

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6年●月

目次

I. 本参考例の利用法について	1
1. 本参考例の目的	1
2. サービス仕様適合開示書について	1
3. SLA 参考例について利用方法及び利用上の留意点	1
4. <u>SLA 参考例の対象読者</u>	4
5. <u>本 SLA 参考例に基づく合意形成の進め方</u>	5
II. 参考例編(サービス仕様適合開示書)	10
1. サービス仕様適合開示書参考例の使い方	10
2. サービス仕様適合開示書	11
III. 参考例編(SLA)	21
1. 本 SLA 参考例の使い方	21
2. 具体的な SLA の項目例	22

I. 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「対象事業者」~~における安全管理ガイドライン」（以下、「2省ガイドライン」という）に基づいて、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~~等~~（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

サービス仕様適合開示書は、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、対象事業者から医療機関等に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、医療機関等はこれ本開示書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、この本開示書のような開示書書面等を用いて、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2省ガイドライン~~に則して、診療所向け診療録の作成・保存医療情報システム等の処理を行うクラウドサービス提供のサービスにおいて合意すべき内容を想定したひとつのサンプル項目を例示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

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）

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、必要な条項項目についてのみ提供することも想定される。

本参考例のなお、SLA (Service Level Agreement) とは別に、SLO (Service Level Objective) という概念もある。これは、サービス事業者がサービス提供にあたって示す目標値のことをいう。SLO は、あくまでも目標値では、各項目あることから、SLA と異なり、その値に達しないことで直ちに契約違反とはならない。

対象事業者において「【本項を定める上での考え方】」を記述、設定した。これは本参考例を記述目標値について、達成義務とする際に想定したか、努力義務とするか、又は一部の項目について達成義務とするかなどは、提供されるサービス内容や、本参考例を変更・加除する際に念頭に置くべき考え方を概説する医療機関等との合意形成の条件などにより異なる。一方で医療機関等に提供するサービスにおいて、何らの保証を行うことなく、すべて努力義務とすることは、結果として品質の保証が必要なサービス提供について、対象事業者に広く免責を認めることにつながり、サービス品質が担保されないなどの懸念があることから、医療情報システム等の重要性等に鑑みて妥当なものである。本参考例を踏まえて、実際に SLA 等を作成する際には、
「【本項を定める上とは言えない。特に医療機関等と事業者の間での考え方】」の役割分担や責任分界などについては、明示的に保証範囲を示して合意する必要がある。

本 SLA 参考例では、SLA に含める内容を理解の上、利用されたい前提として示すものであるが、目標としうる項目は「サービス内容等に応じて SLO として達成努力目標とすることも想定される。」と備考に記した。具体的には、対象事業者が保証しえない要因によりサービス・レベルが影響しうる場合（例えばクラウドサービスなどで、回線の速度や利用者側の動作環境などが、画面表示や検索速度に影響する場合）や、システムやサービスの提供価格と性能とのバランスから、社会通念上、事業者側の義務とするのが妥当でない場合などが想定される。

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。

なお、対象事業者が、提供する医療情報システムのセキュリティ機能に関する説明の標準的記載方法を示すものとして「製造業者／サービス事業者による医療情報セキュリティ開示書（MDS／SDS）」（以下「MDS／SDS」）²がある。これは、事業者が医療機関等に対して、自社の提供する製品やサービスの、「医療情報システムの安全管理に関するガイドライン」（以下、「厚生労働省ガイドライン」）への適合状況やリスク対応策などを示すもので、医療機関等との間でのセキュリティ対応について、複数のサービス等と比較しながら合意するための資料として用いられることが想定されている。

実際の医療機関等との合意に際しては、サービス仕様適合開示書を作成する方法や、MDS/SDS を作成する方法、あるいは自社で提供するサービスについてのセキュリティ対策状況をチェックした資料を提供する等、適宜セキュリティ対策の状況を医療機関等に明示的な形で示したうえで、具体的な合意を行うことが望ましい。

表 1 にサービス仕様適合開示書、SLA 参考例、MDS/SDS の概要を示す。

表 1 サービス仕様適合開示書、SLA 参考例、MDS/SDS の概要

文書名	概要
サービス仕様適合開示書 (総務省/経済産業省)	■ 対象事業者が、自社のサービスに関する厚生労働省ガイドライン・2省ガイドライン（以下「医療情報関連ガイドライン」）等への適合状況や、これに関する情報を、標準的なフォームに従って記載するとともに、サービス提供に当たって、医療機関等側との責任分界や、役割の範囲等を表示 ■ これにより提供するシステム・サービスの品質や内容を示すことが可能 ■ 内容は、各対象事業者が任意で記載するものであるが、前提として医療情報関連ガイドラインの内容に適合したものであることが求められる ■ 各要求事項には、以下の2つのものが含まれており、これらの要求事項のうち、 ②については、対象事業者が、サービス仕様適合開示書に基づいて必要な情報を医療機関等にし、その上で当該項目に関する合意を行う ① 対象事業者がサービス提供する上で、実施すべき内容が一意に決まる事項 ② 対象事業者がサービス提供する上で、実施すべき内容が医療機関等との協議により具体的に決まる事項
SLA 参考例 (総務省/経済産業省)	■ 医療情報システム等の提供において合意すべき具体的な内容を、医療情報関連ガイドラインに則して合意すべき項目について例示として提示。 ■ 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、また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

² 一般社団法人保健医療福祉情報システム工業会(JAHIS)医療システム部会セキュリティ委員会及び一般社団法人日本画像医療システム工業会(JIRA)医用画像システム部会セキュリティ委員会により作成。
(<https://www.jahis.jp/standard/detail/id=987>)

	■ 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
<u>MDS/SDS</u> <u>(JIRA/JAHIS)</u>	■ 各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する説明の標準的記載方法（書式）を定めたもの ■ 以下の目的の利用を想定 ① 製造業者が提供する医療情報システム、又はサービス事業者が提供する医療情報システムを用いたサービス（以下、「対象とするシステム/サービス」とする。）のセキュリティに関して、厚生労働省から公表されている厚生労働省ガイドラインへの適合性を示すことにより、医療機関等側において必要な対策の理解を容易にすること ② 厚生労働省ガイドラインを遵守しなければならない医療機関等にとって有用な情報を提供すること、当該システム/サービス導入医療機関等においてセキュリティマネジメントを実施するにあたって、製造業者/サービス事業者により提供される情報がリスクアセスメントの材料となること ③ 各製造業者/サービス事業者にとって、安全管理ガイドラインへの適合性への自己評価手段として利用すること ④ 医療機関等が製造業者/サービス事業者にセキュリティの説明を求める際の、要求のベースとして利用すること

4. SLA 参考例の対象読者

本 SLA の参考例における対象読者を以下に示す。

4. 1 対象事業者

まず、医療機関等に対して医療情報システム等を提供する事業者が想定される。特に医療機関等に対して、自社が提供する医療情報システム等を製品・サービスとして企画及び提供をする担当者や、医療機関等に対して自社製品・サービス等の説明をする担当者、これらの担当者に対する責任者などが想定される。これらの者は、提供する医療情報システム等に関するセキュリティ対策が、医療機関等に対して適切に提供できるか、又は提供する場合等について、医療機関等が求めるものと齟齬がないかなどを確認することが必要であるため、本参考例を踏まえて、必要な内容について、医療機関等に提供する情報を整理することが求められる。

対象事業者の中には、医療機関等に対して直接、サービス等を提供しない事業者も想定される（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）。これらの事業者においては、直接、医療機関等と SLA 等の合意をしないものの、直接医療機関等に対してシステム・サービス等を提供する他の事業者と連携することが必要である。この観点から、医療機関等に対して直接、サービス等を提供しない事業者においても、本 SLA 参考例を理解する必要がある。

4. 2 医療機関等における医療情報システム等の企画管理者、運用管理者

事業者が提供する製品やサービスに関するセキュリティ対策の情報に対して、医療機関等で必要な対策が講じられているか、セキュリティに対する責任を適切に分担できるかを、医療機関等の担当者においても判断し、その上で事業者の選定や委託等の調整を行い、セキュリティ対策についての合意を行うことになる。

医療機関等における医療情報システムのセキュリティ対応を検討・管理し、その運用の担当者においては、このような合意を外部の事業者に対して委託を行う必要がある。そのため、医療機関等における企画管理者及び運用担当者においても、本 SLA 参考例について理解し、適切な合意に向けた資料とすることが望ましい。

5. 本 SLA 参考例に基づく合意形成の進め方

5. 1 SLA 策定の意義

製品とは異なり、サービスの場合、実施事項は明確であるものの、具体的な品質等が明確とはならないことがある。このような場合において、具体的なサービスの品質等を明示して、その内容について合意するために作成されるものが SLA である。SLA を作成することにより、契約書では抽象的な両者の合意内容を、具体的なサービス内容及び品質等として明示することとなるため、両当事者が遵守すべき旨を明確にすることができる。

このような SLA の作成の前提として、2 省ガイドラインでは、医療機関等と対象事業者の両者がリスクコミュニケーション（5.2(2)参照）を行い、サービス仕様に関して合意することとしており、その内容を SLA とすることも想定される。この場合には、当該サービス仕様を示す内容（サービス仕様適合開示書、MDS/SDS 等）が SLA を構成するなどの形で機能することになる。

