別紙３

クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン

第１版

平成 30 年7月

クラウドサービス事業者が医療情報を
取り扱う際の安全管理に関する
ガイドライン
目次

第１章 本ガイドラインの前提条件及び読み方 1
１．１ 本ガイドラインの目的 1
１．１．１ 医療情報の特殊性とクラウドサービスの利用 1
１．１．２ 本ガイドラインの目的 4
１．２ 本ガイドラインで用いる用語の定義 5
１．２．１ 厚生労働省ガイドラインで使用されている用語 5
１．２．２ クラウドサービス提供における情報セキュリティガイドラインで使用されている用語 6
１．２．３ その他の用語 8
１．３ 本ガイドラインの対象範囲 11
１．３．１ 本ガイドラインが対象とする医療情報 11
１．３．２ 本ガイドラインが対象とするクラウドサービス 12
１．４ 他のガイドラインとの関係 19
１．５ 本ガイドラインの構成 21
第２章 クラウドサービス事業者が医療情報を取り扱う際の責任等 22
２．１ 医療情報を管理する医療機関等の責任 22
２．２ クラウドサービス事業者と医療機関等の管理者との責任分界の考え方 24
２．３ 医療機関等から委託を受けて医療情報の管理を行う場合におけるクラウドサービス事業者の責任 25
２．３．１ 通常運用における責任 25
２．３．２ 事後責任 28
２．３．３ クラウドサービス事業者間の責任分界 30
２．３．４ オンライン診療システムをクラウドサービスにより提供する事業者における責任分界 34
２．４ PHR サービスを提供する場合におけるクラウドサービス事業者の責任分界の考え方 34
２．５ 医療情報に関わるクラウドサービス事業者に関連する第三者認証の考え方 37
第３章 クラウドサービス事業者に対する安全管理に関する要求事項 38
３．１ クラウドサービス事業者に対する要求事項の考え方 38
３．１．１ 厚生労働省ガイドラインにおける安全対策の考え方の概要 38
３．１．２ クラウドサービス事業者が実施すべき内容 38
３．２ 医療情報サービスに求められる安全管理に関する要求事項 39
３．２．１ 組織的安全管理対策 39

３．２．２ 物理的安全管理対策 46
３．２．３ 技術的安全管理対策 54
３．２．４ 人的安全管理対策 80
３．２．５ 情報の破棄に関する安全管理対策 85
３．２．６ 情報システムの改造と保守に関する安全管理対策 88
３．２．７ 情報及び情報機器の持ち出しについての安全管理対策 99
３．２．８ 災害等の非常時の対応についての安全管理対策 107
３．２．９ 個人情報を含む医療情報を外部と交換する場合の安全管理対策 112
３．２．１０ 法令で定められた記名・押印を電子署名で行うことについての安全管理対策 122
３．３ 外部保存に関する要求事項 127
３．３．１ 外部保存に関する要求事項の趣旨 127
３．３．２ 外部保存に関する要求事項が求められる文書 127
３．３．３ 真正性の確保に関する要求事項 129
３．３．４ 見読性の確保に関する要求事項 133
３．３．５ 保存性の確保に関する要求事項 137
３．３．６ 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準 142
３．３．７ 個人情報の保護についての安全管理対策 147
３．４ クラウドサービスの利用終了に関する要求事項 149
３．４．１ クラウドサービスの利用終了における対応 149
３．５ オンライン診療システム提供事業者における安全管理対策 153
３．５．１ オンライン診療におけるセキュリティ上の要求事項 153
３．５．２ オンライン診療システム提供事業者における要求事項 153
３．６ PHR サービス事業者における安全管理対策 154
３．６．１ PHR サービス事業者への要求事項 154
３．６．２ PHR サービス事業者を適用対象とする要求事項 157
３．６．３ PHR サービス事業者を適用対象外とする要求事項 173
第４章 安全管理の実施における医療機関等との合意形成の考え方 174
４．１ サービス仕様適合開示書による情報提供 174
４．２ サービス仕様適合開示書により情報提供される内容 176
４．３ 契約、SLA 等の文書による合意 182
４．４ 合意における注意点 182
４．４．１ サービスレベルとコストに見合った提案 182
４．４．２ 医療機関等との責任分界の明確化 183
４．５ サービスレベルマネジメントの実践 184
（別添）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

第１章 本ガイドラインの前提条件及び読み方

本章では、本ガイドラインの目的、前提条件、使用する用語等について記述する。

１．１ 本ガイドラインの目的

１．１．１ 医療情報の特殊性とクラウドサービスの利用

（１） 医療情報の特殊性

一般的に個人情報は、一旦漏洩した場合に回復が困難なものであり、特に医療情報は患者の生命･身体に関わるほか、差別を受ける等、権利利益が侵害される可能性もあるため、高い保護方策が求められる。また、医療従事者が利用する医療情報の完全性が損なわれると、適切な医療行為が行われない危険性がある。そのため、医療機関等や関係者に対しては、罰則を伴う守秘義務が法律で課せられるほか、法令･各種のガイドライン等により格別の安全管理措置を講じることが求められている。

この観点から、医療機関等向けに「医療情報システムの安全管理に関するガイドライン」（以下「厚生労働省ガイドライン」という。）が策定されており、医療情報を取り扱う情報システムを利用する際には、厚生労働省ガイドラインの安全管理対策を講じることが求められる。

医療機関等が対応すべき安全管理対策は、医療機関等から委託を受けた事業者においても、同様の対策を講じる必要がある。

（２） 医療情報の取扱いにおけるクラウドサービスの意義

他方、医療情報の取扱いにおいて、クラウドサービスの利用も普及しつつある。情報システム管理を行う要員が十分確保できない医療機関等においては、適切に管理されたクラウドサービスを利用することにより、医療機関等の内部で医療情報の保存、管理を行うのに比べて、より安全かつ効率的に管理することが期待できる。

クラウドサービスにおいて医療情報を取り扱う場合は、低コストで高いセキュリティを実現することが重要である。また、クラウドサービスは、当初は ASP･SaaS という形で利用されることが多かったが、仮想化技術の進展などもあり、PaaS、IaaS 等、多様な形で提供されるようになってきた。

また、医療機関等は、クラウドサービスを活用することにより、医療情報連携ネットワークやオンライン診療等、新しい形での医療情報の利活用を、低コスト及び高セキュリティで実現できるようになると考えられる。

（３） クラウドサービス事業者向けのガイドラインの必要性

（１）で示したように、医療機関等による委託に基づいて医療情報を取り扱うクラウドサービス事業者は、厚生労働省ガイドラインに示される安全管理対策を講じる義務を、医療機関等を通じて間接的に負うことになる。そのため、この場合のクラウド

サービス事業者が負う義務の範囲は、医療機関等との契約内容等に依存するところが大きい。

その一方で、クラウドサービスの性格上[1]、医療機関等は、クラウドサービス事業者が提示する医療情報システムの安全管理対策の内容に一定程度対策を委ねざるを得ないケースも生じる。

そこで、クラウドサービス事業者が厚生労働省ガイドラインに準拠したサービスを提供するために、クラウドサービス事業者に対して、必要な安全管理対策を講じるためのガイドラインを直接示す必要がある。

これによりクラウドサービス事業者に、厚生労働省ガイドラインで示す内容に準拠した安全管理対策を講じる直接的な責任を生じさせ、医療機関等が安心してクラウドサービスを利用できる環境が整備される。

（４） クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドラインの策定

（３）に示す観点から、クラウドサービスのうち、当時普及が進んでいた ASP・SaaS について、平成 21 年 7 月に「ASP･SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（以下「総務省 ASP 医療ガイドライン」という）」第 1.0 版が策定された。これは、厚生労働省ガイドラインにおける医療機関等に対する要求事項に対応する形で、クラウドサービス事業者が医療情報を取り扱うサービスを提供する際に安全性の観点から求められる要求事項を示したものである。クラウドサービス事業者が、総務省 ASP 医療ガイドラインを遵守することで、医療機関等に対して、医療情報を適切に取り扱う安全なサービスを提供していることを示せるようにした。

これを踏まえて平成 22 年 2 月に厚生労働省より「『診療録等の保存を行う場所について』の一部改正について」[2]（以下「外部保存改正通知」という。）が示され、診療録等の医療情報を民間事業者が運用するサービスを利用して外部保存することが許容された。

その後、総務省 ASP 医療ガイドラインは、平成 22 年 12 月に第 1.1 版に改定され、クラウドサービス事業者が医療情報を取り扱う際の指針として活用されてきた。

---

[1] クラウドサービスでは、一般的に多数の利用者を対象としてサービス提供をすることを想定していることから、個々の利用者が、個別の状況に従った形で、サービスの内容を調整することができないケースが多い。

[2] 平成 22 年 2 月 1 日　医政発 0201 第 2 号／保発 0201 第 1 号

（５） クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン策定の意義

総務省 ASP 医療ガイドライン第 1.1 版を策定した当時は、医療情報を取り扱うクラウドサービスは、現在のクラウドサービスのうち、ASP･SaaS が中心であった。したがって、総務省 ASP 医療ガイドライン第 1.1 版では ASP･SaaS がクラウドサービスの代表例として取り扱われていた。しかし（２）で示したように、今日では ASP･SaaS のほか、PaaS、IaaS 等、様々なレイヤーのクラウドサービスが提供されている。また、プライベートクラウド、パブリッククラウド、ハイブリットクラウドなど、多様な実現形態が存在している。加えて、それぞれのサービスは、必ずしも１社で提供するとは限らず、複数の事業者が相互に連携して提供されることも多くなっている。

このような状況を踏まえ、医療機関等が安心してクラウドサービスを利用できるようにするため、事業者向けのガイドラインも、ASP･SaaS 事業者だけではなく、広くクラウドサービス事業者を対象とする旨を明示するほうが適切である。

さらに、平成 29 年には、改正個人情報保護法の施行に併せ、医療･介護分野における個別の対応を記した、「医療･介護関係事業者における個人情報の適切な取扱いのためのガイダンス」が策定されたほか、厚生労働省ガイドラインも改定され、第 5 版[3]として内容面でも大きな変更が行われた。

このようなクラウドサービスの多様化や、それを支える技術の進展、各種の法令等の改正等を背景に、総務省 ASP 医療ガイドラインについても改定し、「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（以下「本ガイドライン」という。）として公表することとした。

[3] 「医療情報システムの安全管理に関するガイドライン第 5 版」（厚生労働省　平成 29 年 5 月）

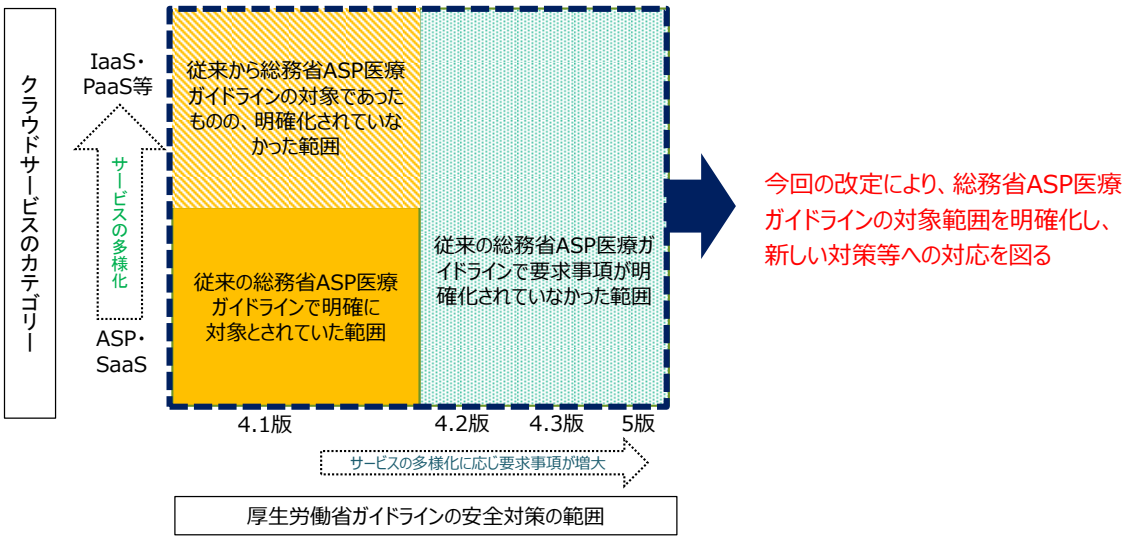


図 1　本ガイドライン策定の意義

策定当時の総務省 ASP 医療ガイドラインは、提供されていたサービスの中心であった ASP･SaaS に焦点を当てて策定された。総務省 ASP 医療ガイドラインの内容は、ASP･SaaS 以外のクラウドサービスの類型に対しても適用しうるものであったが、クラウドサービスが多様化する中で、その旨が必ずしも明らかではなかった。また厚生労働省ガイドラインが改定を重ねる中で、新規に設けられた厚生労働省ガイドライン第 5 版の条項に対応する事業者側への要求事項についても不明確な点や不足している点があった。本ガイドラインにより、これらを改善することとした（図 1）。

１．１．２　本ガイドラインの目的

本ガイドラインでは、１．１．１に示す医療情報の特殊性から来る高度な安全性の要求を踏まえ、クラウドサービス事業者が医療情報を取り扱う際に求められる責任、安全管理対策、医療機関等との合意形成の考え方等を示す。

本ガイドラインでは上記を通じて、クラウドサービス事業者が医療情報を適正かつ安全に取り扱うことにより、医療情報におけるクラウドサービスの利用の促進を図ることを目的とする。

１．２ 本ガイドラインで用いる用語の定義

１．２．１ 厚生労働省ガイドラインで使用されている用語

厚生労働省ガイドライン第 5 版で使用されている以下の用語の定義については、厚生労働省ガイドライン第 5 版又は「医療情報システムを安全に管理するために（第２版）『医療情報システムの安全管理に関するガイドライン』全ての医療機関等の管理者向け読本」（厚生労働省、平成 29 年 5 月）から引用した。

用語	説明
医療機関等	病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等
組織的安全管理対策	安全管理について従業者等の責任と権限を明確に定めて、安全管理に対する規程や手順書を整備･運用し、その実施状況を確認することをいう。
物理的安全管理対策	入退館（室）の管理、個人データの盗難の防止等の措置をいう。
技術的安全対策	個人データ及びそれを取り扱う医療情報システムへのアクセス制御、不正ソフトウェア対策、医療情報システムの監視等、個人データに対する技術的な安全管理措置をいう。
人的安全対策	従業者等との間において、業務上秘密と指定された個人データの非開示契約を締結し、情報保護に関する教育･訓練等を行うことをいう。
真正性	正当な人が記録･確認を行った情報について、第三者にとって作成の責任の所在が明確であり、かつ、故意又は過失による虚偽入力･書換え･消去･混同[4]が防止されていることである。
見読性	電子媒体に保存された内容を、要求に基づき、必要に応じて肉眼で読み取れる状態にすることができることである。見読性とは、本来「診療に用いるため支障がないこと」と「監査等に差し支えないこと」を指し、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わたって真正性を保ち、見読性が確保された状態で保存されることをいう。
盗聴	ネットワークに特有の事象ではなく、広く第三者が意図的に会話の内容･情報を盗み聞くことである。ネットワークでは、一般的には何らかの手段で伝送中の情報（電気信号）を盗み取ることを指す。
改ざん	情報を不正に書き換えることである。例えば、ホームページを不正に書き換えたり、伝送途中の情報を書き換えたりする行為が挙げられる。

[4] 混同とは、患者を取り違えた記録がなされたり、記録された情報間の関連付けを誤ることをいう。

用語	説明
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である。例えば、情報を受け取る人のふりをして不正に情報を取得する行為や、他人の ID やパスワード等を盗み出して、本人しか確認することができない情報を閲覧する行為が挙げられる。

１．２．２　クラウドサービス提供における情報セキュリティガイドラインで使用されている用語

クラウドサービス提供における情報セキュリティ対策ガイドライン第 2 版（平成 30 年 7 月）で使用されている以下の用語の定義については、同ガイドラインから引用した。

用語	説明
可用性	認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。（JIS Q 27001 を基に定義）
完全性	資産の正確さ及び完全さを保護する特性。（JIS Q 27001 を基に定義）
機密性	認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性。（JIS Q 27001 を基に定義）
脅威	組織に損害や影響を与えるリスクを引き起こす要因。（JIS Q 27001 を基に定義）
クラウドコンピューティング	利用者による共有が可能であり、利用者の要求に応じたセルフサービス提供と管理の機能を併せ持つ、拡張性と弾力性に富んだ物理又は仮想資源のプールに、ネットワークを通じてアクセスすることを可能にする情報処理形態。
クラウドサービス	提供形態から、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）及び SaaS（Software as a Service）に分ける。また、実現形態から、プライベートクラウド、パブリッククラウド及びハイブリッドクラウドに分けることができる。
IaaS（Infrastructure as a Service）	CPU、メモリ、ストレージ、ネットワークなどのハードウェア資産をサービスとして提供するクラウドサービス。
PaaS（Platform as a Service）	オペレーティングシステムや、アプリケーションの実行環境（開発環境を含む）をサービスとして提供するクラウドサービス。
ASP・SaaS(Application	アプリケーションの利用をサービスとして提供。

用語	説明
Service Provider・Software as a Service))	
プライベートクラウド	クラウドサービスを、企業の情報セキュリティ管理区域内に閉じたシステム構成で提供。自社開発システムとほぼ同様の運用管理方法で利用可能。利用者の要求に即した運用管理やカスタマイズが可能。
パブリッククラウド	クラウドサービスを、企業の情報セキュリティ管理区域外に構築されたシステムにより提供。
ハイブリットクラウド	プライベートクラウドとパブリッククラウドの両者を組み合わせたクラウドサービス。
サーバ・ストレージ	クラウド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。
情報提供	情報公開、又は情報開示の実施。
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。(JIS Q 27001 を基に定義)
脆弱性	脅威によって悪用される可能性がある欠陥や仕様上の問題。(JIS Q 27001 を基に定義)
プラットフォーム	認証、決済等の付加的機能を提供する、クラウドサービスで提供されるアプリケーションの基盤。
リスク	事象の発生確率と事象の結果との組合せ（目的に対して不確かさが与える影響)。(JIS Q 27001 を基に定義)
リスクアセスメント	リスク分析からリスク評価までの全てのプロセス。(JIS Q 27001 を基に定義)
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。(JIS Q 27001 を基に定義)
IoT	情報社会のために、既存もしくは開発中の相互運用可能な情報通信技術により、物理的もしくは仮想的なモノを接続し、高度なサービスを実現するグローバルインフラのこと。
IoT機器	IoT を構成するネットワークに接続される機器のこと。通信を行う以外の主たる機能としては、計測（センサー)、制御（アクチュエータ）がある。

用語	説明
	センサー及びアクチュエータは、機器本体と通信･制御部の組み合わせで構成されるものである。ただし、制御部が外部コンピュータとして独立しているものはローカルコンピュータと呼ぶ。
SLA (Service Level Agreement)	書面にしたサービス提供者と顧客との合意であって、サービス及び合意したサービスレベルを記述したもの（JIS Q 20000-1:2007）。

１．２．３　その他の用語

１．２．１、１．２．２以外の用語で本ガイドラインで使用する用語の定義は以下のとおりである。

用語	説明
クラウドサービス事業者	クラウドサービスを提供する組織。クラウドサービスを提供するため別の組織が提供するクラウドサービスを利用することもありうる。
オンライン診療	遠隔医療のうち、医師－患者間において情報通信機器を通して、患者の診察及び診断を行い診断結果の伝達や処方等の診療行為を、リアルタイムにより行う行為[5]。
PHR（Personal Health Record）	個人の生涯にわたる医療･健康等に関するデータを時系列で管理し、本人の判断のもと多目的に活用する仕組み。PHR は、広く個人の健康に関連する様々な情報を活用する仕組みを指すが、本ガイドラインにおける PHR は、医療情報を活用する場合を対象とする。
PHRサービス	PHR を提供するクラウドサービス。
PHRサービス事業者	PHR サービスを提供するクラウドサービス事業者。医療情報の取扱いを目的としないクラウドサービス事業者は、本ガイドラインにおける PHR サービス事業者には該当しない。
サービス仕様適合開示書	クラウドサービス事業者が、自ら提供するサービスの仕様につき、本ガイドラインへの適合状況を医療機関等へ開示するために作成するための資料のこと。詳細は、本ガイドライン第 4 章及び別添にて示す。
クリアスクリーン	自席のコンピュータを意図せず第三者に操作されたり画面を盗み見されたりしないための対策を指す。パスワード付きのスクリーンセーバーの起動など。
侵入検知システム	侵入検知システム(IDS)とは、サーバやネットワークの外部との通信を監

[5] 出所：オンライン診療の適切な実施に関する指針（厚生労働省 平成 30 年 3 月 30 日）(P.5)

用語	説明
(IDS)、 侵入防止システム (IPS)	視し、攻撃や侵入の試みなど不正なアクセスを検知して管理者にメール等で通報するシステムを指す。 これに対して、侵入防止システム(IPS)は、検知した結果、管理者への通報のほか、アクセスを遮断する等の防御措置を取る機能をもつシステムを指す。
VPN（仮想私設網、Virtual Private Network）	不特定事業者が接続されるネットワーク上に構築された、特定の事業者間のみを接続する仮想的な閉域網のことを指す。
RAID-1又はRAID-6	RAID（Redundant Arrays of Independent（Inexpensive） Disks）とは、ディスク･サブシステムを、ディスクの障害に対する冗長化、あるいは高速化する技術を指す。 RAID-1 は、同一のデータを複数のディスクに書き込み、一方のディスクが故障しても、他方で処理を続行できるようにすることでディスクの耐障害性を高める方式をいう。 RAID-6 は、1 つのデータ･ブロックにつき、ディスクの故障時に記録データを修復するために「パリティ」と呼ばれる冗長コードを 2 つ生成することで、同時に 2 台のハードディスクが故障しても、元のデータを修復可能とする方式をいう。
無線 LAN	無線でデータの送受信を行なう LAN のこと。特に、IEEE 802.11 諸規格に準拠した機器で構成されるネットワークのことを指すこともある。
BYOD（Bring Your Own Device）	BYOD は、業務における私物利用を指すが、その範囲等については、多義的である。本ガイドラインでは、「組織として私物端末を業務に利用することが決定された状態で、職員が、利用を許可された私物端末（以降 BYOD 端末）を用いて組織が指定した業務を行うこと」を指す[6]。
モバイルデバイスマネジメント（MDM）	モバイルデバイス管理ともいい、企業等で従業員等に支給するスマートフォン等の携帯情報端末を統合的･効率的に管理･運営するために用いる、サーバシステムやアプリ等のツール類やソリューションサービスを指す。管理手法そのものを MDM ということもある。
モバイルアプリケーションマネジメント（MAM）	携帯情報端末で利用されるアプリケーションソフトを統合的･効率的に管理する手法を指す。業務用のアプリケーションソフトやデータをプライベートな領域から隔離し、安全に利用できるようにする。例えばラッピング型あるいはコンテナ型のシステムなどの手法が挙げられる。

[6] 「私物端末の業務利用におけるセキュリティ要件の考え方」（CIO 補佐官等連絡会議　情報セキュリティ WG BYOD 要件検討 SWG、2013 年 3 月）スライド 7

用語	説明
BCP（Business Continuity Plan）	災害等により、特定された重要業務が中断しないこと、また万一事業活動が中断した場合に目標復旧時間内に重要な機能を再開させ、業務中断に伴う顧客取引の競合他社への流出、マーケットシェアの低下、企業評価の低下などから企業を守るための経営戦略。バックアップシステムの整備、バックアップオフィスの確保、安否確認の迅速化、要員の確保、生産設備の代替などの対策を実施することを指す。
コンテンジェンシープラン	コンテンジェンシープランとは、不測の事態に備えて予め定めておく「緊急時対応計画」を指す。これを用意することにより、不足の自体の際の影響範囲を最小限にし、業務への迅速な復旧が可能になる。リスクによるインパクト評価を伴わない点で BCP とは異なる。
IPSec（Security Architecture for Internet Protocol）	暗号技術を使って IP パケットの完全性や機密性を提供する仕組み。IP パケットの暗号化や認証を行う。
IKE（Internet Key Exchange）	鍵交換を行う事ができるプロトコルを指す。IP-Sec による暗号化を行う際に用いる、ISAKMP/Oakley を基礎とした標準の鍵交換プロトコル。
チャネル･セキュリティ	（ネットワーク）チャネルとは、ネットワークの伝送路を意味し、一般的には論理的なネットワーク経路を指す。チャネル･セキュリティとは、ネットワークにおける経路上のセキュリティを指す。
SSL（Secure Sockets Layer）/ TLS（Transport Layer Security）	インターネット上でデータを暗号化して送受信できるプロトコルを指す。データ改ざんやなりすましを防止することが可能となる。SSL での暗号化は公開鍵暗号、秘密鍵暗号、電子署名、電子証明書の技術等を組み合わせて実現される。 TLS（Transport Layer Security）は、SSL をもとに標準化させたもの。一般的には SSL/TLS として用いられる。
S/MIME（Secure Multipurpose Internet Mail Extensions）	電子メールにおいて、内容を暗号化したり電子署名を付加したりする方式の一つ。
SSL-VPN	暗号化に SSL 技術を使用したリモートアクセス VPN をいう。セッション層で実装される点で特徴を有する。ただし実際は下位のトランスポートプロトコルごとに SSL 対応する必要があるとされる。

