リモート保守サービス SLA（Service Level Agreement） サンプル

Ver.1.0

2023 年 4 月

JAHIS/JIRA 合同リモートサービスセキュリティ作成 WG

目　　次

本文書の位置づけ

本文書は、リモートサービスセキュリティガイドライン（以下、「本ガイドライン」という）において定義されたサービスモデルを踏まえ、サンプルのリモート保守サービスを仮定したうえでそのサービスの SLA を設定したものである。

また、本 SLA サンプル作成にあたっては、総務省・経済産業省「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」の添付文書である「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」の SLA を基にしている。

なお、本 SLA サンプルは、SDS サンプルを作成するために設定したものであり、利用する各社はあくまで参考として自社サービスの SLA および SDS 策定の参考とされたい。

A1.　本サービスの目的と対象

A1.1.　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。

⑴　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、リモートサービスを提供することを目的とする。

⑵　本サービスの対象
本サービスの対象は、XX（システム名称）を導入している医療機関等とする。

A1.2.　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。

⑴　故障時の対応
HCF 内の機器に障害が生じ、HCF 側からの連絡に基づき、RSC 側から HCF 内の保守対象機器にアクセスを行い、障害対応を行うものです。

⑵　定期保守
HCF 側からの了解の元に、RSC 側から HCF 内の保守対象機器に対して定期的にアクセスを行い、対象機器の保守作業を行うものです。

⑶　定期監視
HCF 側からの了解の元に、RSC 側から HCF 内の保守対象機器に対して定期的にアクセスを行い、対象機器の監視を行うものです。

⑷　ソフトウェアの改訂
RSC 側から HCF 内の保守対象機器に対してアクセスを行い、保守対象機器のソフトウェアの更新を行うものです。

A1.3.　本サービスの提供時間

本サービスの提供時間は、本 SLA 7．1⑵の「事前に合意された事由」に基づく停止を除き、以下のとおりである。

【平日】 9:00～17:00
【土曜日・日曜・祝日】 提供なし

A2. 本 SLA について

A2.1. 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) 障害対応

医療機関のユーザが機器・システムに異常を発見してベンダのサポート窓口に連絡した時や、自己診断機能で異常がベンダのサポート窓口に自動通知された時などにリモートサービスを用いると、ベンダのサポート担当者が直接対象機器・システムへネットワーク接続をして、短時間で現象を正確に確認し異常箇所を絞り込むことが可能となります。ハードウェア障害であれば何らかの現地作業が必要となりますが、ハードウェア的な問題でなければ直接リモート作業で復旧させることが可能な場合もあります。ハードウェア的障害であったとしても、現地の作業員に適切な指示を送り共同して復旧させることが可能になります。

(2) 予防保守のための情報収集

装置・システムの自己診断機能を定期的に動作させることにより、機能の一部または全体が使えなくなる重大な障害を引き起こすような兆候を、事前に検出できることがあります。機器の消耗部品の劣化度を監視している例もあります。

なんらかの兆候が検出された場合には、その記録を機器・システムの内部に蓄積しますが、リモートサービスを使うとベンダのサポート窓口から定期的に自己診断機能の記録を確認したり、機器の自動メール発信機能等を用いてベンダのサポート窓口に直接伝えたりすることが実現できます。これにより（1）に記載した障害対応に円滑に繋げることが可能になります。

(3) ソフトウェア改訂・更新

異常の原因がソフトウェアである場合や、あるいは特に異常はなくても予防保守やなんらかの機能向上でソフトウェアを更新する必要がある場合は、リモートサービスによって遠隔地から直接改訂・更新作業を行うことが可能な場合があります。

A2.2. 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) ダウンタイムの大幅短縮

近年の医療機器・システムは技術的に高度化しており、保守サービス員の専門性も求められています。

リモートサービスを用いない場合の作業は、原則としてベンダから派遣された保守サービス員のみになります。保守サービス員は現象の詳細把握を行い、場合によっては採取した情報を持ち帰り、その上で必要な部品を入手して改めて現地に赴くことになります。