本 SLA 参考例は、このような対象事業者と医療機関等との間で、リスクコミュニケーションを行い、その結果を SLA として整理する際に、必要な項目や内容の妥当性等を確認する上での参考とすることを想定する。

5. 2 SLA 策定のプロセス

(1) 2 省ガイドラインの合意形成と SLA

SLA は医療情報システム等の提供に関する合意内容を可視化したものである。医療情報システム等のライフサイクルについては、2 省ガイドライン図 3-4 において「医療情報システム等のライフサイクル」が示されているが、これに SLA の位置づけを示したものが図-1 である。

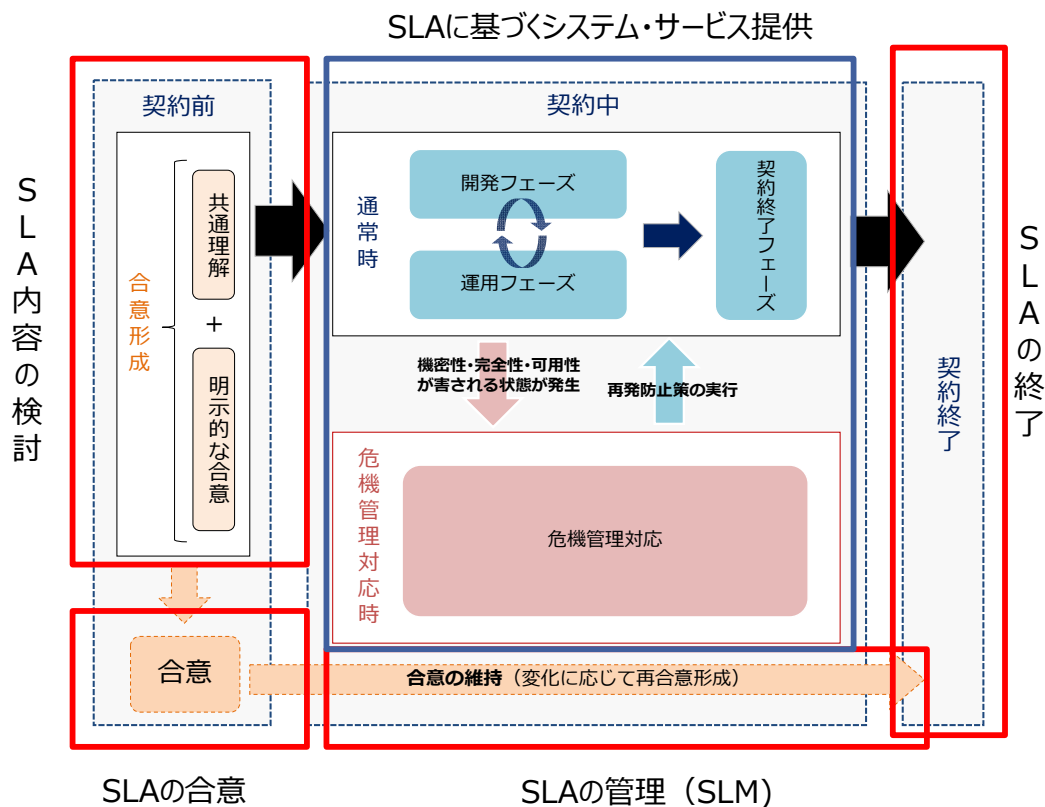


図 1 医療情報システム等のライフサイクルにおける SLA の位置づけ

医療情報システムのライフサイクルの中で、SLA は以下のように位置付けられる。

- ・ 契約前の合意形成において、SLA とする内容に関して、対象事業者は医療機関等と共通理解を作り、その上で明示的な形で合意形成を行う（SLA の内容の検討）。
- ・ 上記合意形成を踏まえて、契約の合意を行い、SLA の内容を合意文書の一部とする（SLA の合意）。
- ・ SLA に基づいて、対象事業者は、システム等の提供を行う（SLA に基づくシステム・サービス提供）。
- ・ 医療機関等は SLA に基づくシステム等の提供がなされているかを管理し、必要に応じて SLA の内容を改訂する（SLA の管理）
- ・ 医療情報システム等の提供に関する契約の終了に伴い、SLA を終了する（残存事項があれば、その範囲で引き続き対応）（SLA の終了）。

(2) SLA の合意形成のプロセス

上述のように、SLA 内容の検討においては、合意形成のプロセスに基づいて実施される。ここでいう合意形成プロセスとは、医療情報システム・サービスの提供に際して、生じるリスク対応に関する内容についての合意形成を指す。

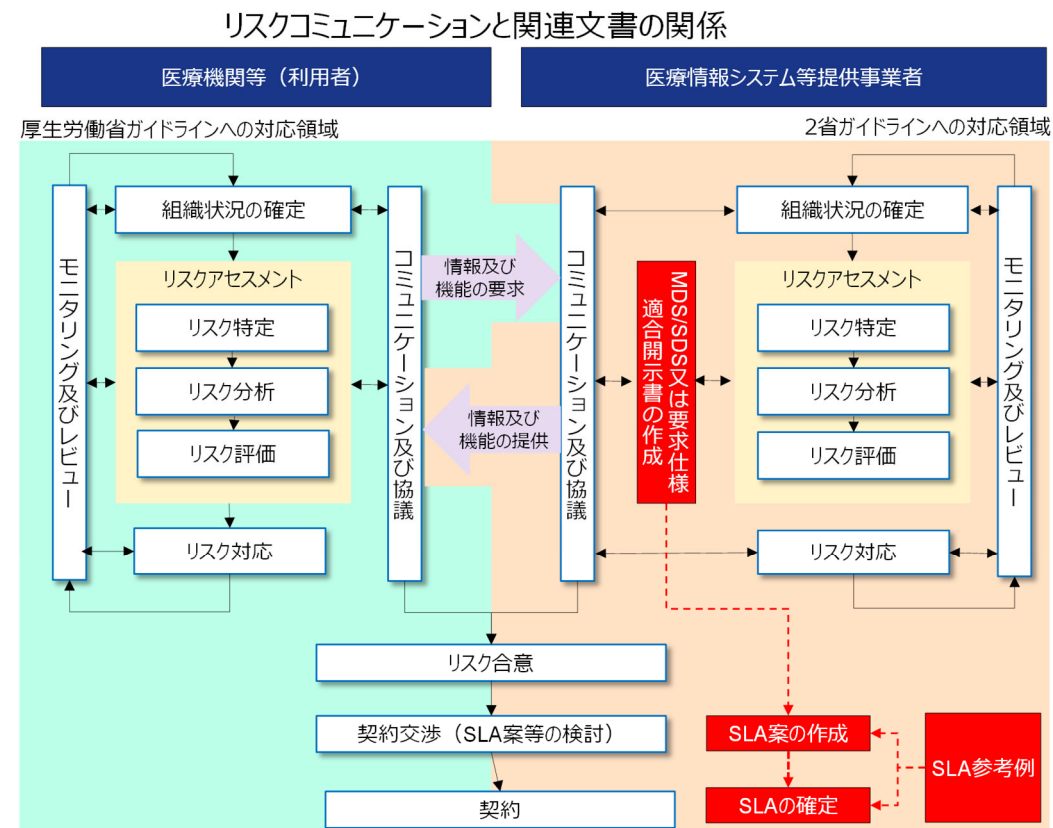
このようなリスク対応に関する合意を目的として行う、当事者間のコミュニケーションは、リスクコミュニケーションと呼ぶ³。リスクコミュニケーションにおいて、2 省ガイドラインでは対象事業者において、以下の対応が求められる⁴。

- ・ 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。
- ・ 具体的には、「リスク対応一覧」や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する。
- ・ 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。
- ・ 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り、合意する。

この具体的な流れの一例を図 2 に示す。

³ 2 省ガイドラインでは、リスクコミュニケーションを以下のように定義する。「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。」

⁴ 2 省ガイドライン「5.1.6. リスクコミュニケーション」



出所:「クラウドサービス環境におけるリスクアセスメントとリスク対応のプロセス関係」(「ISO/IEC 27017:2015(JIS Q 27017:2016)-ISO/IEC 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-解説と活用ガイド」)P250 から作成

図1 リスクコミュニケーションの流れと作成する文書

この流れでは、医療情報システム等提供事業者がサービス仕様適合開示書、MDS/SDS などの、医療情報システム関連ガイドラインにおいて求められるセキュリティ項目等に対する、自社のシステム等の対応状況等に関する資料を提供し、これを踏まえて医療機関等と協議することを想定している。具体的には以下の通りである。

- ・ 対象事業者においては、自社が提供するシステム・サービス等に関するリスクアセスメントを行うとともに、その内容を顧客側である医療機関等に示せるよう、MDS/SDS やサービス仕様適合開示書を策定する。
- ・ 医療機関等側は、医療機関等で管理するシステム等に関するリスクアセスメントを行い、その結果を整理する。
- ・ 医療機関等は、医療情報システム等の採用に際して、対象事業者から MDS/SDS 等の提供を求め、その内容が、医療機関等で想定しているリスク評価と適合するか否かを判断する。

