別紙６－２

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に基づく SLA 参考例

総務省

平成２２年１２月

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に基づく SLA 参考例

I. 本書の利用法について

１． 本書の目的

本書は、「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第 1.1 版」（総務省　平成 22 年 12 月　以下、「ASP・SaaS 事業者向け医療情報安全管理ガイドライン」という）に基づいて、ASP・SaaS 事業者が医療機関等に対してサービス提供を行う際に求められる合意事項等を整理し、SLA の参考例という形でまとめたものである。

ASP・SaaS 事業者向け医療情報安全管理ガイドラインでは、ASP・SaaS 事業者が医療情報を取り扱う際に求められる要求事項を示している。各要求事項には、以下の 2 つのものが含まれている。

・ASP・SaaS 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
・ASP・SaaS 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

前者は、例えば、ASP･SaaS 事業者における管理責任者の指定や、運用等を規程に基づいて実施すること等、サービス内容若しくはサービス提供の前提として一意に決まる項目である。

後者は、例えば、サービス利用に際して採用される利用者認証についてその方法等、サービス内容若しくはサービス提供の際に、具体的な実施方法について ASP・SaaS 事業者と医療機関等との協議によって決定する項目である。

ASP･SaaS 事業者が ASP･SaaS 事業者向け医療情報安全管理ガイドラインにのっとって、医療機関等に対してサービスを提供する際には、これらの項目の内容を明確にすることが求められる。ASP・SaaS 事業者の提供するサービス内容を明らかにすることにより、医療情報が安全に取り扱われていることを確認することが可能となる。

このような趣旨から、SLA の参考例となる本書を作成した。ASP･SaaS 事業者が ASP･SaaS 事業者向け医療情報安全管理ガイドラインにのっとったサービスを提供する際に必要となる SLA を参考例の形で示すことにより、ASP･SaaS 事業者が自ら提供するサービスについて、同様の書面を作成する際の一助となることを目的としている。本書は、ASP･SaaS 事業者が診療所に対して、ASP・SaaS による診療録の作成、その保存、及びそれに伴うサービス（以下、「診療録の作成、保存等のサービス」という）を提供することを想定した参考例となっている。ただし、事業者ごとに提供するサービスは異なり、また、本書で想定した以外のサービスを提供することも十分想定されるため、本書を参考にそれぞれの提供サービスの内容等に鑑みた利用を期待する。

２．本書の利用方法及び利用上の留意点

本書で示す参考例は、サービス提供に関して規定すべき項目について、診療所向け診療録の作成、保存等の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するも

のである。したがって、個々の条項について、提供するサービスの内容や医療機関等とASP･SaaS 事業者との役割分担の範囲等に応じ、または契約当事者間の交渉により、この参考例の内容が変更若しくは削除されまたは新たな条項が追加されることも当然に予定しているものである。上述のとおり、本書はあくまでも参考例として条項案を提示したものであり、その条項案に基づき、当事者間で契約されたそれぞれの契約書や SLA に関する責任の所在は、あくまでも契約当事者にある。

なお、本参考例では、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。

３．本 SLA 参考例で用いる用語の定義

本 SLA 参考例で用いる用語のうち、厚生労働省ガイドラインで使用されている以下の用語については、「医療情報システムを安全に管理するために『医療情報システムの安全管理に関するガイドライン』すべての医療機関等の管理者向け読本」（厚生労働省、平成 21 年３月）から引用した。また、「ASP・SaaS における情報セキュリティ対策ガイドライン」（総務省　平成 20 年１月　以下「情報セキュリティガイドライン」という）で定義されている以下の用語については、情報セキュリティガイドラインの「Ⅰ．９ 用語の定義」を踏襲した。

用語	用語の意味
真正性	正当な人が記録し確認された情報に関し、第三者から見て作成の責任の所在が明確であり、かつ、故意または過失による、虚偽入力、書き換え、消去、及び混同が防止されていることである。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。
見読性	電子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。ただし、見読性とは本来「診療に用いるのに支障が無いこと」と「監査等に差し支えないようにすること」であり、この両方を満たすことが、ガイドラインで求められる実質的な見読性の確保である。
保存性	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をいう。
盗聴	ネットワークに特異な事象ではなく、広く一般的に、意図的に第三者が会話や情報を盗み聞いたり、盗み取る行為。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）を盗み取る行為を指す。
窃視	一般的に、見ることが禁じられている、または同意されないと考えられるものを第三者が意図的に、覗いたり、盗み見たりする行為。情報漏洩との関係では、参照を許されている者が情報を参照している際に、参照等が許可され

