることがないようにして、もし使用された場合には使用されたことが多くの人に分かるようにする等、適切に管理及び監査すること。 ・ 非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更しておくこと。 ・標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場
		④-2	非常時に用いる利用者アカウントの利用状況については定期的にレビューを行う。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		④-3	非常時に用いる利用者アカウントが利用された場合、システム管理者及び運用者がこれを速やかに確認できるための措置を講じる。	◎				・標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、関係先への連絡手段や紙での運用等の代替手段を準備すること。
		④-4	非常時に有効化した利用者アカウント及び非常時用の機能については、正常復帰後、速やかに無効化を図る。	◎				
1.11. サイバー攻撃等による障害発生時の対応	①サイバー攻撃等による障害発生時の医療機関等への速やかな状況報告	①-1	サイバー攻撃等により、サービスの提供に支障が生じた場合において、サービスに生じている障害の状況及び復旧に関する見通し等について、医療機関等に速やかに報告を行う。	◎	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	6.10 災害、サイバー攻撃等の非常時の対応	C.最低限のガイドライン	4.サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、“非常時”と判断した上で所管官庁への連絡を行うこと。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。 連絡先 厚生労働省 医政局研究開発振興課医療技術情報推進室（03-3595-2430） ※独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。 なお、情報処理推進機構は、マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口を開設している。標的型メールを受信した、Web サイトが何者かに改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。 連絡先 情報処理推進機構 情報セキュリティ安心相談窓口（03-5978-7509）
		①-2	サイバー攻撃等により、サービスの提供に支障が生じた場合において、医療機関等が行う必要のある所管官庁への連絡・報告のために提供する資料の範囲、条件等について、医療機関と合意する。	◎				
		①-3	医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の執行が及ぶ場所に設置する。	◎				
	②サイバー攻撃等による原因調査のためのログ等の記録の保全	②-1	サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。	◎	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。			
1.12. ネットワーク上の責任範囲・役割の合意	①外部と医療情報を交換する際の責任範囲・役割の合意	①-1	ネットワーク経路におけるウイルスや不正なメッセージの混入等の改竄に対する防護措置に関する受託事業者の役割の範囲について、医療機関等と合意する。	◎	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	1.ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を行うこと。 セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策を行うこと。上記を満たす対策として、例えば IPsec と IKE を利用することによりセキュアな通信路を確保することが挙げられる。 チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者に確認すること。
		①-2	ネットワーク経路におけるウイルスや不正なメッセージの混入等の改竄に対する防護措置に関する受託事業者の役割の範囲について、医療機関等と合意する。	◎				
		①-3	ネットワークで用いられる医療機関等の施設内のルータについて、これを経由して施設間を結ぶVPNの間で送受信ができないように経路設定すること等に関する受託事業者の役割分担について、医療機関等と合意する。	◎		6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	6.医療機関等の間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等の多くの組織が関連する。そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。 ・診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定 ・送信元の医療機関等がネットワークに接続できない場合の対処 ・送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ネットワークの経路途中が不通又は著しい遅延の場合の対処 ・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 ・伝送情報の暗号化に不具合があった場合の対処 ・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 ・障害が起こった場合に障害部位を切り分ける責任 ・送信元の医療機関等又は送信先の医療機関等が情報交換を中止する場合の対処また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。 ・通信機器、暗号化装置、認証装置等の管理責任の明確化（外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結） ・患者等に対する説明責任の明確化 ・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置
		①-4	回線の管理、品質等に対する受託事業者の責任の範囲、役割等について、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-5	通常運用時及び非常時の医療機関等と受託事業者との起点から終点までの通信手順、その他厚生労働省ガイドライン第5版6.11 C項の6で定めるネットワーク経路及びこれに関連する機器等に係る責任の所在を明確にし、受託事業者の負う責任の範囲、役割等について、医療機関等と合意する。	◎				・交換した医療情報等に対する管理責任及び事後責任の明確化（個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項）
		①-6	交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、医療機関等と合意する。	◎		6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	8.回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。 また、上記 1 及び 4 を満たしていることを確認すること。
		①-7	医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、受託事業者が負う責任の範囲、役割等について、医療機関等と合意する。	◎				
		①-8	サービスにより管理する医療情報を患者等の閲覧に供する場合に、受託事業者において対応すべきセキュリティ上の措置の条件、内容等について、医療機関等と合意する。	◎		6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	9.患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信の TLS 暗号化、PKI 個人認証等の技術を用いた対策を実施すること。また、情報の主体者となる患者等へ危険性や提供目的についての納得できる説明を行い、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にすること。
		①-9	交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、医療機関等と合意する。	◎				
		①-10	医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、受託事業者が負う責任の範囲、役割等について、医療機関等と合意する。	◎				
1.13. 機器・ソフトウェアの品質管理	①医療情報システム等に関する構成図や仕様に係るドキュメント作成	①-1	医療情報システム等における機器及びソフトウェアの構成図を作成する。	◎	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	1.　システムがどのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかが明らかにされており、システムの仕様が明確に定義されていること。
		①-2	医療情報システム等のネットワーク構成図を作成する。	◎				
		①-3	①-1、①-2で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。	◎				
		①-4	医療情報システム等を構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。	◎				
		①-5	①-1～①-4で策定した資料等を医療機関等の求めに応じて提出することについて、開示内容、範囲、条件等を医療機関等と合意する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	②機器・ソフトウェアの導入や変更における事前検証の実施	②-1	保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行う。	◎	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	3.　機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。
		②-2	変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を講じる。	◎				
		②-3	情報処理に供するアプリケーションについては、受託事業者自身で開発したアプリケーションを用いる。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いる。	◎				
		②-4	ソフトウェアに不正プログラムが混入することが無いよう、バイナリコードレベル、ソースコードレベルの双方で検証プロセスを実施することが望ましい。	○				
		②-5	業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入する。	◎				
	③本番環境と開発環境の分離	③-1	ソフトウェア開発を行う際には、運用されているソフトウェアに影響を与えない環境で行う。	◎	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	3.　機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。
		③-2	開発施設では不正プログラムが混入することを避けるため、不特定多数が利用するネットワーク（インターネット等）と接続を持つ場合には不正プログラムへの対策を行う。	◎				
		③-3	運用施設に保存されている医療情報を開発施設及び試験施設にコピーしない。	◎				
		③-4	運用システムの混乱を避けるため、開発用コード又はコンパイラ等の開発ツール類を運用システム上に置かない。	◎				
		③-5	情報処理に不必要なファイル等を運用システム上におかない。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
1.14. 変化に伴う医療機関等への影響の最小化	①医療情報システム等に用いる機器やソフトウェアのサポート	①-1	医療情報を格納する機器、媒体等の見読性が確保されていることを定期的に確認する。	◎	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われない。	7.2 見読性の確保について	C.最低限のガイドライン	（2）見読化手段の管理 電子媒体に保存された全ての情報とそれらの見読化手段は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。
		①-2	受託する医療情報を格納する機器･媒体等の見読性確保が困難となる可能性がある場合（媒体の劣化、読取装置等のサポート切れ等）、速やかに代替的な措置を講じ、見読性確保のための対応を行う。	◎				
		①-3	それぞれの装置は製造元又は供給元が指定する間隔及び仕様に従って保守点検を行い、必要であれば交換を行う。	◎				
		①-4	情報システムに関する機器については、定期的に劣化状況に関する検査を行い、必要な措置を講じる。	◎		7.3 保存性の確保について	C.最低限のガイドライン 【ネットワークを通じて医療機関等の外部に保存する場合】	（2）ネットワークや外部保存を受託する機関の設備の劣化対策を行うこと ネットワークや外部保存を受託する機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策を行うこと。
		①-5	医療情報システム等について、機器やソフトウェア等の提供事業者におけるサポート終了等が生じた場合は、サービスへの影響範囲について分析を行い、必要な措置を講じる。	◎				