- ・ 医療機関等において、判断した結果、対象事業者の対応が採用するに足りる場合には、そのサービスを選定するかどうか、判断することになる。リスク評価と照らして、足りない、あるいはミスマッチがある場合には、対象事業者と調整し、サービス内容に関する協議を行うことになる。
- ・ サービス内容の協議や調整の結果、両当事者においてセキュリティを含む安全管理に関する合意(リスク合意)が得られた場合には、その内容を明文化する。

上記について、医療機関等と事業者において行うべき対応を整理したものが図 3 である。

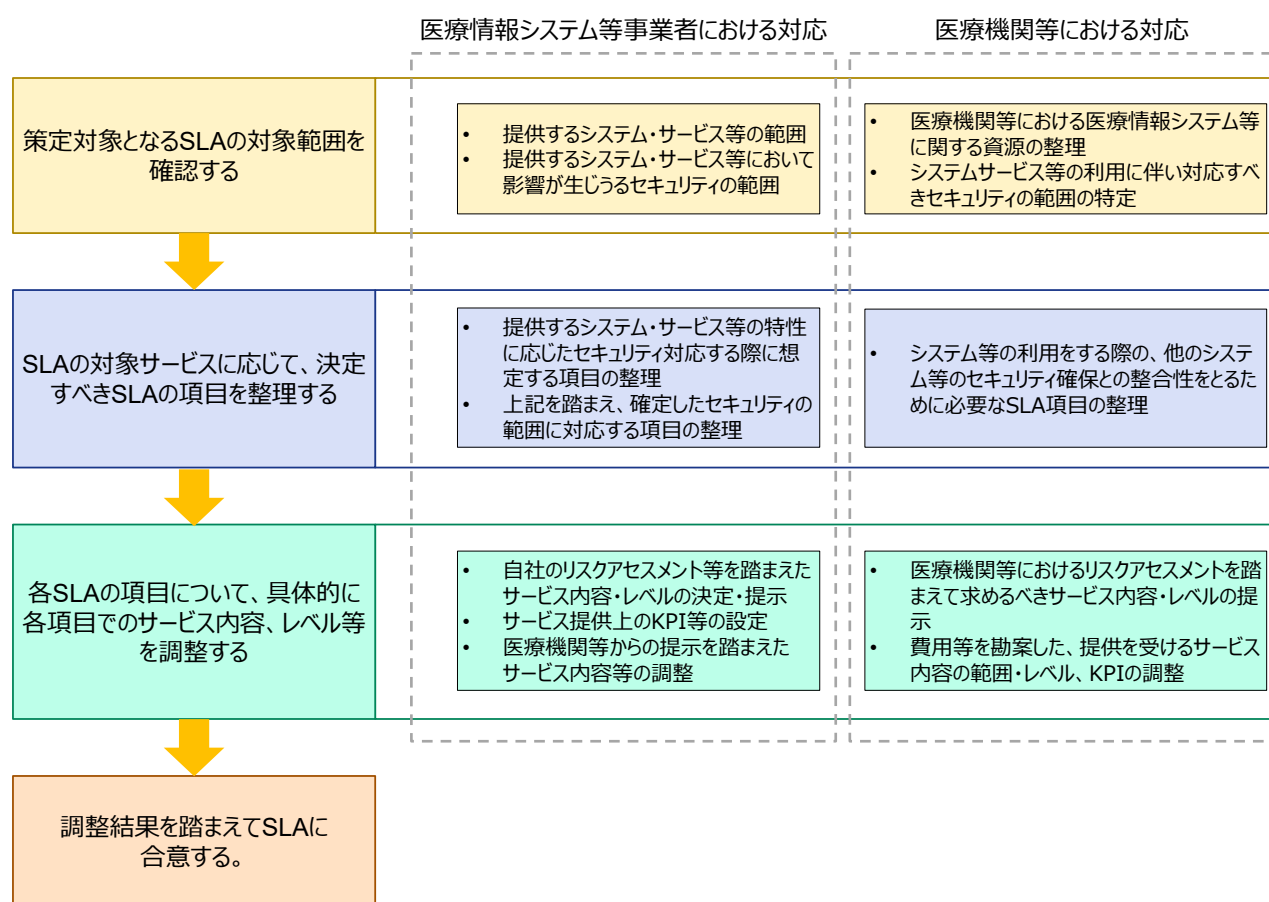


図 2 SLA の合意に至るまでの医療機関等と対象事業者における対応

II. 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の使い方

サービス仕様適合開示書の例を以下に示す。サービス仕様適合開示書の例では、医療情報関連ガイドラインへの適合性を示すという目的で、項目によっては具体的な内容が示されている。

一方で、2省ガイドラインでは、リスクベース・アプローチを採用しており、具体的なリスク対応については、対象事業者がリスクアセスメントに基づいて示すこととしており、その結果、具体的な対策については、サービス内容やリスク対応によって異なる内容が示されることも想定される。

そこで本サービス仕様適合開示書の例を用いる際も、各項目への適合性を示すほか、対象事業者において代替するリスク対応の内容がある場合には、その内容を示すなどの方法も想定される。

2. サービス仕様適合開示書

- (1) 医療機関等が~~医療情報安全管理~~厚生労働省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~~2省ガイドラインの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~~2省ガイドラインの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

⑤ 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

⑥ 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

⑦ 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2省ガイドラインの
5.2 節参照

⑧ 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2省ガイドラインの
5.2 節参照

⑨ 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2省ガイドラインの 5.1.6(2) (ア) 参照

⑩ 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~~ 2省ガイドラインの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
〇×株式会社(例)	サービス提供用システム保守(例)
.....	

⑪ 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~~ 2省ガイドラインの5.1.6(2)(ウ)参照

⑫ 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~~ 2省ガイドラインの5.1.6(2)(エ)参照

⑬ 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~~ 2省ガイドラインの5.1.6(2)(オ)参照

⑭ 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~~ 2省ガイドラインの5.1.6(2)(カ)参照

⑮ サイバー攻撃が生じた場合の情報提供・調査協力等

<u>サイバー攻撃が生じた場合の情報提供・調査協力等</u>
・貴医療機関等が定めるサイバー攻撃を受けた場合、当社サービスに関連して、把握可能な範囲で攻撃に対する状況に関する情報を提供します。(例) ・上記において、サイバー攻撃の内容が当サービスに関与するとあると判明した場合、貴医療機関等が実施する調査に協力いたします。また直接当サービスに関与する内容でない場合には、別途協議の上、調査協力をいたします。(例) ・サイバー攻撃の内容が当サービスに関与すると判明した場合には、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、2省ガイドラインの5.1.6(2)(ク)参照

⑮⑯ 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~~ 2省ガイドラインの5.1.6(2)(キ)参照

⑯⑰ 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~~ 2省ガイドラインの5.1.6(2)(ク)参照

⑭⑮ 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~~2省ガイドラインの5.1.6(2)(ケ)参照

⑭⑮ 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~~ 2省ガイドラインの5.1.6(2)(コ)参照

⑭⑯ 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~~ 2省ガイドラインの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 <u>厚生労働省ガイドライン 7.1-C.最低限 システム運用編 別添 2.「真正性」確保のガイドライン</u> <u>ための対策</u>
(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
<u>医療情報安全管理/厚生労働省ガイドライン 7.1-C.最低限 システム運用編 別添 2.「真正性」確保のガイドラインのための対策</u>	
(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 ^{さん} 」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
<u>医療情報安全管理/厚生労働省ガイドライン 7.2-C.最低限 システム運用編 別添 1.「見読性」確保のガイドラインのための対策</u>	
(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
<u>医療情報安全管理厚生労働省ガイドライン 7.2-D. 推奨されるガイドライン システム運用編 別添 1. 「見読性」確保のための対策</u>	
(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
<u>医療情報安全管理厚生労働省ガイドライン 7.2-D. 推奨されるガイドライン システム運用編 別添 1. 「見読性」確保のための対策</u>	
(1) 緊急に必要なことが予測される診療録等の見読性の確保	
(2) 緊急に必要なことが予測され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
<u>医療情報安全管理厚生労働省ガイドライン 7.3-C. 最低限 システム運用編 別添 3. 「保存性」確保のガイドラインのための対策</u>	
(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	
<u>医療情報安全管理/厚生労働省ガイドライン 7.3-D. 推奨されるガイドライン システム運用編 別添 3. 「保存性」確保のための対策</u>	
(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
<u>医療情報安全管理/厚生労働省ガイドライン 6.12-C. 最低限 企画管理編「14. 法令で定められた記名・押印のガイドラインのための電子署名」</u>	
(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

III. 参考例編（SLA）

1. 本 SLA 参考例の使い方

本 SLA 参考例は、SLA を作成するに際して、事業者と医療機関等との間での取り決めるべき項目として含めることが望ましい、あるいは参考となる事項を整理したものである。

本参考例に記載する内容はあくまでも考え方の例であり、システム・サービスの提供内容に応じて、対応すべき項目は異なることから、実際の SLA の作成にあたっては、個々のサービスや、各社におけるリスクアセスメントの内容などを踏まえて設定されることを予定して記載している。