用語	用語の意味
	ていない第三者が何らかの手段により、その内容を盗み見ることなどを指す。
改ざん	情報を不正に書き換える行為のこと。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、本来情報を受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 やパスワードを盗み出して、本人しか見ることができない情報を見たりする行為を指す。
機密性	認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性。
完全性	資産の正確さ及び完全さを保護する特性。
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。
情報資産	構成要素及び構成要素を介する情報
情報セキュリティ	情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。
リスク	事象の発生確率と事象の結果との組合せ。
リスク分析	リスク因子を特定するための、及びリスクを算定するための情報の系統的使用。
リスクアセスメント	リスク分析からリスク評価までのすべてのプロセス。
構成要素	ASP・SaaS サービスの提供に用いるハードウェア、ソフトウェア、通信機器・回線、建物等の固定資産。
情報セキュリティポリシー	情報セキュリティに関する組織的取組についての基本的な方針及び情報セキュリティ対策における具体的な実施基準や手順等の総称。
利用者	ASP・SaaS サービスを利用する法人又は個人。
連携 ASP・SaaS 事業者	自らの ASP・SaaS サービスに他の ASP・SaaS サービスを組み込むことにより、アプリケーション間の統合・連携を実施する際に、他の ASP・SaaS サービスを提供する ASP・SaaS 事業者。
外部組織	連携 ASP・SaaS 事業者や ASP・SaaS 事業者からサービスの一部を委託された企業等、ASP・SaaS サービスの提供に当たり契約関係のある組織の総称。
ユーザサポート	ASP・SaaS サービスに関する問い合わせ窓口（ヘルプデスク）と ASP・SaaS サービスの品質や継続性を維持するための組織の総称。
情報処理施設	ASP・SaaS 事業者がサービスを提供するための設備が設置された建物。
物理的セキュリティ境界	情報処理施設の特定の領域を保護するために設置される壁、カード制御による出入口等の物理的な仕切り。

サーバ・ストレージ	ASP・SaaS サービスを提供する際に利用するアプリケーション等を搭載する機器及びアプリケーション上の情報を蓄積・保存するための装置の総称。なお、付随する OS 等の基盤ソフトウェア、蓄積されているデータ・ログ等の情報を含む。
プラットフォーム	認証、決済等の付加的機能を提供する、ASP・SaaS サービスで提供されるアプリケーションの基盤。
通信機器	ルータ、スイッチ等、通信を制御するための装置。
情報セキュリティ対策機器	ファイアウォール、IDS 等、コンピュータウイルスや不正アクセス等の情報セキュリティ事象から、ASP・SaaS 事業者の設備を防護するための機器。
外部ネットワーク	情報処理施設とその外部とを結ぶネットワークの総称で、ASP・SaaS 事業者と ISP 間、ASP・SaaS 事業者と連携 ASP・SaaS 事業者間、ASP・SaaS 事業者の保守管理用回線等を指す。本ガイドラインの対象外である、利用者が契約する通信回線及びインターネット・サービスは除く。
SLA	ASP・SaaS における SLA(Service Level Agreement) とは、サービス提供事業者とサービス利用者が ASP・SaaS の利用契約を締結するに当たり、両者がサービス及びサービスレベルについて合意した内容を明文化したものである。

II. 参考例編

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【ASP・SaaS 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、ASP・SaaS 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、いわゆる電子カルテを ASP・SaaS として提供すること、そのサービスの対象は診療所であることを明示している。

・ASP・SaaS の提供目的等により、医療機関等及び ASP・SaaS 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。

・ASP・SaaS 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、ASP・SaaS 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　提供サービス構成」を参照のこと。

(1) ASP・SaaS

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 ASP・SaaS 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、ASP・SaaS 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 ASP・SaaS 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。
・ASP・SaaS では、ASP・SaaS 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、ASP・SaaS 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、ASP・SaaS 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 ASP・SaaS 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。ASP・SaaS 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、ASP・SaaS 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）の意義は下記のとおりである

(1) ASP・SaaS 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、ASP・SaaS 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。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。したがって

・診療録の作成、表示、保存において改ざん等のリスクが極小となるようなサービス品質を想定すること
・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が極小となるサービス品質を想定すること
・万が一利用不能となる事態が生じた際に、速やかに復旧可能となる、あるいは代替措置が講じられる内容も想定すること

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)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

本合意書の適用期間は、下記のとおりとする。なお、本合意書は、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 22 年 4 月 1 日（契約開始日）	平成 23 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、ASP・SaaS 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、ASP・SaaS 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し、必要都度実施する方法と、改定期間を示さずに必要に応じて都度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 ASP・SaaS として提供することに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 リスク評価

本サービスの提供において、乙は、乙が行うリスク評価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評価は、乙は年次及び乙が必要と認める場合に評価を実施する。

本項で示す乙の行うリスク評価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、リスク評価を実施して行う旨を示す。

・医療情報の取扱いに関しては、厚生労働省ガイドラインにおいて医療機関等は情報システムで取り扱う際に、リスク分析を行うこととされ（厚生労働省ガイドライン 6.2 C.）、これを基にして各安全対策を講じることとされている。

・ASP・SaaS を利用し、医療情報を取り扱う場合には、ASP・SaaS 事業者は、医療機関等が行うリスク分析に対応する形で対策を講じることが求められる。したがって、ASP・SaaS 事業者においても、医療情報を取り扱う際のリスク評価を行い、これに応じた安全対策が求められ、その内容は医療機関等が定める内容を満たしていることが必要である。

・この観点からサービス提供の前提条件として、ASP・SaaS 事業者においてリスク評価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。

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３　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。

別添 A 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、別添に規定する方式を採用している（本書では「別紙３」に該当するものは添付していない)。