リモートサービスを用いた場合は、専門知識のある保守サービス員があらかじめ異常個所の特定、対応策を検討してから保守サービス員の派遣が可能となり、リモートサービスセンタから直接機器やシステムにアクセスして情報の収集ができるため、能率的で、ダウンタイムも大幅に短縮することができます。

また、ソフトウェアだけの問題であれば、直接リモート作業で復旧させることが可能な場合もあります。

＜解説＞

本ガイドラインが対象とする医療情報システムで特に留意すべき事項としては、
・ 利用者が監督責任を果たすに必要な提出文書類や監査に関する事項
・ 利用者、提供者および関与する事業者毎の責任分界
・ 提供者が保守に必要なデータを取得する場合の手続き
本ガイドラインが参照する ISMS では「資産の移動には事前の許可が必要」とされており、情報も資産と見なされることから、SLA においてはデータ取得に関する手続きを合意しておくことが実用的です。
・ 提供者の取得データの保管・分析・利用後の破棄に関する安全性確保策（例えば、保管データへのアクセス権限管理、ログの保存期間、など）
・ 提供者から利用者への報告方法や提出内容
・ 緊急時、災害時における非常時対応の規定
などが挙げられます。

(2) 予防保守
自己診断機能などにより装置やシステム自体の稼働状態のモニタ内容をリモートで監視することで、交換が必要な部品の交換時期を予測したり、故障につながる微細な異常を早期に把握したり、より効率的な保守計画を設定できます。

(3) 保守費用の大幅低減
（1）（2）のように、ベンダからの保守サービス員が実際に医療機関に出向く頻度が大幅に減り、保守作業時間の削減が可能になります。この直接的費用削減も見込めますが、ベンダのサービス拠点を集約することも可能となるため、保守サービスを実現するための費用が節減でき、結果的に医療機関が支払う保守契約費用の低減に通じます。

(4) 医療機関側職員の対応も低減
障害によるダウンタイムが大幅に短縮されることで、医療機関側の手間も減ることになります。

A2.3. 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。

契約開始日を適用開始日とし、契約終了日を適用終了日とする。

版数	適用開始日	適用終了日
第 1.0 版	令和 5 年 4 月 1 日（契約開始日）	令和 6 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。

また、本サービス利用契約が自動継続する場合にも、本 SLA が適用されるものとする。

A2.4. 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

A3. 前提条件

A3.1. 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。

乙は、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、サービス事業者による医療情報セキュリティ開示書（以下、「SDS」）を甲に提供する。

> ＜解説＞
> JAHIS 標準の「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」をポイントしています。

A3.2. サービス利用環境

甲は、本サービスで提供するアプリケーションを利用する際には、リモート保守端末を用意する必要がある。乙は、リモート保守端末の要件について、別紙「サービス利用環境」に示す。

別紙の内容は、予告の上、適宜変更を行う。

> ＜解説＞
> HCF リモート保守専用クライアント PC は医療機関の責任で用意することを前提としています。リモート保守ベンダーが PC 等を設置する場合は、医療機関のセキュリティ要件を満たすことを確認します。

A3.3. 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、乙の事業所内にて行う。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、SDS を甲に提供する。

> ＜解説＞
> 自社に設置する保守サイトを利用することを前提としています。アウトソース、もしくはクラウド環境を利用する場合には、外部委託先の環境や条件を含めた記載が必要となります。

A3.4. 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、SDS を甲に提供する。

A3.5. 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
- 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）

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 ）
- 医療情報システムの安全管理に関するガイドライン （厚生労働省）

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。

A3.6. 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
- 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
- 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

> ＜解説＞
> 自社に設置する保守サイトを利用することを前提としています。アウトソース、もしくはクラウド環境を利用する場合には、外部委託先の環境や条件を含めた記載が必要となります。

A3.7. 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、開示が必要な事象が生じた際には、乙において定める規程に基づいて開示する。その規程の具体的な内容については、６．６(3)に基づいて、乙は、甲に提供する。

A4. 役割分担

A4.1. 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、本サービスが正常に提供されることについての責任を有する。乙の責任範囲内のサービスの提供に係るアプリケーションや通信に障害等が発生し、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。

(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、甲が必要とする脆弱性に関する情報などの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、乙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。甲は、乙が必要とする接続情報などの提供を行う。
- 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、甲が必要とする接続情報などの提供を行う。