2. 具体的な SLA の項目例

(1) SLA 設定において求められる事項

① 本サービスの目的と対象

項目	要否	解説	備考
本サービスの目的	必須	- SLA により提供されるサービスの目的を明示する。例えば、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など、提供するサービスにより実現する内容などが示される。 - 医療情報システム等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や期待が異なり、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。	クラウドサービスのように、複数の顧客に対して同じ SLA で対応する場合には、個々の顧客の特定を想定した記載ではなく、一般的なサービスにより実現することなどが目的とされる。
本サービスの対象	必須	- 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、解約の申し入れがない限り、自動更新となっている場合もある。 - 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。	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。

② 本サービスの提供範囲

項目	要否	解説	備考
全般	必須	- 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。 - 提供サービスに含まれない内容については、サービス提供範囲外である旨を明記することが望ましい。	
サービス	任意	- 医療情報システム等提供事業者が提供するサービスでは、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責任分界とも密接に関わる。 - サービス対象の範囲は、サービス対象となるシステムの範囲のほか、具体的な対応内容（クラウドサービス等の提供、納入後の保守、運用、情報提供等）を明示することが重要である。	

項目	要否	解説	備考
ネットワークサービス	任意	・ 提供するサービス内容が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）の提供やそれらの運用、技術的サポートについて示す。	・ これらが提供サービスに含まれる場合には明示する。
使用機器等	任意	・ サービスの利用に際して、医療機関側がサービス利用に必要な端末（PC）、ネットワーク機器等の提供（事業者からの貸与又は設置の場合）、これらに係る運用、技術的サポートについて示す。	・ これらが提供サービスに含まれる場合には明示する。
本サービスの利用に供するソフトウェア	必須	・ サービス利用において、例えば特定の OS やブラウザ 等が必要な場合には、提供するソフトウェア等を明示する必要がある。	
	任意	・ サービスの利用に際して、医療機関側がサービス利用に必要なソフトウェア（OS 及びブラウザ）の提供及びセットアップ等の提供、これらに係る運用、技術的サポートについて示す。	・ これらが提供サービスに含まれる場合には明示する。

③ 本サービスの提供時間

項目	要否	解説	備考
本サービスの提供時間	必須	・ SLA では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。 ・ サービス提供時間の定め方は、例えば定期保守等による停止以外の 24 時間、特定の時間帯を示す、などの方法が想定される。 ・ また、サポートなどを行う対象事業者の通常業務時間は別途示される。 ・ 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。	

(2) 本 SLA について

① 本サービスにおけるサービス・レベル合意書の意義

項目	要否	解説	備考
全般	—	- 一般的な SLA では、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。 - 一方で、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ことを示すことが重要である。SLA 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。	
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	任意	- 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、医療機関等が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、医療機関等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、事業者は、医療機関等がサービスを利用する際に、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、医療機関等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。	

項目	要否	解説	備考
医療業務等への影響の把握	任意	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。	
サービス品質とコストの妥当性を図る	任意	サービスのサービス・レベルを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。	
各役割分担の明確化を図る	任意	医療機関等と事業者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。また医療機関等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な対応が可能となる。	

② 本サービスにおけるサービス・レベル適用の考え方

項目	要否	解説	備考
全般	—	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。SLAではこのような観点を整理して記述する。	

項目	要否	解説	備考
本サービスにおける鑑みたサービス・レベル（または目標）の適用	必須	- 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。例えば、 ➤ 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。	本サービスは、医療機関等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。
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（または目標）	必須	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対象事業者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。	サービス内容等に応じて SLO として達成努力目標とすることも想定される。

③ 本 SLA の適用期間

項目	要否	解説	備考
本 SLA の適用期間	必須	- 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。利用期間を定めない契約もある。この場合、例えば年次の契約更新ごとに適用期間も延長するなど措置がとられる。 - SLA の適用を定め、その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には、例えば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するなどの措置を講じることもある。	

④ 本 SLA の改定

項目	要否	解説	備考
改定の契機	必須	- SLA の改定は定期的実施する場合と、必要に応じて実施する場合がある。 - 改定を定期的実施する場合として、例えば、契約の更新時期に内容の改定又は継続することが想定される（自動更新含む）。 - 必要に応じて実施する場合の例として、「双方の合意事項に明確な変更があった場合」が挙げられる。例えば、新たなサービスを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。	

項目	要否	解説	備考
		また、「双方責任者が必要と認めた場合」等のケースも想定される。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

① リスク評価

項目	要否	解説	備考
リスク評価	必須	- 医療機関等と事業者との合意においては、医療機関等の医療情報システムにおけるリスク対応に対して、事業者におけるリスク評価を踏まえて提供されるサービスが適用できるかを確認することが求められる。そのため、事業者におけるサービス提供上のリスク評価やその考え方を提示して、医療機関等とリスクコミュニケーションを行うことになる。 - そのため、事業者はサービス提供の前提として、2省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、例えば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として定めるなどが想定される。	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。

② サービス利用環境

項目	要否	解説	備考
サービス利用環境	必須	提供する医療情報システム等の利用環境を明示し、医療機関等側の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	

項目	要否	解説	備考
		かにする観点から、その役割分担等も併せて具体的にすることが求められる。 ・ アプリケーションやサービスを利用するための医療機関等側に求められる環境を示す。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。具体的な環境については、更新の柔軟性等を鑑み、別資料等で示すなどの方法も想定される。 ・ 医療情報システムにおいては、Web ブラウザ 等の汎用ソフトウェアが使用されるものもみられる。この場合、適切な動作や表示の正確性・完全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、必要な関連ソフトウェア、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 等に関する仕様や、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することが求められる。	

③ サービス提供環境・運用に係る前提条件

項目	要否	解説	備考
サービス提供環境・運用に係る前提条件	必須	- 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は、例えば、サービス提供に係る機器等の所在、データセンタの所在、運用管理に必要な受託情報等の利用等が挙げられる。 - サービス提供に係る機器等の所在に関し、データの所在については、医療情報を格納するデータセンタの所在地などを示すことになる。またそれらが自社のものか委託先のものを明示することが求められる。さらに委託先の場合、委託先会社名も併記することが求められる。併せて、それらが設置されている地域、国等についても示すことが2省ガイドラインから求められる。一方でデータセンタの具体的な場所等はセキュリティ情報であることから、開示する具体性については留意が求められる。 - 運用・保守等により、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。 - 医療情報を取り扱う医療情報システム等は、国内法の執行の及ぶ範囲にあることを確実場所に設置することが求められる（2省ガイドライン6.1）。SLAにおいて保存場所を示す際にはこの点についても示すことが求められる。	- なお、「I. 参考例編（サービス仕様適合開示書）」では、(2) ⑩（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。 - クラウドサービスの場合には、個々の顧客に対するサービス提供における管理状況に関する情報の提供を行うことは難しいが、事業者による受託した医療情報へのアクセス状況については、医療機関等からの求めがあれば、提供することが求められる。 - 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すこともある。

項目	要否	解説	備考
		またサービス提供の前提として必要となる事業者が取得・利用する情報についても示す。事業者は医療情報を、サービス提供やセキュリティ対応上やむを得ない場合を除き、取得・利用することは認められない。そのため、例えばアプリケーションや機器、回線の利用状況の把握し、管理、障害対応に用いるなどの目的で取得する場合には、その旨を示す。	

④ 機器・ソフトウェアの品質

項目	要否	解説	備考
機器・ソフトウェアの品質	必須	- 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厚生労働省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。 - 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が想定される。対象事業者によっては、ISO 9001 や 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。	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) ⑩ (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。

⑤ 準拠する法令・ガイドライン等

項目	要否	解説	備考
遵守する法令・ガイドライン等	必須	- 対象事業者が遵守すべきガイドラインについては、2 省ガイドラインに示されている。これらについて示すほか、提供サービスの内容に応じて必要な法令やガイドラインを示すことで、事業者が遵守する法令等を医療機関等に明示的に示し、法令遵守についての合意を得る。 - なお、厚生労働省ガイドライン等により、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は、その責務を委託により共有する観点から望ましい。 - 事業者においては、個人情報保護法及び個人情報保護 GL を遵守することが求められるが、医療情報を取り扱う場合、「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」についても併せて理解することが求められる。そのため SLA においても、サービス提供に関連する内容については、同ガイドラインへ対応することを示すなども想定される。	

⑥ 守秘義務等

項目	要否	解説	備考
守秘義務等	必須	- 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（2省ガイドライン 3.1.1）。 - 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して具体的な守秘義務を課すことも、併せて医療機関等に SLA など示すことが求められる。	

⑦ 監査

項目	要否	解説	備考
監査	必須	2省ガイドラインでは事業者に対して、「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。」としており、この評価を行うために、対象事業者内部の独立した監査部門や第三者機関が評価を行うことが望ましいとする（4.3）。	- 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。 - 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。
--	--	--	----------------------