１．３ 本ガイドラインの対象範囲

１．３．１ 本ガイドラインが対象とする医療情報

（１） 本ガイドラインが対象とする医療情報

本ガイドラインが対象とする医療情報は、厚生労働省ガイドライン第 5 版[7]において定義されているものと同一とする。すなわち「医療に関する患者情報（個人識別情報）を含む情報」を対象とする[8]。

（２） 本ガイドラインにおける医療情報の管理主体

医療情報には、医療従事者が作成･記録した情報のほか、医療従事者の指示が記録された情報に基づき介護事業者が作成･記録した情報がある。これらの医療情報は、その情報を作成･記録した者が所属する医療機関等で保管されたり、その医療機関等から他の医療機関等に提供されたりする場合のほか、患者等（患者本人のほか、患者の家族等で、患者の医療情報を閲覧する権限を有する者を含む。以下同じ）に提供される場合もある。

上述を踏まえた本ガイドラインにおける医療情報の管理主体について、図 2 に示す[9]。

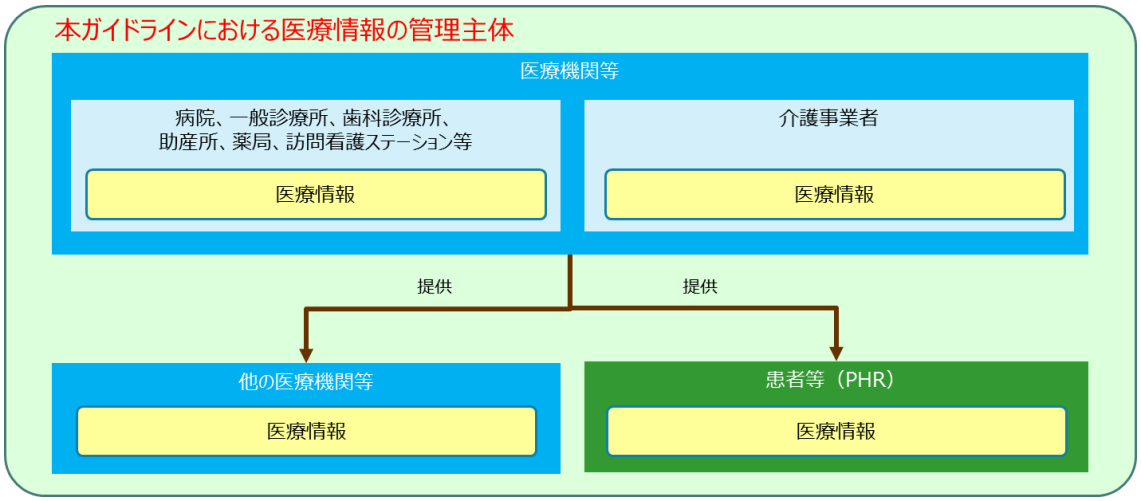


図 2　本ガイドラインにおける医療情報の管理主体

---

[7] 「医療情報システムの安全管理に関するガイドライン第 5 版」（厚生労働省　平成 29 年 5 月）

[8] 厚生労働省ガイドライン第 5 版 P13

[9] なお、医療従事者の指示が記録された医療情報に基づき介護事業者が作成・記録した情報でなく、介護事業者や患者等が作成・記録した情報等の医療情報に該当しない情報だけを管理している介護事業者や患者等は、図 2 で示す医療情報の管理主体には当たらない。

１．３．２ 本ガイドラインが対象とするクラウドサービス

（１） 本ガイドラインで想定するクラウドサービスの提供形態

本ガイドラインで想定するクラウドサービスは、ASP･SaaS のほか、PaaS、IaaS 等を含む。

クラウドサービスの提供にあたっては、クラウドサービス事業者 1 社が、クラウドコンピューティングを実施する際の全ての資源を保有して、サービスの提供を行う場合のほか、一部他のクラウドサービス事業者の資源や、利用者側の資源を活用して提供することが想定される。

そこで、この提供形態に応じた本ガイドラインの適用関係について、以下に示す。

（ア）一つのクラウドサービス事業者が、医療情報を取り扱うクラウドサービスに必要な全ての資源を提供するケース

図 3 は、クラウドサービスの提供に必要な資源を、クラウドサービス事業者 1 社が全て保有し、提供しているケースを示す。

医療機関等は、厚生労働省ガイドラインが示す安全管理対策を実現できるクラウドサービスを選択することになるが、本ケースの場合には、クラウドサービス事業者 1 社でサービスの提供に必要な全ての資源を有していることから、当該事業者に対して厚生労働省ガイドラインが示す安全管理対策の内容を満たしていることを確認すればよい。

クラウドサービス事業者側から見ると、自社で全ての資源を保有していることから、医療情報を取り扱うサービスを提供する自社の情報システムについて、本ガイドラインの要求事項に対応していることを確認して医療機関等に提示すればよい。

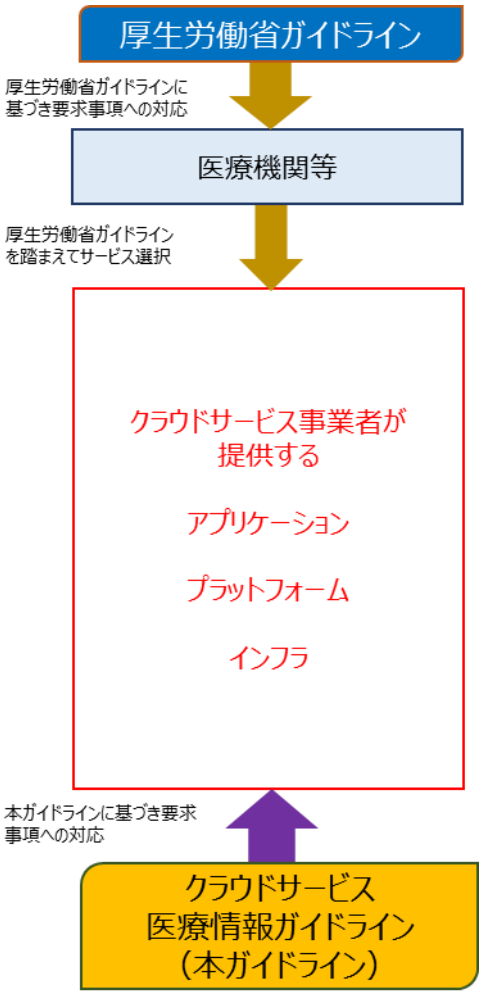


図 3　（ア）　一つのクラウドサービス事業者が、医療情報を取り扱うクラウドサービスに必要な全ての資源を提供するケース

（イ）医療情報を取り扱うクラウドサービスの提供に必要な資源を複数のクラウドサービス事業者が提供するケース

自社以外のサービスも活用してサービスを提供する例を図 4 に示す。ケース 1 は、クラウドサービス事業者 A がクラウドサービス事業者 B のサービス（IaaS）を調達する例である。ケース 2 は、クラウドサービス事業者 A がクラウドサービス事業者 B のサービス（PaaS、IaaS）を調達し、さらにクラウドサービス事業者 B がクラウドサービス事業者 C のサービス（IaaS）を調達する例である。

医療機関等は、（ア）同様、厚生労働省ガイドラインを踏まえて同ガイドラインで示す安全管理対策を実現できるクラウドサービスを選択することになり、契約先である A に対して、A が提供するサービスが厚生労働省ガイドラインに示す内容を満たしていることを確認すればよい。

一方、A は、自社における資源が、本ガイドラインの要求事項に対応していることを確認した上で、サービスの提供を行うことに加え、他のクラウドサービス事業者（B、C）のサービスが、本ガイドラインにおける要求事項を満たしていることを確認した上で調達し、提供する必要がある。このうち、図 4 の左のケース（ケース 1）では、A は、B の選択と管理について直接的な責任を負う。これに対して、右のケース（ケース 2）では、A は、B の選択と管理の直接的な責任を負うほか、C については、B からの報告などに基づく管理責任を負うことになる（C が要求事項を遵守しなかった場合には、A は B に対する管理責任の一環として責任を負うことになる）。なお、図 4 における B や C が提供するサービスのように、他者から提供されるクラウドサービスにおいても、医療情報を取り扱うサービスとして提供する場合には、委託を受けるクラウドサービス事業者（B、C）は、委託元のクラウドサービス事業者（A）から独立して本ガイドラインの要求事項に対応する必要が生じる。ただし、クラウドサービスの内容によっては、本ガイドラインの一部項目の適用が想定されないものも含まれていることから、各クラウドサービスの内容に照らして、必要な要求事項へ対応することが求められる。

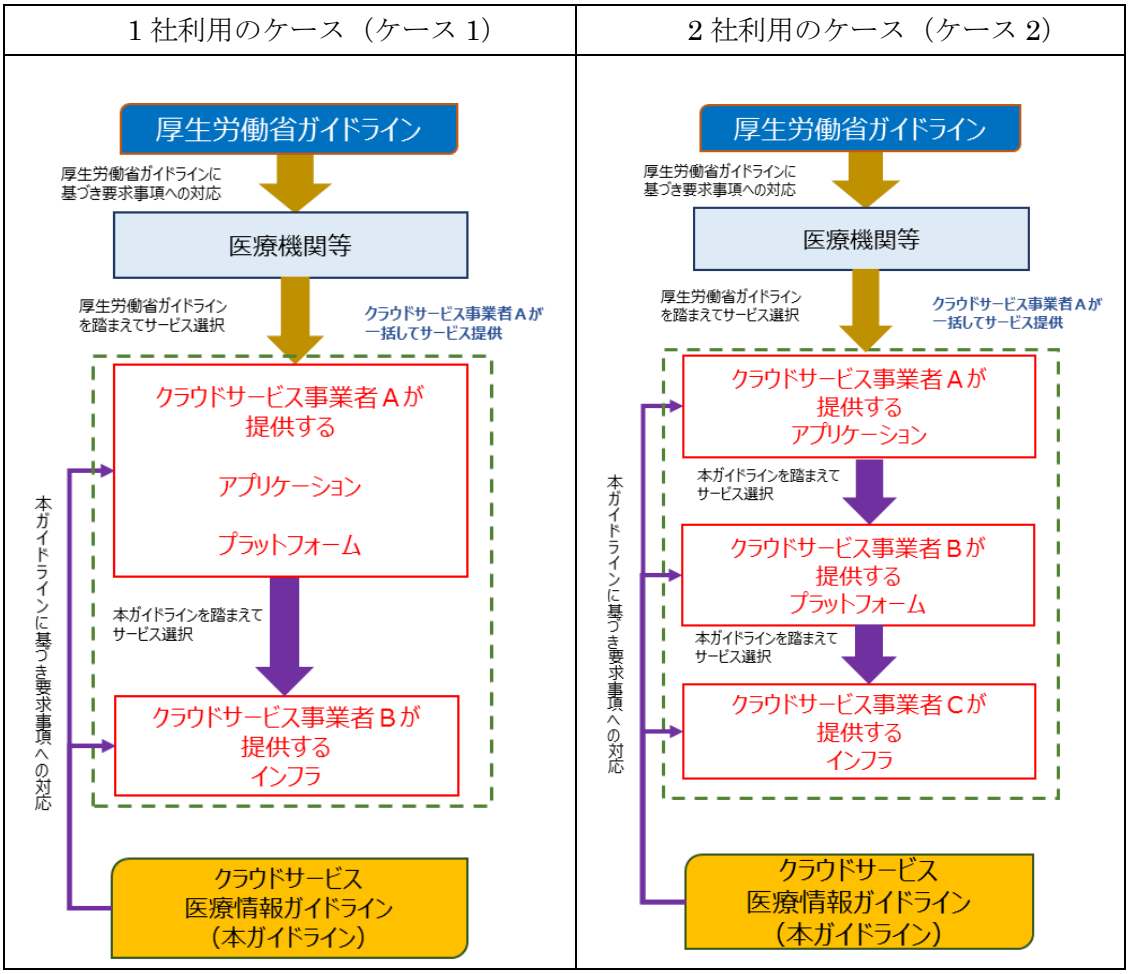


図 4（イ） 医療情報を取り扱うクラウドサービスの提供に必要な資源を複数のクラウドサービス事業者が提供するケース

（２） 医療情報連携ネットワークにおける本ガイドラインの適用

医療情報を取り扱うクラウドサービスの利用については、各医療機関等とクラウドサービス事業者が契約して利用するケースが、基本ケースとして想定される。

しかし、医療情報連携ネットワークの場合においては、提供されるクラウドサービスを複数の医療機関等が共同で利用し、医療機関等の間で情報連携がなされる場合も想定される。この場合における本ガイドラインの適用対象について整理する。

医療情報連携ネットワーク運営主体が、医療情報の取扱いに責任を有する場合には、同主体も、本ガイドラインにおけるクラウドサービス事業者として位置づけられる。具体的には、医療情報連携ネットワークに参加する医療機関等が医療情報の管理（の一部）を運営主体に委託するような場合である。医療機関同士が患者の情報を交換したい場合にはこのような委託が行われる（図 5）。この場合、医療機関等は厚生

労働省ガイドラインに基づいて、医療情報連携ネットワーク運営主体との間で適切な責任分界点を契約等により合意した上で対応する必要がある。また、医療情報連携ネットワーク運営主体が、委託により、別のクラウドサービス事業者と医療情報等の管理を分担して実施する場合には、同主体は、本ガイドラインに基づいて、委託先のクラウドサービス事業者を監督し、管理責任を果たすことが求められる。

なお、医療情報連携ネットワーク運営主体の中には、医療情報に関する管理責任は負わず、参加団体の取りまとめや情報システム仕様の調整等のみを行っている者もあり、そのような運営主体については、本ガイドラインにおけるクラウドサービス事業者とはならない。

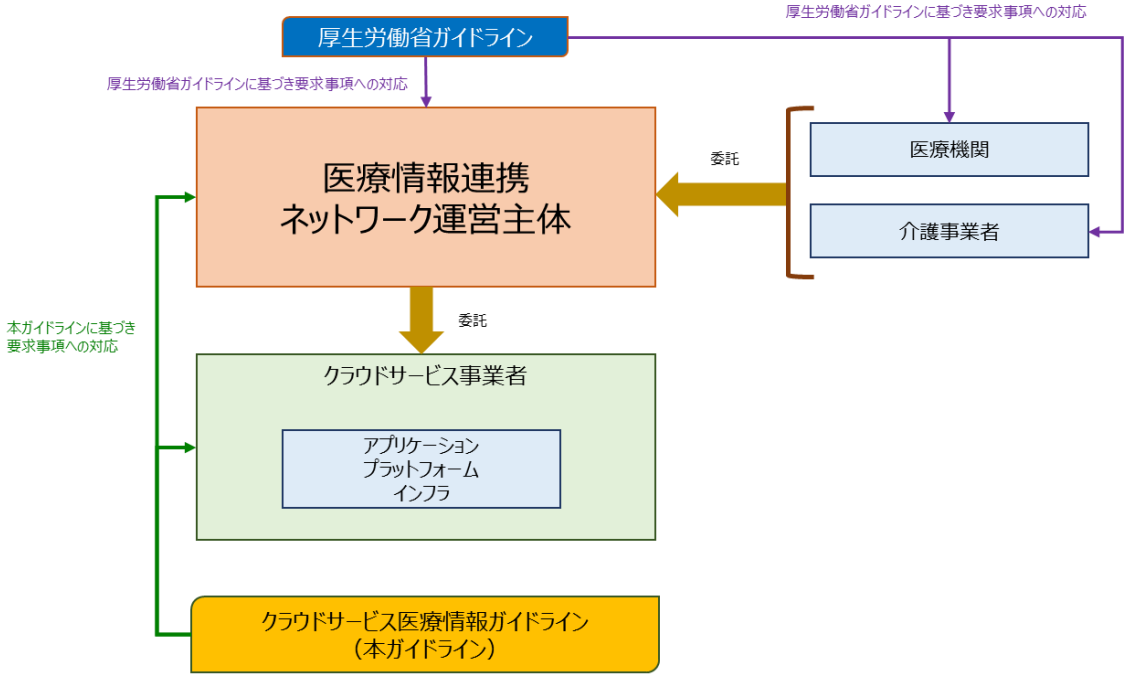


図 5　医療情報連携ネットワーク運営主体における本ガイドラインの適用関係

（3） オンライン診療における適用領域

オンライン診療については、「オンライン診療の適切な実施に関する指針」[10]（以下「オンライン診療指針」という）が策定されており、オンライン診療等における遵守事項や考え方などが示されている。この中で、オンライン診療に用いる機器、情報システム・サービス（オンライン診療システム）に係る情報セキュリティや利用端末に関する要求事項等についても示されている。

---

10 「オンライン診療の適切な実施に関する指針」（厚生労働省　平成 30 年 3 月）

オンライン診療のうち、医療機関の医療情報システムと接続[11]するケースについては、医療情報安全管理関連ガイドラインが適用されることが示されている[12] [13]。

本ガイドラインでは、第３章３．５において、オンライン診療システムが医療情報システムと接続する場合について、オンライン診療システムを提供するクラウドサービス事業者が対応すべき要求事項を整理している。

（４） PHR（パーソナル･ヘルス･レコード）における適用領域

（ア）PHR サービス事業者に対する要求事項

厚生労働省ガイドラインは、医療機関等における医療情報の取扱いを対象としているが、本ガイドラインでは PHR サービス事業者への要求事項を整理している。

本ガイドラインでは、第３章３．６において、PHR サービス事業者に対する要求事項等について整理している。なお、本ガイドラインで対象とする PHR サービスは、患者が管理する医療情報（主に医療機関等が作成し、患者に提供したもの）を扱うクラウドサービス等を対象とする。したがって、患者自らが計測した体温、脈拍数等の情報で、医療従事者の取扱いがない情報を扱うクラウドサービス等は、本ガイドラインの対象とはしない。

（イ）クラウドサービスにおける PHR サービスの取扱い例

クラウドサービスにおける PHR については、医療情報として医療機関等が管理していた情報を患者等に渡し、これを患者等が自ら契約するクラウドサービスを利用してその情報の管理や健康管理を行う形が想定される。

これ以外にも、医療機関等が管理する情報を、患者等の依頼により、患者等が契約するクラウドサービス事業者に医療機関等から送信し、以降の当該情報の管理主体が医療機関等から患者等に移るケースも想定される（図 6）。

いずれの場合も、PHR サービス事業者において取り扱われる医療情報について、医療機関等の管理責任は及ばない。しかし、後者については、医療機関等と PHR サービス事業者との間で、データの受け渡しに関する責任分界点を明確にすることが必要である。

---

[11] 接続とは、医療情報システムに対して、中間的なサーバを設置して、一旦オンライン診療システムからの影響を遮断する等の対策（ネットワーク上の分離）を実施しておらず、保存されている医療情報にアクセス可能な状態を指す。(オンライン診療指針 P19)

[12] オンライン診療指針 P22

[13] なお、医療情報システムと接続しない場合については、本ガイドライン等の適用はないものの、一定の安全管理対策を講じることが示されている。

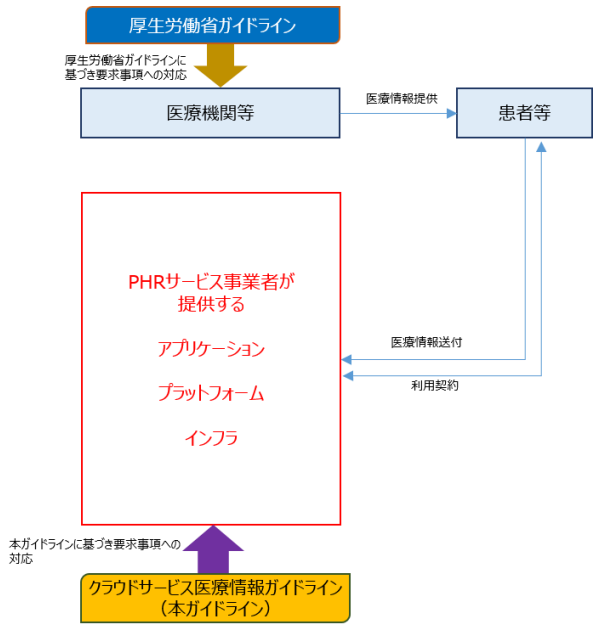
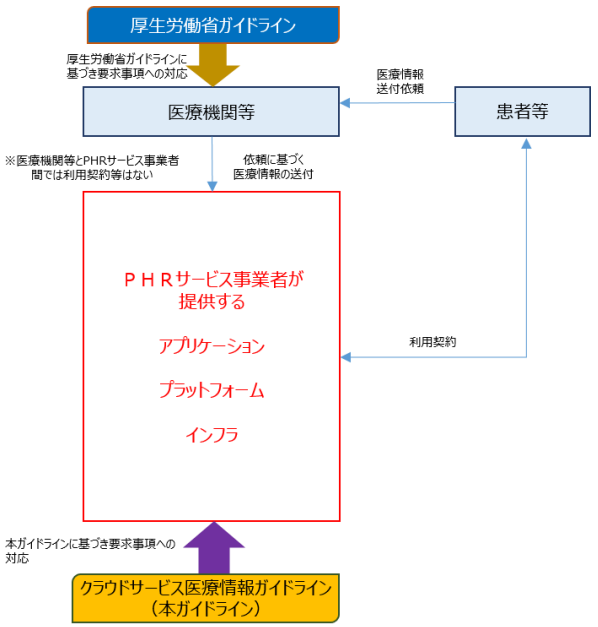
患者等が直接 PHR サービス事業者に医療情報を送信する例	患者等の依頼に基づき医療機関等が PHR サービス事業者に医療情報を送信する例
	

図 6　クラウドサービスにおける PHR サービスの取扱い例

１．４ 他のガイドラインとの関係

医療機関等における医療情報システムの安全管理措置に関しては、前述のとおり、厚生労働省ガイドラインが示されている。これは医療機関等が医療情報システムを利用する際に、医療情報を安全に取り扱うために必要な、医療機関等の管理者の義務や責任、対応すべき内容等を示したものである。また、クラウドサービスにより医療情報を管理する（取り扱う）場合においても、医療機関等の管理者は、同ガイドラインの内容を踏まえることが求められる。

したがって、クラウドサービス事業者においては、クラウドサービスにより医療情報を管理する場合には、厚生労働省ガイドラインの内容が遵守されていることを確認しなければならない。

本ガイドラインでは、厚生労働省ガイドライン第 5 版の内容をベースに、クラウドサービス事業者の観点から義務及び対応すべき事項について、要求事項として示している[14]。

クラウドサービスによる医療情報の管理に関連するガイドラインの例として、厚生労働省ガイドライン第 5 版のほかに、「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」第 2 版（経済産業省　平成 24 年 10 月）（以下「経済産業省ガイドライン」という。）が挙げられる。

医療情報の特殊性を鑑みるに、クラウドサービスが対象とする医療情報の管理において、情報セキュリティ対応は不可欠であることから、クラウドサービス事業者も含めた情報処理事業者に対して、外部保存等を行う際の医療情報のマネジメントシステムを示している経済産業省ガイドラインの内容も考慮する必要がある。

このような観点を踏まえて、本ガイドラインでは、図 7 に示す適用関係に基づいて、要求事項を整理している。

[14] 従来、クラウドサービス事業者が医療情報を取り扱う際に遵守すべき総務省ガイドラインとしては、本ガイドラインの前身である「総務省 ASP 医療ガイドライン」及び「ASP・SaaS における情報セキュリティ対策ガイドライン」（平成 20 年 1 月）の２つのガイドラインを示してきたが、今後は特にクラウドサービス事業者が医療情報を取り扱う際に遵守すべきガイドラインは本ガイドラインと整理し、必要に応じて、「クラウドサービス提供における情報セキュリティ対策ガイドライン」（総務省　平成 30 年 7 月）を参照することとする。