		①-6	医療情報システム等について、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の提供が困難となる場合やサービスに変更が生じる場合には、利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。	◎				
		①-7	①-6においてサービスの一部又は全部の停止、変更等が生じる場合の医療機関等への対応の内容、条件等について、医療機関等と合意する。	◎				
	②保守作業に伴う医療情報システム等停止時間の最小化	②-1	情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画をたてて実施する。	◎	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	該当なし	ー	ー
		②-2	保守業務における事前の通知には、保守業務の影響が及ぶ範囲を明示し、保守業務が完遂しなかった場合を想定して原状回復に必要な時間の予測を含める。	◎				
		②-3	保守業務の実施にあたっては、医療機関等がサービスを利用できない状況に陥らないよう十分な対応策を講じ、その手順を運用管理規程に含める。	◎				
		②-4	②-3に定めた手順を医療機関等に示し、医療機関等と合意する。なお、本手順に基づき保守を行う際に必要となる事項等について、医療機関等と合意する。	◎				
		②-5	②-3で示された手順について、医療機関等が対応すべき事項がある場合、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	③医療情報システム等の停止や仕様変更時の対応	③-1	サービスの一部又は全部の停止やサービス変更の場合（軽微なバージョンアップは含まない）には、医療情報システム等を利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。	◎	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	該当なし	―	―
		③-2	③-1の場合、受託した医療情報を、医療機関等に返却する。返却するデータの範囲（データ種類、期間等）、データ形式(データ項目、項目の詳細、ファイル形式）、返却方法、条件については、医療機関等と合意する。また医療機関等のサービス利用開始後に、医療機関等と合意した内容を変更する場合には、③-1に準じた対応策を講じる。	◎				
		③-3	③-2におけるデータの返却については、厚生労働省ガイドライン第5版「5情報の相互運用性と標準化について」に従って行うこととし、その内容について医療機関等と合意する。なお、返却するデータに、受託事業者において実施した不可逆的な圧縮（画像データ等）や変換（パスワード等）によるデータが含まれる場合があるので、その旨も合わせて、医療機関等と合意する。	◎				
		③-4	③-1においてサービスの変更を含む医療情報システム等の一部又は全部の停止（軽微なバージョンアップは含まない）が生じる場合の医療機関等への対応の内容（移行支援等で、③-2の対応は除く）、条件等について、医療機関等と合意する。	◎				
		③-5	医療機関等の都合により医療機関等の医療情報システム等利用が終了する場合も、③-2、③-3に示す対応策を講じる。	◎				
		③-6	③-1～③-5についての手順等を、運用管理規程等に含める。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
2.物理的対策								
2.1. 入退管理	①機器や媒体の設置場所への認証や入退管理	①-1	機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じる。	◎	許可された者以外が機器や媒体に直接アクセスする。	6.3 組織的安全管理対策（体制、運用管理規程）	C.最低限のガイドライン	2.個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。
		①-2	機器や媒体の設置場所については、許可された者のみが入退できるように制限する。	◎		6.4 物理的安全対策	C.最低限のガイドライン	2.個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることができない対策を講じること。ただし、本対策項目と同等レベルの他の取り得る手段がある場合はこの限りではない。
		①-3	医療情報システム等を設置、医療情報を保管する部屋の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証を行う。	◎		6.4 物理的安全対策	C.最低限のガイドライン	3.個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・ 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・ 入退者の記録を定期的にチェックし、妥当性を確認する。
		①-4	有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用する。	◎				
		①-5	有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認する。	◎				
		①-6	受託事業者の職員の業務に応じて執務室内に滞在できる時間を指定する。	◎				
		①-7	機械式の認証装置で利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN ）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。	○				
		①-8	機器や媒体の設置場所への入退状況の管理（入退記録のレビュー含む）は定期的に行う。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-1	受託事業者の専有する領域に医療情報システム等を設置する場合には、以下に示す物理的安全管理策を施す。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認する。 ・ 医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理を行う。	◎	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	6.4 物理的安全対策	C.最低限のガイドライン	1.個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
		①-2	機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。	◎				
		①-3	サーバ等を格納するラック等について、施錠管理を行う。	◎				
		①-4	媒体等を格納するキャビネット等について、施錠管理を行う。	◎				
		①-5	電子媒体を保存するキャビネット等には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮する。	◎				
		①-6	データセンターを運営する外部事業者が、自社専有の建物と同等な安全管理策を実施する等、受託事業者の管理外にある者の物理的な不正操作に対する十分な安全性が確保されていることを確認する。	◎				
		①-7	医療情報システム等の設置されるサーバラックには施錠を行い、定められた受託事業者の職員以外が鍵を扱わないよう、確実な鍵管理を行う。	◎				
		①-8	受託事業者が医療情報システム等の設置されるサーバラックを解錠して行う作業については、作業者、作業開始時刻、作業終了時刻、作業内容等について記録する。	◎				
		①-9	データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム等、医療情報に影響を与えないことを確認する。	◎				
		①-10	医療情報システム等であることが、同じデータセンター内に立ち入る他事業者にわからないよう、扱う情報の種類、システムの機能等が識別できるような情報を外部から見える状態にしない。	◎				
		①-11	医療情報システム等の設置されるサーバラックの施錠装置については、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。	○				
		①-12	受託事業者の管理外にある者の不正なアクセスに対する十分な安全性が確保されていることを確認する。	◎				
		①-13	機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-14	①-1~①-13につき、運用管理規程等に規定する。	◎				
2.3. 不正な侵入の監視	①防犯カメラ等による医療情報を処理する施設内への侵入監視	①-1	受託事業者の専有する領域に医療情報システム等を設置する場合には、以下に示す物理的安全管理策を施す。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認する。 ・ 傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施す。 ・ 建物、部屋に対する不正な物理的な侵入を抑止するため、監視カメラ等の侵入検知装置を導入する。	◎	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	6.4 物理的安全対策	D.推奨されるガイドライン	1.防犯カメラ、自動侵入監視装置等を設置すること。
		①-2	防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる。	◎				
		①-3	機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、状況を確認することで、不正な入退者がないことを確認する。	◎				
		①-4	サービスの運用･保守端末等を設置している区域は監視カメラ等により適切に監視を行う。	◎				
	②受託事業者の職員に対する職員証等の着用の義務付け	②-1	受託事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した受託事業者の職員証を外部から目視で確認できる状態で携帯することを義務付け、受託事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておく。	◎	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	6.4 物理的安全対策	C.最低限のガイドライン	3.個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・ 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・ 入退者の記録を定期的にチェックし、妥当性を確認する。
		②-2	受託事業者の職員は、受託事業者の専有する領域にて、受託事業者の職員で無い者を識別した際には声掛け等を行い、身分を確認する。	◎				
		②-3	職員証を紛失あるいは不正利用された疑いを持った際には、ただちに管理者に連絡する、受託事業者の職員の退職時には確実に職員証を回収・廃棄する等、職員証の厳密な発行及び失効管理を行う。	◎				
2.4. バックアップ施設における対策	①バックアップ施設に対する物理的安全対策の実施	①-1	医療機関等に提供する医療情報システム等の継続に必要であれば、受託する医療情報のバックアップ施設等、医療情報システム等を継続するための代替情報処理施設を設置し、それらの施設に対しても物理的安全対策を施す。	◎	物理的安全対策が手薄となったバックアップ施設へ侵入される。	6.4 物理的安全対策	C.最低限のガイドライン	1.個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
2.5. 個人所有物の持ち込み制限	①医療情報を処理する施設内への個人所有物の持ち込み制限	①-1	医療情報処理施設内への業務遂行に関係のない個人的所有物の持ち込みを制限する。	◎	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	6.4 物理的安全対策	C.最低限のガイドライン	3.個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・ 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・ 入退者の記録を定期的にチェックし、妥当性を確認する。
		①-2	機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。	◎				
2.6. 機器の盗難への対策	①重要な機器への盗難防止用チェーン等の取付	①-1	個人情報が存在するPC 等の重要な機器には、盗難防止用チェーン等を取り付ける。	◎	個人情報が存在するPC等の重要な機器が盗難される。	6.4 物理的安全対策	C.最低限のガイドライン	4.個人情報が存在する PC 等の重要な機器に盗難防止用チェーン等を設置すること。

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
2.7. 覗き見への対策	①覗き見防止対策	①-1	医療情報等が表示される端末画面等がアクセス権限の無いものが視野に入らないような対応（室内の機器レイアウト等）を行う。	◎	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	6.4 物理的安全対策	C.最低限のガイドライン	5.覗き見防止の対策を実施すること。
		①-2	個人情報の表示中の覗き見を予防するために、端末に覗き見対策のシートを貼る等の対策を行う。	◎		6.9 情報及び情報機器の持ち出しについて	D.推奨されるガイドライン	1.外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。
2.8. 災害等への対策	①地震、水害、落雷、火災等、及び、それに伴う停電等への対策	①-1	機器や媒体を物理的に保存するための施設は、災害（地震、水害、落雷、火災等、及び、それに伴う停電等）に耐えうる機能･構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置する。	◎	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	該当なし	ー	ー