(4) 役割分担

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）

項目	要否	解説	備考
本サービス提供に対する責任	必須	- 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。 - サービスの提供において、事業者が自社のみで提供する場合のほか、複数の事業者と連携し、それぞれのサービス（ネットワークや通信サービス、PC等の端末の管理、クラウドの連携サービス等）を提供した上で、サービスを提供する場合等がある。	
利用環境に関する役割分担と責任	必須	- 医療情報システムにおけるセキュリティ対策においては、事業者側と利用者の双方が適切な対策を行うことが必要とされている。特にクラウドサービスでは、セキュリティに対する責任は共有するという、責任共有モデルの考え方が示されている。 - 事業者と医療機関等の役割分担については、例えば、 ➤ 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）と管理 ➤ 当該対象事業者が関与しない、利用者が利用するクラウドサービスの利用に伴う管理	

項目	要否	解説	備考
		については、医療機関等が担い、提供するサービスに関する機能と品質、セキュリティ対応と、サービスに関連するセキュリティ情報の提供を事業者が担うなどの対応などが想定される。 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。	
障害一般に関する役割分担と責任	必須	- 例えば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、組織内での障害の周知や、障害の原因の協力を医療機関等が担うなどが想定される。 - 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 医療機関等の業務上の役割分担と責任

項目	要否	解説	備考
医療機関等のサービス利用に関する業務上の役割分担	必須	サービス等を提供する上で必要となる業務について、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らかにする必要がある。例えば、以下のような内容が想定される。	具体的には、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、医療機関等が対象事業者に対して申請して、発行する形などが想定される。対象事業者によっては、サ

項目	要否	解説	備考
		➤ 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が想定される。 ➤ 利用者側の権限設定については、医療機関等の管理者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よう、業務分担することが想定される。なお、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、誤った権限設定がなされないように、対象事業者は必要な情報提供等を行うことが求められる。 ➤ 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。 ➤ 患者に対する情報提供を行う場合（例えば、情報漏洩（えい）が発生した等）において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の役割や、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、 ・ 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。	ービス提供に際して、医療機関等からの申請に基づいて、ID 及びパスワードを送付する等なども想定される。

③ 再委託事業者・連携クラウドサービス事業者等

項目	要否	解説	備考
業務の再委託	必須	- 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がある場合には、これについて明示する。 - 医療情報システム等の提供においては、単一の事業者がすべてを行うほか、一部のシステムやサービス等を他の事業者にも再委託を行うことも想定される。これは、他の事業者にも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。 - 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、厚生労働省ガイドラインでは、事業者はその内容の提供を求めている。 - 医療情報システム等の提供の場合には、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。 - 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、すべて契約を行った事業者が責任を有する。自らは契約主体となるだけで、医療情報システム等の提	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。

項目	要否	解説	備考
		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ことが想定される。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、サービス提供にあたって、高度の注意義務を課する趣旨である。 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。	
再委託先・連携事業者の詳細	任意	- サービス提供にあたり、再委託事業者や、連携する事業者がある場合には、それらの事業者名のほか、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。 - なお、自社が提供するサービスのレベルと、再委託先や連携サービスとの間で、サービス・レベルの矛盾がないことを示すことが求められる。その点について、医療機関等との間で理解の齟齬がないよう、留意することが求められる。	

④ 連絡体制

項目	要否	解説	備考
通常時の連絡体制	必須	- SLA 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する。 - 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。	- 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。 - なお、「I. 参考例編（サービス仕様適合開示書）」では、（２）⑮で問い合わせ窓口について示している。
障害時・非常時の連絡体制・告知方法	必須	- SLA では、通常業務時間及びそれ以外の時間帯等の連絡先を明示することが求められる。 - 事業者の用意する問合せ先については、電話によるほか、メールやweb上のフォーム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。サービスを提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

① ネットワークセキュリティに関するサービス仕様

項目	要否	解説	備考
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）	必須	- 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、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する等が想定される。 - 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示すことも想定される。	- 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、厚生労働省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。
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）	必須	- SLA では、事業者が採用する「不正アクセス対策」に示すことが求められる。採用する不正アクセス対策については、厚生労働省ガイドラインで求められる内容や、自社のリスクアセスメント結果等を踏まえて、必要に応じて具体的な内容を示すことになる。 - また対象事業者は採用する不正対策の内容について、自社の運用管理規程等に含め、これに基づいて不正アクセス対策の実施を行う旨を示すなども想定される。 - なお、必要に応じて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含めることも想定される。	- 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、厚生労働省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。

② 受託情報に関するサービス仕様

(c) 真正性に関するサービス仕様

項目	要否	解説	備考
利用者認証（利用者資格認証、電子署名等）	必須	- SLA では、提供するシステム・サービスにおいて採用する利用者認証に関するアクセス制御について示すことが求められる。また、その対応を事業者の運用管理規程等を含め、これに基づいて、アクセス制御の実施を行うことが求められる。 - 採用するアクセス制御については、厚生労働省ガイドラインで求められる内容や、自社のリスクアセスメント結果等を踏まえて、必要に応じて具体的な内容を示すことになる。 - 事業者の実施するアクセス制御等につき、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示すことも想定される。	- 本項では、（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、厚生労働省ガイドラインによりアクセス制御の実施が求められる。
職種等に基づくアクセス制御	任意	- 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。 - SLA ではこの点を踏まえ、提供するシステム・サービスの内容に応じて、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する。	

項目	要否	解説	備考
		- また、例えば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、その内容や役割分担等を記述することが想定される。 - 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含めることも想定される。	
電子署名	任意	- SLA では、提供するシステム・サービスにおいて電子署名を採用する場合、その内容が厚生労働省ガイドラインに従ったものであることを示すことが求められる。 - なお対応可能な電子署名の情報について、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含めることも想定される。	
診療記録の確定（本人による確定、代行確定等）	任意	- 電子カルテにおける記録の確定は、作成責任者による入力完了、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ことが求められる。また作成責任者による入力完了については、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。電子カルテに関するシステム・サービスを提供する場合、SLA においてこれらの内容を示すことが求められる。 - なお、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	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）⑩(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。

項目	要否	解説	備考
		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。 また、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。	
データの更新履歴管理	必須	- 診療録の作成等を電磁的記録により行う場合には、厚生労働省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。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。電子カルテに関するシステム・サービスの提供を行う場合、SLAにおい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示すことが求められる。 - サービス等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。	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）⑩（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。

(d) 見読性に関するサービス仕様（または目標）

項目	要否	解説	備考
表示仕様	必須	- 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。厚生労働省ガイドラインにおいても、上記に加えて、「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。 - 電子カルテに関するシステム・サービスの提供を行う場合、SLAにおいて表示仕様を含む旨を示すことが求められる。 - また、例えば表示仕様については、正常な再現性を保証する環境を示すことなども想定される。 - 提供する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。	- 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）⑩(b)（イ）で示している。 - サービス内容等に応じて SL0 として達成努力目標とすることも想定される。
応答時間	必須	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ことから、SLA において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、スループットタイムを保証しない形式で示すことなども挙げられる	サービス内容等に応じて SL0 として達成努力目標とすることも想定される。

項目	要否	解説	備考
冗長性	必須	・ 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。そのほか、ランサムウェア対策などの観点から必要なバックアップ対策などを具体的に示すなども想定される。 ・ 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。 ・ 例えば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示すことも想定される。	

(e) 保存性に関するサービス仕様

項目	要否	解説	備考
データの破壊防止対策 (ウイルス等による攻撃対策等)	必須	・ SLA では、事業者が採用する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することが求められる。 ・ 採用するデータの破壊防止の対策については、厚生労働省ガイドラインで求められる内容や、自社のリスクアセスメント結果等を踏まえて、必要に応じて具体的な内容を示すことになる。 ・ 例えば、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	

項目	要否	解説	備考
		ル（いわゆるセキュリティパッチ）の適用の対応等を示すなどが想定される。 - 具体的な内容については、事業者において必要とされる対策について、設定することが想定される。 - サービス等における対策に関する仕様、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。	
データの劣化、滅失対策	必須	2省ガイドライン電子保存の要求事項への対応を求めている(6.2)。SLA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することが求められる。 - また例えば、併せて、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、旧方式のものととの互換性を確保することについて含めるなども想定される。 - そのほか、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示すことなども想定される。 - 具体的な内容については、事業者において必要とされる内容を設定することが想定される。 - 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。	- 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）⑩（b）（ウ）で示している。 - 厚生労働省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。

項目	要否	解説	備考
データ仕様について	必須	- 厚生労働省ガイドラインでは、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。 - SLA では、対象事業者が採用するデータ仕様について、例えば情報の相互運用性と標準化に関する内容を示すことが想定される。 - 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。	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。

(6) 運用内容

① 運用組織・規程等

(f) 運用組織・体制

項目	要否	解説	備考
運用組織・体制	必須	・ SLA では、対象事業者の運用体制を示すことが求められる。 ・ 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） ➤ 再委託事業者、連携対象事業者を利用する場合には、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。	・ 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。

(g) 運用に関する規程

項目	要否	解説	備考
本サービス提供上、根拠とする運用管理規程等	必須	・ 2省ガイドラインでは5.1.6に基づき事業者における運用管理規程等の文書化を求める。 ・ SLA では、事業者において運用管理規程を定めて、医療情報システム等を提供する旨を示すとともに、必要に応じて、その内容が医療機関等が定める内容と齟齬がある場合には、調整するなどを示すことが想定される。	