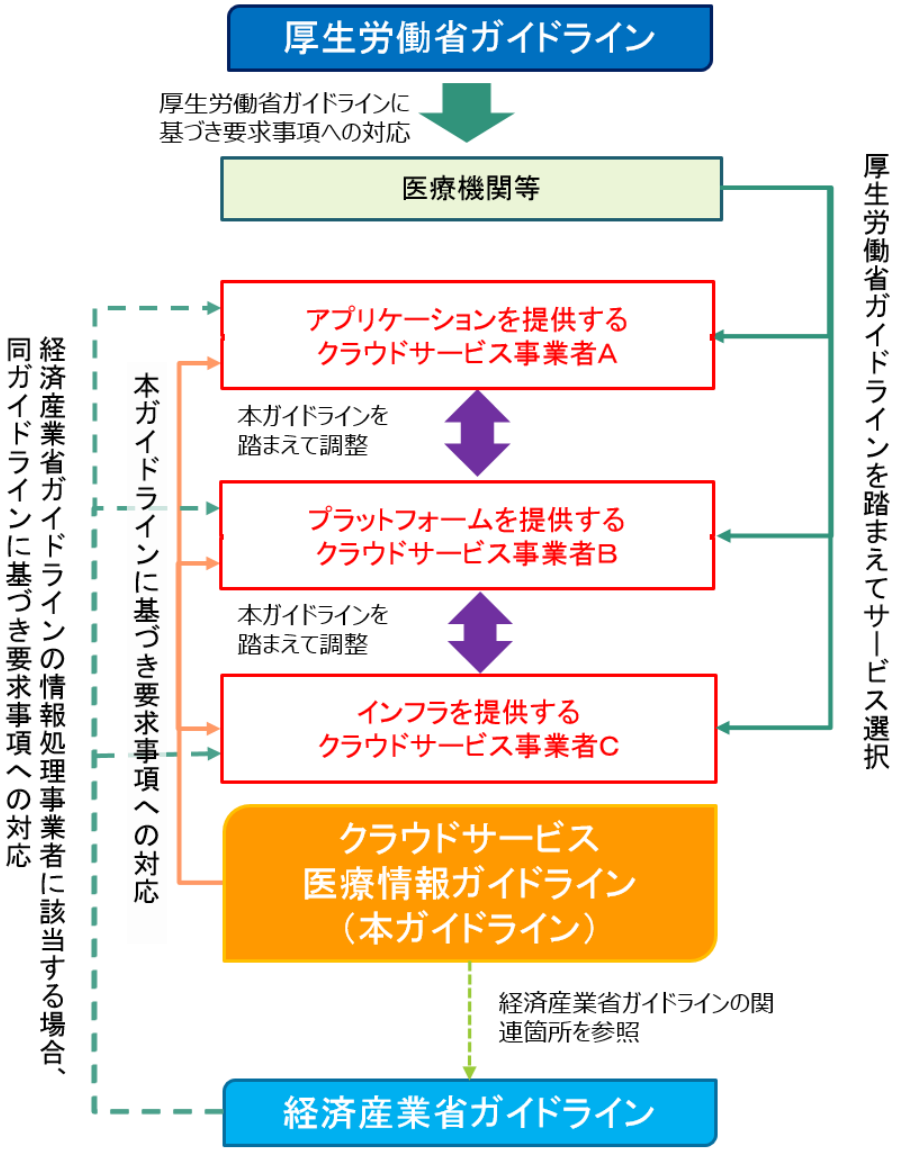


図 7　本ガイドラインと各ガイドラインの関係

１．５ 本ガイドラインの構成

本ガイドラインの構成を 図 8 に示す。

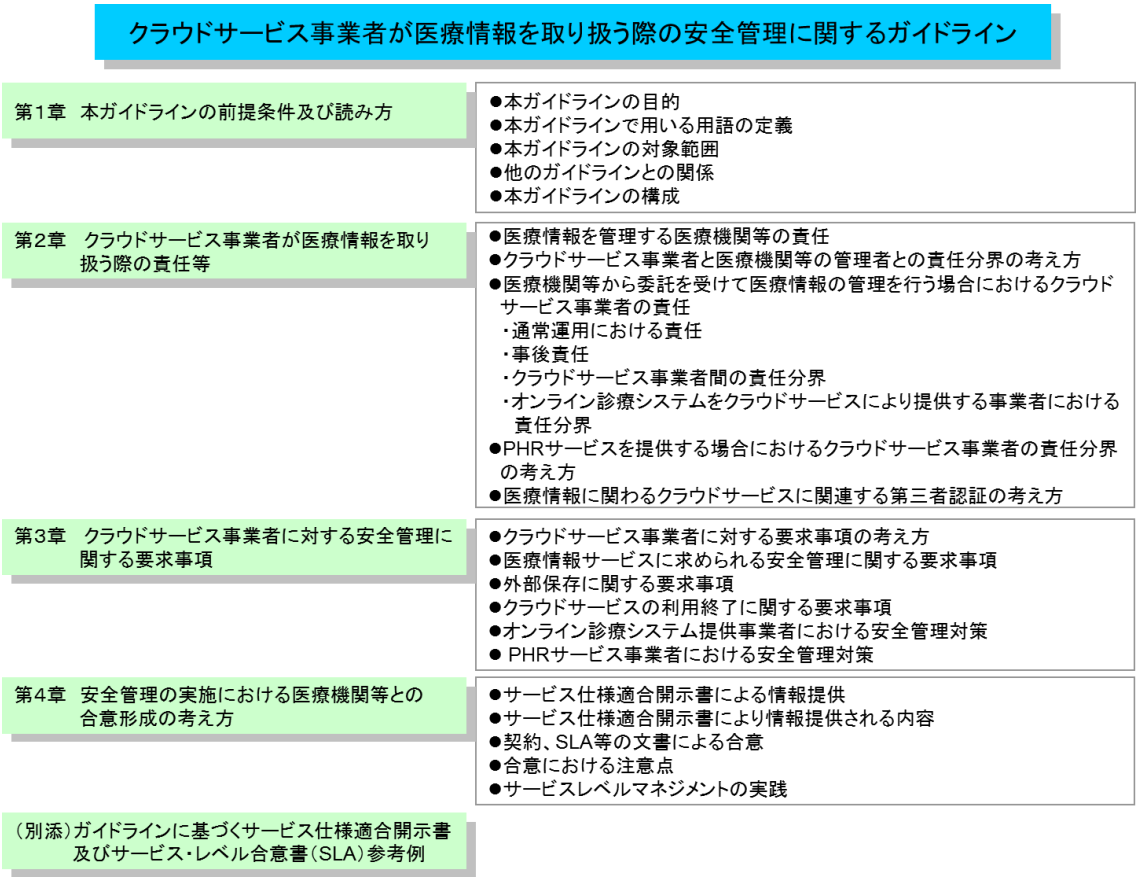


図 8　本ガイドラインの構成

第 1 章では、本ガイドラインの対象となるクラウドサービス事業者や、具体的な対応をとる上で前提とすべき事項を整理した。

第 2 章では、クラウドサービス事業者の責任や責任分界点の考え方を整理した。

第 3 章では、医療機関等の管理者に対して求められる実施事項に基づくクラウドサービス事業者への要求事項について示している。

第 4 章では、クラウドサービス事業者への要求事項のうち、医療機関等との合意形成が必要な場合の項目、考え方等を整理した。

別添として、第 1 章から第 4 章までを踏まえ、医療機関等との合意形成に当たって活用することを想定したサービス仕様適合開示書及び SLA の参考例を掲載した。

第２章 クラウドサービス事業者が医療情報を取り扱う際の責任等

本章では、クラウドサービス事業者が医療情報を取り扱う際に有する責任と責任分界の考え方をまとめる。２．１から２．３については、医療機関等からの委託によりクラウドサービス事業者が医療情報を取り扱う場合、２．４については、PHR サービス提供のためにクラウドサービス事業者が医療情報を取り扱う場合について記載する。

２．１ 医療情報を管理する医療機関等の責任

【「医療機関等の管理者の責任」に関する記述】（厚生労働省ガイドライン第 5 版[15]）（図 9 参照）

【医療機関等の管理者の責任】

・「医療に関わる全ての行為は医療法等で医療機関等の管理者の責任で行うことが求められており、医療情報の取扱いも同様である。」（「4 電子的な医療情報を扱う際の責任のあり方」）

【医療機関等の情報保護責任について】

・「医療機関等の管理者が医療情報を適切に管理するための善管注意義務を果たすためには、通常の運用時において、医療情報保護の体制を構築し管理する局面での責任と、医療情報について何らかの不都合な事態（典型的には情報漏えい）が生じた場合に対処をすべき責任とがある。便宜上、本ガイドラインでは前者を「通常運用における責任」、後者を「事後責任」と呼ぶこととする。」（「4.1 医療機関等の管理者の情報保護責任について」）

【通常運用における責任】

・「ここでいう通常運用における責任とは、医療情報の適切な保護のための適切な情報管理ということになるが、適切な情報管理を行うことが全てではなく、以下に示す 3 つの責任を含む必要がある。」（4.1(1) 通常運用における責任について」）

【事後責任】

・「医療情報について何らかの不都合な事態（典型的には漏えい）が生じた場合には、以下の責任がある。」（4.1(2)「事後責任について」）

[15] 厚生労働省ガイドライン第 5 版 P.22-23

図 9　医療機関等の管理者が電子的な医療情報を扱う際の責任の構成

２．２ クラウドサービス事業者と医療機関等の管理者との責任分界の考え方

厚生労働省ガイドライン第５版では、本ガイドライン２．１のとおり、医療情報を電子的な形で取り扱う場合、医療機関等の管理者がこれに関連する責任を負う。しかし、クラウドサービスで医療情報を取り扱う場合、医療機関等との契約に基づいてクラウドサービス事業者の情報処理事業者が情報システムやデータの管理等を行う。この場合、医療情報を取り扱う際の責任を、医療機関等の管理者とクラウドサービス事業者とで分担することが必要となる。そのためには、医療機関等の管理者とクラウドサービス事業者が以下の２点を明らかにする必要がある。

・医療機関等とクラウドサービス事業者との責任分界
・クラウドサービス事業者が提供するサービスの内容及び具体的なレベル

また、責任分界を定める前提として、クラウドサービスによって医療情報を取り扱うに当たり医療機関等の管理者が対応すべき事項等を整理する必要がある。その際、クラウドサービス事業者は高い専門性を持っているので、医療機関等の管理者に対して情報システムの安全管理に関する助言･情報提供等を行うことが求められる。

２．３ 医療機関等から委託を受けて医療情報の管理を行う場合におけるクラウドサービス事業者の責任

医療機関等が医療情報をクラウドサービスにより取り扱う場合には、医療機関等の管理者が負う責任の一部をクラウドサービス事業者が分担することになる。

例えばクラウドサービスの情報システムの仕様や運用、サービスの品質及びそれらに対する定期的な監査等については、直接的な管理をしているクラウドサービス事業者が分担する。

２．３．１　通常運用における責任

厚生労働省ガイドライン第５版では、医療機関等の管理者が患者等に対して負う「通常運用における責任」とは「医療情報の適切な保護のための適切な情報管理」であるが、「適切な情報管理を行うことが全てではなく」、「説明責任」、「管理責任」、「定期的に見直し必要に応じて改善を行う責任」の三つを含む必要があると記述されている。

これを踏まえて、この三つの責任について、クラウドサービス事業者が負う責任の内容を整理する（具体的な実施内容については、第３章に示すクラウドサービス事業者への要求事項を参照）。

（１） 説明責任

(ア) 厚生労働省ガイドラインの記述

「通常運用における責任」のうち「説明責任」に関する医療機関等の管理者の情報保護責任及び委託における責任分界についての厚生労働省ガイドラインの記述を以下に示す（()内の数字は厚生労働省ガイドラインの記述箇所）。

【医療機関等の管理者の情報保護責任について】(4.1(1)①)

電子的に医療情報を取り扱うシステムの機能や運用方法が、その取扱いに関する基準を満たしていることを患者等に説明する責任である。これを果たすためには、以下のことが必要である。

- システムの仕様や運用方法を明確に文書化すること
- 仕様や運用方法が当初の方針のとおりに機能しているかどうかを定期的に監査すること
- 監査結果をあいまいさのない形で文書化すること
- 監査の結果問題があった場合は、真摯に対応すること
- 対応の記録を文書化し、第三者が検証可能な状況にすること

【委託における責任分界】(4.2.1(1)①)

患者等に対し、いかなる内容の医療情報保護の仕組みが構築されどのように機能しているかの説明責任は、いうまでもなく医療機関等の管理者にある。

ただし、医療機関等の管理者が説明責任を果たすためには、受託する事業者による情報提供が不可欠の場合があり、受託する事業者は医療機関等の管理者に対し説明責任を負うといってよい。 従って、受託する事業者に対し適切な情報提供義務･説明義務を委託契約事項に含め、その履行を確保しておく必要がある。

(イ) クラウドサービス事業者が負う「説明責任」

医療機関等の管理者が「電子的に医療情報を取り扱うシステムの機能や運用計画が、その取扱いに関する基準を満たしていることを患者等に説明する責任」を果たすために、クラウドサービス事業者は以下の責任を負わなくてはならない。

・提供するクラウドサービスの仕様、運用、及びセキュリティ対策に関する事項の文書化
・提供するクラウドサービスの仕様及び品質に関する説明及び必要な情報提供
・提供するクラウドサービスに関する監査等の情報の提供

（２） 管理責任

(ア) 厚生労働省ガイドラインの記述

「通常運用における責任」のうち「管理責任」に関する医療機関等の管理者の情報保護責任及び委託における責任分界についての厚生労働省ガイドライン第 5 版の記述を以下に示す（()内の数字は厚生労働省ガイドライン第 5 版の記述箇所)。

【医療機関等の管理者の情報保護責任について】(4.1(1)②)

医療情報を取り扱うシステムの運用管理を行う責任であり、当該システムの管理を請負事業者に任せきりにしているだけでは、これを果たしたことにはならないため、医療機関等においては、以下のことが必要である。

・少なくとも管理状況の報告を定期的に受けること
・管理に関する最終的な責任の所在を明確にする等の監督を行うこと

さらに、個人情報保護法上は、以下の事項を定め、請負事業者との対応にあたる必要がある。

・個人情報保護の責任者を定めること
・電子化された個人情報の保護について一定の知識を有する責任者を決めること

【委託における責任分界】(4.2.1(1)②)

管理責任を負う主体はやはり医療機関等の管理者にある。しかし、現実に情報処理に当たりその安全な保守作業等を行うのは、委託先事業者である場面が多いと考えられる。医療機関等の管理者としては、委託先事業者の管理の実態を理解し、その監督を適切に行う仕組みを作る必要があり、契約事項に含めるべきである。

(イ) クラウドサービス事業者が負う「管理責任」

医療機関等の管理者が「医療情報を取り扱うシステムの運用管理を行う責任」を果たすために、クラウドサービス事業者は以下の責任を負わなくてはならない。

・医療機関等の管理者に対するクラウドサービス事業者側の最終的な管理責任者の明確化
・個人情報保護責任者を含むクラウドサービスの提供体制の明確化
・クラウドサービスの提供に関する運用状況等の定期的な報告
・医療機関等の管理者からの問合せ等に対して、一元的に対応できる体制の構築

（３） 定期的に見直し必要に応じて改善を行う責任

(ア) 厚生労働省ガイドラインの記述

「通常運用における責任」のうち「定期的に見直し必要に応じて改善を行う責任」に関する医療機関等の管理者の情報保護責任及び委託における責任分界についての厚生労働省ガイドライン第 5 版の記述を以下に示す（()内の数字は厚生労働省ガイドライン第 5 版の記述箇所)。

【医療機関等の管理者の情報保護責任について】(4.1(1)③)

・情報保護に関する技術は日進月歩であるため、情報保護体制が陳腐化するおそれがあり、それを適宜見直して改善するためには以下の責任を果たさなくてはならない。
・当該情報システムの運用管理の状況を定期的に監査すること
・問題点を洗い出し、改善すべき点があれば改善すること

そのために医療機関等の管理者は、医療情報保護の仕組みの改善を常にこころがけ、現行の運用管理全般の再評価･再検討を定期的に行う必要がある。

【委託における責任分界】(4.2.1(1)③)

当該システムの運用管理の状況に対する定期的な監査により、問題点を洗い出し、改善すべき点があれば改善していく責任の分担、また、情報保護に関する技術進展に配慮した定期的な再評価･再検討を実施し、その結果に基づき対策を行う際の医療機関等との協議について、委託先事業者との契約事項に含めるべきである。

(イ) クラウドサービス事業者が負う「定期的に見直し必要に応じて改善を行う責任」

医療機関等の管理者が「情報保護体制が陳腐化するのを防止し、それを適宜見直して改善する」責任を果たすために、クラウドサービス事業者は以下の責任を負わなければならない。

・サービス及びセキュリティの向上についての定期的なレビュー結果の報告等

２．３．２ 事後責任

医療機関等の管理者が負う「事後責任」については、厚生労働省ガイドライン第 5 版の 4.1 に記述されている。「事後責任」には、「説明責任」及び「善後策を講じる責任」が含まれる。

以下、医療機関等の管理者が負う責任を踏まえて、事後責任に含まれる各責任のうち、クラウドサービス事業者が負う責任の内容を整理する（具体的な実施内容については、第３章に示すクラウドサービス事業者への要求事項を参照）。

（１） 事後責任における説明責任

(ア) 厚生労働省ガイドラインの記述

「事後責任」のうち「説明責任」に関する医療機関等の管理者の情報保護責任及び委託における責任分界についての厚生労働省ガイドライン第 5 版の記述を以下に示す（()内の数字は厚生労働省ガイドライン第 5 版の記述箇所）。

【医療機関等の管理者の説明責任について】(4.1(2)①)

特に医療機関等は一定の公共性を有するため、個々の患者に対する説明責任があることは当然ながら、併せて監督機関である行政機関や社会への説明･公表も求められる。そのため、以下のことが必要である。

・医療機関等の管理者はその事態発生を公表すること

・原因とそれに対していかなる対処を行うかについて説明すること

【委託における責任分界】(4.2.1(2)①)

前項で述べたように、医療情報について何らかの不都合な事態が生じた場合、医療機関等の管理者にはその事態発生を公表し、その原因といかなる対処法をとるかについて説明する責任が求められている。

しかし、情報に関する事故は、説明に際して受託する事業者の情報提供や分析が不可欠な場合が多いと考えられる。そのため、あらかじめ可能な限りの事態を予想し、受託する事業者との間で、説明責任についての分担を契約事項に含めるべきである。

(イ) クラウドサービス事業者が負う説明責任

医療機関等の管理者が「個々の患者に対する説明責任」及び「監督機関である行政機関や社会への説明･公表」の責任を果たすために、クラウドサービス事業者は以下の責任を負わなければならない。

・緊急時に医療機関等の管理者に対して提供する情報の内容、役割分担等の明確化

・クラウドサービスの提供状況に関する記録の収集及び緊急時の報告体制の構築

・媒体及び機器の管理等に関する手順の明確化及び緊急時の報告体制の構築

・緊急時に備えた、アクセス制御等の手順等の明確化

（２） 事後責任における善後策を講ずる責任

(ア) 医療機関等の管理者の責任

「事後責任」のうち「善後策を講ずる責任」に関する医療機関等の管理者の情報保護責任及び委託における責任分界についての厚生労働省ガイドライン第 5 版の記述を以下に示す（()内の数字は厚生労働省ガイドライン第 5 版の記述箇所)。

【医療機関等の管理者の情報保護責任について】(4.1(2)②)

医療機関等の管理者には善後策を講ずる責任も発生する。その責任は以下に分けられる。

・原因を追及し明らかにする責任

・損害を生じさせた場合にはその損害填補責任

・再発防止策を講ずる責任。

【委託における責任分界】(4.2.1(2)②)

事故が医療情報の処理を委託した事業者の責任による場合、適切な委託契約に基づき、受託する事業者の選任･監督に適切な注意を払っていれば、法律上、医療機関等の管理者の善管注意義務は果たされていると解される。

ただし、本章冒頭に述べたように、医療機関等では医療情報の管理を医療機関等の管理者の責任において行うことが求められている。よって、医療情報に関する事故の原因究明、被害者への損害填補、さらに再発防止について、少なくとも責任の一端を負わなければならない。また、現実的にも、受託する事業者が医療情報の全てを管理しているとは限らないため、事故を契機として、医療情報保護の仕組み全体について善後策を講ずる責任は医療機関等の管理者が負わざるを得ない。

上記のように、医療機関等の管理者は、患者に対して、「原因を追及し明らかにする責任」、「損害を生じさせた場合にはその損害填補責任」、「再発防止策を講ずる責任」等、の善後策を講ずる責任を免れるものではない。

ただし、医療機関等の管理者の、患者等に対するすべての責任が免ぜられることはないとしても、受託する事業者との間での責任分担はそれとは別の問題である。特に、事故が受託する事業者の責任で生じた場合、医療機関等の管理者がすべての責任を負うことは、原則としてあり得ない。

しかし、医療情報について何らかの事故が生じた場合、医療機関等と受託する事業者の間で責任の分担について争うことに優先して、まず原因を追及し明らかにすること、そして再発防止策を講ずることが重要である。

そのためには、委託契約に、医療機関等と受託する事業者が協力してこれらの措置を優先させることを明記しておく必要がある。

委託内容によっては、より詳しく受託する事業者の責任での原因追及と再発防止策の提案義務を明記することも考えられる。

損害填補責任の分担については、事故の原因が受託する事業者にある場合、最終的には受託する事業者が負うのが原則である。ただし、この点は、原因の種類や複雑さによっては原因究明が困難になること、また損害填補責任分担の定め方によっては原因究明の妨げになるおそれがあること、あるいは保険による損害分散の可能性等、考慮すべき様々な要素がある。それらを考慮した上で、委託契約において損害填補責任の分担を明記することが必要である。

(イ) クラウドサービス事業者が負う「善後策を講ずる責任」

医療機関等の管理者が「原因を追及し明らかにする責任」、「損害を生じさせた場合にはその損害填補責任」及び「再発防止策を講ずる責任」を果たすために、クラウドサービス事業者は以下の責任を負わなければならない。

・情報事故（個人情報漏洩等）等が発生した場合の原因追及に必要な情報提供の範囲、条件等の合意、及び情報提供の実施
・善後策の提案
・情報事故が発生した場合の損害填補責任に関する合意

２．３．３ クラウドサービス事業者間の責任分界

ここまでは、医療機関等の管理者の責任及び医療機関等とクラウドサービス事業者間における責任分界と、これを踏まえたクラウドサービス事業者の責任について整理した。

第１章で述べたように、例えば一つの事業者が医療情報を取り扱うクラウドサービスの提供に必要な全ての資源を保有して、クラウドサービスを提供するケースのほか、他のクラウドサービス事業者のサービスを利用して、クラウドサービスの提供を行うケースが想定される。このようなケースにおけるクラウドサービス事業者間の責任分界について整理を行う。

（１） 他のクラウドサービス事業者のサービスと自社が提供するサービスを一体として、医療機関等にサービスを提供する場合

例えば、クラウドサービス事業者Ａ（以下「A」という。）が、クラウドサービス事業者Ｂ（以下「B」という。）のIaaSと自社のサービスとを一体として、医療機関等に提供するケースである。

この場合、Aは医療機関等との間では、２．３に示すクラウドサービス事業者の責任を全て負うことになる。

この場合の A、B における契約上及びサービス提供上の責任分界について、整理する（図 10）。

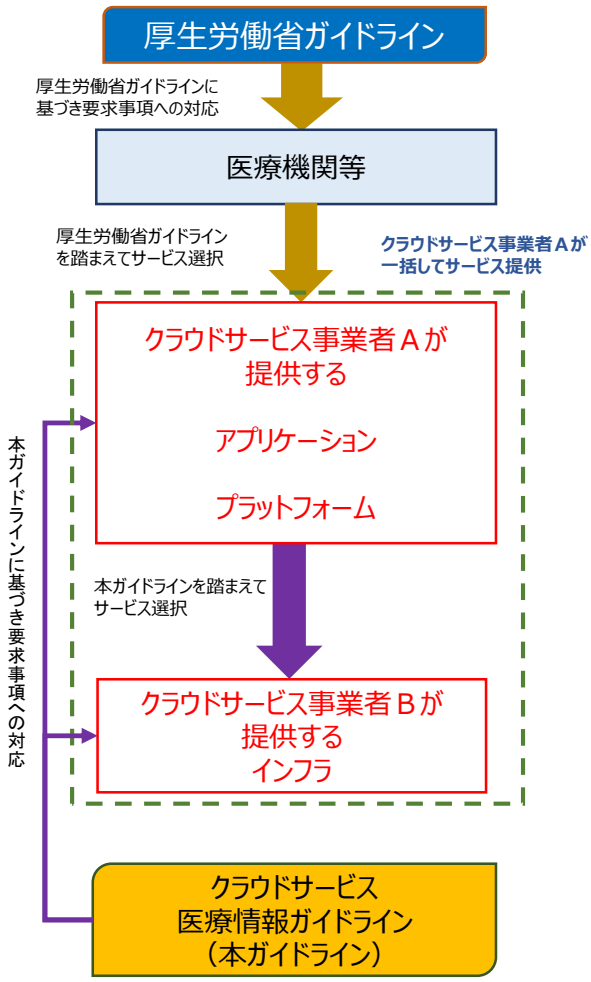


図 10　クラウドサービス事業者 A が、他社のサービスも含めて、医療機関等にサービスを提供するケース

医療情報を取り扱うクラウドサービスを提供する観点からは、A 及び B は、本ガイドラインの適用対象であることから、それぞれ独立した立場で、本ガイドラインが求める要求事項に対応することが求められる。