＜解説＞

参考例にある最後の項目「・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。」は、リモート保守の対象外のため削除しています。

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、乙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、乙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。

＜解説＞

ネットワークは責任分界において、乙側にあるため、主体を乙に変更しています。また、参考例にある最後の項目「・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。」は、リモート保守の対象外のため削除しています。

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かが不明な場合は､甲乙協議の上、対応を行う。

＜解説＞
参考例が示す「甲乙いずれにも起因しない」という趣旨になっていますが､「不明な場合は」という表記としています。
また、同じく参考例が示す「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」については、リモート保守の範囲外となる項目なので削除しています。

A4.2. 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。

・　乙における保守作業員の ID の発行、変更、削除、初期パスワード発行等に関する業務
・　本サービスに係る各保守作業員の権限設定

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)　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

本サービスの利用終了に当たり、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。

・　サービス利用時に使用した設定情報（保守作業員の ID 等）について、確実な削除を実施する。

＜解説＞
リモート保守のためデータ移行が発生しないことから、利用開始時の項目は削除しました。また、サービス利用終了に関する項目に修正しています。

(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。

A4.3. 再委託事業者・連携対象事業者等

(1)　業務の再委託

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××】(以下、丙とする)

・　RSC におけるオペレーション業務

【株式会社△△】(以下、丁とする)

・　障害発生時のデータ解析に関する業務

＜解説＞
本事例では自社内に RSC（保守サイト）を設置しているため、データセンター業務の項目を削除しています。また、リモート保守サービスの再業務委託の想定される候補を追加しています。

(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。

A4.4.　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】

(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】

＜解説＞ 連絡先の例としては、 ・窓口の電話番号 ・電子メールアドレス ・Web 問い合わせフォーム等の URL などが考えられます。

A5.　サービス仕様

A5.1.　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 JAHIS により規定された「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」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。

＜解説＞ 経産省・総務省の適合開示書ではなく、JAHIS の開示書をポイントしています。

(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 JAHIS により規定された「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」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。

＜解説＞
経産省・総務省の適合開示書ではなく、JAHIS の開示書をポイントしています。

A5.2. 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）

甲が本サービスを利用する際に必要となる乙の利用者認証については、甲が発行するアカウント情報に基づき保守端末に設定された認証方式により行う。

本サービスの提供に際して、乙は JAHIS により規定された「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」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。

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乙の利用者認証については、下記の機能を含む。

- 甲は乙の保守作業員に対し、個別のアカウントを発行する
- 甲が乙に発行する利用者 ID において、保守サービスのためのアクセス機能があること

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。

＜解説＞
参考例が示す「③電子署名」、「④診療記録の確定（本人による確定、代行確定等）」、および「⑤データの更新履歴管理」については、本サービスに含まれないため、項目ごと削除しています。

(2) 保存性に関するサービス仕様

＜解説＞
参考例が示す「(2) 見読性に関するサービス仕様」は、リモート保守サービスの実施は甲の診療業務に対するアクセスとは異なるため見読性に関する本項目は削除しています。参考例では本項は「(3) 保存性に関するサービス仕様」として記載されています。

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 JAHIS により規定された「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」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。

＜解説＞
本モデルのリモート保守サービスは常時監視を含んでいないため、参考例が示す定常的なサービスに対する要求事項を削除しています。
また、参考例が示す「② データの劣化、滅失対策」および「③ データ仕様について」については、本サービスでは診療録等の原本を管理しないため項目を削除しています。

A6. 運用内容

A6.1. 運用組織・規定等

(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】

⑵　運用に関する規定

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。

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。

- 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
- 個人情報保護方針等

＜解説＞

リモート保守サービスのため甲向けの運用管理における基本方針や管理目的に関しては、対象外としています。

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、６．６⑶に基づいて、乙は、甲に提供する。

⑶　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、保守サービスの目的外での分析、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。