		①-2	①-1の施設を設置する建築物について、医療機関等と合意する。	◎				
		①-3	火災発生時の消火設備が機器に損傷を与えないよう配慮する。	◎				
		①-4	医療情報システム等を配置する室内での喫煙、飲食を禁止する。	◎				
		①-5	医療情報システム等を配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮する。	◎				
		①-6	医療情報システム等を設置するサーバラックについては以下の安全管理策を実施する。 ・ 震災時に転倒することが無いよう確実に設置する。 ・ 熱による障害を防ぐため十分な空調設備を保有し、サーバラック内が十分に換気されている。 ・ 扉には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮する。	◎				
3.技術的対策								
3.1. 利用者認証の実装	①利用者を一意に識別する方式の採用	①-1	医療情報システム等にて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行う。	◎	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	6.5 技術的安全対策	C.最低限のガイドライン	1.情報システムへのアクセスにおける利用者の識別と認証を行うこと。
		①-2	医療情報システム等の利用者を特定し識別できるように、アカウントの発行を行う（複数の利用者によるIDの共同利用は行わない。ただし当該医療情報システム等が他の医療情報システム等を利用するためのID（non interactive ID）は除く）。	◎				
		①-3	利用者のなりすまし等を防止するための認証を行う。	◎				
		①-4	医療情報システム等の運用若しくは開発に従事する者又は管理者権限を有する者に対するIDの発行は必要最小限とし、定期的な棚卸しを行う。	◎				
	②一時的な認証手段の用意	②-1	利用者の認証に際して、何らかの物理的な媒体･身体情報等を必要とする場合に、例外的にそれらの媒体等がなくても一時的に認証するための代替的手段･手順を事前に定める。	◎	利用者の認証に用いる物理的な媒体・身体情報等が欠損した場合、情報システムが利用できない。	6.5 技術的安全対策	C.最低限のガイドライン	3.本人の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合には、IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		②-2	代替的手段･手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差が最小となるようにする。	◎				
		②-3	代替的手段･手順により、医療情報システム等利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理する。	◎				
		②-4	その他、一時的な利用者の認証方法について医療機関等と合意する。	◎				
	③長時間離席時の対策	③-1	離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐ。	◎	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	6.5 技術的安全対策	C.最低限のガイドライン	4.入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力のおそれがある場合には、クリアスクリーン等の防止策を講じること。
		③-2	サービスの運用･保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。	◎				
		③-3	医療機関等に設置されている医療情報の参照等が可能な利用者端末等に対するクリアスクリーン等の情報漏洩防止策について、医療機関等と合意する。	◎				
		③-4	端末又はセッションの乗っ取りのリスクを低減するため、利用者のログオン後に一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを行う。	◎		6.5 技術的安全対策	D.推奨されるガイドライン	2.離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等）。
		③-5	離席の場合のクローズ処理の具体的な適用について、医療機関等と合意する。	◎				
	④安全なパスワード要件の定義	④-1	パスワードについては、第三者から容易に推定されにくい内容を含む品質基準を策定し、すべてのパスワードが品質基準を満たしていることを確実とする。	◎	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	6.5 技術的安全対策	C.最低限のガイドライン	11.パスワードを利用者識別に使用する場合 システム管理者は以下の事項に留意すること。 (1) システム内のパスワードファイルでパスワードは必ず暗号化（可能なら不可逆変換が望ましい）され、適切な手法で管理及び運用が行われること。また、利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。 (2) 利用者がパスワードを忘れたり、盗用されたりするおそれがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）し、本人以外が知り得ない方法で再登録を実施すること。 (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること（設定ファイルにパスワードが記載される等があってはならない）。 また、利用者は以下の事項に留意すること。 (1) パスワードは定期的に変更し（最長でも 2 ヶ月以内 ※D.5 に規定する 2 要素認証を採用している場合を除く。）、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。 (2) 類推しやすいパスワードを使用しないこと、かつ類似のパスワードを繰り返し使用しないこと。類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。
		④-2	パスワードポリシーについて、医療機関等と合意する。	◎				
		④-3	パスワードには有効期限の設定を行い、定期的な変更を強制する。ただし、利用者が患者等である場合には、他のサービスで利用しているパスワードを使わないよう特に促すだけでなく、サービス提供側から患者等に対して定期的なパスワードの変更を要求しないようにする。	◎				
		④-4	パスワードの世代管理を行い、パスワード変更に際して、安全性を確保するために必要な範囲で、過去に設定したパスワードを設定できないような運用を行う。	◎				
		④-5	パスワード発行時には、乱数から生成した仮の医療情報システム等へのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施する。	◎				
		④-6	パスワードをシステムに記憶させる自動ログオン機能を利用しないよう利用者に徹底する。	◎				
		④-7	利用者がパスワードを登録及び変更する際には、予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、利用者が設定しようとする品質の低いパスワードを認めないシステムの導入等を行う。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		④-8	本人の識別・認証に用いる情報は、本人しか知り得ない状態に保つよう対策を行う。	◎				
		④-9	利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと医療情報システム等にアクセスできないようにする。	◎				
		④-10	初期パスワード以外のパスワードは、利用者本人に設定させるとともに、利用者本人しか知りえない内容を設定するよう求める。	◎				
		④-11	パスワードの設定に際しては、複数の文字種（英数字・大文字・小文字・記号等）を用い、また、8文字以上等、十分に安全な長さの文字列等から構成されるルールとする。	◎				
		④-12	利用者がIDやパスワードを失念した場合には、予め策定した手順（本人確認を含む）に則り、本人への通知又は再発行を行う。	◎				
		④-13	パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とする。	◎		6.5 技術的安全対策	D.推奨されるガイドライン	4.パスワードを利用者識別に使用する場合、以下の基準を遵守すること。 （1）パスワード入力が不成功に終わった場合の再入力に対して一定不応時間を設定すること。 （2）パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。
		④-14	パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定する。連続してログオンが失敗した場合は再入力を一定期間受付けない機構とする。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入する。	◎				
	⑤多要素認証方式の採用	⑤-1	ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN）又はパスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせた多要素認証とすることが望ましい。	○	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	6.5 技術的安全対策	D.推奨されるガイドライン	5. 認証に用いられる手段としては、ID・パスワード＋バイオメトリクス又は IC カード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように 2 つの独立した要素を用いて行う方式（2 要素認証）等、より認証強度が高い方式を採用すること。ただし、情報システムを利用する端末に 2 要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め 2 要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証がなされていれば、2 要素認証と同等と考えてよい。
		⑤-2	医療情報システム等の運用若しくは開発に従事する者又は管理者権限を有する者の情報システム利用に係る認証は、多要素認証とする。	◎				
		⑤-3	利用者の認証で採用する認証方式について、医療機関等と合意する。	◎				
		⑤-4	利用者の認証において、ID･パスワードによる認証方式を採用している場合には、ID･パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン 第5版の公表（平成29年5月）から約10年後を目途に2要素認証について厚生労働省ガイドライン6.5章「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。	◎				
3.2. アクセス権限の管理	①必要最小限となるようなアクセス権限の管理	①-1	医療情報システム等の操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、閲覧、編集、削除等を防止する。	◎	一般利用者の権限が高いため、任意のソフトウェアのインストール、持込機器接続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	6.5 技術的安全対策 ----- 8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準	C.最低限のガイドライン ----- C.最低限のガイドライン D.推奨されるガイドライン	6.医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセ

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-2	医療機関等の利用者の職種等に応じたアクセス制御の設定について医療機関等に示し、医療機関等と必要な協議を行い、実際に設定する作業に関する役割分担も含めて合意する。	◎				ス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。 ----- (C.最低限のガイドライン) ③ 医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合 (エ) 保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。なお保守に関しては、「6.8 情報システムの改造と保守」を遵守すること。 (D.推奨されるガイドライン) (ウ)「②行政機関等が開設したデータセンター等に保存する場合」及び「③医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」では、技術的な方法として、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保すること。 (エ) 外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつこと。具体的には、「暗号化を行う」、「情報を分散保管する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を併せ持つこと。
		①-3	医療情報システム等の構成要素（情報処理装置、ソフトウェア）それぞれのアクセス管理に係るセキュリティ要求事項を整理する。	◎				
		①-4	それぞれの情報にアクセスする権限を持つ利用者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行う。	◎				
		①-5	業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定する。	◎				