・ASP・SaaS の場合、多くは Web ブラウザー等が使用されるが、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 やブラウザーの製品名、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、若しく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 ASP・SaaS 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、ASP・SaaS 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、ASP・SaaS 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、上記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。
・医療情報を取り扱う ASP・SaaS に供する機器等については、ASP・SaaS 事業者向け医療情報安全管理ガイドラインにより、国内法の適用が及ぶ場所に設置することが求められる（ASP・SaaS 事業者向け医療情報安全管理ガイドライン 3.2.8）。上記例第 2 段落はこの内容を示すものである。
・上記例第 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。
・上記例第 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。

・第5段落では、ASP･SaaS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、ASP･SaaS 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。
・品質管理については、ASP・SaaS 事業者向け医療情報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求められている。
・本例では、同ガイドラインの記述内容に準じた対応を ASP･SaaS 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。ASP・SaaS 事業者によっては、ISO9001 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 5 月 30 日法律第 57 号）
・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　1.1 版（総務省　平成 22 年 10 月）
・ASP・SaaS における情報セキュリティ対策ガイドライン（総務省　平成 20 年 1 月 30 日）
・医療情報を受託管理する情報処理事業者向けガイドライン（平成 20 年 7 月 24 日経済産業省）

なお、上記ガイドラインの遵守は、下記の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ドライン（厚生労働省　平成 16 年 12 月 24 日通達、平成 18 年 4 月 21 日改正）
・医療情報システムの安全管理に関するガイドライン　第 4.1 版（厚生労働省　平成 22 年 2 月）

乙は、甲から受託する個人情報につき、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、5,000 件未満の個人情報、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、ASP・SaaS 事業者が遵守すべき法令及びガイドラインについて明示する。
・ASP・SaaS 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 3 つの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 2 つのガイドラインについても、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、5,000 件未満の個人情報を保有する事業者は、個人情報保護法の適用対象となる「個人情報取扱事業者」に当たらないとされている。また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、機微性にかんがみると、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対策を講じる必要性は変わらない。ASP・SaaS 事業者向け医療情報安全管理ガイドラインでは、この趣旨から、これらの場合についても個人情報保護法の取扱いに準じて対応すべき旨が示されている。本項第 3 段落は、上記趣旨を明示している。

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程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若しくは連携 ASP･SaaS 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、ASP・SaaS 事業者の負うべき守秘義務に関して、ASP・SaaS 事業者が使用する従業員や再委託事業者、連携 ASP・SaaS 事業者に対する具体的な守秘義務について明示する。
・ASP・SaaS 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 ASP・SaaS 事業者が使用する従業員や再委託事業者、連携 ASP・SaaS 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、ASP・SaaS 事業者向け医療情報安全管理ガイドラインにおいても示されており（3.2.6 等）、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、ASP･SaaS 事業者が実施する監査について明示する。

・厚生労働省ガイドラインでは、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)。ASP・SaaS 事業者向け医療情報安全管理ガイドラインにおいてもこれを受けて、ASP･SaaS 事業者への要求事項として同様の内容を規定している（3.2.1)。

・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、ASP･SaaS 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、ASP･SaaS の特殊性から、報告方法については、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。

・ASP･SaaS 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。

・ASP･SaaS 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 ASP・SaaS を活用する場合等がある。

・本項では ASP･SaaS 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 ASP・SaaS 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。

・ASP･SaaS 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 ASP･SaaS の利用や、当該 ASP･SaaS 事業者が関与しない ASP･SaaS 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、ASP･SaaS 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、ASP･SaaS 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、甲の連絡若しく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、及び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、及び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、ASP･SaaS 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、ASP･SaaS 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、ASP･SaaS 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、ASP･SaaS 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、下記以外については、甲と乙で協議の上、対応を行う。

・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。
・厚生労働省ガイドラインでは、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、ASP・SaaS 事業者が提供するサービスにおいて利用できない場合、若しくは逆に ASP・SaaS 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、ASP・SaaS 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、ASP･SaaS 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、ASP･SaaS 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、及び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 ASP･SaaS 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 ASP･SaaS 事業者に対して申請して、発行する形を想定している。ASP･SaaS 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。ASP･SaaS 事業者のサービスによっては、ASP･SaaS 事業者が設定することも想定される。サービス内容にしたがって変更されることを想定する。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、ASP･SaaS 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。

・患者に対する説明は、厚生労働省ガイドラインでは、個人情報の保管・管理状況等や、情報漏えい等が生じた場合に、医療機関等が患者に対して説明を行うことを求めている（8.1.3 等）。ASP･SaaS 事業者は、医療情報の取扱いについて受託する場合、この責任を医療機関等と分担することが想定され、この趣旨から ASP・SaaS 事業者向け医療情報安全管理ガイドラインにおいても ASP･SaaS 事業者に対しては、医療機関との役割分担を協議し、必要な資料等の提供を行う旨を求めている（3.3.5(2)等）。

・本例では、ASP･SaaS 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、ASP･SaaS 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、ASP･SaaS 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 ASP・SaaS 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対策管理業務

・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 ASP・SaaS 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 ASP・SaaS 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 ASP・SaaS 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 ASP・SaaS 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 ASP･SaaS 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、ASP･SaaS 事業者が行う業務の再委託事業者及び連携 ASP・SaaS 事業者について明示する。