一方で、A と B は委託関係にあることから、医療機関等と A との関係同様に、A は B に対して、本ガイドラインが規定する要求事項への対応を求めることにになる。また、B は医療機関等から A が求められる要求事項への対応を、A に対して行う必要がある。この場合の A、B それぞれの本ガイドラインを踏まえた契約上の責任を、図 11 に示す。

A が医療機関等に対して負う責任	B が医療機関等に対して 間接的に負う責任
・A と医療機関等の間の委託契約の範囲で、本ガイドライン等を遵守したサービスを提供する責任 ・本ガイドライン等に基づくサービスを選定する責任 ・B に本ガイドライン等を遵守させる管理監督責任	・AB 間で締結した契約の範囲において、本ガイドライン等を遵守したサービスを提供する責任

図 11　クラウドサービス事業者が、他社のサービスも含めて、医療機関等にサービス提供するケースにおける受託者（A）及び再委託先（B）の責任

なお、クラウドサービスの提供に際しては、B が提供するサービスの情報システム上の機能等と、A が提供するサービスの情報システム上の機能等に関する責任分界についても取り決めることが必要である。この場合、情報システム等の内容に応じて A、B のそれぞれの責任は変わってくることから、A は、B のサービスを選択する時点で、A と B の情報システム上の機能連携を行うのに必要な対応や、障害時における責任分界点について合意することが求められる。

（２） 医療機関等が契約するクラウドサービス事業者のサービスと自社のサービスとを組み合わせて、医療機関等にサービスを提供する場合

図 12 は、クラウドサービス事業者 A（以下「A」という。）が、医療機関等に対して ASP･SaaS 及び PaaS の提供を行うものの、医療機関等の指示により、医療機関等が契約するクラウドサービス事業者 B（以下「B」という。）の IaaS を利用するケースである。

この場合、A は医療機関等との間では、A が提供するサービスの範囲で、２．３に示すクラウドサービス事業者の責任を負うことになる。

この場合の A 及び B における契約上及びサービス提供上の責任分界について整理する。

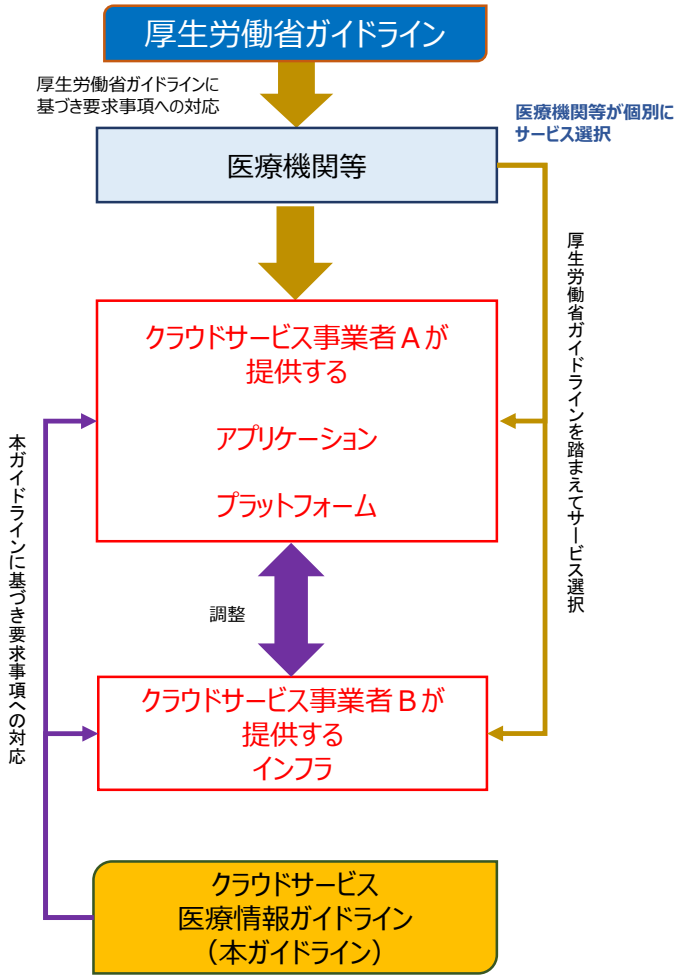


図 12　クラウドサービス事業者 A が、医療機関等が契約する他社のクラウドサービスを利用してサービスを提供するケース

A も B も、医療情報を取り扱うサービスを提供するので、本ガイドラインの適用対象であり、それぞれ本ガイドラインの要求事項に対応することが求められる。

このケースでは、A と B は委託関係にはなく、それぞれ独立して医療機関等との間の委託契約に基づいてサービスの提供を行っている。したがって、契約上は A、B は医療機関等に対しては、それぞれ独立してサービスの提供義務を負うだけであり、それぞれのサービスの提供に必要な範囲で、A と B の間で調整を行うことになる。（図 13）

A が医療機関等に対して負う責任	B において医療機関等に対して負う責任
・A と医療機関等の間の委託契約の範囲で、本ガイドライン等を遵守したクラウドサービスを提供する責任	・B と医療機関等の間の委託契約の範囲で、本ガイドライン等を遵守したクラウドサービスを提供する責任

図 13　クラウドサービス事業者が、医療機関等が契約する他社のクラウドサービスを使ってサービスを提供するケースにおける受託者（A）及び他社（B）の責任

なお、サービスの提供に際しては、A の情報システムの機能と B の情報システムの機能に関する責任分界についても取り決めることが必要である。この場合、基本的には医療機関等が各クラウドサービス事業者と取り決めることになるが、A と B は、医療機関等に対して、A と B の情報システムの機能連携に必要な対応、障害時における責任分界点等に関する必要な情報提供を行うとともに、これらの情報に基づいて医療機関等を含めて調整し、合意する必要がある。

２．３．４ オンライン診療システムをクラウドサービスにより提供する事業者における責任分界

オンライン診療の実施に当たっては、オンライン診療指針にあるように、患者、医師（医療機関）及びオンライン診療システム提供事業者の三者で、情報セキュリティ対策にかかる責任分界を合意しておくことが重要である。その際、オンライン診療システムをクラウドサービスにより提供する事業者が直接患者との間で責任分界を合意する場合や、医療機関を介して患者と責任分界を合意する場合が想定されるが、いずれの場合でもクラウドサービス事業者には患者又は医療機関に対して責任分界の合意に必要な情報を提供することが求められる。

２．４ PHR サービスを提供する場合におけるクラウドサービス事業者の責任分界の考え方

クラウドサービス事業者が PHR サービス事業者である場合の責任分界については、例えば図 14 に示すようなケースが想定される。この場合、クラウドサービスの利用は患者のみが行っており、情報も患者自らが送付していることから、医療機関等は患者が契約する PHR サービス事業者とは全く関係を有しておらず、医療機関等と PHR サービス事業者との間には責任分界の問題は生じない。

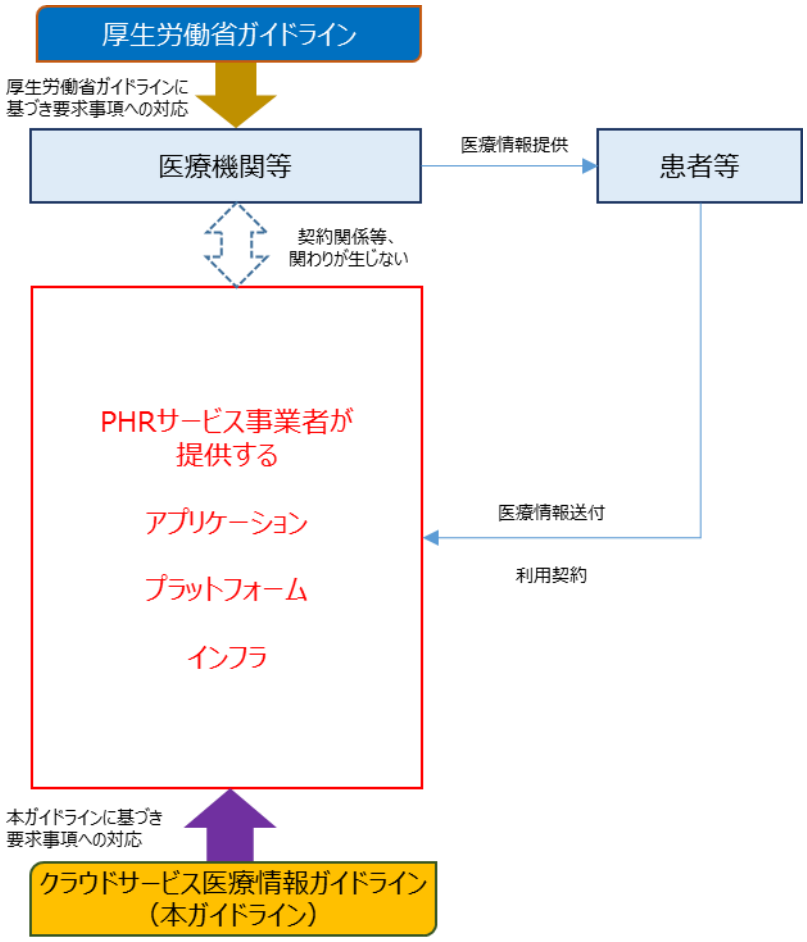


図 14　患者等が PHR サービス事業者に自らデータの送付等を行う場合

一方、患者等が医療機関等に対し、自身の医療情報を PHR サービス事業者に送付するよう依頼する場合も想定される（図 15）。

この場合、医療機関等に医療情報を PHR サービス事業者まで到達させる責任があると解すると医療機関等の負担が過大となる。そこで、医療情報を送付する情報システムの機能を勘案し、通常であれば相手方に到達すると考えられる手法により、医療機関が PHR サービス事業者向けに送信行為を行った場合、当該医療情報は相手方へ伝達されたと見なすことが適当である。

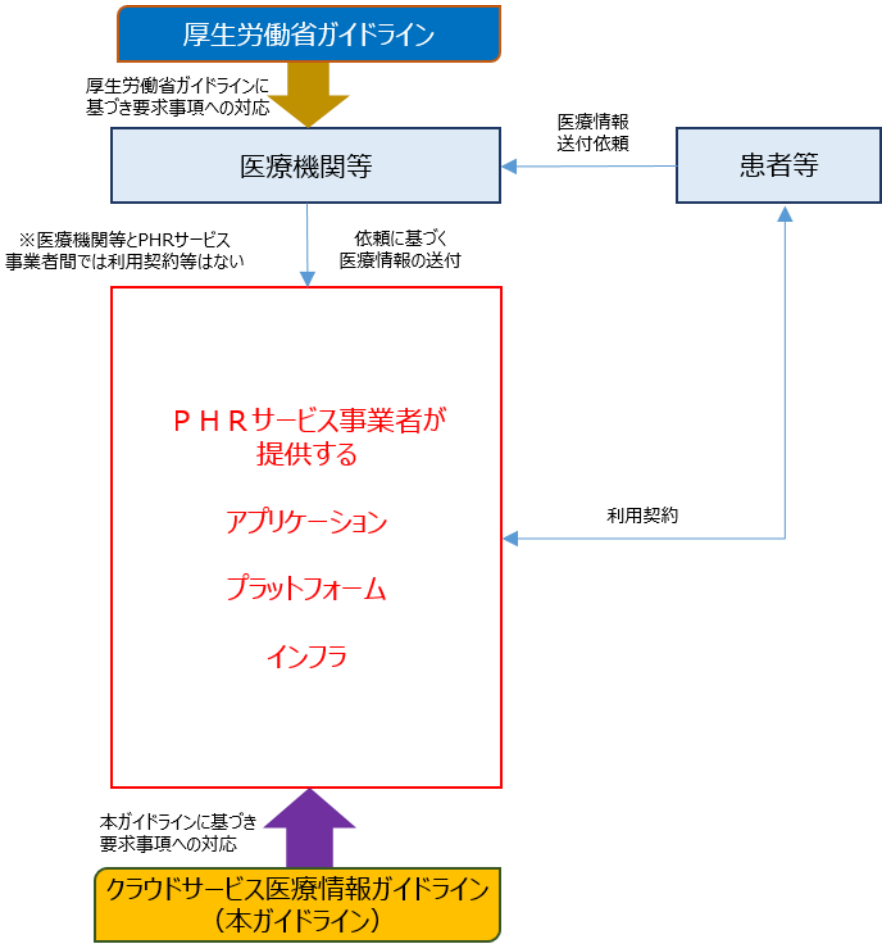


図 15　患者等の依頼で、医療機関等が患者の医療情報を送付する場合

２．５ 医療情報に関わるクラウドサービス事業者に関連する第三者認証の考え方

医療情報は特に高い注意義務による保護を要することから、クラウドサービス事業者が医療情報を取り扱う際に、公正な第三者の認証等を取得することは、医療機関等の管理者に対し情報システムや運用情報等の説明責任を果たす際に有効な手段であると考えられる。

そのため、クラウドサービス事業者が情報処理事業者の場合には、プライバシーマーク認定･ISMS 認証[16]等の公正な第三者の認証等を取得することが必須であると考えられる。これ以外のクラウドサービス事業者の場合においても、プライバシーマーク認定を取得することが強く求められる。また、ISMS 認証の取得も望ましい。ただし、これらの第三者認証を取得していることをもって、本ガイドラインにおける要求事項を全て満たすことにはならない点に留意すること。

なお、保健医療福祉分野においては「保健医療福祉分野のプライバシーマーク認定指針（第 4 版）」[17]が策定されている。医療情報を取り扱うクラウドサービス事業者がプライバシーマーク認定を取得する際には、この認定指針を参照し、遵守に努めることが望まれる[18] [19]。

---

[16] ISMS に関する一般的な基準である JIS Q 27001:2006 (ISO/IEC 27001:2005) に基づく認証のほか、クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針である JIS Q 27017:2016 (ISO/IEC 27017:2015)やパブリッククラウドにおける個人情報保護に関する指針である ISO/IEC 27018:2014 に基づく認証等がある。

[17] http://privacy.medis.jp/file/shishin33.pdf

[18] 経済産業省ガイドライン P 10 参照

[19] 医療情報を取り扱う場合のプライバシーマークとしては、「保健医療福祉分野のプライバシーマーク制度」（一般財団法人 医療情報システム開発センター）がある。

第３章 クラウドサービス事業者に対する安全管理に関する要求事項

３．１ クラウドサービス事業者に対する要求事項の考え方

３．１．１ 厚生労働省ガイドラインにおける安全対策の考え方の概要

厚生労働省ガイドライン第 5 版では、医療情報全般について、6.3 章～6.12 章で、安全管理対策を示している。また、法定保存義務のある文書については、e-文書法令等により、電子化が可能な文書が定められており、それに関する要求事項を第 7 章で「電子保存の要求事項」として示している。さらに、第 8 章では外部保存改正通知に基づいて、外部保存のための基準を示している。取り扱う医療情報の種類と、それに応じて対応すべき厚生労働省ガイドライン第 5 版における安全管理対策の関係を図 16 に示す。

クラウドサービス事業者には、これらの安全管理対策を講じることが求められる。

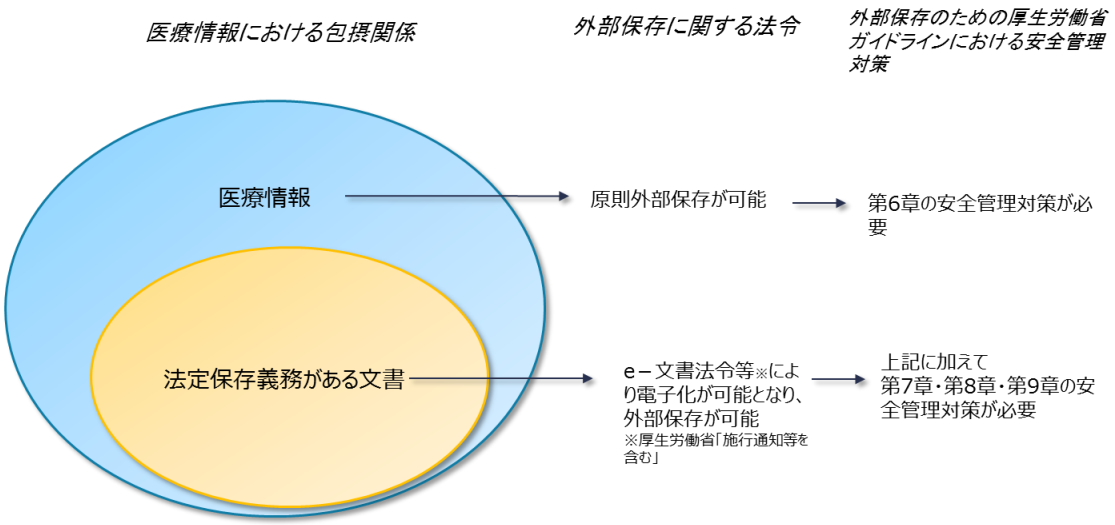


図 16　厚生労働省ガイドライン第 5 版における医療情報を外部保存するための安全管理対策

３．１．２ クラウドサービス事業者が実施すべき内容

以下では、医療機関等の管理者への要求事項に対応するクラウドサービス事業者への要求事項を整理する。

クラウドサービス事業者は、以下の要求事項に基づき、安全管理対策を行うとともに、医療機関等の管理者に対する説明責任を十分に果たしていくことが必要である。

３．２ 医療情報サービスに求められる安全管理に関する要求事項

３．２．１ 組織的安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、組織的安全管理対策について、6.3 章に以下の内容を記述している。

・安全管理対策を講じるための組織体制の整備
・安全管理対策を定める規程等の整備と規程等に従った運用
・医療情報の取扱い台帳の整備
・医療情報の安全管理対策の評価、見直し及び改善
・情報や情報端末の外部持ち出しに関する規則等の整備
・情報端末等を用いて外部から医療機関等の情報システムにリモートアクセスする場合は、その情報端末等の管理規程
・事故又は違反への対処

厚生労働省ガイドライン第 5 版では具体的には以下の内容が規定されている。

6.3 C.最低限のガイドライン

1. 情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。	
2. 個人情報が参照可能な場所においては、来訪者の記録･識別、入退を制限する等の入退管理を定めること。	
3. 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。	
4. 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。	
5. 運用管理規程等において次の内容を定めること。	
	(a) 理念（基本方針と管理目的の表明）
	(b) 医療機関等の体制
	(c) 契約書･マニュアル等の文書の管理
	(d) リスクに対する予防、発生時の対応の方法
	(e) 機器を用いる場合は機器の管理
	(f) 個人情報の記録媒体の管理（保管･授受等）の方法
	(g) 患者等への説明と同意を得る方法
	(h) 監査
	(i) 苦情･質問の受け付け窓口

（２） クラウドサービス事業者への要求事項

上述のように組織的安全管理対策においては、

・組織･体制の整備

・運用管理規程の整備

・運用管理規程に基づく文書類の整備

等が求められる。

これらの観点から、クラウドサービス事業者への要求事項として、以下の対応を行うことが求められる。

(ア) 組織･体制の整備についての要求事項

本項は、組織的安全管理対策を講じるための組織･体制の整備に関する要求事項を示す。

組織･体制の整備	①　サービスの提供についての管理責任を有する責任者を設置する。 ②　情報システムについての管理責任を負い、これについて十分な技術的能力及び経験[20]を有する責任者（システム管理者）を設置する。 ③　サービスの提供に係る情報システムの運用に関する事務を統括する責任者を設置する。 ④　①から③に掲げた責任者の任命･解任等のルールを策定する。

(イ) クラウドサービスの提供契約についての要求事項

1. 守秘義務	①　サービスに係る情報及び受託した情報に関する守秘義務について、サービス提供に係る契約に含める。契約には、守秘義務に違反したクラウドサービス事業者にはペナルティが課されること、及び委託した情報の取扱いに対する医療機関等による監督に関する内容を含める。
2. 運用規定等の遵守	①　サービス提供に係る契約において、次項（ウ）1. に定める運用管理規程等の内容、その他最新の関連法令等[21]を遵守し、安全管理措置を実施する旨を明らかにする。
3. 関係ガイドラインの遵守	①　サービス提供に係る契約において、本ガイドラインのほか、厚生労働省ガイドライン及び経済産業省ガイドラインを遵守する旨を含める。 ②　①に示す各ガイドラインの遵守状況を医療機関等に提示する際は、可能な

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

[21] 当該サービスに関係する日本国外の法令を含む。

	限り具体的に行う（例えば、総務省が定める「ASP･SaaS（医療情報取扱いサービス）の安全･信頼性に係る情報開示指針」[22]（平成 29 年 3 月 31 日）に定める事項に準じた情報の提供を行う等）

(ウ) 運用管理規程についての要求事項

本項は、安全管理対策を講じるための運用管理規程の整備に関する要求事項を示す。厚生労働省ガイドライン第 5 版では、運用管理規程において含めるべき内容について 9 項目を定めている。ここではこれらの項目に従って、クラウドサービス事業者において、自社の運用管理規程の策定や、医療機関との合意等において、対応すべき要求事項を示す。

1. 基本方針と管理目的の表明	① 経営者は、自社における個人情報保護指針、プライバシーポリシー等について明確にする。 ② ①の指針等には個人情報保護法及び個人情報保護委員会のガイドラインに定める安全管理措置等を実施する旨を含める。 ③ ①の指針等には、個人情報保護法の対象外の情報（死者に関する情報等）であっても、医療情報の特殊性から個人情報保護法における運用に準じて取り扱う旨を含める。 ④ 情報セキュリティに関する基本方針、運用管理規程等の情報セキュリティポリシーを策定する。 ⑤ 情報セキュリティポリシーの遵守を担保する組織体制の構築とその文書化を行う。 ⑥ 情報セキュリティポリシーについて、サービス仕様適合開示書に基づき、医療機関等と合意する。
2. サービス提供先の体制	① サービスの提供に係る体制を、緊急時の対応も含めて明確にする。 ② サービスの提供に係る体制等に関する情報（再委託による体制に関する情報を含む）の開示等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
3. 契約書・マニュアル等の文書の管理	① 情報セキュリティに関する基本方針や運用管理規程等、重要な文書の作成や管理に関する規程を策定し、これに基づき文書の管理を行う。 ② サービスの運用や資源管理に関して、適切に文書化を行い、セキュリティ情報として管理する。

[22] 「ASP・SaaS（医療情報取扱いサービス）の安全・信頼性に係る情報開示指針」について、具体的な運用の例として「医療情報 ASP・SaaS 情報開示認定制度」（運営：クラウドサービス安全・信頼性情報開示認定制度事務局）が挙げられる。

	③　サービスの運用等に係るマニュアル等の文書管理に関して、開示可能範囲、開示に必要な条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④　医療情報の管理状況に関係する資料の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。
4.リスクの発現の予防、発生時の対応の方法	①　サービスに係るリスクの分析を行い、必要な対応措置等を講じる旨を定める。 ②　サービスに係るリスク分析の結果、対応措置及び事故等の発生時の対応等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
5.機器を用いる場合の機器等の管理	①　機器等の管理方法について、文書化を行う。 ②　機器等について、台帳管理等により所在確認等を行う旨を定める。 ③　機器等の管理等に関する自社の運用規程について、サービス仕様適合開示書に基づき、医療機関等と合意する。
6.個人情報の記録媒体の管理方法	①　個人情報を記録した媒体の管理等に関する運用規程を策定する。 ②　個人情報を記録した媒体の管理等に関する運用規程について、サービス仕様適合開示書に基づき、医療機関等と合意する。
7.患者等への説明と同意を得る方法	①　医療機関等で患者等への説明及び同意を得る際のクラウドサービス事業者の情報提供に関して、その提供範囲やクラウドサービス事業者が担う役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
8.監査	①　サービスを提供する情報システム、組織体制、運用等に関する監査の方針、内容等について明文化を行う。 ②　第三者が提供するクラウドサービスを利用する場合については、これに対する監査又は代替する対応についての方針、内容を明確にする。 ③　監査実施について記録し、当該記録の保存･管理方法を明確にする。 ④　自社において実施する情報システム監査等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤　医療機関等に開示する監査記録等の範囲･条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
9.苦情･質問の受け付け窓口の設置	①　医療機関等の管理者からの問合せ窓口を設ける。また受付の時間帯等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ②　自社で契約した第三者が提供するクラウドサービスを利用してサービスを提供する場合でも、医療機関等からの問合せ窓口を一元化する。