		①-6	定められたアクセス制御方針がファイル、ディレクトリパーミッション、データベースアクセス等のアクセス制御機構として適切に反映されていることを定期的に検証することが望ましい。	○				
		①-7	予定された保守･運用等を行う際に受託した医療情報を許可なく閲覧できないようにするために、権限設定等の対策を講じる。	◎				
		①-8	システム管理者、運用担当者、保守担当者等が、意図しない閲覧を行わないことを担保するための措置（データベースの暗号化等）を講じる。	◎				
	②医療情報に対するアクセス制御	②-1	医療情報とそれ以外の情報を区分できる措置を講じる。	◎	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	6.5 技術的安全対策	D.推奨されるガイドライン	1.情報の区分管理を実施し、区分単位でアクセス管理を実施すること。
		②-2	医療情報については、情報区分に従ってアクセス制御を行えるようにする。	◎				
		②-3	仮想化技術を用いた資源をサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じる。	◎				
		②-4	医療機関等による情報資産の区分の設定や、これに対するアクセス制御の設定の対応について、医療機関等と合意する。	◎				
3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-1	利用者は医療情報システム等上においてユニークな利用者ごとのID により識別する。	◎	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	6.5 技術的安全対策	C.最低限のガイドライン	6.医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。
		①-2	利用者のID を発行する際に、既存の ID との重複を排除する仕組みを導入する。	◎				
		①-3	複数利用者で共用するためのグループ ID の利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、利用者ごとのID でログオンしてからグループ ID に変更する仕組みを利用する。	◎				
		①-4	利用者のID の発行は医療情報システム等の管理に必要な最小限の人数に留める。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-5	監視ログの監査時に利用者を確実に特定するため、利用者の ID は過去に使われたものを再利用しない。	◎				
		①-6	アクセスを許可された利用者 のID によるアクセス可能範囲が許可された通りとなっていること（不正に変更されていないこと）を定期的に確認することが望ましい。	○				
		①-7	不正なアカウントの利用又は試みが行われたことを利用者自身で検出するため、利用者のログオン後に前回のログオンが成功していれば成功日時を表示し、前回のログオンが失敗していれば、第三者による不正なログオンの試みが行われた可能性があるという内容の警告メッセージとともに失敗日時を表示することが望ましい。	○				
		①-8	不正なアカウントの利用を防ぐため、利用者のログオンを許可する曜日、時間帯は作業に必要な曜日、時間帯に制限することが望ましい。	○				
		①-9	認可されていない利用者あるいは第三者がログオンを試みた際に「パスワードが異なります」と表示すると当該 ID が存在していることを知る手がかりとなるため、「認証に失敗しました」、あるいは単にログオンプロンプトを再表示するといった特段の情報を与えないようなメッセージのみの表現に留めることが望ましい。	○				
		①-10	緊急時の作業のため、規定時間外にログオンを行う必要が発生した場合の妥当な承認プロセスを策定することが望ましい。	○				
		①-11	医療情報システム等に許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知する。	◎				
		①-12	利用者が変更あるいは退職した際には、ただちに当該作業者 ID を利用停止とする。	◎		6.8 情報システムの改造と保守	C.最低限のガイドライン	4.保守要員の離職や担当替え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付け、また、それに応じるアカウント管理体制を整えておくこと。
		①-13	不要な利用者の ID が残っていないことを定期的に確認する。	◎				
	②特権IDの最小限の利用及び作業実施内容の記録	②-1	特権 ID の発行は必要な最小限のものに留める。	◎	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	6.5 技術的安全対策	C.最低限のガイドライン	6.医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。
		②-2	特権使用者に昇格可能な利用者の ID を制限する。	◎				
		②-3	特権の使用時には作業実施内容を記録する。	◎				
		②-4	管理端末以外からの特権 ID による直接ログオンを禁止する。	◎				
		②-5	特権の種類に応じてアカウントを分離し、ファイルやディレクトリに対するアクセスを制限することが望ましい。	○				
		②-6	医療情報システム等の機能として可能であれば、特権 ID で使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改竄、削除など不正な行為を防止することが望ましい。	○				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	③パスワードの管理・運用	③-1	各利用者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護する。	◎	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	6.5 技術的安全対策	C.最低限のガイドライン	2.本人の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。
						6.8 情報システムの改造と保守	C.最低限のガイドライン	3.そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。
		③-2	医療情報システム等及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等の棚卸を行い、必要のないアカウントについては削除あるいはパスワード変更を行う。	◎		6.5 技術的安全対策	C.最低限のガイドライン	11.パスワードを利用者識別に使用する場合 システム管理者は以下の事項に留意すること。 (1) システム内のパスワードファイルでパスワードは必ず暗号化（可能なら不可逆変換が望ましい）され、適切な手法で管理及び運用が行われること。また、利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。 (2) 利用者がパスワードを忘れたり、盗用されたりするおそれがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）し、本人以外が知り得ない方法で再登録を実施すること。 (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること（設定ファイルにパスワードが記載される等があってはならない）。 また、利用者は以下の事項に留意すること。 (1) パスワードは定期的に変更し（最長でも 2 ヶ月以内 ※D.5 に規定する 2 要素認証を採用している場合を除く。）、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。 (2) 類推しやすいパスワードを使用しないこと、かつ類似のパスワードを繰り返し使用しないこと。類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。
		③-3	パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管する。	◎				
		③-4	パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用する。また、一般の作業者による閲覧を制限する。	◎				
		③-5	パスワード等の情報の漏洩が生じた場合（不正な第三者からの攻撃による場合を含む）には、直ちに当該IDを無効化し、予め策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知する。	◎				
		③-6	パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知した上で、当該パスワードを無効化し、変更できるような対応を講じる。	◎				
3.4. ログの取得と検証	①ログの取得と検証	①-1	利用者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録したログを作成し、一定期間保存する。	◎	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	6.5 技術的安全対策	C.最低限のガイドライン	7.アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、並びにログイン中に操作した患者が特定できること。情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容等）を必ず行うこと。
		①-2	ログを定期的に検証して不正な行為、システムの異常等を検出する。	◎				
		①-3	ログに記録する事項としては次のようなものが考えられる。 ・ 利用者情報（利用者の ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元 IP アドレス） ・ ファイル及びデータへのアクセス、変更、削除記録（利用者の ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類） ・ データベース操作記録（利用者のID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元 IP アドレス、設定変更時にはその内容）修正パッチの適用作業（利用者の ID、変更されたファイル） ・ 特権操作（特権取得者 ID、特権取得の可否、利用時刻及び時間、実行作業内容） ・ システム起動、停止イベント ・ ログ取得機能の開始、終了イベント外部デバイスの取り外し ・ IDS・IPS 等のセキュリティ装置のイベントログ ・ サービス及びアプリケーションの動作により生成されたログ（時刻同期に関するログを含む）	○				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-4	ログを集中させ問題の検出を一箇所で確実に行うことを目的として、システムとして可能な場合は専用のログサーバにログデータを集約して分析管理する。	◎				
		①-5	運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得する。	◎				
		①-6	システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得する。	◎				
		①-7	医療情報システム等の運用若しくは開発に従事する者又は管理者権限を有する者によるアクセスの記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。	◎				
		①-8	①-7に関する情報の医療機関等への提供について、医療機関等と合意する。	◎				
		①-9	ログの取得機能を有しない場合には、医療機関等と合意する。	◎				
		①-10	医療情報システム等の保守に従事する者及び管理者権限を有する者が、その業務の目的で当該医療情報システム等にアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。	◎		6.8 情報システムの改造と保守	C.最低限のガイドライン	2.メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。
		①-11	①-10で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。	◎				
		①-12	医療情報システム等の保守において実施した操作結果について、操作ログ等により記録し、管理する。	◎		6.8 情報システムの改造と保守	D.推奨されるガイドライン	1.詳細なオペレーション記録を保守操作ログとして記録すること。
		①-13	取得した操作ログ等により、アクセスされた医療情報についての状況をレビューする。	◎				
		①-14	ログを検証するため、利用者がアクセスした医療情報等を迅速に確認できるよう、利用者の ID と、情報の識別子（資産台帳記載の番号等）、生成時系列、アクセス時系列等、多様な指標での並び替え、情報の種別、アクセス時間等での絞り込み等が行うことができるようなシステムを整備することが望ましい。	○		6.8 情報システムの改造と保守	D.推奨されるガイドライン	5.保守作業に関わるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べて表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。
	②ログの改竄や削除を防止するためのアクセス制限や外部保存	②-1	ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用する。 ・ ログデータにアクセスする利用者及び操作を制限する。 ・ 容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとる。 ・ ログデータに対する不正な改竄及び削除行為に対する検出・防止策を施す。	◎	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	6.5 技術的安全対策	C.最低限のガイドライン	8.アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること。