・ASP･SaaS 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 ASP･SaaS の提供を行わず、自らは契約主体となるだけで、ASP･SaaS の提

供を専ら連携 ASP･SaaS に委ねて者についても、本書では「ASP･SaaS 事業者」に当たるものとし、ASP･SaaS 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、ASP･SaaS 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、安全管理の必要性が高いことから、利用者である医療機関等においても、再委託先については関心事となる。したがって、再委託の事実だけではなく、再委託先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 ASP･SaaS 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、他の業務を行う場合も想定される。ASP･SaaS 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。

・ASP･SaaS 事業者間の連携は、他の事業者が提供する ASP･SaaS 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、ASP･SaaS 事業者は再委託事業者に関する情報と同様の内容を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、特定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、連携 ASP･SaaS 事業者が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 ASP･SaaS 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 ASP･SaaS 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 ASP･SaaS 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 ASP･SaaS 事業者に対して、ASP 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 ASP･SaaS 事業者を用いる場合、それらの事業者の情報についても、ASP･SaaS 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、ASP･SaaS 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、ASP･SaaS 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：　　【ASP・SaaS 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。

【ASP・SaaS 事業者側ヘルプデスク窓口】(通常業務時間)

【ASP・SaaS 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 ASP・SaaS 事業者との連絡体制について明示する。

・本例では、医療機関等側の責任者と ASP・SaaS 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。

・ASP・SaaS 事業者が提供するサービスにおいて、連携 ASP・SaaS 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 ASP・SaaS 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 ASP・SaaS 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。

・ASP・SaaS 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、乙は巻末別表の「不正アクセス」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対策を実施する。

本項で示すネットワーク経路の安全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対策の実施が求められる（例えば、6.11 C 等）。医療機関等が医療情報を ASP・SaaS 事業者に寄託する場合、ASP・SaaS 事業者向け医療情報安全管理ガイドラインでは ASP･SaaS 事業者の運用において必要なネットワーク経路における安全対策を講じることを求めている（例えば、3.2.9)。

・そこで、本 SLA 参考例では、上記の趣旨を反映した運用内容を巻末別表「ネットワーク経路上の安全対策」に示し、ASP･SaaS 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対策の実施を行う旨を明示している。

・また、ASP･SaaS 事業者の実施するネットワーク経路の安全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、ASP・SaaS 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、乙は巻末別表の「不正アクセス」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、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（例えば、6.11 C、7.1 C 等）。医療機関等が医療情報を ASP・SaaS 事業者に寄託する場合、ASP・SaaS 事業者向け医療情報安全管理ガイドラインでは ASP･SaaS 事業者の運用において不正アクセス対策を講じることを求めている（例えば、3.2.9)。

・そこで本 SLA 参考例では、上記の趣旨を反映した運用内容を巻末別表「不正アクセス対策」に示し、これを ASP･SaaS 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、ASP･SaaS 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、ASP･SaaS 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、乙は巻末別表の「アクセス制御」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、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（例えば、6.5 C、7.1 C 等）。医療機関等が医療情報を ASP・SaaS 事業者に寄託する場合、ASP・SaaS 事業者向け医療情報安全管理ガイドラインでは、ASP･SaaS 事業者の運用においてアクセス制御を講じることを求めている（例えば、3.2.3)。

・そこで本 SLA 参考例では、上記の趣旨を反映した運用内容を巻末別表「アクセス制御」に示し、これを ASP･SaaS 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。

・また、ASP･SaaS 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、ASP・SaaS 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、複数の担当業務若しくは職種に関するアクセス権限を設定できること。
・甲が利用する、複数の担当業務若しく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、法令に基づいて職種等の法律上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 参考例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 ASP・SaaS 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（ASP・SaaS 事業者向け医療情報安全管理ガイドライン 3.3.2）。
・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た。
・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、ASP・SaaS 事業者は、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、ASP・SaaS 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

本サービスの利用者認証において、甲と乙は協議の結果、電子署名による認証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表 1 の内容を満たす。

表 1　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 認証局の発行する電子証明書、若しくは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 ・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、利用者認証に電子署名を採用する場合の仕様等について明示する。

・電子署名認証法では、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。そして厚生労働省ガイドラインでは、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)。

・診療録は、上記で示す「法令で署名または記名・押印が義務付けられた文書等」には当たらないため、上述の電子署名による署名を採用することは必須とされない。ただし、診療録だけではなく、診療情報提供書など記名押印が求められる書類の作成を提供サービスに含める場合には電子署名機能を提供する必要があり、保健医療福祉分野 PKI 認証局の仕様に準じた電子署名に準じた仕様を採用することを例示している。

・本サービスで電子署名を利用者認証に採用する場合、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、ASP・SaaS 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者用の ID 及び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。

本サービスの提供に際して、乙は巻末別表の「アクセス制御」に示す事項を実施することにより、診療記録の確定における安全性を確保する。

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。
・記録の確定については、ASP・SaaS 事業者向け医療情報安全管理ガイドラインでは、記録を確定した代行操作者及び作成責任者が特定できることが求められる（3.3.2)。
・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、作成責任者若しく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、ASP・SaaS 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。
・診療記録のデータの更新履歴管理については、ASP・SaaS 事業者向け医療情報安全管理ガイドラインにおいて、記録の更新につき、その履歴管理ができることが求められている。
・診療録の作成等を電磁的記録により行う場合には、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(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。ASP・SaaS 事業者向け医療情報安全管理ガイドラインでもこの趣旨を受けて、上述の要求事項を定義している。
・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、運用による ASP･SaaS 事業者対応も想定される。
・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、原因の究明、警察等への通報、データの回復措置等などが想定される。
・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、ASP・SaaS 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き、乙は、予告の上、適宜変更を行う。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、甲の連絡若しくは自己の判断に基づき、調査し、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若しくは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。