なお、運用管理規程に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.2.1　資産台帳】

実施すべき安全管理策

(1)　医療機関等から預かる情報を管理するための管理台帳の整備について文書化して管理すること。

(2)　預託された情報の全てを資産台帳に記録すること。

(3)　必要に応じて資産台帳の閲覧が速やかに行うことができる状態で管理しておくこと。

(4)　資産台帳等へのアクセスについては、閲覧･編集が必要な作業者に制限すること。

(5)　資産台帳等を電磁的記録として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について記録すること。

推奨される安全管理策

(1)　資産台帳等を紙文書として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について検出･記録できるような仕組みを実装することが望ましい。

(2)　資産台帳等に記録する情報には次のようなものが考えられる。

- 整理番号
- 資産の名称（医療情報の名称）
- 資産の医療情報としての種別
- データ形式及び見読化手段
- 資産の所在地と複製の可否及び複製の所在地
- 資産を保存する情報処理装置、電子媒体の識別番号等
- 資産を扱う医療機関等業務の概要
- 情報処理事業者における管理責任者
- 設定されたアクセス権限とアクセス権限者
- 資産の発生日時、保有する期限、廃棄予定日
- 資産に対する処理の履歴（保存、配送、複製、廃棄等）

【7.3 組織的安全管理策（体制、運用管理規程)】

実施すべき安全管理策

(4)　情報処理の安全管理に関わる手順書、運用管理規程を整備すること。

(5)　運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内の体制及び施設、医療機関等及び清掃事業者等の外部事業者との契約書の管理、情報処理に関わるハードウェア･ソフトウェアの管理方法、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理（保管･授受等)、第三者による情報セ

キュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載しておくこと。

(エ)運用管理規程に基づく文書類の整備についての要求事項

本項は、運用管理規程に基づく文書類の整備に関する要求事項を示す。厚生労働省ガイドライン第5版では、個人情報が参照可能な施設等の入退管理に関する規程等や、アクセス管理規程、委託契約において含めるべき内容について定めている。ここではこれらの項目に従って、クラウドサービス事業者が対応すべき要求事項を示す。

1. アクセス管理規程の策定	**① クラウドサービス事業者における情報システムへのアクセス権限、アカウント管理、認証及びアクセス等に対する記録の収集と保存、並びにアクセス管理の運用状況に関する定期的なレビューの実施等を内容とするアクセス管理規程を策定する。** **② サービスの提供に係るアクセス記録（外部からのアクセス、利用者によるアクセス等を含む）の保存、記録の定期的なレビューと改善を実施する旨を内容とするアクセス管理規程を策定する。**
2. 委託契約に含めるべき事項	**① 医療情報の取扱いに関する委託契約に、以下の内容を含める。** **・個人情報に関して、他の情報と区別して適切に管理を行う。** **・医療情報は、死者に関する情報についても個人情報に準じて取り扱う旨を明確にする。**

なお、運用管理規程に基づく文書類の整備に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.2.2　情報の分類】

実施すべき安全管理策

(1) 情報を分類するための指針を決定し、情報の所有者、管理責任者が指針に従って適切な分類を行うことができるようにしておくこと。

(2) 情報の所有者、管理責任者は情報の分類が正しく行われていることを定期的に確認すること。

(3) 預託される情報に対して分類にもとづいたリスク分析を実施すること。

(4) リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること。

(5) 分類がわかるように情報にラベルをつけること（電磁的記録にラベルをつける方

式には様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得ること)。

(6) 各ラベルに応じた処理方式（保存、配送、複製、廃棄等）を定めること。

３．２．２ 物理的安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、物理的安全管理対策について、6.4 章に記述している。

物理的安全管理対策とは、医療情報を取り扱う機器、媒体等を物理的な措置によって保護することであり、安全性の確保を講じるための方策を指す。

主に

・入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理）
・盗難、覗き見等の防止
・機器･装置･情報媒体等の盗難や紛失防止も含めた物理的な保護及び措置

等の対策が想定される。

厚生労働省ガイドライン第 5 版では具体的には以下の内容が規定されている。

6.4 C.最低限のガイドライン

1. 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
2. 個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることができない対策を講じること。ただし、本対策項目と同等レベルの他の取り得る手段がある場合はこの限りではない。
3. 個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・ 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・ 入退者の記録を定期的にチェックし、妥当性を確認する。
4. 個人情報が存在する PC 等の重要な機器に盗難防止用チェーンを設置すること。
5. 覗き見防止の対策を実施すること。

6.4 D.推奨されるガイドライン

1. 防犯カメラ、自動侵入監視装置等を設置すること。

（２） クラウドサービス事業者への要求事項

（１）を踏まえ、クラウドサービス事業者が行うべき要求事項について以下に記述する。

（ア）サービスに供する機器、媒体等の設置場所等における物理的安全管理対策としての要求事項

（イ）個人情報が参照可能な運用端末等の設置場所等における物理的安全管理対策としての要求事項

（ウ）個人情報が格納されている機器や媒体に対する物理的安全管理対策としての要求事項

なお、本項では、厚生労働省ガイドライン第5版6.4章に対応する要求事項について記載するが、一部、厚生労働省ガイドライン第5版7.3章「保存性の確保について」で示される要求事項のうち、物理的安全管理対策に関するに対応する要求事項も含めることとする。そのため、厚生労働省ガイドライン第5版6.4章では、個人情報の取扱いを対象としているが、ここでは「医療情報を取り扱うサービス」に供する情報全般（例えばサービス提供上の設定データ等、情報が保存されている媒体及び機器の適切な保管･取扱いに必要な情報）を対象としている。

（ア） サービスに供する機器、媒体等の設置場所等における物理的安全管理対策としての要求事項

本項は、サービスに供する機器、媒体等の設置場所に対して、物理的な安全対策を求めるものである。具体的には、機器等の設置場所の施錠管理とアクセス管理（不正なアクセスの防止とそのための管理･監視措置）を内容とする。

1. 施錠管理	① サービスに供する機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。 ② サービスに供するサーバ等を格納するラック等について、施錠管理を行う。 ③ サービスに供する媒体等を格納するキャビネット等について、施錠管理を行う。
2. アクセス制御	① サービスに供する機器や媒体の設置場所については、許可された者のみが入退できるように制限する。 ② サービスに供する機器や媒体の設置場所への入退状況の管理（入退記録のレビュー含む）は定期的に行う。 ③ サービスに供する機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退

	者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じる。 ④　サービスに供する機器や媒体の設置場所への不明者の入退を発見するために、入退者に名札等の着用を義務付ける。 ⑤　サービスに供する機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。 ⑥　サービスに供する機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。 ⑦　①～⑥につき、運用管理規程等に規定する。
3. サービスに供する機器や媒体を保存する施設	①　サービスに供する機器や媒体を物理的に保存するための施設は、災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能･構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置する。 ②　①の施設を設置する建築物は、サービス仕様適合開示書に基づき、医療機関等と合意する。
4. カメラによる監視	①　サービスに供する機器等が保存されている建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等を設置する。 ②　防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる。 ③　サービスに供する機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、状況を確認することで、不正な入退者がないことを確認する。

なお、医療情報が物理的に保存されている機器、媒体の設置場所等における物理的安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.5.1 医療情報処理施設の建物に関する要求事項】

実施すべき安全管理策

(1) 情報処理事業者の専有する領域に医療情報システムを設置する場合には、以下に示す物理的安全管理策を施すこと。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認すること。

● 医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理が行われていること。

● 傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施すこと。

● 建物、部屋に対する不正な物理的な侵入を抑止するため、監視カメラ等の侵入検知装置を導入すること。

● 自然災害、人的災害による損傷を避けるため、建物自体の防災対策を適切に実施すること。

【7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項】

① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合

実施すべき安全管理策

(1) 医療情報システムを設置、医療情報を保管する部屋の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証を行うこと。

(2) 有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用すること。

(3) 有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認すること（履歴の保全については「7.6.12 ログの取得及び監査」を参照）。

(4) 情報処理事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した情報処理事業者の職員証を外部から目視で確認できる状態で携帯することを義務付け、情報処理事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておくこと。

(5) 情報処理事業者の職員は、情報処理事業者の専有する領域にて、情報処理事業者の職員で無い者を識別した際には声掛け等を行い、身分を確認すること。

(6) 職員証を紛失あるいは不正利用された疑いを持った際には、ただちに管理者に連絡する、情報処理事業者職員の退職時には確実に職員証を回収･廃棄する等、職員証の厳密な発行及び失効管理を行うこと。

(7) 情報処理事業者の職員の業務に応じて執務室内に滞在できる時間を指定すること。

(8) 医療情報処理施設内への業務遂行に関係のない個人的所有物の持ち込みを認めないこと。

② 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用

する場合

実施すべき安全管理策

(1) データセンターを運営する外部事業者が、①と同等な安全管理策を実施する等、情報処理事業者の管理外にある者の物理的な不正操作に対する十分な安全性が確保されていることを確認すること。

(2) 医療情報システムの設置されるサーバラックには施錠を行い、定められた情報処理事業者の職員以外が鍵を扱わないよう、確実な鍵管理を行うこと。

(3) 情報処理事業者が医療情報システムの設置されるサーバラックを解錠して行う作業については、作業者、作業開始時刻、作業終了時刻、作業内容等について記録すること。

(5) 医療情報システムであることが、同じデータセンター内に立ち入る他事業者にわからないよう、扱う情報の種類、システムの機能等が識別できるような情報を外部から見える状態にしないこと。

推奨される安全管理策

(1) 医療情報システムの設置されるサーバラックの施錠装置については、ハードウェアトークン又はICカード等の認証デバイス、暗証番号（PIN）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。

③ 外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合

実施すべき安全管理策

(1) サーバ環境を運営する外部事業者が、①及び②と同等な安全管理策を実施する等、情報処理事業者の管理外にある者の不正なアクセスに対する十分な安全性が確保されていることを確認すること。

【7.5.3 情報処理装置のセキュリティ】

実施すべき安全管理策

(5) 火災発生時の消火設備が機器に損傷を与えないよう配慮すること。

(6) 医療情報システムを配置する室内での喫煙、飲食を禁止すること。

(7) 医療情報システムを配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮すること。

(10) 医療情報システムを設置するサーバラックについては以下の安全管理策を実施すること。

- 震災時に転倒することが無いよう確実に設置すること。
- 熱による障害を防ぐため十分な空調設備を保有し、サーバラック内が十分に換気されていること。
- 扉には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配

慮すること。
【7.6.5 第三者が提供するサービスの管理】 実施すべき安全管理策 (4) サービスを実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れないこと。 (5) サービス実施中に第三者が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯すること。 (6) サービス実施にともなう処理施設内への立ち入り手順に関しては、情報処理事業者の職員の入室、退室手順に準ずること。
【7.6.12 ログの取得及び監査】 実施すべき安全管理策 (1) 作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成し、管理すること。 (2) 監査ログを定期的に検証して不正な行為、システムの異常等を検出すること。 (3) ログを利用して正確に事故原因等を検証するため、医療情報システムのすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておくこと。 (4) 標準時刻に同期するための時刻提供元は信頼できる機関を利用すること。 (5) ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用すること。 ● ログデータにアクセスする作業者及び操作を制限すること。 ● 容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。 ● ログデータに対する不正な改ざん及び削除行為に対する検出･防止策を施すこと。 推奨される安全管理策 (1) 医療情報システムのすべてのサーバ機器等の時刻が時刻サーバ等の提供する標準時刻に同期していることを定期的に検証することが望ましい。 (2) 監査ログに記録する事項としては次のようなものが考えられる。 ● 作業者情報（作業者 ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元 IP アドレス） ● ファイル及びデータへのアクセス、変更、削除記録（作業者 ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類） ● データベース操作記録（作業者 ID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元 IP アドレス、設定変更時にはその内容） ● 修正パッチの適用作業（作業者 ID、変更されたファイル） ● 特権操作（特権取得者 ID、特権取得の可否、利用時刻及び時間、実行作業内容）

● システム起動、停止イベント ● ログ取得機能の開始、終了イベント ● 外部デバイスの取り外し ● IDS･IPS 等のセキュリティ装置のイベントログ ● サービス及びアプリケーションの動作により生成されたログ（時刻同期に関するログを含む） (1) 監査ログを検証するため、作業者がアクセスした医療情報等を迅速に確認できるよう、作業者 ID と、情報の識別子（資産台帳記載の番号等）、生成時系列、アクセス時系列等、多様な指標での並び替え、情報の種別、アクセス時間等での絞り込み等が行うことができるようなシステムを整備することが望ましい。
【7.6.13　アクセス制御方針】 実施すべき安全管理策 (1) 情報処理に用いる情報処理装置それぞれのセキュリティ要求事項を整理すること (2) 情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理すること

(イ) 個人情報が参照可能な運用端末等に対する物理的安全管理対策としての要求事項

本項は、個人情報が参照可能な運用端末等に対する物理的な安全管理対策を求めるものである。具体的には、覗き見等の防止を内容とする。

1. 覗き見等の防止	**① 個人情報の表示中の覗き見を予防するために、運用端末に覗き見対策のシートを貼る等の対策を行う。** **② 運用中の画面が、運用者以外の者の視野に入らないような対応等を行う。**

(ウ) 個人情報が格納されている機器、媒体に対する物理的安全管理対策としての要求事項

本項は、個人情報が物理的に保存されている機器、媒体の盗難･紛失等を避けるための物理的措置を講じることを求めるものである。

1. 機器･媒体等の盗難･紛失防止	**① 個人情報が物理的に保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。** **② 個人情報が存在する PC 等の重要な機器には、盗難防止用チェーンを取り付ける。** **③ 受託する個人情報を運用や保守に用いる端末に保存しない旨、自社の運用管理規程等に定める。**

なお、個人情報が格納されている機器、媒体に対する物理的安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

> 【7.5.3 情報処理装置のセキュリティ】
> 実施すべき安全管理策
> (4) 医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにすること。

３．２．３ 技術的安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、技術的安全管理対策について、6.5 章に記述している。

技術的安全管理対策は、医療情報システムに対する脅威への技術的な対策である。具体的には、

・利用者の識別及び認証
・情報の区分管理とアクセス権限の管理
・アクセスの記録（アクセスログ）
・不正ソフトウェア対策
・ネットワーク上からの不正アクセス
・医療等分野における IoT 機器のセキュリティ対策

等の対策が示されている。具体的な対策として規定されている内容を以下に示す。

6.5 C.最低限のガイドライン

1. 情報システムへのアクセスにおける利用者の識別と認証を行うこと。
2. 本人の識別･認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。
3. 本人の識別･認証に IC カード等のセキュリティ･デバイスを用いる場合には、IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。
4. 入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力のおそれがある場合には、クリアスクリーン等の防止策を講じること。
5. 動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。
6. 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。
7. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、並びにログイン中に操作した患者が特定できること。情報システムにアクセス記録機能があることが前提であ

るが、ない場合は業務日誌等で操作の記録（操作者及び操作内容等）を必ず行うこと。
8.　アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること。
9.　アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。
10.　システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
11.　パスワードを利用者識別に使用する場合 システム管理者は以下の事項に留意すること。 (1) システム内のパスワードファイルでパスワードは必ず暗号化(可能なら不可逆変換が望ましい)され、適切な手法で管理及び運用が行われること。また、利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。 (2) 利用者がパスワードを忘れたり、盗用されたりするおそれがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知り得ない方法で再登録を実施すること。 (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること。(設定ファイルにパスワードが記載される等があってはならない。) また、利用者は以下の事項に留意すること。 (1) パスワードは定期的に変更し（最長でも 2 ヶ月以内 ※D.5 に規定する 2 要素認証を採用している場合を除く。）、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。 (2) 類推しやすいパスワードを使用しないこと。かつ類似のパスワードを繰り返し使用しないこと。類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。

12. 無線 LAN を利用する場合

システム管理者は以下の事項に留意すること。

(1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策をとること。

(2) 不正アクセスの対策を施すこと。少なくとも SSID や MAC アドレスによるアクセス制限を行うこと。

(3) 不正な情報の取得を防止すること。例えば WPA2/AES 等により、通信を暗号化し情報を保護すること。

(4) 電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。

(5) 無線 LAN の適用に関しては、総務省発行の「一般利用者が安心して無線 LAN を利用するために」や「企業等が安心して無線 LAN を導入･運用するために」を参考にすること。

13. IoT 機器を利用する場合

システム管理者は以下の事項に留意すること。

(1) IoT 機器により患者情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。

(2) セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置の IoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。

(3) IoT 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用すること。

(4) 使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を講じること。

6.5 D.推奨されるガイドライン

1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。

2. 離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等）。
3. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクションやそれと同等の機能を含む）を設置し、ACL(アクセス制御リスト)等を適切に設定すること。
4. パスワードを利用者識別に使用する場合以下の基準を遵守すること。 (1) パスワード入力が不成功に終わった場合の再入力に対して一定不応時間を設定すること。 (2) パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。
5. 認証に用いられる手段としては、ID･パスワード＋バイオメトリクス又は IC カード等のセキュリティ･デバイス＋パスワード若しくはバイオメトリクスのように 2 つの独立した要素を用いて行う方式（2 要素認証）等、より認証強度が高い方式を採用すること。ただし、情報システムを利用する端末に 2 要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時･端末利用時を含め 2 要素以上（記憶･生体計測･物理媒体のいずれか 2 つ以上）の認証がなされていれば、2 要素認証と同等と考えてよい。
6. 無線 LAN のアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば 802.1x や電子証明書を組み合わせたセキュリティ強化をすること。
7. IoT 機器を含むシステムの接続状況や異常発生を把握するため、IoT 機器･システムがそれぞれの状態や他の機器との通信状態を収集･把握し、ログとして適切に記録すること。

（２） クラウドサービス事業者への要求事項

（１）を踏まえ、クラウドサービス事業者は技術的安全管理対策として、

・利用者の識別及び認証
・情報の区分管理とアクセス権限の管理
・アクセスの記録（アクセスログ）
・不正ソフトウェア対策
・サービス利用に係る機器等（無線 LAN、IoT 機器）のセキュリティ対策

等が求められる。

これに加えて、「ｅ-文書法の対象となる医療情報を含む文書等の作成における真正性の確保」、「ソフトウェア･機器の品質管理」、「応答時間に関する対応」、「医療情報等の保存」に関する要求事項も、技術的安全管理対策に含めている。

厚生労働省ガイドライン第 5 版では「ｅ-文書法の対象となる医療情報を含む文書等の作成における真正性の確保」、「ソフトウェア･機器の品質管理」は、「7.1　真正性の確保について」、「応答時間に関する対応」は「7.2　見読性の確保について」、「医療情報等の保存」は「7.3　保存性の確保について」で対策が示されている。いずれも外部保存を行うための追加的な要件として示されているものであるが、クラウドサービスにおいては、外部保存による対応ができるものが中心であることから、技術的安全管理対策として規定した。

以上を踏まえて、クラウドサービス事業者が医療情報を取り扱うサービスを提供する上で対応すべき内容、医療機関等と合意すべき内容について要求事項として整理する。

(ア)利用者の識別及び認証に対する要求事項

本項は、利用者認証に関する要求事項について記載する。厚生労働省ガイドライン第 5 版では、医療情報システムの不正な利用（なりすまし）を防止する観点から、利用者を特定･識別するための認証を求めている。認証方法としては、ID 及びパスワードの組み合わせ以外の認証方法を推奨しているが、ID 及びパスワードの組み合わせによる認証による場合にとるべき対策、複数要素認証による場合の対応策等についても示している。これに対応するクラウドサービス事業者に対するの具体的な要求事項を以下に示す。

1. 利用者の識別	①　情報システムの利用者を特定し識別できるように、アカウントの発行を行う（複数の利用者による ID の共同利用は行わない。ただし当該情報システムが他の情報システムを利用するための ID（non interactive ID）は除く）。 ②　利用者のなりすまし等を防止するための認証を行う。

	③　利用者には、医療機関等においてサービスを利用する者のほか、情報システムの運用若しくは開発に従事する者又は管理者権限を有する者も含める。 ④　情報システムの運用若しくは開発に従事する者又は管理者権限を有する者に対する ID の発行は必要最小限とし、定期的な棚卸しを行う。
2. 本人識別のためにパスワードを設定する時のルール	①　本人の識別･認証に、ユーザ ID とパスワードを組み合わせて用いる場合には、それらを、本人しか知り得ない状態に保つよう対策を行う。具体的には以下のような対策を行う。 ・利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと情報システムにアクセスできないにようにする。 ・初期パスワード以外のパスワードは、利用者本人に設定させるとともに、利用者本人しか知りえない内容を設定するよう求める。 ・パスワードの設定に際しては、複数の文字種（英数字･大文字･小文字･記号等）を用い、また、8 文字以上等、十分に安全な長さの文字列等から構成されるルールとする。 ②　パスワード認証に係る以下のルールを実現する措置を講じる。 ・パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定する。 ・パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない仕組みとする。 ③　パスワードには十分な安全性を満たす有効期間を設定する。ただし、利用者が患者等である場合には、他のサービスで利用しているパスワードを使わないよう特に促すだけでなく、サービス提供側から患者等に対して定期的なパスワードの変更を要求しないようにする。[23] ④　認証に際して ID 及びパスワードによらない場合でも、上記と同等以上の安全性を確保する。
3. パスワードの管理	①　利用者のパスワードは、ハッシュ値での保存を行う等、暗号化して管理する。 ②　サービスを提供する製品等の導入に際しては、初期パスワードを変更するだけでなく、アカウントの棚卸しを行い、不要なものについては削除を行う。 ③　利用者が ID やパスワードを失念した場合には、予め策定した手順（本人確認を含む）に則り、本人への通知又は再発行を行う。 ④　パスワード等の情報の漏洩が生じた場合（不正な第三者からの攻撃による

[23] 総務省「国民のための情報セキュリティサイト」においても、パスワードは「定期的に変更するよりも、機器やサービスの間で使い回しのない、固有のパスワードを設定すること」が求められる旨及び「米国国立標準技術研究所（NIST）からガイドラインとして、サービスを提供する側がパスワードの定期的な変更を要求すべきではない旨が示された」と記載されている。http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-2.html

	場合を含む）には、直ちに当該 ID を無効化し、予め策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知する。 ⑤　パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知した上で、当該パスワードを無効化し、変更できるような対応を講じる。 ⑥　利用者が設定するパスワードについては、第三者から容易に推定されにくい内容を含む品質基準を策定し、これに基づく運用を行う。 ⑦　利用者のパスワードの世代管理を行い、パスワード変更に際して、安全性を確保するために必要な範囲で、過去に設定したパスワードを設定できないような運用を行う。 ⑧　利用者のパスワードポリシーについて、サービス仕様適合開示書に基づき、医療機関等と合意する。
4.複数要素認証への対応	①　情報システムの運用若しくは開発に従事する者又は管理者権限を有する者の情報システム利用に係る認証は、2 要素認証以上の認証強度のある方法による。 ②　利用者の認証で採用する認証方式について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③　利用者の認証において、固定式の ID･パスワードによる認証方式を採用している場合には、固定式の ID･パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン 第 5 版の公表（平成 29 年 5 月）から約 10 年後を目途に 2 要素認証について厚生労働省ガイドライン 6.5 章「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。 ④　利用者の認証に際して、何らかの物理的な媒体･身体情報等を必要とする場合に、例外的にそれらの媒体等がなくても一時的に認証するための代替的手段･手順を事前に定める。 ⑤　代替的手段･手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差が最小となるようにする。 ⑥　代替的手段･手順により、情報システム利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理する。 ⑦　その他、一時的な利用者の認証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、利用者の識別及び認証に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項】

推奨される安全管理策

(1) 機械式の認証装置で利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN ）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。

【7.6.6 ネットワークセキュリティ管理】

実施すべき安全管理策

(10) 医療情報システムのサーバ機器等への同時ログオンユーザ数 (OS アカウント等) に適切な上限を設けること。

【7.6.10 アプリケーションに対するセキュリティ要求事項】

実施すべき安全管理策

(4) アプリケーションにて医療事業者側の作業者を認証する情報 (ID／パスワード認証の際のパスワード) は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。