	③時刻の標準時刻への同期	③-1	ログを利用して正確に事故原因等を検証するため、医療情報システム等のすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておく。	◎	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができな	6.5 技術的安全対策	C.最低限のガイドライン	9.アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		③-2	医療情報システム等のすべてのサーバ機器等の時刻が時刻サーバ等の提供する標準時刻に同期していることを定期的に検証することが望ましい。	○	い。			
		③-3	ログの時刻の信頼性を確保するために、医療情報システム等の時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で行う。	◎				
	④リモートメンテナンスにおける不正な侵入防止とログの取得・検証	④-1	リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、医療情報システム等への不正な侵入が生じないよう安全管理措置を講じる。	◎	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できない。	6.8 情報システムの改造と保守	C.最低限のガイドライン	8.リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。
		④-2	リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認する。	◎				
		④-3	サービス提供に必要な医療情報システム等の保守をリモートメンテナンスで行う場合、医療機関等と合意する。	◎				
	⑤取り扱う医療情報の法定保存年限に基づくログの保存期間の設定	⑤-1	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、診療録等に関するログ又はこれに代わる記録について、当該法定年限以上の保存期間を設ける。	◎	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	6.5 技術的安全対策	C.最低限のガイドライン	7.アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、並びにログイン中に操作した患者が特定できること。情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容等）を必ず行うこと。
		⑤-2	法定保存年限が経過した医療情報及び法定保存年限が設けられていない医療情報の保存期間について、医療機関等と合意する。なお、本項におけるログの管理方法について保存期間を設けた場合には、原則として法定保存年限がある医療情報に準じて取り扱う。	◎				
3.5. 不正プログラムへの対策	①不正プログラム対策ソフトウェアの導入と管理	①-1	最新の脅威についての情報収集に努め、導入している不正プログラム対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認する。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。	◎	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	6.5 技術的安全対策	C.最低限のガイドライン	10.システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
		①-2	不正プログラム対策ソフトウェアにおいて次の設定を行う。 ・ リアルタイムスキャン（ディスク書き出し・読み込み、ネットワーク通信）リスク評価の結果として必要であれば定期的にスキャンを実施 ・ 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又は十分な頻度による手動での更新 ・ 管理者以外による設定変更やアンインストールの禁止	◎				
		①-3	一定期間、不正プログラムのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止又は隔離措置をとる。	◎				
		①-4	医療情報システム等の構築に際しては、不正プログラム等の混入が生じないようにするための手順を策定し、これに則って構築する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-5	不正プログラム対策ソフトウェアのパターン定義ファイルを常に最新のものに更新する。	◎				
		①-6	医療情報システム等の構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新の不正プログラム対策ソフトウェア等の導入を行う。また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。	◎				
		①-7	医療情報システム等利用環境がウイルス等による攻撃を受けた場合に、医療情報システム等提供に係る影響について、速やかに医療機関等に周知し、必要な対応等を求める。	◎				
3.6. 端末やサーバの堅牢化	①端末やサーバの堅牢化	①-1	医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにする。	◎	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	6.5 技術的安全対策	C.最低限のガイドライン	10.システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
		①-2	ウェブブラウザの接続するサーバを業務上必要なサーバに限定する。	◎				
		①-3	ウェブブラウザの設定で、認可していないサイトから、ActiveX、Java アプレット、Flash 等のプログラムコードをダウンロード及び実行することができない設定とする（管理ソフトウェアが実行されるサーバのみを認可する）。	◎				
		①-4	認可したサイトからダウンロードされるコードについても不正プログラム対策ソフトウェアにより検査する。	◎				
		①-5	ウェブブラウザからメールクライアント等の業務処理において想定しない外部アプリケーションが明示的な確認なしに起動されないよう設定を行うことが望ましい。	○				
		①-6	医療情報システム等のサーバ機器等への同時ログオンユーザ数（OS アカウント等）に適切な上限を設ける。	◎				
		①-7	医療情報システム等に用いる装置には、必要のないアプリケーション等をインストールしない。	◎		6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	9.持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールすること。業務に使用しないアプリケーションや機能については削除あるいは停止するか、業務に対して影響がないことを確認して用いること。
		①-8	医療情報システム等に関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。	◎				
		①-9	医療情報システム等に関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。	◎				
3.7. 機器・ソフトウェアの脆弱性への対応	①安全性が確認できるネットワーク機器の利用	①-1	ルータ等のネットワーク機器は、安全性が確認できる機器を利用する。	◎	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	4.ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲット若しくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。
		①-2	ルータ等のネットワーク機器は、ISO/IEC 15408で規定されるセキュリティターゲット又はそれに類する文書が、本ガイドラインに適合しているものを選定する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	②パッチ適用等の実施	②-1	医療情報システム等に関連する技術的脆弱性については台帳等を利用して管理する。	◎	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等に不具合が生じる。	6.5 技術的安全対策	C.最低限のガイドライン	10.システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
		②-2	潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定する。	◎				
		②-3	修正パッチの適用前にパッチが改竄されていないこと及び有効性を検証する。	◎				
		②-4	オペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システム等に対する影響を評価し、試験結果を確認してから実施する。	◎				
	③医療情報システム等への脆弱性診断の実施	③-1	提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行う。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入する。	◎	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	6.5 技術的安全対策	C.最低限のガイドライン	10.システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
		③-2	アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行うことが望ましい。	○				
		③-3	開発されたソフトウェアの脆弱性検出をソースコードレベルで行うことが望ましい。 パッケージソフトウェア等、ソースコードの提供を要求できない場合には、ソースコードレベルではなく、アプリケーションを動作させて、外形的な脆弱性検査を行う。	○				
	④最新の脆弱性に関する情報の収集	④-1	アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとる。	◎	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	6.5 技術的安全対策	C.最低限のガイドライン	10.システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
		④-2	医療情報システム等の脆弱性に関する情報は、JPCERTコーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得し、確認する。	◎				
	⑤IoT機器に関する情報収集及び脆弱性への対応	⑤-1	IoT機器の利用を含むサービスを提供する場合、医療機関等との役割分担について、医療機関等と合意する。	◎	IoT機器について製造販売業者が想定していない利用方法により、脆弱性が生じる。	6.5 技術的安全対策	C.最低限のガイドライン	13.IoT 機器を利用する場合 システム管理者は以下の事項に留意すること。 (1)IoT 機器により患者情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。 (2)セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。 (3)IoT 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用すること。 (4)使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を講じること。
		⑤-2	IoT機器の利用を含むサービスを提供する場合、利用が想定されるIoT機器に対する脆弱性に関する情報を定期的に収集し、必要な対策を講じる。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
3.8. ネットワーク上のアクセス制御	①ネットワークのアクセス制御	①-1	セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行う。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置（サーバ）にて、同様のアクセス制御を行う。	◎	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	6.5 技術的安全対策	D.推奨されるガイドライン	3. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクションやそれと同等の機能を含む。）を設置し、ACL（アクセス制御リスト）等を適切に設定すること。
		①-2	セキュリティゲートウェイでは、不正な IP アドレスを持つトラフィックが通過できないように設定する（接続機器類の IP アドレスをプライベートアドレスとして設定して、ファイアウォール、VPN 装置等のセキュリティゲートウェイを通過しようとするトラフィックを IP アドレスベースで制御する等）。	◎				
		①-3	医療情報システム等において、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定する。他に必要なサービスがある場合には、医療機関等の合意を得てから利用する。 ・ 外部からの医療情報システム等の稼動監視・遠隔保守 ・ セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード ・ オペレーティングシステム及び利用アプリケーションのセキュリティパッチファイル等のダウンロード ・ 電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認証局へのアクセス ・ ファイアウォール、IDS・IPS などのセキュリティ機器に対する不正アクセス監視 ・ 時刻同期のための時刻配信サーバへのアクセス ・ これらのサービスを利用するために必要なインターネットサービス（ドメインネームサーバへのアクセス等） ・ その他の医療情報システム等の稼動に必要なサービス（外部認証サーバ、外部医療情報データベース等）	◎				