・電磁的記録による場合には、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おり、ASP・SaaS 事業者向け医療情報安全管理ガイドラインでもこの趣旨を受けて要求事項を定義している。

・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、ASP･SaaS 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 参考例では ASP･SaaS 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、ASP･SaaS 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。本例での記述はあくまでも ASP・SaaS 事業者向け医療情報安全管理ガイドラインで要求事項とされる最低限の内容を示すものであり、その他 ASP･SaaS 事業者の対応にしたがって記述することが求められる。

・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、ASP･SaaS 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業務において、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、医療機関において代替的措置を講じられる対応をとれる内容と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、ASP･SaaS 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、巻末別表「不正アクセス対策」及び「受託情報の管理」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、及び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、必要な措置を講じた上で、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。
・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、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)。ASP・SaaS事業者向け医療情報安全管理ガイドラインでもこの趣旨を受けて、ウイルス対策に関する要求事項を定義している。
・本SLA参考例では、ASP･SaaS事業者がサービス提供にあたって講じるべきデータの破壊防止対策について、巻末別表「不正アクセス対策」及び「受託情報の管理」の中で、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、ASP･SaaS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、ASP･SaaS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、ASP・SaaS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

本サービスの運用に供する乙の施設において、乙は、巻末別表「定期監視」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。
・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（7.3 B)。ASP・SaaS 事業者向け医療情報安全管理ガイドラインでもこの趣旨を受けて、データの劣化、滅失対策に関する要求事項を定義している。
・本 SLA 参考例では、ASP･SaaS 事業者がサービス提供にあたって講じるべきデータの劣化、滅失防止対策について、巻末別表「定期監視」の中で、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、ASP･SaaS 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。
・また、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 ASP･SaaS 事業者に対して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。本例は、あくまで例示であり、データ転送中のトラブルへの対応方法については、各 ASP･SaaS 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、ASP・SaaS 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4.1版」の「5情報の相互運用性と標準化について」にしたがって実施する。

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。
・厚生労働省ガイドラインでは、媒体・機器･ソフトウェアの整合性不備による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（7.3C)。ASP・SaaS事業者向け医療情報安全管理ガイドラインでもこの趣旨を受けて、データ仕様に関する要求事項を定義している（3.3.4)。
・本例では、ASP･SaaS事業者が採用するデータ仕様について、厚生労働省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。ASP･SaaS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もしく手順を講じる等による等が想定される。
・本サービスにおけるASP･SaaS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、ASP・SaaS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、ASP・SaaS 事業者の運用体制を明示する。

・本例では、ASP・SaaS 事業者の運用体制図を示す形をとっている。

・医療情報を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が求められる（厚生労働省ガイドライン 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、ASP・SaaS 事業者の運用管理体制を明示することが求められる。

・ASP・SaaS 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 ASP・SaaS 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の考え方を明示する。

・厚生労働省ガイドラインでは、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、ASP・SaaS 事業者においても、情報セキュリティ対策ガイドラインにより、情報資産の運用管理の文書化が求められる（情報セキュリティ対策ガイドラインⅡ.4.1.1)。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 ASP・SaaS 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、ASP・SaaS 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内容で、ASP・SaaS 事業者の運用管理規程等と内容が異ならない部分は、ASP・SaaS 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内容で、ASP・SaaS 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 ASP・SaaS 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 ASP・SaaS 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、ASP・SaaS 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 乙規程等に含む運用管理項目

巻末別表に、乙規程等に記述される運用管理項目等を挙げる。これらの項目は３．５に掲げる法令、ガイドライン等において、乙規程等に含むことが求められるものであり、これに基づいて、乙は、本サービスに係る運用を実施する。

【本項を定める上での考え方】

・本項では、ASP・SaaS 事業者が運用管理規程等で文書化した上で対応すべき項目について明示する。

・巻末別表の各項目については、ASP・SaaS 事業者向け医療情報安全管理ガイドラインで文書化を行い、運用することが求められているものである。

・巻末別表では、各項目に備考欄を設けている。これは、各項目に記述されている内容につき、ASP･SaaS 事業者により記述することを予定するものである。例えば、各項目に記述されている運用事項について、代替する方式により同程度若しくはそれ以上の安全対策を講じている場合に、その内容を記述すること等が想定される。

③ 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）

④ 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、巻末別表に示す事項に関す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

⑤ 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、ASP･SaaS 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 ASP・SaaS 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 ASP･SaaS 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

本サービスで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、独自に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、ASP･SaaS 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 ASP･SaaS 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、ASP･SaaS 事業者は医療機関等に対して必要な説明を行い、医療機関等において不測の混乱が生じないように留意することが求められる。