【7.6.14 作業者アクセス及び作業者 ID の管理】

パスワード管理について実施すべき安全管理策

(1) 情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。

(2) 医療情報システムへのログオン用パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管すること。

(3) 医療情報システムへのログオン用パスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。

(4) 医療情報システムへのログオン用パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。

(5) パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とすること。

(6) パスワード発行時には、乱数から生成した仮の医療情報システムへのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施すること。

(7) パスワードの満たすべき品質の基準を策定し、すべてのパスワードが品質基準を満たしていることを確実とすること。

(8) パスワードを情報システムに記憶させる自動ログオン機能を利用しないよう作

業者に徹底すること。

(9) パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用すること。また、一般の作業者による閲覧を制限すること。

パスワード管理について推奨される安全管理策

(1) 作業者が医療情報システムへのログオン用パスワードを登録及び変更する際には、予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、作業者が設定しようとする品質の低いパスワードを認めない情報システムの導入等を検討することが望ましい。

(2) パスワードの品質基準としては、パスワードを十分に長くすること（8 文字以上等）、アルファベット及び数字並びに記号を一つ以上含むこと、等が考えられる。

作業者のログオンについて実施すべき安全管理策

(2) パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定すること。連続してログオンが失敗した場合は再入力を一定期間受付けない機構とすること。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入すること。

作業者のログオンについて推奨される安全管理策

(1) 不正なアカウントの利用又は試みが行われたことを作業者自身で検出するため、作業者のログオン後に前回のログオンが成功していれば成功日時を表示し、前回のログオンが失敗していれば、第三者による不正なログオンの試みが行われた可能性があるという内容の警告メッセージとともに失敗日時を表示することが望ましい。

(2) 不正なアカウントの利用を防ぐため、作業者のログオンを許可する曜日、時間帯は作業に必要な曜日、時間帯に制限することが望ましい。

(3) 認可されていない作業者あるいは第三者がログオンを試みた際に「パスワードが異なります」と表示すると作業者 ID が存在していることを知る手がかりとなるため、「認証に失敗しました」、あるいは単にログオンプロンプトを再表示するといった特段の情報を与えないようなメッセージのみの表現に留めることが望ましい。

(4) 緊急時の作業のため、規定時間外にログオンを行う必要が発生した場合の妥当な承認プロセスを策定することが望ましい。

(5) ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。

【7.6.15　作業者の責任及び周知】

実施すべき安全管理策

(1) 各作業者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合

は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護すること。

(2) 情報システムに許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知すること。

(イ) 情報の区分管理とアクセス権限の管理に対する要求事項

本項は、医療情報を取り扱うクラウドサービスにおける情報システム上の利用権限に関する要求事項について示す。厚生労働省ガイドライン第5版では、医療情報に対して、医療従事者の資格に応じたアクセス権限の設定を厳格に行えるようにするための対応策等について示している。

クラウドサービス事業者の対応として、受託する情報のほか、医療情報を取り扱うクラウドサービスに係る情報も含めて、情報区分を設定し、それぞれについて適切な権限設定･付与を行うこと等に対応するための要求事項を示す。

1. 情報管理区分	① 医療情報とそれ以外の情報を区分できる措置を講じる。 ② 医療情報については、情報区分に従ってアクセス制御を行えるようにする。 ③ 仮想化技術を用いた資源をサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じる。 ④ 医療機関等による情報資産の区分の設定や、これに対するアクセス制御の設定の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。
2. 権限設定	① サービスには、医療従事者、関係職種ごとにアクセス権限･範囲等のアクセス制御が可能な機能を含める。 ② 医療機関等の利用者の職種等に応じたアクセス制御の設定について医療機関等に示し、医療機関等と必要な協議を行い、実際に設定する作業に関する役割分担も含めて合意する。なお、アクセス制御に係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 運用管理規程に従い、アクセス管理に関する運用を行い、医療機関等の求めに応じて資料を提出できるようにする。資料の提供に係る条件等については、サービス仕様適合開示書に基づき、医療機関等と合意する。
3. アクセス対象の設定	① サービスには、受託する医療情報を患者等ごとに管理できる機能を含める。

なお、情報の区分管理とアクセス権限の管理に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.13　アクセス制御方針】

実施すべき安全管理策

(3)　アクセス権限の登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセスを規定すること。

(4)　それぞれの情報にアクセスする権限を持つ作業者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行うこと。

(5)　業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定すること。

推奨される安全管理策

(1)　作業者に与えられた権限外の情報や権限外の操作画面を表示しないよう権限管理を行うことが望ましい。

(2)　定められたアクセス制御方針がファイル、ディレクトリパーミッション、データベースアクセス等のアクセス制御機構として適切に反映されていることを定期的に検証することが望ましい。

(ウ) e-文書法の対象となる医療情報を含む文書等の作成における真正性の確保に対する要求事項

(a)　入力者及び確定者の識別及び認証に関する安全管理対策

1. PC 等の汎用入力端末により記録が作成される場合	①　e-文書法の対象となる医療情報を含む文書等の作成に PC 等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・医療機関等の職務権限等に応じたアクセス制御の可否を含め、入力者及び確定者の識別及び認証に関する仕様
2. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合	①　e-文書法の対象となる医療情報を含む文書等の作成に臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムを利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・サービスとの連携におけるインタフェースの構築に関する役割分担

なお、入力者及び確定者の識別及び認証に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.10 アプリケーションに対するセキュリティ要求事項】
実施すべき安全管理策
（5） アプリケーションによる情報操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止すること。

(b) 記録の確定手順の確立と、作成責任者の識別情報の記録に関する安全管理対策

1. PC 等の汎用入力端末により記録が作成される場合	① e-文書法の対象となる医療情報を含む文書等の作成に PC 等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・確定された登録情報（入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時）に関する仕様 ・入力された内容についての記録確定前における確認の可否等についての仕様 ・記録の確定権限に関する仕様 ・確定した記録の追記･削除の機能等に関する仕様 ・確定した記録の原状回復の機能等に関する仕様 ・記録の自動確定機能等に関する仕様 ・代替的な確定権限の機能等に関する仕様

(c) 更新履歴の保存に関する安全管理対策

1. 更新履歴比較機能	① 真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新前と更新後のデータが保存される、又は更新履歴等が保存される等、更新前後の内容を照らし合せることができる機能を含める。
2. 更新順序識別機能	① 真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新履歴が保存され、更新の順序性が識別できる機能を含める。

(d) 代行入力の承認機能に関する安全管理対策

① 真正性が求められる医療情報を取り扱うサービスにおける代行入力を実施するアカウント及び権限設定に関する機能や運用方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 真正性が求められる医療情報を取り扱うサービスには、代行入力の内容（代行者及び被代行者、代行対象となった記録、代行の日時等）を記録する機能を含める。 ③ 真正性が求められる医療情報を取り扱うサービスには、代行入力後の確定操作(承認)に関する機能を含める。

(エ)アクセス記録(アクセスログ)に対する要求事項

本項は、医療情報を取り扱うクラウドサービスを提供する情報システムへのアクセス記録に関する要求事項を示す。アクセス記録が、不正な情報システムの利用や情報漏洩が生じた場合の原因究明に必須の記録であることを踏まえ、厚生労働省ガイドライン第 5 版では、その証拠となる記録の正確性に関する対応策等について示している。

この目的を達するのに必要な保存期間やアクセス記録に対する機密性、完全性、可用性の観点から対応すべき要求事項を示す。

1. アクセス記録の取得	① 情報システムへのアクセスを記録し、一定期間保存する。 ② アクセス記録には、アクセスした ID、アクセス時刻、アクセス時間、アクセス対象（情報主体単位）等を含める。 ③ アクセス記録の機能を有しない場合には、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ 取り扱う医療情報に法定保存年限が設けられている場合、診療録等に関するアクセス記録又はこれに代わる記録について、当該法定年限以上の保存期間を設ける。 ⑤ ④で定める法定保存年限が経過した医療情報及び法定保存年限が設けられていない医療情報の保存期間について、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、本項におけるアクセス記録の管理方法については、サービス仕様適合開示書で保存期間を設けた場合には、原則として法定保存年限がある医療情報に準じて取り扱う。 ⑥ 情報システムの運用若しくは開発に従事する者又は管理者権限を有する者によるアクセスの記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。 ⑦ ⑥に関する情報の医療機関等への提供について、サービス仕様適合開示書

	に基づき、医療機関等と合意する。
2. アクセス記録の保全のための要件	**① アクセス記録が保存されている資源に対して、アクセス制限を行い、不正なアクセスを防止する。** **② アクセス記録の保存に必要な容量を十分確保し、可用性、完全性の確保を図る。** **③ アクセス記録を暗号化する、あるいは定期的に追記不能な媒体への記録を行う等、改ざん防止の措置を講じる。**
3. 時刻の設定	**① アクセス記録の時刻の信頼性を確保するために、情報システムの時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で行う。**

なお、アクセス記録（アクセスログ）に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.2.2 情報の分類】 推奨される安全管理策 (1) 情報の処理について履歴を取得し、資産台帳等に記録することが望ましい。
【7.6.6 ネットワークセキュリティ管理】 実施すべき安全管理策 (11) ネットワーク接続のログ（認証ログ及び接続ログ）を記録すること。 (12) ネットワーク接続ログを定期的に検証し不審な活動が行われていないことを検証すること。
【7.6.9 医療情報システムに対するセキュリティ要求事項】 実施すべき安全管理策 (4) 運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。 (5) システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得すること。
【7.6.12 ログの取得及び監査】 実施すべき安全管理策 (1) 作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成し、管理すること。 (2) 監査ログを定期的に検証して不正な行為、システムの異常等を検出すること。 (3) ログを利用して正確に事故原因等を検証するため、医療情報システムのすべての

サーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておくこと。

(4) 標準時刻に同期するための時刻提供元は信頼できる機関を利用すること。

(5) ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用すること。

- ログデータにアクセスする作業者及び操作を制限すること。
- 容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。
- ログデータに対する不正な改ざん及び削除行為に対する検出･防止策を施すこと。

推奨される安全管理策

(1) 医療情報システムのすべてのサーバ機器等の時刻が時刻サーバ等の提供する標準時刻に同期していることを定期的に検証することが望ましい。

(2) 監査ログに記録する事項としては次のようなものが考えられる。

- 作業者情報（作業者 ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元 IP アドレス）
- ファイル及びデータへのアクセス、変更、削除記録（作業者 ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類）
- データベース操作記録（作業者 ID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元 IP アドレス、設定変更時にはその内容）
- 修正パッチの適用作業（作業者 ID、変更されたファイル）
- 特権操作（特権取得者 ID、特権取得の可否、利用時刻及び時間、実行作業内容）
- システム起動、停止イベント
- ログ取得機能の開始、終了イベント
- 外部デバイスの取り外し
- IDS･IPS 等のセキュリティ装置のイベントログ
- サービス及びアプリケーションの動作により生成されたログ（時刻同期に関するログを含む）

(1) 監査ログを検証するため、作業者がアクセスした医療情報等を迅速に確認できるよう、作業者 ID と、情報の識別子（資産台帳記載の番号等）、生成時系列、アクセス時系列等、多様な指標での並び替え、情報の種別、アクセス時間等での絞り込み等が行うことができるようなシステムを整備することが望ましい。

(オ)端末等に表示される医療情報の漏洩に対する要求事項

本項は、参照権限を有しない者が端末を使って医療情報を閲覧することへの防止策に関する要求事項を内容とする。厚生労働省ガイドライン第 5 版では、主にクリ

アスクリーン等、医療機関等における利用者の端末の対応策等について示されている。

クラウドサービス事業者における運用等の端末への対応のほか、医療機関等における利用者の端末への適用に関する要求事項を以下に示す。

1. 端末表示からの漏洩対策	**① サービスの運用･保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。** **② サービスの運用･保守端末等を設置している区域は監視カメラ等により適切に監視を行う。** **③ 医療機関等に設置されている医療情報の参照等が可能な利用者端末等に対するクリアスクリーン等の情報漏洩防止策について、サービス仕様適合開示書に基づき、医療機関等と合意する。** **④ 端末又はセッションの乗っ取りのリスクを低減するため、利用者のログオン後に一定の使用中断時間が経過したセッションを遮断する、あるいは強制ログオフを行うことができるようにする。** **⑤ 医療機関等における利用者端末への④の措置の具体的な適用について、サービス仕様適合開示書に基づき、医療機関等と合意する。**

なお、端末等に表示される医療情報の漏洩に対する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける記述内容

【7.5.3 情報処理装置のセキュリティ】 実施すべき安全管理策 (3) 医療情報等が表示される端末画面等をアクセス権限の無いものが閲覧することが無い様に室内の機器レイアウトを行うこと。このようなレイアウトが難しい場合には、端末画面に覗き見防止用フィルターを設置する等の対策を行うこと。
【7.6.14 作業者アクセス及び作業者 ID の管理】 作業者のログオンについて実施すべき安全管理策 (1) 端末又はセッションの乗っ取りのリスクを低減するため、作業者のログオン後に一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを行うこと。
【7.6.15 作業者の責任及び周知】 実施すべき安全管理策 (3) 離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利

用を未然に防ぐこと。

(カ)情報漏洩対策等に対する要求事項

本項は、情報漏洩対策等に関する要求事項について示す。厚生労働省ガイドライン第5版では、情報システム構築時における対応や動作確認における対応、外部からの不正アクセスへの防護措置等について示している。なお動作確認における個人情報の利用については、３．２．６に統合する。

これらを踏まえて、情報漏洩対策等に関する要求事項を以下に示す。

1.ウイルスやマルウェア等への対策	① 情報システムの構築に際しては、ウイルスやマルウェア等の混入が生じないようにするための手順を策定し、これに則って構築する。 ② ウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新する。 ③ 情報システムの構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新のウイルス対策ソフト等の導入を行う。また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。 ④ サービス利用環境がウイルス等による攻撃を受けた場合に、サービス提供に係る影響について、速やかに医療機関等に周知し、必要な対応等を求める。 ⑤ 情報システムの脆弱性に関する情報は、JPCERT コーディネーションセンター（JPCERT/CC)、内閣サイバーセキュリティセンター（NISC)、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得し、確認する。
2.外部からの攻撃等への対策	① 外部のネットワークと医療情報を格納する機器との接続に際しては、セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行う。 ② 医療機関等との接続ネットワーク境界には、侵入検知システム（IDS)、侵入防止システム（IPS）等を導入してネットワーク上の不正なイベントを検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じる。 ③ 侵入検知システム等が、常に最新の攻撃･不正アクセスに対応可能なように、シグネチャ･検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行う。 ④ ホスティングの利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行う。

なお、情報漏洩対策等に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.5.3 情報処理装置のセキュリティ】 実施すべき安全管理策 (13) 不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、脆弱性パッチが適用されていること等を接続前に検査を行う仕組みを整備運用すること。
【7.5.4 情報処理装置の廃棄及び再利用に関する要求事項】 実施すべき安全管理策 (3) ハードディスクを機器に接続する際には、再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証すること。
【7.6.1 情報処理装置及びソフトウェアの保守】 実施すべき安全管理策 (8) 潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。 (9) 修正パッチの適用前にパッチが改ざんされていないこと及び有効性を検証すること。
【7.6.3 悪意のあるコードに対する管理策】 実施すべき安全管理策 (1) 最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。 (2) 悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。 ● リアルタイムスキャン（ディスク書き出し･読み込み、ネットワーク通信） ● リスク評価の結果として必要であれば定期的にスキャンを実施 ● 電子媒体へのデータ書き出し･読み込み時におけるオンデマンドスキャン ● 定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新 ● 管理者以外による設定変更やアンインストールの禁止
【7.6.6 ネットワークセキュリティ管理】 実施すべき安全管理策

(1) セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行うこと。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置（サーバ）にて、同様のアクセス制御を行うこと。

(2) セキュリティゲートウェイでは、不正な IP アドレスを持つトラフィックが通過できないように設定すること（接続機器類の IP アドレスをプライベートアドレスとして設定して、ファイアウォール、VPN 装置等のセキュリティゲートウェイを通過しようとするトラフィックを IP アドレスベースで制御する等）。

(5) 医療機関等との接続ネットワーク境界には侵入検知システム（IDS）、侵入防止システム（IPS）等を導入してネットワーク上の不正なイベントの検出、あるいは不正なトラフィックの遮断を行うこと。ホスティング利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行うこと。

(6) 侵入検知システム等が、常に最新の攻撃･不正アクセスに対応可能なように、シグネチャ･検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行うこと。

(7) 侵入検知システム等が、緊急度の高い攻撃･不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定にしていること。

(8) 侵入検知の記録には不正アクセス等の事後処理に必要な項目が含まれていること。

推奨される安全管理策

(1) 医療情報システムから、不正･不審なトラフィックが内部ネットワークから外部ネットワークへと流れていないことをネットワーク境界において監視することが望ましい。

(2) 侵入検知システム自身が攻撃･不正アクセスの対象とならないように、その存在を外部から隠す設定（ステルスモード）や、侵入検知システムへのアクセスの適切な制御を実施することが望ましい。

【7.6.7 電子媒体の取扱】

推奨される安全管理策

(2) 医療情報システムにおいてはサーバ等に接続できる電子媒体の種別を限定するため、不要なデバイスドライバを削除することが望ましい。加えて、認められていない種類の装置の接続を防止する為に、管理者以外がデバイスドライバのインストールやアンインストールが出来ない設定とすることが望ましい。

(3) 不要なデバイスドライバが追加されていないことを定期的に検証することが望ましい。

【7.6.8 情報交換に関するセキュリティ】

実施すべき安全管理策

(2) 情報交換手順では搬送の形態によらず次の事項を確実にすること。

- 発送者、受領者を識別し記録すること。
- 発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止対策を行うこと。
- 交換する情報の機密レベルに関して合意すること（受領側で機密レベルが低くならないこと）。
- 交換された情報に悪意のあるコードが含まれていないことを確実とすること。

【7.6.10 アプリケーションに対するセキュリティ要求事項】

実施すべき安全管理策

(1) 提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行うこと。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入すること。

(2) アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとること。

(3) アプリケーションにて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行うこと。

推奨される安全管理策

(1) アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行うことが望ましい。

(キ) 応答時間に関する要求事項

① 医療機関等がサービスを利用する際の、応答時間（一般的な表示速度、検索結果の表示時間等）について、サービス仕様適合開示書に基づき、医療機関等と合意する。

(ク) 医療情報等の保存に対する要求事項

本項は、医療情報を取り扱うクラウドサービスを提供する情報システム等の保存場所及びバックアップに関する要求事項を内容とする。厚生労働省ガイドライン第5版では、外部保存の対象となるデータについて、「7.3 保存性の確保について」において、バックアップ等に関する対応策等を示している。クラウドサービスでは、外部保存は原則としてどのサービスでも生じうることから、本ガイドラインでは一般的な技術的な対応策として規定することとした。

情報システムの保存領域管理に関する内容のほか、バックアップのルールや採用すべき手法等に関する要求事項を以下に示す。

1. 保存管理	① 各医療機関等が利用可能な、保存可能資源の残量については、随時提供できる措置を講じる。 ② 医療機関等がサービスを利用する際に、利用可能な資源に係る情報（保存可能容量、利用可能期間、リスク、バックアップ頻度、バックアップ方法等）について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 情報システムが情報を保存する場所（内部、可搬媒体）、その場所ごとの保存可能容量、保存可能期間、リスク等を運用管理規程等に含める。 ④ ③において、他の事業者が提供するクラウドサービスを利用する場合においても、同様の情報を収集して、対応する。仮想化技術によるクラウドサービスを利用する場合には、クラウドサービス事業者が他の事業者との契約上利用可能な資源に関する情報を確認する。 ⑤ ③により運用管理規程に定める管理方法に関する教育を従業員等に対して行う。 ⑥ サービスに係る委託先に対しても、③の運用管理規程に定める管理方法への対応等を求める。
2. バックアップルール	① ３．２．１（２）（ウ）4. ①において実施するリスク分析結果に基づき情報システムのバックアップを取得する。バックアップの取得対象、取得頻度、保存方法･媒体、管理方法等を定め、その内容を運用管理規程等に含める。 ② ①に従い取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、記録内容の改ざん･破壊等がないことを確認する。 ③ 記録媒体に格納するバックアップについては、その媒体の特性（テープ／ディスクの別、容量等）を踏まえたバックアップ内容、使用開始日、使用終了日を明らかにして管理する。 ④ ③の対象となるバックアップの記録媒体につき、使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複写する。 ⑤ ①～④の手順を運用管理規程等に含め、従業員等及び再委託業者に対して必要な教育を行う。 ⑥ バックアップに係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。
3 冗長化措置	① 情報システム、ネットワーク等に関し、通常の診療等に影響が生じないようサービスの継続に必要な冗長化対策を講じる。

	② 診療録等の情報をハードディスク等の記録機器に保存する場合、RAID-1 又は RAID-6 相当以上のディスク障害対策を講じる。 ③ ①を踏まえて、障害等が生じた場合のサービスの継続性を保証する水準について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ 障害時等でも診療等が継続できるようにするための医療機関等の側の代替措置等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
4.毀損した情報の取扱い	① 情報が毀損した場合、速やかに回復するための措置を講じ、その内容･手順等について、運用管理規程等に含める。 ② ①に示す措置によっても毀損された情報の回復が困難となる場合を想定した対応について、運用管理規程等に含める。 ③ ②で示す場合の、毀損した情報に関する責任の範囲、免責条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
5.保存データの見読性確保	① 医療情報を格納する機器、媒体等の見読性が確保されていることを定期的に確認する。 ② 受託する医療情報を格納する機器･媒体等の見読性確保が困難となる可能性がある場合（媒体の劣化、読取装置等のサポート切れ等）、速やかに代替的な措置を講じ、見読性確保のための対応を行う。

なお、医療情報等の保存に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.5.3 情報処理装置のセキュリティ】 実施すべき安全管理策 (12) 情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施すること。
【7.6.7 電子媒体の取扱】 実施すべき安全管理策 (5) 電子媒体の損傷等による情報喪失のリスクを最小限にするため電子媒体の製造者により指定される保管環境にて保管すること。 (6) 製造者の定める有効利用限度期間を超過することがないよう、電子媒体の有効利用限度期間が近づいた場合は、他媒体に複写すること。 (7) 情報を保管するためにハードディスク装置を用いる場合には、RAID-1 もしくは RAID-6 相当以上のディスク障害に対する対策を取ること。 (8) 全ての電子媒体には格納される情報の機密レベルを示すラベル付けを行うこと。

(ケ)ソフトウェア･機器等の品質管理に対する要求事項

本項は、医療情報を取り扱うクラウドサービスを提供する情報システムにおけるソフトウェアの品質管理に関する要求事項を内容とする。厚生労働省ガイドライン第 5 版では、外部保存の対象となる情報について、「7.1　真正性の確保について」において、ソフトウェア･機器等の品質管理に関する対応策等を示している。

ソフトウェア、機器の品質管理に関する要求事項を以下に示す。

1. 情報システムに関するドキュメント作成	①　情報システムにおける機器及びソフトウェアの構成図を作成する。 ②　情報システムのネットワーク構成図を作成する。 ③　①、②で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。 ④　情報システムを構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。 ⑤　①～④で策定した資料等を医療機関等の求めに応じて提出することについて、サービス仕様適合開示書に基づき、開示内容、範囲、条件等を医療機関等と合意する。
2. 品質管理に関する運用	①　サービスに供する機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等に含める。 ②　サービスに供する機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う。 ③　サービスに係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。 ④　システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等に含める。

なお、ソフトウェア･機器等の品質管理に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.5.3　情報処理装置のセキュリティ】

実施すべき安全管理策

(1)　不正な装置を識別するため、医療情報システム内で利用する情報処理装置を登録したリストを作成･維持すること。

(2)　医療情報システムに用いる装置には、必要のないアプリケーション等をインスト

ールしないこと。

(8) それぞれの装置は製造元または供給元が指定する間隔及び仕様に従って保守点検を行い、必要であれば交換を行うこと。

【7.6.1 情報処理装置及びソフトウェアの保守】

実施すべき安全管理策

(1) 保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行うこと。

(2) 変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討すること。

(6) 不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施すること。

(7) 医療情報システムに関連する技術的脆弱性については台帳等を利用して管理すること。

【7.6.2 開発施設、試験施設と運用施設の分離】

実施すべき安全管理策

(1) 情報処理に供するアプリケーションについては、情報処理事業者自身で開発したアプリケーションを用いること。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いること。

(2) ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用施設とは直接に接続されていない開発用の情報処理施設を用いて行うこと。

(3) 開発施設では悪意のあるコードが混入することを避けるため、不特定多数が利用するネットワーク（インターネット等）と接続を持つ場合には「7.6.3 悪意のあるコードに対する管理策」に従うこと。