項目	要否	解説	備考
		• なお、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として機能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。	
運用の方針となる規程	必須	• 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。 • SLAではこれらが存在する場合には、その規定状況等を示すことが求められる。なお上記の方針等の名称は、事例であり、実際に各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①に示すように小規模医療機関等の運用管理規程として機能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ことも想定される。	

(h) 運用における遵守事項

項目	要否	解説	備考
禁止事項等	必須	・ SLA では、対象事業者におけるサービス提供上の禁止事項を明示する。 ・ 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。事業者においては、これらの観点から、特に禁止されるべき内容があり、その遵守を SLA において示すことが求められる。 ・ 例えば、以下のような内容が想定される。 ➤ 受託した医療情報を、匿名化されたものを含めて、医療機関等との同意又は指示がない限り、分析、解析等を実施しない。 ➤ 受託した医療情報を、許可無く第三者に提供しない。 ➤ 医療機関等の依頼がある場合であっても、代行操作等は実施しない。	

② 受託情報の取り扱い

項目	要否	解説	備考
受託情報の取り扱い範囲	必須	・ 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べきである。その上で、例えば ➤ 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 SLA において、求められる。	
受託情報の管理	必須	・ SLA では、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等を示すことが求められる。 ・ 医療機関等においては、厚生労働省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。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あるが生じうる。	

項目	要否	解説	備考
		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、あるいは適切な対応を実施している旨の誓約を行うなどが想定される。	
受託情報の提供	必須	- SLA 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。 - 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。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しる等を示すことも想定される。 - 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、例えば厚生労働省ガイドラインにおける情報の相互運用性と標準化に対応する内容で提供すべき旨を含むことも想定される。また、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含めることも想定される。	
受託情報の返却等	必須	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。	

項目	要否	解説	備考
		- 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。 - 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。	

③ 運用仕様及びその指標

(i) 機密性

項目	要否	解説	備考
物理的セキュリティ	必須	・ 医療機関等においては、厚生労働省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。 ・ SLA では、事業者が講じる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、これに基づいて実施する旨を含めることが求められる。 ・ 採用する物理的セキュリティ対策については、厚生労働省ガイドラインで求められる内容や、自社のリスクアセスメント結果等を踏まえて、必要に応じて具体的な内容を示すことになる。 ・ 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含めることも想定される。	
セキュリティ管理	必須	・ SLA では、事業者が講じる運用上のセキュリティの管理に関する事項を運用管理規程に含め、これに基づいて実施する旨を含めることが求められる。 ・ 採用するセキュリティ管理については、厚生労働省ガイドラインで求められる内容や、自社のリスクアセスメント結果等を踏まえて、必要に応じて具体的な内容を示すことになる。	

項目	要否	解説	備考
		- 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、それ以外に必要に応じて、運用業務に求められる事項を挙げるなどが想定される。 - 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含めることも想定される。	

(j) 可用性

項目	要否	解説	備考
稼働率ほか	必須	- SLA 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する。 - 医療情報システム等、特に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。これを具体的な指標としては、例えばサービス稼働率や、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。 - 具体的な内容としては例えば、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）等が挙げられる。またサービスの内容に応じて事	- 例えば電子カルテなどでは、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等が一例として挙げられる。 - 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、事業者がネットワークサービスの提供を行っていない場合には、これに起因する

項目	要否	解説	備考
		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、追記することも想定される。 - 稼働率においては、いつから障害等が発生したのかを定めることも求められる。例えば事業者による検知又は医療機関等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を想定するなどが挙げられる。 - 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含めることも想定される。	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、含めることは難しい。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。 サービス内容等に応じて SLO として達成努力目標とすることも想定される。

(k) 完全性

項目	要否	解説	備考
アクセス記録の管理等	必須	- 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、保存することが想定される。 - SLA においては、この内容を示すことが求められる。 - アクセス記録の保存期間については、対象となる医療情報に求められる法定保存年限を踏まえることが求められる。一方で、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。 - 事業者はその旨も含めて、医療機関等の理解を得た上で適切な保存期間に関する合意を行うことが求められる。 - 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、事業者は一定の条件でアクセス記録を含む運用状況の資料についての資料提供を行う旨を含むことも想定される。	事業者が利用するネットワークサービスのアクセス記録等については、事業者側のリスクアセスメントに基づいて設定する。利用者側のネットワークサービスのアクセス記録の保存期間については、提供サービスの内容に応じて決定することになる。

④ 非常時の対応

項目	要否	解説	備考
非常時の対応	必須	- SLA では、障害のほか、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について、その対応手続等を事前に事業者が定めて、これに従い対応を行うことを示すことが求められる。この場合、非常時の定義についても併せて示すことが求められる。 - 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らかにすることも重要である。 - 具体的な内容については、厚生労働省ガイドラインでは、災害等とサイバー攻撃、障害の3つの場面に応じた対策を求めていることから、これらを参考にして示すことが望ましい。	

⑤ 報告事項・事前連絡

(a) 報告事項と頻度

項目	要否	解説	備考
月次報告事項	必須	SLA 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ことが求められる。	

項目	要否	解説	備考
		- 対象事業者から医療機関等に対してなされる報告は、医療機関等が厚生労働省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することも、サービス内容により想定される。 - 報告項目は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。また報告時期については定めていない。必要があれば、例え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。また報告の方法は、例えば Web によるものや、個別報告など、サービス内容により異なることが想定される。	
年次報告事項	必須	- SLA では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ことが求められる。 - 医療機関等は、定期的に運用状況のレビューを行い、改善することが厚生労働省ガイドラインにより求められている。そこで、事業者は、提供するサービスに係る提供状況に関す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。 - 具体的な報告項目は、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、年次の報告とすることが想定される。また報告の方法	

項目	要否	解説	備考
		は、例えば Web によるものや、個別報告など、サービス内容により異なることが想定される。	
発生の都度に報告する事項	必須	- SLA では例えば障害の発生状況等、運用上、不定期で発生する事項に関して、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。 - 例えば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、医療機関等に対して周知する必要性が高い場合などが想定される。 - 具体的な内容については、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。	

(b) 報告方法

項目	要否	解説	備考
報告方法	任意(いずれかの方法)	- SLA において、必要に応じて報告事項に関する報告方法について明示する。 - 例えば報告内容が特定の医療機関等を対象として行う必要がない場合には、Web 上や、同報発信によるメールにより報告することとし、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等も想定される。 - 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が求められる。 - 具体的な内容については、対象事業者において上記観点から必要とされる項目を、追記することが想定される。	

(c) 事前連絡及び承認等

項目	要否	解説	備考
保守業務に伴うサービスの停止の告知	必須	- SLA 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。 - 例えば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、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	

項目	要否	解説	備考
		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等を定めるなどが一例として挙げられる。 - 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。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。 - また、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、示すことも想定される。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。 - これらの場合、例えば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などが挙げられる。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	

項目	要否	解説	備考
		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が望ましい。	
受託情報等に関する保守業務の事前連絡・承認	任意	- SLA 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。 - 例えば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示すなどが想定される。 - 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。 - 但し上記の場合において、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	

項目	要否	解説	備考
		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も生じる。このような場合の例外的な対応について示すことも望ましい。 事前連絡及び承認に基づいて、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することも想定される。但しこれらは、提供するサービスの特性に応じて、対応の可否等を検討し、医療機関等とその内容を合意することが求められる。	
保守業務に関する事前連絡等	必須	- 厚生労働省ガイドラインでは、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。 - SLA 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。 - 医療情報システム等の中には、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ものがあり、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場合もある。例えば、保守業務の内容により、 ➤ 事後報告のみを要する保守内容 ➤ 事前告知及び事後報告を要する保守内容 ➤ 事前承認及び事後報告要する保守内容	

項目	要否	解説	備考
		に分けるなども想定される。これにより、医療機関等に求められる医療情報システム等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も想定される。	

⑥ サポート

(a) 利用者に対するサポート

項目	要否	解説	備考
サポート内容	必須	- 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。 - 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。そのため、例えば利用者側の OS やネットワークに関する設定、Web ブラウザ等の設定等については、サポート外にする、あるいは問い合わせ窓口を区別するなども想定される。 - そのほか、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	

項目	要否	解説	備考
		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）。	
サポート対応方法・時間	必須	- サポートの対応時間や方法を示すことが求められる。 - サポート対応方法は、電話によるほか、メールやweb ページによる受付を行う等がある。 - 具体的内容については、Web ページ等を併せて明示することで、円滑に医療機関等からの問い合わせに対応できることに留意することが求められる。	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）⑮で示している。

(b) 技術情報提供について

項目	要否	解説	備考
技術情報提供について	必須	- 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、仕様等を明記するほか、具体的な内容は明記せず、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し、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、という記載とする場合などが想定される。 - 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	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。

		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。 - また情報の提供に際しては、例えば ➤ 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 などを示すことなども想定される。 - 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。	
--	--	---	--