	②なりすましの防止	②-1	次の情報交換方法について予め合意しておく。 ・ 情報を電子媒体に記録して交換する際の手順 ・ 情報をネットワーク経由で文書ファイル形式にて交換する際の手順 ・ 情報をネットワーク経由でアプリケーション入力にて交換する際の手順 ・ 情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順	◎	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	2. データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法を用いるのが望ましい。
		②-2	情報交換手順では搬送の形態によらず次の事項を確実にする。 ・ 発送者、受領者を識別し記録する。 ・ 発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止対策を行う。 ・ 交換する情報の機密レベルに関して合意する（受領側で機密レベルが低くならないようにする）。 ・ 交換された情報に悪意のあるコードが含まれていないことを確実とする。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		②-3	電子的に情報を転送する際には以下の対策を実施する。 ・ 送信者、受信者は相互に電子的に認証を行って相手の正当性を検証する。認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。 ・ 送受信する経路は適切な方法で傍受のリスクから保護されている。 ・ 受信した情報について経路途中での損傷、改竄が無いことを検証する対策を講じる。 ・ 送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施する。	◎				
		②-4	医療機関等から受託事業者までのネットワークにおいて、医療機関等の送受信の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で経路の確認を行う。	◎				
		②-5	②-4において、医療機関等が外部接続するサーバ等と受託事業者のサーバとの間の相互認証を行う。	◎				
		②-6	②-4について、受託事業者が保守業務を再委託している場合には、受託事業者と再委託先との接続では、別途なりすましを防止する策を講じる。	◎				
		②-7	厚生労働省ガイドライン第5版6.11 C項の2に基づいて医療機関等が採用する通信方式認証手段が妥当なものであることの確認について、医療機関等と合意する。	◎				
	③ネットワークポートへの不正な装置の接続制限	③-1	ネットワーク機器及びサーバ、端末の利用していないネットワークポートへの物理的な接続を制限する。	◎	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	3.施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を行うこと。これに関しては、「6.5 技術的安全対策」で包括的に述べているので、それを参照すること。
		③-2	不正な装置を識別するため、医療情報システム等内で利用する情報処理装置を登録したリストを作成・維持する。	◎				
		③-3	不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、脆弱性パッチが適用されていること等を接続前に検査を行う仕組みを整備運用する。	◎				
	④無線LAN利用時の対策	④-1	医療情報を取り扱うサービスの利用に際して、医療機関等が無線LANを利用する場合に必要なセキュリティ対策について、医療情報システム等事業者の役割分担等について、医療機関等と合意する。	◎	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	6.5 技術的安全対策	C.最低限のガイドライン	12.無線 LAN を利用する場合 システム管理者は以下の事項に留意すること。 (1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策を行うこと。 (2) 不正アクセスの対策を施すこと。少なくとも SSID や MAC アドレスによるアクセス制限を行うこと。 (3) 不正な情報の取得を防止すること。例えば WPA2/AES 等により、通信を暗号化し情報を保護すること。 (4) 電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。 (5) 無線 LAN の適用に関しては、総務省発行の「一般利用者が安心して無線 LAN を利用するために」や「企業等が安心して無線 LAN を導入・運用するために」を参考にすること。

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
						6.5 技術的安全対策	D.推奨されるガイドライン	6. 無線 LAN のアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば 802.1x や電子証明書を組み合わせたセキュリティ強化をすること。
		④-2	業務上、医療情報システム等に関する情報を格納するモバイル端末を持ち出す場合には、公衆無線LANへの接続は行わない。	◎		6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	8.持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネットワークに接続する場合は「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線 LAN を利用できる場合があるが、公衆無線 LAN は 6.5 章 C-11 の基準を満たさないことがあるため、利用できない。ただし、公衆無線 LAN しか利用できない環境である場合に限り、利用を認める。利用する場合は 6.11 章で述べている基準を満たした通信手段を選択すること。
3.9. 不正な通信の検知や遮断	①ネットワーク上の不正な通信の検知や遮断	①-1	医療機関等との接続ネットワーク境界には侵入検知システム（IDS）、侵入防止システム（IPS）等を導入してネットワーク上の不正なイベントの検出、あるいは不正なトラフィックの遮断を行う。ホスティング利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行う。	◎	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	6.5 技術的安全対策	D.推奨されるガイドライン	3. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクションやそれと同等の機能を含む。）を設置し、ACL（アクセス制御リスト）等を適切に設定すること。
		①-2	侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行う。	◎				
		①-3	侵入検知システム等が、緊急度の高い攻撃・不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定とする。	◎				
		①-4	侵入検知の記録には不正アクセス等の事後処理に必要な項目が含める。	◎				
		①-5	医療情報システム等から、不正・不審なトラフィックが内部ネットワークから外部ネットワークへと流れていないことをネットワーク境界において監視することが望ましい。	○				
		①-6	侵入検知システム自身が攻撃・不正アクセスの対象とならないように、その存在を外部から隠す設定（ステルスモード）や、侵入検知システムへのアクセスの適切な制御を実施することが望ましい。	○				
		①-7	IoT機器の利用を含むサービスを提供する場合、IoT機器による医療情報システム等へのアクセス状況を記録し、不正なアクセスがないことを定期的に監視する。	◎		6.5 技術的安全対策	D.推奨されるガイドライン	7. IoT 機器を含むシステムの接続状況や異常発生を把握するため、IoT 機器・システムがそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録すること。
3.10. 外部へ持ち出す機器や情報の管理	①持ち出しを行う機器の認証	①-1	機器等については、起動パスワードの設定を行う。	◎	紛失・盗難した機器が起動され、機器を不正に利用される。	6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	6.情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。
		①-2	起動パスワードは、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じる。	◎				
		①-3	医療情報システム等に関する情報を格納する情報機器へのログイン及びアクセスについては、複数の認証要素を組み合わせて行う。	◎		6.9 情報及び情報機器の持ち出しについて	D.推奨されるガイドライン	2.情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	②搬送する情報に対する対策	②-1	情報を格納する機器･媒体等を持ち出す場合の手順には、機器･媒体自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる、パスワードを設定する等の事項を含める。	◎	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	7.盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。
3.11. 仮想デスクトップやMDM・MAMによる情報漏洩への対策	①個人所有の機器の管理	①-1	利用者が個人所有する機器による医療情報システム等利用に関する対応策について、医療機関等と合意する。 なお具体的には以下の内容を参考にする。 ・利用者が所有する機器からの情報漏洩等を防止する観点から、例えば、仮想デスクトップを用いてOS レベルで業務利用領域と個人利用領域を分け、業務利用領域を医療機関等が管理できるようにするほか、モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すことで、医療機関等が所有し管理する端末と同等のセキュリティ対策の徹底を図ることなどが考えられる。	◎	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	10.個人保有の情報機器（パソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者は 1～5 の対策を行うとともに、管理者の責任において上記の 6、7、8、9 と同様の要件を順守させること。
		①-2	サービスの提供に係る目的（開発、保守、運用含む）で従業員等の個人所有の機器を利用することは原則禁止とする。	◎		6.9 情報及び情報機器の持ち出しについて	D.推奨されるガイドライン	4.スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。 ・ BYOD は原則として行わず、機器の設定の変更は管理者のみが可能とすること。 ・ 紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者情報にアクセスできる場合は、一定回数パスワード入力を誤った場合は端末を初期化する等の対策を行うこと。
	②端末側に情報を残さない技術の導入	②-1	医療機関等の利用者が、医療機関等の外部からサービスを利用する場合に、医療機関等の利用者が用いるPCの作業環境に仮想デスクトップ等の技術を導入するための受託事業者の役割分担等につき、医療機関等と合意する。	◎	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	D.推奨されるガイドライン	1.やむを得ず、従業者による外部からのアクセスを許可する場合は、PC の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに、運用等の要件を設定すること。
3.12. 未登録の電子媒体の接続制限	①サーバ等への未登録の電子媒体の接続制限	①-1	医療情報システム等においてはサーバ等に接続できる電子媒体の種別を限定するため、不要なデバイスドライバを削除する。加えて、認められていない種類の装置の接続を防止する為に、管理者以外がデバイスドライバのインストールやアンインストールが出来ない設定とすることが望ましい。	○	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	6.9 情報及び情報機器の持ち出しについて	D.推奨されるガイドライン	3.情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。
		①-2	不要なデバイスドライバが追加されていないことを定期的に検証することが望ましい。	○				
3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-1	ネットワークにおいて、情報の盗聴、改竄、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）を行う。	◎	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装される。	6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	1.ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を行うこと。 セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策を行うこと。上記を満たす対策として、例えば IPsec と IKE を利用することによりセキュアな通信路を確保することが挙げられる。 チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者に確認すること。