(4) 不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改ざん防止、検知策を実施すること

推奨される安全管理策

(1) ソフトウェアに悪意のあるコードが混入することが無いよう、バイナリコードレベル、ソースコードレベルの双方で検証プロセスを実施することが望ましい。

【7.6.3 悪意のあるコードに対する管理策】

実施すべき安全管理策

(1) 最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。

(2) 悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。

● リアルタイムスキャン（ディスク書き出し･読み込み、ネットワーク通信）

● リスク評価の結果として必要であれば定期的にスキャンを実施 ● 電子媒体へのデータ書き出し･読み込み時におけるオンデマンドスキャン ● 定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新 ● 管理者以外による設定変更やアンインストールの禁止 (3) 一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止または隔離措置をとるといった対策が行われていること。
【7.6.9 医療情報システムに対するセキュリティ要求事項】 実施すべき安全管理策 (3) 業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入すること。 (5) システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得すること。
【7.9 医療情報システムの改造と保守】 推奨される安全管理策 (1) 開発されたソフトウェアの脆弱性検出をソースコードレベルで行うことが望ましい。パッケージソフトウェア等、ソースコードの提供を要求できない場合には、ソースコードレベルではなく、アプリケーションを動作させて、外形的なぜい弱性検査を行う。

(コ) 無線 LAN･IoT 機器の利用に対する要求事項

本項は、無線 LAN 及び IoT 機器の利用に対する要求事項を内容とする。無線 LAN や、IoT 機器の利用については、クラウドサービス事業者が提供した機器等を利用する場合のほか、医療機関等が管理する機器等を利用する場合等、いくつかのケースが挙げられる。クラウドサービス事業者が、これらについてどこまでをサービスや責任の範囲にするのかを明確にすることが重要である。

厚生労働省ガイドライン第 5 版では、医療機関等が無線 LAN や IoT 機器を利用する場合に講じるべき技術的な対策について定めている。

クラウドサービス事業者においては、自社が提供するサービスとの関係や医療機関等との間での責任分界や、（自社が提供するか否かを問わず）サービスに利用さ

れる IoT 機器に対して技術的な観点から講じるべき安全対策についての要求事項を以下に示す[24]。

1. 医療機関等における無線 LAN の利用	① 医療情報を取り扱うサービスの利用に際して、医療機関等が無線 LAN を利用する場合に必要なセキュリティ対策について、クラウドサービス事業者の役割分担等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
2. IoT 機器を利用したサービス提供時	① IoT 機器の利用を含むサービスを提供する場合、医療機関等との責任分界について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② IoT 機器の利用を含むサービスを提供する場合、IoT 機器による医療情報システムへのアクセス状況を記録し、不正なアクセスがないことを定期的に監視する。 ③ IoT 機器の利用を含むサービスを提供する場合、利用が想定される IoT 機器に対する脆弱性に関する情報を定期的に収集し、必要な対策を講じる。

[24] IoT 機器を含む医療機器のサイバーセキュリティの確保について、「医療機器のサイバーセキュリティの確保に関するガイダンス」（厚生労働省 平成 30 年 7 月 24 日）が策定されているので、併せて参照されたい。

３．２．４ 人的安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、人的安全管理対策について、6.6 章に記述している。そこでは、医療機関等における、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減を図るため、人による誤りの防止を目的とした人的安全対策が策定されており、これには守秘義務と違反時の罰則に関する規程や教育、訓練に関する事項が含まれる。

具体的な対策として規定されている内容を以下に示す。

(ア) 従業者に対する人的安全管理措置

6.6 C.最低限のガイドライン

1．医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。	
	① 法令上の守秘義務のある者以外を事務職員等として採用するに当たっては、雇用及び契約時に守秘･非開示契約を締結すること等により安全管理を行うこと。
	② 定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。
	③ 従業者の退職後の個人情報保護規程を定めること。

6.6 D.推奨されるガイドライン

1. サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。

(イ) 事務取扱委託業者の監督及び守秘義務契約

6.6 C.最低限のガイドライン

1. 医療機関等の事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。	
	① 受託する事業者に対する包括的な罰則を定めた就業規則等で裏付けられた守秘契約を締結すること。
	② 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者･作業内容･作業結果の確認をおこなうこと。
	③ 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。

	④ 委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。
2. プログラムの異常等で、保存データを救済する必要があるとき等、やむを得ない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行うこと。	

（２） クラウドサービス事業者への要求事項

クラウドサービス事業者は、厚生労働省ガイドライン第５版における「委託事業者」に当たることから、これを踏まえたクラウドサービス事業者における対応策は、

・クラウドサービス事業者の従業者等に対する人的安全管理措置

・再委託事業者における人的安全管理措置

の２つの内容に整理できる。この２つに関する要求事項以下にを示す。

(ア)従業者等に対する守秘義務等に関する対応

1.就業開始時における対応	①　サービスの提供に従事する要員（被用者、派遣従業者等）については、守秘義務に関する内容を、雇用契約又は派遣契約に含めるか、就業規則等に含める。
2.就業時における教育等	①　サービスの提供に従事する要員に対して、個人情報保護ポリシー及び個人情報の安全管理に関する教育･訓練を行う。 ②　この教育･訓練は就業開始時及び就業後定期的に行う。
3.退職後の守秘義務等	①　サービスの提供に従事する要員が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等に含める。 ②　サービスの提供に従事する要員が業務上管理していた個人情報については、離職時（内部の異動含む）に返却を求め、システム管理者が返却されたことを確認する。 ③　サービスの提供に従事する要員の退職時又は契約終了時以降の守秘義務について、上記 2.における教育･訓練に含める。
4.守秘義務違反者への対応措置	①　上記 1.～3.に違反した被用者、派遣事業者等に対して、適切なペナルティを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。
5.従業者等への教育状況･守秘義務等の状況	①　サービスの提供に従事する要員に対する教育･訓練の実施状況や、守秘義務等への対応状況等に関する資料の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、従業者等に対する守秘義務等に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.7 人的安全対策】

実施すべき安全管理策

(1) 医療情報を操作する可能性のある情報処理事業者職員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求めること。派遣従業員については秘密保持義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求めること。

(2) 医療情報を操作する可能性のある情報処理事業者職員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定すること。派遣従業員に関しては、派遣元に対し、情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行うこと。この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行うこと。

(3) 情報処理事業者職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改ざん又は破壊等の行為が行われていないことを検証すること。

(4) 医療情報を操作する情報処理事業者職員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておくこと。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求めること。派遣従業員については、派遣契約解除時に同等の合意書への署名を求めること。

(5) 医療機関等との委託契約において、情報処理事業者職員との秘密保持契約を結ぶこと、情報セキュリティ教育を受けさせること、及び、規定に反して預託情報を不正に扱った際の懲罰規定等、預託情報の機密管理に関する条項を設けること。

推奨される安全管理策

(1) 医療情報を操作する情報処理事業者職員については、規定の安全管理策に違反する行為を行った場合の懲戒手続きについて予め定めておくことが望ましい。これは服務規程等に含めることもできる。定めた懲戒手続きについては各職員に周知し、理解したことの確認を行うこと。

(イ) 再委託先に対する人的安全管理措置

1. 委託契約に含めるべき事項	**① 情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、当該再委託に係る契約において体制を明確にする。** **② 再委託先には、自社と同等の個人情報保護指針等を遵守させる。** **③ 再委託に係る契約に、委託業務に係る守秘義務を含める。** **④ 再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。**

	⑤　再委託先が、本ガイドラインに規定する安全管理対策を行っていることを確認する。

なお、再委託先に対する人的安全管理措置に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.5　第三者が提供するサービスの管理】

実施すべき安全管理策

（1）　第三者により提供されるサービスの安全管理策及びサービスレベルが十分であることを確認すること。

（2）　サービスの実施、運用、維持について定期的に検証すること。

（3）　サービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。

推奨される安全管理策

（1）　外部事業者がサービスを実施する際は、情報処理事業者もしくは外部事業者の正規職員が管理している状況で作業を行うことが望ましい。

３．２．５ 情報の破棄に関する安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、情報の破棄について、6.7 章に記述している。

医療に係る電子情報は破棄に関しても安全性を確保する必要があることから、情報の破棄の手順の明確化に関する対応のほか、講じるべき対策が示されている。具体的な対策として規定されている内容を以下に示す。

6.7 C.最低限のガイドライン

1. 「6.1 方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。
2. 情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること。
3. 外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策 (2) 事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。
4. 運用管理規程において下記の内容を定めること。 (a) 不要になった個人情報を含む媒体の破棄を定める規程の作成

（２） クラウドサービス事業者への要求事項

厚生労働省ガイドライン第 5 版における規定に対応した要求事項を以下に示す。

(ア) 情報の破棄に関する安全管理対策

1. 情報の破棄の保証	① サービスに供する情報を格納する機器、媒体等を破棄する手順に、不可逆的な破壊･抹消等により元のデータを復元できなくする措置を含める。 ② 情報の破棄を実施した場合に、医療機関等の求めに応じて、実施担当者及び情報の削除方法（電磁記録媒体の消磁･物理的破壊等）を含む実施内容を医療機関等に対して報告し、破棄記録等を提出する。 ③ ①で講じる措置及び②の資料を提供するのに必要な条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
2. 情報破棄手順の文書化	① 運用管理規程に以下の内容を定める。 ・管理する個人情報又はこれを格納する媒体等について、サービス提供上の要否の確認を定期的に行うこと。 ・サービス提供上不要とされた個人情報及びこれを格納する媒体についての破棄手順。 ・サービス提供上不要とされた個人情報及びこれを格納する媒体の破棄に際して、医療機関等が不測の損害を被らないようにするための措置(事前に破棄の基準等を告知する等)。 ② 情報の破棄手順について、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、情報の破棄に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.5.4 情報処理装置の廃棄及び再利用に関する要求事項】

実施すべき安全管理策

(1) ハードディスク等を医療情報システム内の別の機器で再利用する場合には、再利用前に、複数回のデータ書き込みによる元データの消去等の確実な方法でデータを消去し、再利用前に情報が消去されていることを確認すること。

(2) サーバ等の BIOS パスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去すること。

(4) ハードディスクの廃棄については、再利用及びデータの読み出しが不可能となるよう、複数回のデータ書き込みによる元データの消去、強磁気によるデータ消去措

置、物理的な破壊措置（高温による融解、裁断等）等を適用し、当該装置に実施した措置の概要の記録（対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等）について、医療機関等の求めに応じ、速やかに提出できるよう整備すること。

推奨される安全管理策

(1) 物理的な破壊措置については情報処理事業者自身で行うことが望ましいが、外部の事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し外部委託の了承を得ておくこと。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておくこと。

【7.6.7 電子媒体の取扱】

実施すべき安全管理策

(1) 電子媒体について情報処理事業者施設外への不要な持ち出しを行わないこと。CD、DVD、MO 等の電子媒体については、追記のできない光学メディア（CD-R、DVD-R 等）を用い、情報交換作業終了後、電子媒体を（9）に示す方式にて確実に廃棄処分すること。

(9) 電子媒体を廃棄する場合には、物理的な破壊措置（高温による融解、裁断等）を適用し、情報の読み出しが不可能であることを確認すること。

推奨される安全管理策

(1) 物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については情報処理事業者自身で行うことが望ましい。外部の専門事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し十分な理解を得ること。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておくこと。

【7.8 情報の破棄】

実施すべき安全管理策

(1) CD-R 等の廃棄については「7.6.7 電子媒体の取扱」を参照すること。

(2) ハードディスク等の廃棄については「7.5.4 情報処理装置の廃棄及び再利用に関する要求事項」を参照すること。

(3) 情報処理事業者は医療情報安全管理ガイドラインに従って情報の破棄を行った記録を提出すること。

３．２．６ 情報システムの改造と保守に関する安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、情報システムの改造と保守に関する安全管理対策について、6.8 章に記述している。

そこでは、

・個人情報保護の点では、修理記録の持ち出しによる暴露、保守センター等で解析中のデータの第三者による覗き見や持ち出し等
・真正性の点では、管理者権限を悪用した意図的なデータの改ざんや、オペレーションミスによるデータの改変等
・見読性の点では、意図的なマシンの停止や、オペレーションミスによるサービス停止等
・保存性の点では、意図的な媒体の破壊及び初期化や、オペレーションミスによる媒体の初期化やデータの上書き等

の脅威に対する対策が示されている。具体的な対策として規定されている内容を以下に示す。

6.8 C.最低限のガイドライン

1. 動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うともに、終了後は確実にデータを消去する等の処理を行うことを求めること。
2. メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別･認証についても同様である。
3. そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。
4. 保守要員の離職や担当替え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付け、また、それに応じるアカウント管理体制を整えておくこと。
5. 保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。
6. 保守会社と守秘義務契約を締結し、これを遵守させること。

7.　保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。
8.　リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。
9.　再委託が行われる場合は、再委託する事業者にも保守会社と同等の義務を課すこと。

6.8 D.推奨されるガイドライン

1.　詳細なオペレーション記録を保守操作ログとして記録すること。
2.　保守作業時には病院医療機関等の関係者立会いのもと下で行うこと。
3.　作業員各人と保守会社との守秘義務契約を求めること。
4.　保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。
5.　保守作業にかかわるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べで表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。

（２） クラウドサービス事業者への要求事項

厚生労働省ガイドライン第 5 版が示すように情報システムの改造と保守に関する安全管理対策においては、6.8 章に示すように

・保守に用いるアカウント管理
・保守の実施に関する管理（実施記録の管理･監督関係）
・保守等における個人情報の利用制限

等が求められる。

これに加えて、本項では、（エ）において、「保守における整合性･継続性確保のための安全管理対策」に関する要求事項も含めている。これは厚生労働省ガイドライン第 5 版では 7.2 章「見読性の確保について」で対策が示され、外部保存を行うための追加的な要件として示されているものである。

以上を踏まえた要求事項を以下に示す。

(ア) 保守に用いるアカウント管理に関する安全管理対策

1. 保守用のアカウント	**① 情報システムの保守に従事する者及び管理者権限を有する者が、その業務の目的で当該情報システムにアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。** **② ①で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。**
2. 保守用のアカウントの管理	**① 情報システムの保守に従事する者及び管理者権限を有する者は、業務上用いるアカウントが漏洩しないよう厳重に管理する。**

なお、保守に用いるアカウント管理に関する安全管理対策について、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.7 電子媒体の取扱】 推奨される安全管理策 (1) 物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については情報処理事業者自身で行うことが望ましい。外部の専門事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し十分な理解を得ること。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておくこと。
【7.6.14 作業者アクセス及び作業者 ID の管理】 作業者 ID について実施すべき安全管理策

(1) 作業者は情報処理装置上においてユニークな作業者 ID により識別されること。
(2) 作業者 ID を発行する際に、既存の ID との重複を排除する仕組みを導入すること。
(3) 複数作業者で共用するためのグループ ID の利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、作業者 ID でログオンしてからグループ ID に変更する仕組みを利用すること。
(4) 作業者 ID の発行は医療情報システムの管理に必要な最小限の人数に留めること。
(5) 作業者が変更あるいは退職した際には、ただちに当該作業者 ID を利用停止とすること。
(6) 監視ログの監査時に作業者を確実に特定するため、作業者 ID は過去に使われたものを再利用しないこと。
(7) 不要な作業者 ID が残っていないことを定期的に確認すること。

作業者 ID について推奨される安全管理策

(1) アクセスを許可された作業者 ID のアクセス可能範囲が許可された通りとなっていること（不正に変更されていないこと）を定期的に確認することが望ましい。

特権 ID について実施すべき安全管理策

(1) 特権 ID の発行は必要な最小限のものに留めること。
(2) 特権使用者に昇格可能な作業者 ID を制限すること。
(3) 特権の使用時には作業実施内容を記録すること。

特権 ID について推奨される安全管理策

(1) 特権の種類に応じてアカウントを分離し、ファイルやディレクトリに対するアクセスを制限することが望ましい。
(2) システムの機能として可能であれば、特権 ID で使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改ざん、削除など不正な行為を防止することが望ましい。

(イ) 保守実施に関する安全管理対策

1. リモートメンテナンス	**① リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、情報システムへの不正な侵入が生じないよう安全管理措置を講じる。** **② リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認する。** **③ サービス提供に必要な情報システムの保守をリモートメンテナンスで行う場合、サービス仕様適合開示書に基づき、医療機関等と合意する。**
2. ログによ	**① 情報システムの保守において実施した操作結果について、操作ログ等によ**

る保守結果のレビュー	り記録し、管理する。 ② 取得した操作ログ等により、アクセスされた医療情報についての状況をレビューする。
3. 医療機関等内における保守対応	① 情報システムの保守業務を医療機関等の施設内で行う際の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。
4. 保守業務の実施報告	① 情報システムの保守業務を行う際には、原則として業務の事前及び事後に医療機関等の管理者に対して書面等による通知を行う。事前の了解を必要とする業務及びその業務について事前の了解を得ることができない場合の対応方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② ①における事前の通知には、保守業務の影響が及ぶ範囲を明示し、保守業務が完遂しなかった場合を想定して原状回復に必要な時間の予測を含める。 ③ 保守業務の実施にあたっては、医療機関等がサービスを利用できない状況に陥らないよう十分な対応策を講じ、その手順を運用管理規程に含める。 ④ ③に定めた手順を医療機関等に示し、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、本手順に基づき保守を行う際に必要となる事項等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤ ④で示された手順について、医療機関等が対応すべき事項がある場合、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑥ 保守業務実施後には、医療機関等に対し報告等を行い、医療機関等の管理者の確認を得る。本手順の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、保守実施に関する安全管理対策に関し、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項】 ② 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合 実施すべき安全管理策 (4) データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム、医療情報に影響を与えないことを確認すること。
【7.6.1 情報処理装置及びソフトウェアの保守】

実施すべき安全管理策 （4） 情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画をたてて実施すること。 （5） 情報処理装置及びソフトウェアの適切な変更手順を策定すること。保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受けること。 推奨される安全管理策 （1） 変更手順に含まれる事項には次のようなものが考えられる。 ● 変更についての影響が及ぶ関係者への通知プロセス ● 装置の変更申請書のフォーマット（申請者情報、承認者情報、対象機器情報、変更作業開始日時、変更作業期間、変更理由、機器に納められている情報の概要、変更に伴うリスク評価の結果、機器が損傷した場合の対応策、等） ● 申請承認プロセス ● 変更試験プロセス ● 変更作業に支障が発生した場合の復旧手順 ● 変更終了確認プロセス ● 変更に伴う影響を監視するプロセス、等。
【7.6.5 第三者が提供するサービスの管理】 実施すべき安全管理策 （3） サービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。
【7.6.9 医療情報システムに対するセキュリティ要求事項】 実施すべき安全管理策 （4） 運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。 （5） システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得すること。

(ウ) 保守に用いるデータの取扱いに関する安全管理対策

1. 保守で用いるデータ	① 情報システムの動作確認に際しては、原則として受託した個人情報を含むデータを使用せず、テスト用のデータを使用する。 ② 情報システムの動作確認に際し、受託した個人情報を含むデータをやむを得ず使用する場合には、３．２．４で示す守秘義務が課された要員･委託先等により動作確認を行う旨を含めた手順を定める。 ③ 情報システムの動作確認に際し、受託した個人情報をやむを得ず使用する場合について、サービス仕様適合開示書に基づき、医療機関等と合意する。
2. 保守目的	① 医療情報を格納する機器等を、保守（例えば機器の修理等）の目的で、医療

での医療情報の持ち出し	機関等又はクラウドサービス事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、その手順を策定する。 ② ①で定める手順及び情報の提供条件について、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、保守に用いるデータの取り扱いに関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.2 開発施設、試験施設と運用施設の分離】 実施すべき安全管理策 (5) 運用施設に保存されている医療情報を開発施設及び試験施設にコピーしないこと。 (6) 医療情報を開発及び試験用データとして直接、利用しないこと。利用する場合には、個人情報の消去及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関等に示し、了解を得た上で利用すること。
【7.6.9 医療情報システムに対するセキュリティ要求事項】 実施すべき安全管理策 (1) 運用システムの混乱を避けるため、開発用コードまたはコンパイラ等の開発ツール類を運用システム上に置かないこと。 (2) 情報処理に不必要なファイル等を運用システム上におかないこと。
【7.6.10 アプリケーションに対するセキュリティ要求事項】 推奨される安全管理策 (1) アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行うことが望ましい。

(エ) 保守における整合性･継続性確保のための安全管理対策

1. データ項目の標準形式の採用	① 診療録等のデータ項目で、厚生労働省における保健医療情報分野の標準規格（以下、「厚生労働省標準規格」という。）が定められているものについては、それを採用する。 ② 厚生労働省標準規格が定められていないデータ項目については、変換が容易なデータ形式とし、サービス仕様適合開示書に基づき、医療機関等と合意

	する。
2. レコード管理方法等	① 医療情報に係るマスターテーブルの変更に際して、レコードの管理方法やとるべき措置等について、診療録等の情報に変更が生じない機能及び検証方法を情報システムに備える。 ② ①に示す機能等を備えることが困難な場合の情報システム更新･移行の手順について、サービス仕様適合開示書に基づき、医療機関等と合意する。
3. データ形式及び転送プロトコルのバージョン管理と継続性の確保	① データ形式や転送プロトコルをバージョンアップ又は変更しようとする場合には、サービスの利用に与える影響を確認する。 ② ①の結果、サービスの利用に影響があると認められる場合には、医療機関等が対応を図るために十分な期間を想定してバージョンアップ又は変更に係る告知を行うほか、対応に必要な措置に関する具体的な情報提供を行う。 ③ ②は、他の情報システムとのデータ連携等を考慮して行う。医療機関等に対する互換性確保に係る情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ データ形式･転送プロトコルの変更等の結果、医療機関等がサービスの利用を終了する場合には、３．４に示す対策を講じる。
4. サービスに供する機器の劣化対策	① サービスに供する情報システムに関する機器については、定期的に劣化状況に関する検査を行い、必要な措置を講じる。 ② サービスに供する情報システムについて、機器やソフトウェア等の提供事業者におけるサポート終了等が生じた場合は、サービスへの影響範囲について分析を行い、必要な措置を講じる。 ③ サービスに供する情報システムについて、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の提供が困難となる場合やサービスに変更が生じる場合には、利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。 ④ ③においてサービスの一部又は全部の停止、変更等が生じる場合の医療機関等への対応の内容、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
5. サービスに供する情報システムの互換性確保や他の事業者のサー	① 医療情報を取り扱うサービスに供する情報システムに関する機器及びソフトウェアについては、将来的な互換性確保を視野に入れて決定するとともに、サービス提供後に標準仕様等の変更が生じた場合のリスクについても検討を行う。 ② 他のクラウドサービス事業者が提供するクラウドサービスを用いて、サービスを提供する場合には、他のクラウドサービス事業者がサービスを停止し

ビスとの関係	**た際にも、自社のサービス提供に支障が生じないようにするための対応策を検討し、対策を講じる。なお、他のクラウドサービス事業者のクラウドサービスの停止･変更に伴い、自社が提供するサービスの一部又は全部の停止、変更（軽微なバージョンアップは含まない）等が生じる場合には、「4. サービスに供する機器の劣化対策」②～④に示す対応策を講じる。** **③ 医療情報を取り扱うサービスに供する情報システムに係る機器若しくはソフトウェア等の更新を行う場合、又は利用する他のクラウドサービス事業者のクラウドサービスの変更を行う場合には、①、②を考慮して行う。**

なお、保守における整合性･継続性確保のための安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.1 情報処理装置及びソフトウェアの保守】 実施すべき安全管理策 (3) 医療情報を保存･交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートすること。
【7.6.5 第三者が提供するサービスの管理】 実施すべき安全管理策 (7) サービスの変更時には、引き続き安全性が維持されていることについて適切な検証を行うこと。
【7.9 医療情報システムの改造と保守】 実施すべき安全管理策 (1) オペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システムに対する影響を評価し、試験結果を確認してから実施すること。

(オ)保守の体制･再委託に関する安全管理対策

1. 保守体制の変更	**① 情報システムの保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等及びその情報の提供に関する条件について、サービス仕様適合開示書に基づき、医療機関等と合意する。**
2. 再委託先の体制	**① 情報システムの保守に関して、外部事業者にその一部又は全部を委託する場合には、自社において実施している運用管理規程及び安全管理措置等への**

	対応を、当該外部事業者に対して求める。 **② ①の実施状況に関して、契約実施ごとに又は定期的に、外部事業者に対して報告を求め、確認する。**

なお、保守の体制･再委託に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.1 情報処理装置及びソフトウェアの保守】