(c) 運用状況に係る情報提供について

項目	要否	解説	備考
----	----	----	----

運用状況に係る情報提供について	必須	・ 本項では、運用状況に係る情報提供について示すことがある。例えば2省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、等を示すなどが想定される。 ・ また、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や、その場合の一定の条件が必要な場合にはその調整を行うなどを取り決める場合もある。例えば運用状況の記録の中には、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あることから、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。	・ 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示すというような記載にしている。
-----------------	----	---	---

(7) サービス・レベルに関する合意事項

① サービス・レベルの評価方法

(a) 管理指標及び評価方法

項目	要否	解説	備考
評価指標(または目標指標)	必須	- 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一定の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。 - これらの指標については、その達成を医療機関等との間での遵守事項とする場合と、目標指標として示すことなどが想定される。 - どのような指標を採用するか、どのような位置づけ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、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。	
評価方法	必須	- 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ことがある。 - 例えば、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するなどが挙げられる。各項目について特に軽重を置かずに、評価する方法や、情報漏洩事故などのアクシデント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。	目標指標とした場合には、未達の場合には、その点に関するリスク認識や改善策およびその方針を示すなどの対応が想定される。

項目	要否	解説	備考
		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。具体的に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	

② サービス・レベルマネジメント

項目	要否	解説	備考
サービス・レベルマネジメント	任意	- 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がサービス・レベルマネジメントである。 - サービス・レベルの達成状況による対応を示すほか、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も想定される。 - 具体的に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。	- 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。 - 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。

2. 2 サービスごとの各項目への SLA 項目の適用

(1) 相対契約によるサービス

大項目	中項目	小項目	詳細	相対契約	
				運用受託	保守サービス受託
1. 本サービスの目的と対象	1.1 本サービスの目的	(1) 本サービスの目的		○	○
		(2) 本サービスの対象		○	○
	1.2 本サービスの提供範囲	(1) サービス		・運用受託におけるサービスの提供範囲を記載	・故障時、定期保守、監視、ソフトウェアの改定、Windows アップデート、ルータの責任範囲などを記載
		(2) ネットワークサービス			
		(3) 使用機器等			
		(4) 本サービスの利用に供するソフトウェア			
	1.3 本サービスの提供時間			○	○ ・問い合わせなどの営業時間 ・時間外の取り決め
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	(1) 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		○	○
		(2) 医療業務等への影響の把握		○	○
		(3) サービス品質とコストの妥当性を図る		○	○
		(4) 各役割分担の明確化を図る		○	○
	2.2 本サービスにおけるサービス・レベル適用の考え方	(1) 本サービスにおけるサービス・レベルの適用		○	○

		(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		○	○
	2.3 本 SLA の適用期間			○	○
	2.4 本 SLA の改定	(1) 改定の契機		○	○
		(2) 変更の手続き		○	○
3・前提条件	3.1 リスク評価			○	○
	3.2 サービス利用環境			○	○
	3.3 サービス提供環境・運用に係る 前提条件			○	○
	3.4 機器・ソフトウェアの品質			○	○
	3.5 準拠する法令・ガイドライ ン 等			○	○
	3.6 守秘義務等			○	○
	3.7 監査			○	○
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		○	○
		(2) 本サービスの医療機関 等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	○	○
			②障害一般に関する役割 分担と責任	○	○

			③医療機関等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	△サービス提供していなければ不要	△サービス提供していなければ不要
	4.2 医療機関等の業務上の役割分担と責任	(1) 医療機関等のサービス利用に関する業務上の役割分担		○	○
		(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		○	○
		(3) 医療機関等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		○	○
	4.3 再委託事業者・連携クラウドサービス事業者等	(1) 業務の再委託	①データセンタ業務	○	○
			②保守業務	○	○
		(2) 連携クラウドサービス事業者		○	○
		(3) 再委託先・連携事業者に対する管理責任等		○	○
		(4) 再委託先・連携事業者に関する情報提供		○	○
	4.4 連絡体制	(1) 通常時の連絡体制		○	○
		(2) 障害時・非常時の連絡体制・告知方法		○	○
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)		○	○

	(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)		○	○
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)	○	○
		②職種等に基づくアクセス制御	○	○
		③電子署名	△サービス提供していなければ不要	△サービス提供していなければ不要
		④診療記録の確定(本人による確定、代行確定等)	△サービス提供していなければ不要	△サービス提供していなければ不要
		⑤データの更新履歴管理	△サービス提供していなければ不要	△サービス提供していなければ不要
	(2) 見読性に関するサービス仕様	①表示仕様	△サービス提供していなければ不要	△サービス提供していなければ不要
		②応答時間	△サービス提供していなければ不要	△サービス提供していなければ不要
		③冗長性	△サービス提供していなければ不要	△サービス提供していなければ不要

6. 運用内容		(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（ウィルス等による攻撃対策等）	△サービス提供していなければ不要	△サービス提供していなければ不要
			②データの劣化、滅失対策	△サービス提供していなければ不要	△サービス提供していなければ不要
			③データ仕様について	△サービス提供していなければ不要	△サービス提供していなければ不要
	6.1 運用組織・規程等	(1) 運用組織・体制		○	○
		(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	○	○
			②運用の方針となる規程	○	○
			③運用管理を構成する規程・要領・手順等	○	○
			④本項で示す運用管理規程類等の提供	○	○
		(3) 運用における遵守事項		○	○
	6.2 受託情報の取り扱い	(1) 受託情報の取り扱い範囲		△医療情報の受託がある場合に必要	△医療情報の受託がある場合に必要

6.3 運用仕様及びその指標	(2) 受託情報の管理		同上	同上
	(3) 受託情報の提供		同上	同上
	(4) 受託情報の返却等		同上	同上
	(1) 機密性	①物理的セキュリティ	○	○
		②セキュリティ管理	○	○
	(2) 可用性		○	○
	(3) 完全性		○	○
6.4 非常時の対応			○	○
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	○	○
		②年次報告事項	○	○
		③発生の都度に報告する 事項	○	○
	(2) 報告方法	①書面または電子メール により報告を要する項 目	○	○

			②書面または電子メール によるほか、対象事業者において管理する対象事業者の名義における Web 上で公開による報告が可能な項目	○	○
			(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	○
				②受託情報等に関する保守業務の事前連絡・承認	○
				③保守業務に関する事前連絡等	○
	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	○	○
			②サポート対応時間	○	○
		(2) 技術情報提供について		○	○
		(3) 運用状況に係る情報提供について		○	○
		(1) 管理指標及び評価方法	① 管理指標	○	○
			② 評価方法	同上	同上
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				

		(2) サービス・レベル算定 除外事項		同上	同上
	7.2 サービス・レベルマネジメン ト			同上	同上

(2) 約款契約によるサービス

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
1. 本サービスの目的と対象	1. 1 本サービスの目的	(1) 本サービスの目的		○	○
		(2) 本サービスの対象		○	○
	1. 2 本サービスの提供範囲	(1) サービス		故障時、定期保守、監視、 ソフトウェアの改定、 Windows アップデート、 ルータの責任範囲などを 記載	○ ・約款上、個人情報を取り扱わないとしている SaaS サービスにおいては、SaaS サービスに保存された情報という表記も想定される
		(2) ネットワークサービス		※JAHIS 参照 ⁵	○
		(3) 使用機器等			○
		(4) 本サービスの利用に供 するソフトウェア			○
	1. 3 本サービスの提供時間			○ ・問い合わせなどの営業時間	○ ・SaaS の提供時間(24 時間 365 日)など ・問い合わせなどは営業時間等を示す

⁵ 「JAHIS 参照」とは、当該項目について「JAHIS リモートサービス セキュリティガイドライン Ver. 3. 1a」(一般社団法人 保健医療福祉情報システム工業会 医療システム部 会 セキュリティ委員会 JAHIS/JIRA 合同リモートサービスセキュリティ作成 WG)に付属する「リモート保守サービス SLA サンプル(見本)」、及び「リモート保守サービス SLA サンプル解説付き(テンプレート)」の内容を参照して、検討することが望ましい旨を示す。

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
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	(1) 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		○ ※JAHIS 参照	○
		(2) 医療業務等への影響の把握		○ ※JAHIS 参照	○
		(3) サービス品質とコストの妥当性を図る		○ ※JAHIS 参照	○
		(4) 各役割分担の明確化を図る		○ ※JAHIS 参照	○
	2.2 本サービスにおけるサービス・レベル適用の考え方	(1) 本サービスにおける鑑みたサービス・レベルの適用		○ ※JAHIS 参照	○
		(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		○ ※JAHIS 参照	○
	2.3 本 SLA の適用期間			○ ※JAHIS 参照	○契約自動更新を加味した記載にする等も想定される

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
	2.4 本 SLA の改定	(1) 改定の契機		○ ※JAHIS 参照	○ ・ 双方合意が想定しにくいいため、例えば「本サービスの仕様に変更が生じた場合」などが改定の契機として想定される
		(2) 変更の手続き		○ ※JAHIS 参照	○ ・ 双方合意が想定しにくいいため、「本 SLA の改定が必要となった場合は、都度、サービス・レベルの変更内容を通知する」などの記載が想定される
3・前提条件	3.1 リスク評価			○ ※JAHIS 参照	○ ※JAHIS 参照
	3.2 サービス利用環境			○ ※JAHIS 参照	○