		①-2	アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐのに必要な措置(サーバ証明書の導入等）を行う。	◎				
		①-3	経路の安全性確保のため、IPsec + IKEへの対応や閉域ネットワークへの対応等及びその条件等について、医療機関等と合意する。	◎				
		①-4	情報伝送に用いるケーブル類については直接の傍受リスクについて配慮することが望ましい。	○				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-5	暗号アルゴリズムは十分な安全性を有するものを使用する。選択基準としては電子政府推奨暗号リスト 等を用いる。	◎		6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	5.送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。例えば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。
		①-6	送信元と送信先の間で、暗号化等の情報そのものに対するセキュリティ対策を実施する。	◎				
		①-7	サービスの提供においてSSL/TLSを用いる際には、TLS1.2に対応した措置を講じる。	◎				
		①-8	①-7のほか、医療機関等がメールの暗号化（S/MIME 等）やファイルの暗号化への対応を求める場合には、その対応に必要な措置及び条件等について、医療機関等と合意する。	◎				
		①-9	VPN 接続を行う場合には以下の事項に従う。 ・ 接続時に VPN 装置間で相互に認証を行う。 ・ 傍受、リプレイ等のリスクを最小限に抑えるために、適切な暗号技術を利用する。 ・ インターネット上のトラフィックが VPN チャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しない。 ・ 複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるためVPN チャンネルを医療機関等別に構築する等の対策を実施する。	◎		6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	10.オープンなネットワークを介して HTTPS を利用した接続を行う際、IPsec を用いた VPN 接続等によるセキュリティの担保を行っている場合を除いては、SSL/TLS のプロトコルバージョンを TLS1.2 のみに限定した上で、クライアント証明書を利用した TLS クライアント認証を実施すること。その際、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。いわゆる SSL-VPN は偽サーバへの対策が不十分なものが多いため、原則として使用しないこと。また、ソフトウェア型の IPsec 若しくは TLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃からの防護について、適切な対策を実施すること。
		①-10	オープンなネットワークを介してHTTPS を利用した接続を行う際は、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」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。	◎				
		①-11	SSL-VPNは、原則として使用しない。	◎				
		①-12	サービス提供に際して、ソフトウェア型のIPsec 又はTLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃について、適切な対策を実施する。	◎				
		①-13	医療機関等における利用者がソフトウェア型のIPsec 又はTLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃についての、適切な対策に関する情報提供を行う。情報提供の範囲、条件等について、医療機関等と合意する。	◎				
②暗号アルゴリズムの危殆化や暗号鍵の漏洩に備えた暗号鍵及び電子署名の管理		②-1	暗号鍵が漏洩した場合に備えた対応策を策定しておく。	◎	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読もしくは偽装される。	6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	5.送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。例えば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。
		②-2	電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとする。	◎				
		②-3	暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		②-4	医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証する。	◎				
		②-5	暗号モジュールが外部のソースコードやライブラリを利用する場合には、その真正性を、製造元による電子署名等による完全性の検証を行った上で利用することが望ましい。	○				
		②-6	暗号鍵の生成は耐タンパー性 を有する IC カード、USB トークンデバイスといった安全な環境で実施することが望ましい。	○				
		②-7	暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うことが望ましい。	○				
		②-8	電子署名法にもとづき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できるようにすることが望ましい。	○				
3.14. リモートメンテナンスのアクセス管理	①リモートメンテナンスの不必要なログインを防止するためのアクセス管理	①-1	リモートメンテナンスにより保守を行う場合、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置を講じる。	◎	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	C.最低限のガイドライン	7.リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること。 また、メンテナンス自体は「6.8 情報システムの改造と保守」を参照すること。
3.15. 電子署名を利用する場合の管理	①信頼できる第三者機関が発行した電子証明書の利用	①-1	医療情報システム等において電子署名を利用する場合、保健医療福祉分野PKI 認証局の発行する署名用電子証明書等の信頼できる第三者機関が発行した電子証明書を利用する。	◎	信頼できる第三者機関と同等の厳格さで本人確認や署名の検証が行われない。	6.12 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	C.最低限のガイドライン	（1）厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局若しくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと 1.　保健医療福祉分野 PKI 認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。従ってこの保健医療福祉分野 PKI 認証局の発行する電子署名を活用することが推奨される。 ただし、当該電子署名を検証しなければならない者の全てが、国家資格を含めた電子署名の検証が正しくできることが必要である。 2.　電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくても A の要件を満たすことは可能であるが、同等の厳密さで本人確認を行い、さらに監視等を行う行政機関等が電子署名を検証可能である必要がある。 3.　「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成 14 年法律第 153 号）に基づき、平成 16 年 1 月 29 日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者が全て公的個人認証サービスを用いた電子署名を検証できることが必要である。
	②電子署名を施す場合のタイムスタンプの付与	②-1	電子署名を施す情報に対しては、タイムスタンプを付与する。この場合には、タイムスタンプの内容・検証方法について、医療機関等と合意する。	◎	電子署名を行う機器等の時刻情報が改竄されることで、電子署名付与時点の時刻及び当該時刻以降の改竄の有無が証明できない。	6.12 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	C.最低限のガイドライン	（2）電子署名を含む文書全体にタイムスタンプを付与すること 1.　タイムスタンプは、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの 安全な長期保存のために－」（総務省、平成 16 年 11 月）等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能であること。 2.　法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。 3.　タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を講じる必要がある。
		②-2	タイムスタンプを付与した情報を取り扱う場合に、法定保存年限内における当該タイムスタンプの有効性を検証する方法、対応方法等について、医療機関等と合意する。	◎				
		②-3	タイムスタンプを付与した情報を取り扱う場合に、当該情報を長期保存する場合に講じる対策等について、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	③タイムスタンプを付与する時点で有効な電子証明書の使用	③-1	タイムスタンプを付与した情報を取り扱う場合に、電子証明書の失効前の電子署名の有効性を担保するためのタイムスタンプの付与方法等について、医療機関等と合意する。	◎	タイムスタンプ付与時点で電子署名を検証することができない。	6.12 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	C.最低限のガイドライン	（3）上記タイムスタンプを付与する時点で有効な電子証明書を用いること 1.　当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば電子署名を含めて改変の事実がないことが証明されるため、タイムスタンプ付与時点で電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策が必要である。
3.16. 改竄防止・検知策の実装	①ソフトウェアの改竄防止・検知策の実装	①-1	不正な改竄を受けていないことを検証するため、定期的にソフトウェアの整合性検査（改竄検知）を実施する。	◎	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	3.　機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。
		①-2	不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改竄防止、検知策を実施する。	◎				
3.17. 患者ごとの情報の管理	①患者ごとに情報を管理する機能の実装	①-1	医療情報システム等には、受託する医療情報を患者等ごとに管理できる機能を含める。	◎	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	7.2 見読性の確保について	C.最低限のガイドライン	（1）情報の所在管理 紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者ごとの情報の全ての所在が日常的に管理されていること。
3.18. 利用目的に応じた応答時間の確保	①医療情報システム等の利用目的に応じた応答時間の確保	①-1	医療機関等が医療情報システム等を利用する際の、応答時間（一般的な表示速度、検索結果の表示時間等）について、医療機関等と合意する。	◎	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支障が生じる。	7.2 見読性の確保について	C.最低限のガイドライン	（3）見読目的に応じた応答時間 目的に応じて速やかに検索表示若しくは書面に表示できること。
3.19. 冗長化による障害対策	①医療情報システム等の停止に備えた冗長化	①-1	情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施する。	◎	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	7.2 見読性の確保について	C.最低限のガイドライン	（4）システム障害対策としての冗長性の確保 システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするために、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意すること。
		①-2	医療情報システム等、ネットワーク等に関し、通常の診療等に影響が生じないようサービスの継続に必要な冗長化対策を講じる。	◎				