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、ASP･SaaS 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 ASP・SaaS 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 ASP・SaaS 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、乙は巻末別表「受託情報の管理」に示す内容を実施することにより、管理を行う。

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、ASP･SaaS 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 参考例では、ASP･SaaS 事業者が行うべき受託情報の管理について、巻末別表「受託情報の管理」に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、ASP･SaaS 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、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（例えば、6.7 C、6.9 C 等)。そのため医療機関等は ASP・SaaS 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。そこで本例は、医療機関等からの要請があった場合に、ASP・SaaS 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 4.1 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若しく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 ASP･SaaS 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。
・ASP･SaaS 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。
・ASP･SaaS 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、厚生労働省ガイドラインの「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 4.1 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若しく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、ASP･SaaS 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 ASP･SaaS 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 ASP･SaaS 事業者で協議して決める旨を明記している。ASP･SaaS 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、ASP･SaaS 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、乙は巻末別表「物理的セキュリティ」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物理的セキュリティを確保する。

本項で示す物理的セキュリティ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、ASP･SaaS 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、厚生労働省ガイドラインにより物理的安全対策の実施が求められる（例えば、6.4 C 等)。そのため医療機関等が医療情報を ASP・SaaS 事業者に寄託する場合、ASP・SaaS 事業者向け医療情報安全管理ガイドラインでは ASP･SaaS 事業者の運用において必要な物理的安全対策を講じることを求めている（例えば、3.2.2)。
・そこで本 SLA 参考例では、上記の趣旨を反映した運用内容を巻末別表「物理的セキュリティ」に示し、これを ASP･SaaS 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 ASP･SaaS 事業者の実施する物理的セキュリティ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、ASP・SaaS 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窃視防止措置の実施
・バックアップデータにつき、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。

【本項を定める上での考え方】

・本項では、ASP･SaaS 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、ASP･SaaS 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 ASP･SaaS 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 ASP･SaaS 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。
・本例で示した報告項目は、あくまでも例示であり、ASP・SaaS 事業者向け医療情報安全管理ガイドラインにおいて要求事項として示されている内容である。したがって ASP･SaaS 事業者において必要とされる項目について、追記することが想定される。
・また ASP･SaaS 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、ASP・SaaS 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．「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、乙による感知若しく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（項目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。

・ASP･SaaS 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、ASP・SaaS 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、ASP・SaaS 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、サービス稼働率及び、問題

管理対応時間等、また、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 ASP･SaaS 事業者がサービス提供上必要とされる可用性に項目や指標について、追記することが想定される。

・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、ASP･SaaS 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。ASP･SaaS 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。

・ASP･SaaS 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、ASP・SaaS 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、乙は取得後 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、ASP･SaaS 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 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。ASP・SaaS 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、ASP･SaaS 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。ASP･SaaS 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。
・ASP･SaaS 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、ASP・SaaS 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、乙は巻末別表「非常時対応」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。

・【http://+++.****.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 ASP･SaaS 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、ASP･SaaS 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。ASP･SaaS 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、ASP･SaaS 事業者が行うものとして示している。
・ASP･SaaS 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、ASP・SaaS 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、ASP･SaaS 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。

・ASP･SaaS 事業者から医療機関等に対してなされる報告は、これを通じて医療機関等が医療機関等に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、不正に使用がなされていないこと等を確認でき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 ASP･SaaS 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、ASP･SaaS 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
・巻末別表「要員教育」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、ASP･SaaS 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、妥当な委託先と契約をしていること、また、継続してよいかの確認をする必要があることから、ASP･SaaS 事業者は、自身の運用の信用に係る情報や、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。特に外部保存を伴うサービスでは、厚生労働省ガイドラインにおいて、契約開始段階で一定の条件を満たした事業者であ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、定期的に条件を満たしていることを確認することが求められていることを認識しなくてはならない。
・上記の観点から、本例では、ASP･SaaS 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、ASP･SaaS 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、ASP･SaaS 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 発生都度報告事項

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、発生都度、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、乙が受託する個人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、保守作業を実施結果
・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、ASP･SaaS 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 ASP･SaaS 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、ASP･SaaS 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、メール若しくは書面により直接、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、書面若しく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 書面また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、乙が受託する個人情報を参照した際の作業結果

② 書面また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、メール若しくは書面により直接、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若しくは暗号化を施した電子メールに限定することを明示する。

・本項(1)で示した報告項目は、あくまでも例示であり、ASP･SaaS 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 文では、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、ASP・SaaS 事業者により可変されることを想定している。

・第 2 文は、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、速やかに正常なサービス提供を回復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、メール若しくはサービス利用画面等で行うことが望ましい。

・第 3 文は、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。なお、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
・乙が業務上、受託した情報を組織外に持出し、また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 文前段では、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 ASP･SaaS 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 ASP･SaaS 事業者のサービス内容によっては、医療機関等が ASP･SaaS 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 文後段は、前段の原則に対する例外を明示している。
・ASP・SaaS 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、等の利用者側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 文では、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、ASP・SaaS 事業者向け医療情報安全管理ガイドラインにおいて求められる内容である。上記の観点から、ASP・SaaS 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。