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
	3.3 サービス提供環境・運用に係る前提条件			○ ※JAHIS 参照	○ ・具体的な運用においては、サービス仕様適合開示書への記載と併せて検討
	3.4 機器・ソフトウェアの品質			○ ※JAHIS 参照	○ ・具体的な運用においては、サービス仕様適合開示書への記載と併せて検討
	3.5 準拠する法令・ガイドライン等			○ ※JAHIS 参照	○
	3.6 守秘義務等			○ ※JAHIS 参照	○

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
	3.7 監査			○ ・年次で内部監査を報告することが難しい場合には、下記例などの記載も想定される 「対象事業者は、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いて ISO/IEC 27001 の認証を受けており、年1回、審査登録機関により評価される。当該認証に係る検査の結果をもって監査の実施とする。」	○ ・年次で内部監査を報告することが困難な場合には、下記例などの記載も想定される 「対象事業者は、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いて ISO/IEC 27001 の認証を受けており、年1回、審査登録機関により評価される。当該認証に係る検査の結果をもって監査の実施とする。」
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		○ ※JAHIS 参照	○ SLA の可用性目標値

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
		(2) 本サービスの医療機関等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	○ ※JAHIS 参照	○
			②障害一般に関する役割分担と責任	○ ※JAHIS 参照	○
			③医療機関等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	X ※JAHIS 参照	△ サービス提供していなければ不要
	4.2 医療機関等の業務上の役割分担と責任	(1) 医療機関等のサービス利用に関する業務上の役割分担		○ ※JAHIS 参照	○
		(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		○ ※JAHIS 参照	○

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
		(3) 医療機関等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		○ ※JAHIS 参照	△ ・サービス仕様適合開示書への記載と併せて検討
	4.3 再委託事業者・連携クラウドサービス事業者等	(1) 業務の再委託	①データセンタ業務	△データセンタで受託情報を管理する場合のみ必要 ※JAHIS 参照	○ ・データセンタやプラットフォーム事業者などを記載する。
			②保守業務	△データセンタで受託情報を管理する場合のみ必要 ※JAHIS 参照	△ ・保守委託がある場合のみ必要
		(2) 連携クラウドサービス事業者		△ ※JAHIS 参照	△ ・API 連携の相手先が複数あるケースにおいては代表的なものを示すとともに必要に応じて詳細の情報を示す

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
		(3) 再委託先・連携事業者に対する管理責任等		△ ※JAHIS 参照	△ ・再委託の際は「管理責任を有する」でよいが、連携対象事業者は連携先ベンダーの責任範囲 ・AWS, Azure 等プラットフォームは責任共有モデルの範囲 ・API 連携先ベンダー: サービス仕様適合開示書への記載と併せて検討
		(4) 再委託先・連携事業者に関する情報提供		△ ※JAHIS 参照	△ ・サービス仕様適合開示書への記載と併せて検討
	4. 4 連絡体制	(1) 通常時の連絡体制		△約款の場合、医療機関等対象事業者の関係を記載できない ※JAHIS 参照	△ ・サービス仕様適合開示書への記載と併せて検討
		(2) 障害時・非常時の連絡体制・告知方法		△ ※JAHIS 参照	△ ・サービス仕様適合開示書への記載と併せて検討

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
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)		○ ※JAHIS 参照	○ ・サービス仕様適合開示書への記載と併せて検討
		(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)		○ ※JAHIS 参照	△ ・サービス仕様適合開示書への記載と併せて検討
	5.2 受託情報に関するサービス仕様 ※約款上、医療情報を取り扱わないとしている汎用 SaaS サービスにおいては、受託情報ではなく、SaaS サービスに保存された	(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)	○ ※JAHIS 参照	△ ・サービス仕様適合開示書への記載と併せて検討
			②職種等に基づくアクセス制御	○ ※JAHIS 参照	△ ・サービス仕様適合開示書への記載と併せて検討

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
	情報を示す		③電子署名	△サービス提供していなければ不要	△ ・サービス提供していなければ不要
			④診療記録の確定 (本人による確定、代行確定等)	△サービス提供していなければ不要	△ ・サービス提供していなければ不要 ・サービス仕様適合開示書への記載と併せて検討
			⑤データの更新履歴管理	△サービス提供していなければ不要	△ ・サービス提供していなければ不要 ・サービス仕様適合開示書への記載と併せて検討
		(2) 見読性に関するサービス仕様	①表示仕様	△サービス提供していなければ不要	△ ・サービス提供していなければ不要 ・サービス仕様適合開示書への記載と併せて検討

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
			②応答時間	△サービス提供していなければ不要	△ ・SaaS の場合、ネットワークやその他外的要因に左右される場合には、下記例の記載も想定される 「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、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、対象事業者は、医療機関等からの連絡又は自己の判断に基づき、調査し、医療機関等への報告を行う。」
			③冗長性	△サービス提供していなければ不要	△ ・プラットフォーム事業者やサービスの組み方に依存する場合には、そのことを加味した記載内容とすることを検討
		(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(ウィルス等による攻撃対策等)	△サービス提供していなければ不要	△ ・サービス提供していなければ不要

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
			②データの劣化、滅失対策	△サービス提供していなければ不要	△ ・プラットフォーム事業者やサービスの組み方に依存する場合には、そのことを加味した記載内容とすることを検討にする ・また、バックアップの実施頻度等も記載する
			③データ仕様について	△サービス提供していなければ不要	△
6・運用内容	6.1 運用組織・規程等	(1) 運用組織・体制		○	○
		(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	○ ※JAHIS 参照	○
			②運用の方針となる規程	○ ※JAHIS 参照	○ ※JAHIS 参照
			③運用管理を構成する規程・要領・手順等	○ ※JAHIS 参照	△ ・詳細は個別のサービス目的に応じて検討

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
			④本項で示す運用管理 規程類等の提供	△ ・具体的な提供情報はサー ビス仕様適合開示書への 記載と併せて検討	X ・一般的な約款契約による場合には、運 用規程等は省略可
		(3)運用における遵守事項		○ ※JAHIS 参照	○
	6.2 受託情報の取り扱い	(1)受託情報の取り扱い範 囲		△ ・医療情報の受託がある場	△ ・医療情報の受託がある場合に必要
		(2)受託情報の管理		同上	同上
		(3)受託情報の提供		同上	同上
		(4)受託情報の返却等		同上	同上
	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	○ ※JAHIS 参照	○ SDS の提供
			②セキュリティ管理	○ ※JAHIS 参照	○ ・第三者認証 (ISMS 認証、SOC1、SOC2、 SOC3 取得のデータセンタで適切にデー タを取り扱う等) などを記載する

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
		(2) 可用性		○ ※JAHIS 参照	○ ・提供内容はサービス毎にことなるので、適切な可用性を記載する
		(3) 完全性		○ ※JAHIS 参照	○ ・提供内容はサービスにより異なるので、適切な可用性を記載する
	6.4 非常時の対応			○ ※JAHIS 参照	○ ・サービス仕様適合開示書への記載と併せて検討
	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	△ ※JAHIS 参照 月次報告はサービス提供内容による	△ ・サービス仕様適合開示書への記載と併せて検討
			②年次報告事項	△ ※JAHIS 参照	△ ・サービス仕様適合開示書への記載と併せて検討

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
			③発生の都度に報告する事項	△ ※JAHIS 参照	○ ・ サービス提供の範囲で、都度報告が必要な事項を記載する
		(2) 報告方法	①書面または電子メールにより報告を要する項目	○ ※JAHIS 参照	△ ・ SaaS サービスで可能な通知方法を記載する
			②書面または電子メールによるほか、対象事業者において管理する対象事業者の名称における Web 上で公開による報告が可能な項目	○ ※JAHIS 参照	△ ・ SaaS サービスで可能な通知方法を記載する
		(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	○ ※JAHIS 参照	△ ・ SaaS サービスで可能な通知方法を記載する
			②受託情報等に関する保守業務の事前連絡・承認	△ ※JAHIS 参照	△ ・ 受託情報の保守が必要なサービス提供の場合のみ

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
			③保守業務に関する事前連絡等	△ ※JAHIS 参照	△ ・サービス仕様適合開示書への記載と併せて検討
	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	○ ※JAHIS 参照	○サービス提供に関するサポート内容を記載する ・利用やからの問い合わせ ・ID 再発行など
			②サポート対応時間	○ ※JAHIS 参照	○
		(2)技術情報提供について		○SDS ※JAHIS 参照	○ ・ JAHIS 同様に SDS を提示。
		(3)運用状況に係る情報提供について		○ ※JAHIS 参照 ・ 保守レポート、リモート報告など	△ ・サービス仕様適合開示書への記載と併せて検討

大項目	中項目	小項目	詳細	約款	
				リモート保守	SaaS のみ提供
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	○ ※JAHIS 参照 ・ 共同評価や情報提供につ いて、どこまで可能か要 検討	△ ・ 情報提供について、どこまで可能か要 検討
			② 評価方法	同上	同上
		(2) サービス・レベル算定 除外事項		同上	同上
	7.2 サービス・レベルマネジメン ト			同上	同上