		①-3	①-2を踏まえて、障害等が生じた場合のサービスの継続性を保証する水準について、医療機関等と合意する。	◎				
		①-4	障害時等でも診療等が継続できるようにするための医療機関等の側の代替措置等について、医療機関等と合意する。	◎				
	②ディスク障害対策	②-1	診療録等の情報をハードディスク等の記録機器に保存する場合、RAID-1又はRAID-6相当以上のディスク障害対策を講じる。	◎	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じる。	7.3 保存性の確保について	D.推奨されるガイドライン 【医療機関等に保存する場合】 （2）記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止	診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1 若しくは RAID-6 相当以上のディスク障害に対する対策を行うこと。
3.20. システム障害時の措置	①医療情報システム等障害時における機能の実装	①-1	医療情報を医療機関等に保存する場合に、障害時における見読性確保のために医療機関等側で講じうる方策に関する情報提供について、医療機関等と合意する。	◎	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	7.2 見読性の確保について	D.推奨されるガイドライン 【医療機関等に保存する場合】	（1）バックアップサーバ システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-2	ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、見読性が確保される形式（PDF、JPEG 及び PNG 等のフォーマット）で外部ファイルに出力可能とすることなどの方策を講じる。	◎		7.2 見読性の確保について	D.推奨されるガイドライン 【医療機関等に保存する場合】	（2）見読性確保のための外部出力 システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力することができること。
		①-3	医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容について、医療機関等と合意する。	◎				
		①-4	医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために遠隔地に保存するバックアップデータの利用のための機能、利用に必要な情報の提供、条件等について、医療機関等と合意する。	◎		7.2 見読性の確保について	D.推奨されるガイドライン 【医療機関等に保存する場合】	（3）遠隔地のデータバックアップを使用した見読機能 大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップし、そのバックアップデータと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。
		①-5	緊急時に備えた医療機関等における診療録等の見読性の確保を支援する機能（例えば画面の印刷機能、ファイルダウンロードの機能等)をサービスに含め、これに必要なセキュリティ等の情報提供について、医療機関等と合意する。	◎		7.2 見読性の確保について	D.推奨されるガイドライン 【ネットワークを通じて外部に保存する場合】	（1）緊急に必要になることが予測される診療録等の見読性の確保 緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しても複製又は同等の内容を医療機関等の内部に保持すること。
		①-6	障害等が生じた場合の役割分担を明確にした上で、稼動を保証するサービスの範囲について、医療機関等と合意する。	◎		7.2 見読性の確保について	D.推奨されるガイドライン 【ネットワークを通じて外部に保存する場合】	（2）緊急に必要になるとまではいえない診療録等の見読性の確保 緊急に必要になるとまではいえない情報についても、ネットワークや外部保存を受託する機関の障害等に対応できるような措置を行っておくこと。
3.21. バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-1	電子媒体の損傷等による情報喪失のリスクを最小限にするため電子媒体の製造者により指定される保管環境にて保管する。	◎	情報が毀損や滅失した場合にバックアップされたデータを用いて元の状態に復元できない。	7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （2）不適切な保管・取扱いによる情報の滅失、破壊の防止	1.　記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと。
		①-2	各医療機関等が利用可能な、保存可能資源の残量については、随時提供できる措置を講じる。	◎		7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （2）不適切な保管・取扱いによる情報の滅失、破壊の防止	2.　システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること。
		①-3	医療機関等が医療情報システム等を利用する際に、利用可能な資源に係る情報（保存可能容量、利用可能期間、リスク、バックアップ頻度、バックアップ方法等）について、医療機関等と合意する。	◎				
		①-4	医療情報システム等が情報を保存する場所（内部、可搬媒体）、その場所ごとの保存可能容量、保存可能期間、リスク等を運用管理規程等に含める。	◎				
		①-5	①-4において、他の事業者が提供する医療情報システム等を利用する場合においても、同様の情報を収集して、対応する。仮想化技術による医療情報システム等を利用する場合には、受託事業者が他の事業者との契約上利用可能な資源に関する情報を確認する。	◎				
		①-6	①-4により運用管理規程に定める管理方法に関する教育を従業員等に対して行う。	◎				
		①-7	医療情報システム等に係る委託先に対しても、①-4の運用管理規程に定める管理方法への対応等を求める。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-8	情報が毀損した場合、速やかに回復するための措置を講じ、その内容・手順等について、運用管理規程等に含める。	◎		7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （2）不適切な保管・取扱いによる情報の滅失、破壊の防止	5.　各保存場所における情報がき損した時に、バックアップされたデータを用いてき損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと。
		①-9	①-8に示す措置によっても毀損された情報の回復が困難となる場合を想定した対応について、運用管理規程等に含める。	◎				
		①-10	①-9で示す場合の、毀損した情報に関する責任の範囲、免責条件等について、医療機関等と合意する。	◎				
		①-11	リスク分析結果に基づき医療情報システム等のバックアップを取得する。バックアップの取得対象、取得頻度、保存方法・媒体、管理方法等を定め、その内容を運用管理規程等に含める。	◎		7.3 保存性の確保について	D.推奨されるガイドライン 【医療機関等に保存する場合】 （1）不適切な保管・取扱いによる情報の滅失、破壊の防止	3.　診療録等のデータのバックアップを定期的に取得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備えること。
		①-12	取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、記録内容の改竄・破壊等がないことを確認する。	◎				
	②バックアップに用いる記録媒体の管理	②-1	記録媒体に格納するバックアップについては、その媒体の特性（テープ／ディスクの別、容量等）を踏まえたバックアップ内容、使用開始日、使用終了日を明らかにして管理する。	◎	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （3）記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止	1.　記録媒体が劣化する以前に情報を新たな記録媒体又は記録機器に複写すること。記録する媒体及び機器ごとに劣化が起こらずに正常に保存が行える期間を明確にして、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体又は記録機器については、そのデータを新しい記録媒体又は記録機器に複写すること。これらの一連の運用の流れを運用管理規程にまとめて記載し、関係者に周知徹底すること。
		②-2	バックアップの記録媒体の使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複写する。	◎				
		②-3	製造者の定める有効利用限度期間を超過することがないよう、電子媒体の有効利用限度期間が近づいた場合は、別の媒体等に複写する。	◎				
		②-4	②-1～②-3の手順を運用管理規程等に含め、従業員等及び再委託業者に対して必要な教育を行う。	◎				
		②-5	バックアップに係る情報の提供について、医療機関等と合意する。	◎				
3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-1	診療録等のデータ項目で、厚生労働省における保健医療情報分野の標準規格（以下、「厚生労働省標準規格」という。）が定められているものについては、それを採用する。	◎	医療情報システム等を更改等により移行する際、移行元で記録された情報が移行後に正しく読みだせない。	7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （4）媒体・機器・ソフトウェアの不整合による情報の復元不能の防止	1.　システム更新の際の移行を迅速に行えるように、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること。
		①-2	厚生労働省標準規格が定められていないデータ項目については、変換が容易なデータ形式とし、医療機関等と合意する。	◎				
		①-3	医療情報に係るマスターテーブルの変更に際して、レコードの管理方法やとるべき措置等について、診療録等の情報に変更が生じない機能及び検証方法を医療情報システム等に備える。	◎		7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （4）媒体・機器・ソフトウェアの不整合による情報の復元不能の防止	2.　マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えていること。
		①-4	①-3に示す機能等を備えることが困難な場合の医療情報システム等更新・移行の手順について、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの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

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-5	医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートする。	◎		7.3 保存性の確保について	C.最低限のガイドライン 【ネットワークを通じて医療機関等の外部に保存する場合】	（1）データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと 保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する機関は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持しなくてはならない。
		①-6	データ形式や転送プロトコルをバージョンアップ又は変更しようとする場合には、サービスの利用に与える影響を確認する。	◎				
		①-7	①-6の結果、サービスの利用に影響があると認められる場合には、医療機関等が対応を図るために十分な期間を想定してバージョンアップ又は変更に係る告知を行うほか、対応に必要な措置に関する具体的な情報提供を行う。	◎				
		①-8	①-7は、他の医療情報システム等とのデータ連携等を考慮して行う。医療機関等に対する互換性確保に係る情報提供について、医療機関等と合意する。	◎				
		①-9	データ形式・転送プロトコルの変更等の結果、医療機関等がサービスの利用を終了する場合には、見読性確保の対策を講じる。	◎				
		①-10	医療情報システム等に関する機器及びソフトウェアについては、将来的な互換性確保を視野に入れて決定するとともに、サービス提供後に標準仕様等の変更が生じた場合のリスクについても検討を行う。	◎		7.3 保存性の確保について	D.推奨されるガイドライン 【ネットワークを通じて医療機関等の外部に保存する場合】 （1）ネットワークや外部保存を受託する機関の設備の互換性を確保すること	1. 回線や設備を新たなものに更新した場合、旧来のシステムに対応した機器が入手困難となり、記録された情報を読み出すことに支障が生じるおそれがある。従って、外部保存を受託する機関は、回線や設備の選定の際は将来の互換性を確保するとともに、システム更新の際には旧来のシステムに対応し、安全なデータ保存を保証できるような互換性のある回線や設備に移行すること。
		①-11	他の事業者が提供する医療情報システム等を用いて、サービスを提供する場合には、他の事業者がサービスを停止した際にも、自社のサービス提供に支障が生じないようにするための対応策を検討し、対策を講じる。なお、他の事業者のサービスの停止・変更に伴い、自社が提供するサービスの一部又は全部の停止、変更（軽微なバージョンアップは含まない）等が生じる場合には、機器の劣化対策を講じる。	◎				
		①-12	医療情報システム等に係る機器若しくはソフトウェア等の更新を行う場合、又は利用する他の事業者のサービスの変更を行う場合には、①-10、①-11を考慮して行う。	◎				