・厚生労働省ガイドラインは、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ASP･SaaS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、事後報告だけで済む保守内容、事前告知及び事後報告で済む保守内容、事前承認・事後承認を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、ASP･SaaS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 や Web ブラウザー、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及び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は含まない）
・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。
・ASP・SaaS 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。
・ASP・SaaS 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 ブラウザー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 やブラウザー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、ASP･SaaS 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。

・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 ASP･SaaS 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。
・本 SLA 参考例では、ASP・SaaS 事業者が講じるべき安全対策のうち、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、３．５に示す法令・ガイドラインを満たす対応を実施する、という表現を採用している。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 ASP・SaaS 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、変更都度資料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、ASP・SaaS 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。
  ✓ASP・SaaS 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。

  という記述をしている。
・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、ASP・SaaS 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。
・本例では、巻末別表に記述する各項目について、ASP・SaaS 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 ASP・SaaS 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。
  ✓ASP・SaaS 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。
  という記述をしている。
・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、ASP・SaaS 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及び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
・巻末別表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ASP・SaaS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ASP･SaaS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巻末別表の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、ASP･SaaS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。ASP･SaaS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及び 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。
巻末別表に示す事項の実施状況	実施していない事項ごとに、年次で 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、サービスの内容や性格等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、巻末別表に示す事項について、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、ASP･SaaS 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。ASP･SaaS 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、ASP･SaaS 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、ASP･SaaS 事業者、医療機関等の両当事者に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。ASP･SaaS 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 ASP･SaaS 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、ASP･SaaS 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、ASP･SaaS 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。ASP･SaaS 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 で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 に評価になった場合で、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。

・巻末別表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、ASP･SaaS 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、ASP･SaaS 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。ASP･SaaS 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。

巻末別表　乙の運用管理規程等に記述されている事項

	実施項目	備考
物理的セキュリティ	サーバルーム及びラック等の鍵管理の実施	
	受託する個人情報を格納するサーバ以外の機器等が設置されている部屋の鍵管理の実施	
	受託する個人情報を格納する記録媒体等の鍵管理の実施	
	受託した個人情報データが格納されているサーバルーム、データセンター等に関する入退館管理の実施及び記録の作成	
	受託する個人情報を参照可能な事務室等における入退室管理の実施及び記録の作成	
	受託する個人情報データの記録媒体の保管場所に関する自社の入退室管理の実施及び記録の作成	
	受託する個人情報を参照できる端末が設置されている区画若しくはサーバルーム等への入退室できる者の制限	
	受託する個人情報を格納するサーバルーム等の重要な物理的セキュリティ境界に監視カメラを設置等及び監視・その記録の作成と保存	
	受託する個人情報を参照できる端末のクリアスクリーン等の実施	
	受託する個人情報を格納するデータベースの暗号化等の実施	
	受託する個人情報を参照できる端末につき、窃視防止措置の実施	
アクセス制御	受託するデータの区分設定に応じた管理内容（利用責任者、利用可能者、利用目的、利用方法、返却方法等）	
	受託する情報の区分に応じたアクセス制御の実施	
	情報システム管理者、ネットワーク管理者のアクセス制限	
	サービスの利用者及び管理者のアクセス制御のための利用者識別及び認証の実施	
	パスワード入力の運用に関するポリシー	
	パスワード入力の運用につき、下記の措置の実施 ・パスワード入力が不成功に終わった場合の再入力に対する一定不応時間の設定 ・パスワード再入力の失敗が一定回数を超えた場合の再入力を一定期間受け付けない機構の採用	
	利用者及び管理者の ID,パスワード等について、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、それらの情報を、本人しか知り得ないようにするための措置（ハッシュ値等）	
	利用者の関係職種ごとの診療録等へのアクセス制御の内容等	
	サービス提供に供する機器に関する時刻同期の実施及びその手順等	
	採用する認証方法における仕様（複数の要素を組み合わせる、認証強度が高い方式を採用する等）	
	利用者のアクセスコントロールに関する手順	
	管理者及び運用者において、受託情報への入力操作に関する権限を必要最低限にする措置	