＜解説＞

リモート保守サービスの業務には分析、解析作業が含まれるため、「保守サービスの目的外での」という文言を追加しています。

A6.2.　受託情報の取扱い

⑴　受託情報の取り扱い範囲

本サービスで、乙が取得又は保管等を受託した情報の取り扱える範囲につき、乙は、下記の内容を遵守する。

- 乙は法令の定めによる等の場合を除き、受託した情報の目的外利用を行わない。
- 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。

(2) 受託情報の管理

本サービスで乙が取得又は保管等を受託した情報につき、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。

(3) 受託情報の提供

甲が乙に対し、乙が取得又は保管等を受託した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」の「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

＜解説＞ 安全管理ガイドラインの各章のタイトルについては、最新版の表記に沿うように確認が必要です。

(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

＜解説＞ リモート保守で生成される操作ログについては、クエリログ等が含まれる場合がありますが、監査報告の一部として必要となることもあり、医療機関側との協議が必要となることがあります。

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」の「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。

A6.3. 運用仕様及びその指標

(1) 機密性

① 物理セキュリティ

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、SDS 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。

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
- バックアップを行う場合には、その内容の改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。

(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。

  サービス時間帯 ●%

  サービス時間帯以外のサービス稼働率の目標値はありません。

  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。

(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。

・ 保守要員における個人情報へのアクセス状況（保守要員のID、アクセス対象、日時等）

上記の記録につき、乙は法定保存年限が指定されている情報に関してはその期間、これ以外は●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。

A6.4. 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。

A6.5. 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作業件数
・ 乙の本サービスの作業状況（サービス種別ごとのアクセス状況等）
・ ７．１(1)に示す管理指標

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

１．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
２．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運用状況
３．３．７により実施した本サービス提供に係る監査結果
４．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
５．乙における経営状況等を示す資料（財務状況等）

＜解説＞

上記２については、経済産業省や個人情報保護委員会からの情報漏えい等による指導等があった場合は、その旨を報告するようにします。特段の事故等が無い場合は、これを報告するようにします。４いついても、報告に含めるようにします。

また、下記の各項目については、それぞれのドキュメントを提出します。

１．SDSの提出

３．監査報告書

５．決算書

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
- 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
- 情報セキュリティインシデントが生じた際の経緯・顛末
- 障害等に伴うサービスの停止に関する経緯、顛末
- リモートサービスに対する保守等に伴うシステムの変更の結果

＜解説＞
「システムの変更の結果」については、保守対象機器に対する保守ではなく、リモートサービスに係る SaaS サービス等の設定変更等を指します。

(2) 報告方法

(1)に示す事項につき、乙は甲に対して報告を行う。
個人情報を含む報告については、安全管理ガイドラインに適合する方法にて、安全に情報を甲に送付する。

(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

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。

＜解説＞
リモートサービスに係る SaaS サービス等の保守によるサービス停止を指しています。
また、参考例が示す「②受託情報等に関する保守義務の事前連絡・承認」および「③保守義務に関する事前連絡等」については、SLA がリモートサービスそのものに対するものなので、項目は不要です。

A6.6. 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。

1．医療機関が障害等の一次切り分けの支援を実施する際に、リモート保守ベンダに対し SaaS サービスの状況等これに必要な情報を提供する
2．本サービスの利用上の障害に関する内容
3．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

＜解説＞
1．医療機関の一次切り分け支援
2．リモート保守サービス自体の障害
3．リモート保守サービスに起因する保守対象機器の障害（マルウェア感染等）に対するサポート
を指します。

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。

【平日】 9:00～17:00
【土曜日・日曜・祝日】 提供なし

(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、乙は最新のSDSを提供する。

(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、6.5に従い情報提供を行う。

A7. サービスレベルに関する合意事項

A7.1. 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。
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。
＜ここに計算方法が入る＞
■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。
＜ここに評価指標が入る＞

(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。
＜ここに算定除外事項が入る＞

A7.2. 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、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、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。

＜解説＞
損害賠償に関する記載については、リモートサービスのサービスレベルの低下に起因して賠償責任がリモートサービスベンダに発生するシーンが極めて少ないと考えられるため削除しています。
これによって、乙を原因としたセキュリティ事故に関する損害賠償責任を逃れるものではありません。

改定履歴		
日付	バージョン	内容
2023/4	Ver. 1.0	初版