	実施項目	備考
	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措置	
ネットワーク経路上の安全対策	リモートメンテナンス用の通信経路を含むネットワーク構成図の作成・管理	
	情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するために、外部ネットワークを通じた情報交換の際の実施基準・手順	
	サービス提供に際する、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するための、通信の暗号化の実施	
	ASP・SaaS 事業者と医療機関等との間で送受信される情報に対して、ファイル等の暗号化等の措置の実施	
	サービス提供に供するネットワーク経路について、メッセージ挿入、ウイルス混入、パスワード盗聴、本文の盗聴等の防止措置の実施	
	医療機関等と ASP・SaaS 事業者等との、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の相手方の認証の実施及びその認証手段	
	APS・SaaS 事業者がサービス提供に用いるルータ等のネットワーク機器における、施設内のルータを経由して異なる施設間を結ぶ VPN の間の送受信を不能とする経路設定	
不正アクセス対策	アクセス制御に関する方針及びこれに基づく手順	
	アクセスログへのアクセス制御の実施、不当な削除や追加、改ざん防止等の措置の実施	
	・ASP・SaaS 事業者の管理者及び運用者におけるアクセス認証方法 ・リモートアクセスを用いる場合の回線及び認証方法 ・パスワード情報の保存方法（ハッシュ値の利用の有無等）	
	サービス提供に供する機器及びソフトウェアについて、技術的ぜい弱性に関する定期的な情報収集（OS、その他ソフトウェアのパッチ発行情報等）、随時パッチによる更新等	
	サービス提供に際して、セッション乗っ取り、IP アドレス詐称等のなりすましの防止措置の実施	
	外部からの侵入等を防ぐための不正な通過パケットの自動発見、若しくは遮断する措置（ID/IPS の導入等）の実施	
	サーバのなりすまし（フィッシング等）を防ぐために必要な対応策（サーバ証明書の取得等）の実施	
	VPN 等の閉域ネットワーク以外からの利用者に対する不正侵入を防止するためのアクセス制御の実施	
	安全性が確認できるルータ等のネットワーク機器の使用	
	４．３に示す事業者と ASP・SaaS 事業者の間でのなりすまし防止措置の実施	
受託情報の管理	紙、磁気テープ、光メディア等の媒体管理の実施	
	受託した各種情報資産の種別に応じた情報の消去及び廃棄の実施	
	受託した情報資産の管理方法の、業務に従事する者への周知	
	受託したデータを格納する機器、媒体の廃棄に関する手順等	
	受託したデータを格納する機器、媒体の廃棄に関する記録の作成・保存	
	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	

	実施項目	備考
	受託した情報資産を記録する媒体及び情報機器の取扱いに関する作業履歴を作成	
	受託した情報を業務上外部に持出す際の、媒体及び機器に対する適切なウイルス対策等の実施	
	受託したデータを組織外への持出し、若しくは再委託事業者への保存等を行う場合の手順、記録の収集等	
	ASP・SaaS 事業者側の受託した各種情報資産、並びにこれを格納機器の持ち出しの管理	
	受託した情報資産につき、下記の管理の実施 ・記録媒体が劣化以前に受託情報を新たな記録媒体又は記録機器への複写すること ・記録媒体及び機器毎の正常保存期間を明確にすること ・記録媒体、機器等の使用開始日、使用終了日を管理し、月に一回程度の頻度でチェックを行うこと ・使用終了日が近づいた記録媒体、記録機器等についての格納データを新たな記録媒体又は記録機器に複写すること。	
	受託した情報資産の持出し及び情報機器の管理	
	サービス提供に必要なシステム関係のドキュメント(契約書、サービス仕様書、カスタマイズ仕様書、テーブルフォーマット等）の適切な管理	
定期監視	サービスの提供に用いるサーバ・ストレージ、回線等の稼働監視、障害監視、パフォーマンス監視の結果の定期的な評価・総括、劣化等への対策	
	サービスに供す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、情報セキュリティ対策機器等の、通信機器の稼働監視（応答確認等）、通信機器のパフォーマンス監視（サービスのレスポンス時間の監視）の実施	
	サービス提供に使用する受託情報、及びシステム管理情報、構成情報等につき、定期的なバックアップの実施	
	バックアップに供する媒体及び機器の定期的に正常な書き込み及び読み出しができることの確認	
	サービス提供に供するネットワークの障害を監視し、障害を感知した場合の対応措置	
保守	システムの動作確認に際して原則的にテスト用のデータを使用する旨	
	システムの動作確認において、ASP・SaaS 事業者が受託した個人情報の使用する際の手順(手続等)	
	保守要員が用いるすべての ID において採用する認証方法	
	メンテナンスを実施するためにサーバに作業員がアクセスする際に用いるアカウント及びアクセス権限に関する発行・変更・削除等についての手順	
	保守要員の離職や異動時のアカウントの削除の手順	
	保守業務に携わる従業員の雇用が終了、若しくは変更となる場合のアカウント削除に関する手続等の手順	
	リモートメンテナンスによりシステムの改造・保守を行う場合のアクセスログ等の記録、及び方法	
	リモートにより行う顧客側のシステムの改造・保守の手順	

	実施項目	備考
	受託したデータの利用等を行う業務上利用する運用管理端末への導入プログラムの管理の実施	
	リモートメンテナンスのために行うリモートログインの適切かつ必要最小限の範囲での実施	
	サービス提供に供する機器、ソフトウェアの品質管理の実施手順	
	ASP・SaaS の提供に供するサーバ等の機器管理規程等	
要員教育	従業員の雇用終了、異動、業務替えに伴うアクセス権の管理	
	ASP・SaaS 事業者において従業員が業務上知り得た個人情報等に関する退職後の守秘義務	
	受託する個人情報を格納するサーバルーム等における従業員の行動についての管理	
	従業員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関する守秘義務の規定、違反時の罰則等の措置	
	従業者への個人情報の安全管理に関する定期的な教育訓練の実施	
	個人保有の情報機器への情報資産の持ち出しの原則禁止、例外的な個人保有の情報機器を利用する場合の手順	
	従業員が個人保有の情報機器への情報資産の持ち出し禁止等に関する規程に違反した場合の措置	
	受託した情報資産を記録する媒体及び情報機器の管理に関する業務に従事する者に対する教育の実施	
	サービス提供に供する機器、ソフトウェアの品質管理についての従業員への教育の実施	
非常時対応	非常時の BCP 運用手順	
	非常時から正常時復帰の対応手順	