実施すべき安全管理策

(1) 保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行うこと。

(2) 変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討すること。

(3) 医療情報を保存･交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートすること。

(4) 情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画をたてて実施すること。

(5) 情報処理装置及びソフトウェアの適切な変更手順を策定すること。保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受けること。

(6) 不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施すること。

(7) 医療情報システムに関連する技術的脆弱性については台帳等を利用して管理すること。

(8) 潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。

(9) 修正パッチの適用前にパッチが改ざんされていないこと及び有効性を検証すること。

(10) 保守作業を外部事業者に再委託する場合には、上記要件を満たしていることを確認して選定し､｢7.6.5 第三者が提供するサービスの管理｣の管理策を実施すること。選定した外部事業者について医療機関等に報告し、合意を得ること。

【7.6.5 第三者が提供するサービスの管理】

実施すべき安全管理策

(1) 第三者により提供されるサービスの安全管理策及びサービスレベルが十分であ

ることを確認すること。

(2) サービスの実施、運用、維持について定期的に検証すること。

(3) サービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。

(4) サービスを実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れないこと。

(5) サービス実施中に第三者が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯すること。

(6) サービス実施にともなう処理施設内への立ち入り手順に関しては、情報処理事業者の職員の入室、退室手順に準ずること。

(7) サービスの変更時には、引き続き安全性が維持されていることについて適切な検証を行うこと。

(8) 医療情報システムの保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関するガイドライン第 4.1 版」6.8 章 C 項の管理策を実施すること。

推奨される安全管理策

(1) 外部事業者がサービスを実施する際は、情報処理事業者もしくは外部事業者の正規職員が管理している状況で作業を行うことが望ましい。

３．２．７ 情報及び情報機器の持ち出しについての安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、情報及び情報機器の持ち出しについての安全管理対策について、6.9 章に記述している。具体的には、

・情報及び情報機器の持ち出しに関する運用管理規程等における文書化
・持ち出し対象となる機器、媒体等の台帳管理
・持ち出し対象となる機器、媒体等に対する技術的漏洩対策
・無線 LAN の利用制限
・BYOD の原則的禁止

等の対策が示されている。その内容を以下に示す。

6.9 C.最低限のガイドライン

1. 組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。
2. 運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。
3. 情報を格納した可搬媒体若しくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。
4. 運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと。
5. 医療機関等や情報の管理者は、情報が格納された可搬媒体若しくは情報機器の所在について台帳を用いる等して把握すること。
6. 情報機器に対して起動パスワードを設定すること。設定に当たっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。
7. 盗難、置き忘れ等に対応する措置として、情報に対して暗号化したり、アクセスパスワードを設定する等、容易に内容を読み取られないようにすること。
8. 持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネットワークに接続する場合は「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線 LAN を利用できる場合があるが、公衆無線 LAN は 6.5 章 C-11 の基準を満たさないことがあるため、利用できない。ただし、公衆無線 LAN しか利用できない環境である場合に

限り、利用を認める。利用する場合は 6.11 章で述べている基準を満たした通信手段を選択すること。
9. 持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールすること。業務に使用しないアプリケーションや機能については削除あるいは停止するか、業務に対して影響がないことを確認して用いること。
10. 個人保有の情報機器（パソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者は 1～5 の対策を行うとともに、管理者の責任において上記の 6、7、8、9 と同様の要件を順守させること。

6.9 D.推奨されるガイドライン

1. 外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。
2. 情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。
3. 情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。
4. スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。 ・BYOD は原則として行わず、機器の設定の変更は管理者のみが可能とすること。 ・紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者情報にアクセスできる場合は、一定回数パスワード入力を誤った場合は端末を初期化する等の対策を行うこと。

（２） クラウドサービス事業者への要求事項

クラウドサービス事業者への要求事項について、厚生労働省ガイドライン第５版が示す内容を踏まえ、

・運用管理規程等に関する安全管理対策

・機器･媒体の台帳管理

・情報機器等の持ち出しにおける漏洩対策に関する安全管理対策

について整理する。クラウドサービス事業者への要求事項を以下に示す。

(ア)運用管理規程等に関する安全管理対策

1.機器･媒体の持ち出しに関する方針策定	①　サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（委託元からの持ち出しを含む）に関する方針及び規則等を、運用管理規程に定める。 ②　①における「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。 ③　①で定める内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。
2.サービスに供する記録媒体･記録機器に関する対応	①　サービスに供する記録媒体･記録機器に関し、以下の内容を運用管理規程に含める。 ・管理体制及び管理方法 ・記録媒体･記録機器の取扱い ・サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等（「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。） ・サービスに関する情報を持ち出した場合で、当該情報を格納する機器･媒体等の盗難･紛失（持ち出し時の機器･媒体等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等（第三者による悪意の送信、従業者等における誤送信等を含む。））が起きた場合の対応 ・外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改ざんが生じないようにするための具体的な措置（マルウェア対策、暗号化、ファイアウォール導入等））
3.従業員等及び委託先に対する対応	①　「2.サービスに供する記録媒体･記録機器に関する対応」に示した内容に関する教育を従業員等に対して行う。 ②　上記の運用管理規程については、再委託先に対しても遵守等を求める。

4. 医療機関等との合意	① 「2. サービスに供する記録媒体･記録機器に関する対応」、「3. 従業員等及び委託先に対する対応」に示す情報の持ち出しに関する運用管理規程等における対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、運用管理規程等に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.5.3 情報処理装置のセキュリティ】

実施すべき安全管理策

(9) 保守点検で障害不良等が発見された際の対応作業等を行う際には情報処理事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにすること。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去してから持ち出すこと。記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的な破壊を行ってからの廃棄を選択すること。

【7.5.5 情報処理装置の外部への持ち出しに関する要求事項】

実施すべき安全管理策

(1) 情報処理装置が設置されている室内及び情報処理事業者の管理する領域から持ち出す場合に備え、適切な持ち出し手順を策定すること。

(2) 持ち出した機器を再度設置するための適切な検証手順を策定すること。

推奨される安全管理策

(1) 持ち出し手順に含まれる事項には次のようなものが考えられる。

- 装置の持ち出し申請書のフォーマット（申請者情報、承認者情報、対象機器情報、持ち出し日時、返却予定日時、持ち出す場所の情報、持ち出す理由、機器に納められている情報の概要、持ち出しに伴うリスク評価の結果、機器が紛失･損傷した場合の対応策、等）
- 申請承認プロセス
- 返却確認プロセス、等。

(2) 返却時の検証手順に含まれる事項には次のようなものが考えられる。

- 装置の動作確認
- 盗聴装置等、情報の安全性を脅かす装置の有無
- 悪意のあるプログラムの検出作業
- 収められている情報の検証作業（不正な改ざん等）、等。

【7.6.8 情報交換に関するセキュリティ】

実施すべき安全管理策

(3) 物理的に情報を搬送する際には以下の対策を実施すること。

- 医療機関等が合意する基準にもとづいて信頼できる配送業者を選択すること。
- 配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。
- 配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること。
- 配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用すること。
- 電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。
- 電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施すこと。

(イ) 機器･媒体の台帳管理

① サービスに関する情報を格納する機器･媒体等については、台帳管理等を行い、定期的に所在確認を行う。

なお、機器･媒体の台帳管理に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.7 電子媒体の取扱】

実施すべき安全管理策

(2) 情報交換目的やバックアップ目的でMT、DAT、半導体記憶装置、ハードディスク等の大容量の電子媒体を用いる場合には、その管理を厳重に行うこと。これらの電子媒体に複数回の情報記録を行う場合には、単に上書きするのではなく、確実な情報消去等の情報漏洩対策を行うこと。

(3) 電子媒体は台帳を作成して管理すること。台帳と電子媒体を定期的に検証し、盗難、紛失の発生を検証すること。台帳においては利用に関する記録を行い、電子媒体の廃棄後も一定期間にわたり記録を維持すること。

(4) 電子媒体を保存するキャビネット等には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。

(ウ) 情報機器等の持ち出しにおける漏洩対策に関する安全管理対策

1.起動パスワードの設定	① サービスに供する機器等については、起動パスワードの設定を行う。 ② 起動パスワードは、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じる。 ③ サービスに関する情報を格納する情報機器へのログイン及びアクセスについては、複数の認証要素を組み合わせて行う。
2.機器を持ち出す場合の手順	① サービスに関する情報を格納する機器･媒体等を持ち出す場合の手順には、機器･媒体自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる、パスワードを設定する等の事項を含める。
3.持ち出し機器等におけるアプリケーション	① サービスに関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。 ② サービスに関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。
4.BYODへの対応	① サービスの提供に係る目的（開発、保守、運用含む）で従業員等の個人所有の機器を利用することは禁止する。 ② 利用者が個人所有する機器によるサービス利用に関する対応策については、サービス仕様適合開示書に基づき、医療機関等と合意する。[25] なお具体的には以下の内容を参考にする。 ・利用者が所有する機器からの情報漏えい等を防止する観点から、例えば、仮想デスクトップを用いてOS レベルで業務利用領域と個人利用領域を分け、業務利用領域を医療機関等が管理できるようにするほか、モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すことで、医療機関等が所有し管理する端末と同等のセキュリティ対策の徹底を図ることなどが考えられる。
5.公衆無線LAN の利用禁止	① 業務上、サービスに関する情報を格納するモバイル端末を持ち出す場合には、公衆無線LANへの接続は行わない。

なお、情報機器等の持ち出しにおける漏洩対策に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

[25] なおBYODを利用するために用いる仮想デスクトップについては、３．２．９（２）（ア）を参照。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.5.3 情報処理装置のセキュリティ】

実施すべき安全管理策

(11) 起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードを設定すること。設定されるパスワードの品質、管理については「7.6.14 作業者アクセス及び作業者 ID の管理」に従うこと。

【7.6.6 ネットワークセキュリティ管理】

実施すべき安全管理策

(13) 医療情報を保存する医療情報システムにおいて無線ネットワーク（Bluetooth 等の近距離無線通信を含む）LAN を利用しないこと。

【7.6.8 情報交換に関するセキュリティ】

実施すべき安全管理策

(3) 物理的に情報を搬送する際には以下の対策を実施すること。

- 医療機関等が合意する基準にもとづいて信頼できる配送業者を選択すること。
- 配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。
- 配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること。
- 配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用すること。
- 電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。
- 電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施すこと。

【7.6.14 作業者アクセス及び作業者 ID の管理】

パスワード管理について実施すべき安全管理策

(1) 情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。

(2) 医療情報システムへのログオン用パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管すること。

(3) 医療情報システムへのログオン用パスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。

(4) 医療情報システムへのログオン用パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。

(5) パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード

入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とすること。

(6) パスワード発行時には、乱数から生成した仮の医療情報システムへのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施すること。

(7) パスワードの満たすべき品質の基準を策定し、すべてのパスワードが品質基準を満たしていることを確実とすること。

(8) パスワードをシステムに記憶させる自動ログオン機能を利用しないよう作業者に徹底すること。

(9) パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用すること。また、一般の作業者による閲覧を制限すること。

<u>パスワード管理について推奨される安全管理策</u>

(1) 作業者が医療情報システムへのログオン用パスワードを登録及び変更する際には、予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、作業者が設定しようとする品質の低いパスワードを認めないシステムの導入等を検討することが望ましい。

(2) パスワードの品質基準としては、パスワードを十分に長くすること（8 文字以上等)、アルファベット及び数字並びに記号を一つ以上含むこと、等が考えられる。

３．２．８ 災害等の非常時の対応についての安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、災害等の非常時の安全管理対策について、6.10 章に記述している。そこでは、非常時における医療情報システムに関する対策が示されている。具体的な対策として規定されている内容を以下に示す。

6.10 C.最低限のガイドライン

1. 医療サービスを提供し続けるための BCP の一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。
2. 正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること。
3. 非常時の情報システムの運用 ・「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。 ・非常時機能が定常時に不適切に利用されることがないようにして、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理及び監査すること。 ・非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更しておくこと。 ・標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、関係先への連絡手段や紙での運用等の代替手段を準備すること。
4. サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、“非常時”と判断した上で所管官庁への連絡を行うこと。 また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。 連絡先：厚生労働省 医政局研究開発振興課医療技術情報推進室（03-3595-2430） ※独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。 なお、情報処理推進機構は、マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口を開設している。標的型メールを受信した、Web サイトが何者かに改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。 連絡先：情報処理推進機構 情報セキュリティ安心相談窓口（03-5978-7509）

（２） クラウドサービス事業者への要求事項

厚生労働省ガイドライン第 5 版が示す内容を踏まえ、

・BCP 等への対応

・非常時に実施すべき代替措置と、その復旧方法

・サイバー攻撃等への対応策

等について、要求事項を以下に示す。

(ア) 障害時における見読性確保に関する安全管理対策

1. 障害時の責任分界	① 障害等が生じた場合の責任分界を明確にした上で、稼動を保証するサービスの範囲について、サービス仕様適合開示書に基づき、医療機関等と合意する。
2. 医療機関への情報提供	① 医療情報を医療機関等に保存する場合に、障害時における見読性確保のために医療機関等側で講じうる方策に関する情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。
3. 外部ファイル等の出力	① 医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。
4. 遠隔地のバックアップに関する見読性	① 医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために遠隔地に保存するバックアップデータの利用のための機能、利用に必要な情報の提供、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
5. 見読性の確保の支援機能	① 緊急時に備えた医療機関等における診療録等の見読性の確保を支援する機能（例えば画面の印刷機能、ファイルダウンロードの機能等）をサービスに含めること及びこれに必要なセキュリティ等の情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、障害時における見読性確保に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.10.1　要求事項の識別】

実施すべき安全管理策

(6)　ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、

見読性が確保される形式（PDF、JPEG 及び PNG 等のフォーマット ）で外部ファイルに出力可能とすることなどの方策を検討すること。

(7) 医療機関等に提供する情報処理サービスの継続に必要であれば、受託する医療情報のバックアップ施設等、情報処理サービスを継続するための代替情報処理施設を設置し、それらの施設に対しても本ガイドラインで提示する物理的安全対策を施すこと。

(イ) 災害等の非常時の対応に関する安全管理対策

1.BCP 等の策定	① サービスに係る BCP 及びコンテンジェンシープランの策定を行う。 ② ①で策定する BCP 及びコンテンジェンシープランには、非常時における体制及びサービス回復手順等の内容を含める。 ③ ①で策定した BCP 及びコンテンジェンシープランに基づくサービス内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。
2.非常時のサービスの運用	① 非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 非常時に用いる利用者アカウントの利用状況については定期的にレビューを行う。 ③ 非常時に用いる利用者アカウントが利用された場合、システム管理者及び運用者がこれを速やかに確認できるための措置を講じる。 ④ 非常時に有効化した利用者アカウント及び非常時用の機能については、正常復帰後、速やかに無効化を図る。
3.サイバー攻撃等への対応	① サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。 ② ①の場合において、サービスに生じている障害の状況及び復旧に関する見通し等について、医療機関等に速やかに報告を行う。 ③ ①の場合において、医療機関等が行う必要のある所管官庁への連絡･報告のために提供する資料の範囲、条件等について、サービス仕様適合開示書に基づき、医療機関と合意する。 ④ ③で定める、医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、サービスの提供に用いるアプリケーション、プラットフォーム、サーバ･ストレージ等は国内法の執行が及ぶ場所に設置する。
4.サービス回復後のデータ整合性の確保	① 非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定･検証方法の規定等）を講じる。

なお、災害等の非常時の対応に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.14　作業者アクセス及び作業者 ID の管理】 作業者のログオンについて推奨される安全管理策 （4） 緊急時の作業のため、規定時間外にログオンを行う必要が発生した場合の妥当な承認プロセスを策定することが望ましい。
【7.10.1　要求事項の識別】 実施すべき安全管理策 （1） 医療情報処理に関わる業務プロセス（プロセスを実施するための作業員を含む）、情報処理装置等について識別すること。 （2） 業務プロセス間の相互関係を評価すること。 （3） 事業を継続するための業務プロセスの優先順位を明確にすること。 （4） 医療情報システムに発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別すること。 （5） 医療情報システムに発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別すること。
【7.10.2　事業継続計画の立案及びレビュー】 実施すべき安全管理策 （1） 医療情報システムのサービス提供における業務プロセス及び医療情報システムの優先順位にもとづいて、医療情報処理に関する事業継続計画を策定すること。 （2） 策定した事業継続計画について模擬試験を含めた適切な方法でレビューすること。 （3） 事業継続計画について定期的に見直しを行うこと。 推奨される安全管理策 （1） 策定される事業継続計画には次のような事項を含むことが望ましい。 ● 事前準備計画 ● 「非常時」判断手順 ● 関係者の召集、対応本部の設置 ● 機器及び作業員の縮退措置及び代替施設の手配措置 ● バックアップ施設等、代替施設への切替え措置 ● 代替施設運用中の考慮事項（非常時アカウントの運用手順、復帰後に医療情報を正常システムに同期するための配慮等）

- 障害の拡大範囲に関する判断手順、基準
- 正常復帰の判断手順、基準
- 正常復帰後の医療情報システムの点検手順（不正侵入、情報改ざん、情報破損等の検出等）
- 所管官庁への連絡体制、等

３．２．９ 個人情報を含む医療情報を外部と交換する場合の安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、個人情報を含む医療情報を外部と交換する場合の安全管理対策について、6.11 章に記述している。

個人情報を含む医療情報を外部と交換する場合の安全管理対策では、

・ネットワーク経路の安全管理対策

・ネットワーク経路以外の、通信上の安全管理対策

・医療機関等と委託先等との責任分界の設定

等の対策が示されている。具体的な対策として規定されている内容を以下に示す。

6.11 C.最低限のガイドライン

1. ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を行うこと。 セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策を行うこと。 上記を満たす対策として、例えば IPSec と IKE を利用することによりセキュアな通信路を確保することが挙げられる。 チャネル･セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者に確認すること。
2. データ送信元と送信先での、拠点の出入り口･使用機器･使用機器上の機能単位･利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法を用いるのが望ましい。
3. 施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を行うこと。これに関しては、「6.5 技術的安全対策」で包括的に述べているので、それを参照すること。
4. ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲット若しくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。

5.　送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。例えば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。

6.　医療機関等の間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等の多くの組織が関連する。そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。

・診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定
・送信元の医療機関等がネットワークに接続できない場合の対処
・送信先の医療機関等がネットワークに接続できなかった場合の対処
・ネットワークの経路途中が不通又は著しい遅延の場合の対処
・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処
・伝送情報の暗号化に不具合があった場合の対処
・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処
・障害が起こった場合に障害部位を切り分ける責任
・送信元の医療機関等又は送信先の医療機関等が情報交換を中止する場合の対処

また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。

・通信機器、暗号化装置、認証装置等の管理責任の明確化（外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結）
・患者等に対する説明責任の明確化
・事故発生時における復旧作業･他施設やベンダとの連絡に当たる専任の管理者の設置
・交換した医療情報等に対する管理責任及び事後責任の明確化（個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項）

7.　リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること。

また、メンテナンス自体は「6.8　情報システムの改造と保守」を参照すること。

8.　回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。また、上記 1 及び 4 を満たしていることを確認すること。
9.　患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信の TLS 暗号化、PKI 個人認証等の技術を用いた対策を実施すること。また、情報の主体者となる患者等へ危険性や提供目的についての納得できる説明を行い、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にすること。
10. オープンなネットワークを介して HTTPS を利用した接続を行う際、IPsec を用いた VPN 接続等によるセキュリティの担保を行っている場合を除いては、SSL/TLS のプロトコルバージョンを TLS1.2 のみに限定した上で、クライアント証明書を利用した TLS クライアント認証を実施すること。その際、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。いわゆる SSL-VPN は偽サーバへの対策が不十分なものが多いため、原則として使用しないこと。また、ソフトウェア型の IPsec 若しくは TLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃からの防護について、適切な対策を実施すること。

6.11 D.推奨されるガイドライン

1.　やむを得ず、従業者による外部からのアクセスを許可する場合は、PC の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに、運用等の要件を設定すること。

（２） クラウドサービス事業者への要求事項

クラウドサービス事業者への要求事項については、厚生労働省ガイドライン第 5 版の 6.11 章に示す内容に加えて、7.2 章「真正性の確保について」で示されている「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（ア）「ネットワークに関する安全管理対策」に含めて規定する。

以上を踏まえて、クラウドサービス事業者が医療情報を取り扱うクラウドサービスを提供する上で対応すべき内容、医療機関等と合意すべき内容について、要求事項として示す。

(ア) ネットワークに関する安全管理対策

1. ネットワーク経路における全般的な安全管理対策	① ネットワークにおいて、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）を行う。 ② アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐのに必要な措置(サーバ証明書の導入等）を行う。 ③ 経路の安全性確保のため、IPSec + IKE への対応や閉域ネットワークへの対応等及びその条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ ネットワーク経路におけるウイルスや不正なメッセージの混入等の改ざんに対する防護措置に関するクラウドサービス事業者の役割の範囲について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤ 医療機関等がチャネル･セキュリティの確保を閉域ネットワークの採用に期待する場合、サービスの閉域性の範囲に関する情報について、サービス仕様適合開示書に基づき、医療機関等と合意する。
2. 医療機関等からのネットワーク経路の確認	① 医療機関等からクラウドサービス事業者までのネットワークにおいて、医療機関等の送受信の拠点の出入り口･使用機器･使用機器上の機能単位･利用者等の必要な単位で経路の確認を行う。 ② ①において、医療機関等が外部接続するサーバ等とクラウドサービス事業者のサーバとの間の相互認証を行う。 ③ ①について、事業者が保守業務を再委託している場合には、事業者と再委託先との接続では、別途なりすましを防止する策を講じる。 ④ 厚生労働省ガイドライン第 5 版 6.11 C 項の 2 に基づいて医療機関等が採用する通信方式認証手段が妥当なものであることの確認について、サービス仕様適合開示書に基づき、医療機関等と合意する。
3. ネットワ	① ルータ等のネットワーク機器は、ISO15408 で規定されるセキュリティター

ーク経路対応に用いる機器	ゲット又はそれに類する文書が、本ガイドラインに適合しているものを選定する。 ② ネットワークで用いられる医療機関等の施設内のルータについて、これを経由して施設間を結ぶ VPN の間で送受信ができないように経路設定すること等に関するクラウドサービス事業者の役割分担について、サービス仕様適合開示書に基づき、医療機関等と合意する。
4.暗号化対策	① 送信元と送信先の間で、暗号化等の情報そのものに対するセキュリティ対策を実施する。 ② サービスの提供において SSL/TLS を用いる際には、TLS1.2 に対応した措置を講じる。 ③ ②のほか、医療機関等がメールの暗号化（S/MIME 等）やファイルの暗号化への対応を求める場合には、その対応に必要な措置及び条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
5.通信経路の暗号化対策	① オープンなネットワークを介して HTTPS を利用した接続を行う際は、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行う。 ② SSL-VPN は、原則として使用しない。 ③ サービス提供に際して、ソフトウェア型の IPsec 又は TLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃について、適切な対策を実施する。 ④ 医療機関等における利用者がソフトウェア型の IPsec 又は TLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃についての、適切な対策に関する情報提供を行う。情報提供の範囲、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
6.回線の品質等	① 回線の管理、品質等に対するクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
7.医療機関等の外部からのサービス利用	① 医療機関等の利用者が、医療機関等の外部からサービスを利用する場合に、医療機関等の利用者が用いる PC の作業環境に仮想デスクトップ等の技術を導入するためのクラウドサービス事業者の役割分担等につき、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、ネットワークに関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.5.3 情報処理装置のセキュリティ】

推奨される安全管理策

(1) 情報伝送に用いるケーブル類については直接の傍受リスクについて配慮することが望ましい。

【7.6.3 悪意のあるコードに対する管理策】

実施すべき安全管理策

(1) 最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。

(2) 悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。

- リアルタイムスキャン（ディスク書き出し･読み込み、ネットワーク通信）
- リスク評価の結果として必要であれば定期的にスキャンを実施
- 電子媒体へのデータ書き出し･読み込み時におけるオンデマンドスキャン
- 定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新
- 管理者以外による設定変更やアンインストールの禁止

(3) 一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止または隔離措置をとるといった対策が行われていること。

【7.6.4 ウェブブラウザを使用する際の要求事項】

実施すべき安全管理策

(1) ウェブブラウザの接続するサーバを業務上必要なサーバに限定すること

(2) ウェブブラウザの設定で、認可していないサイトから、ActiveX、Java アプレット、Flash 等のプログラムコードをダウンロード及び実行することができない設定になっていること（管理ソフトウェアが実行されるサーバのみを認可する）。

(3) 認可したサイトからダウンロードされるコードについても「7.6.3 悪意のあるコードに対する管理策」に即して検査されること。

推奨される安全管理策

(1) ウェブブラウザからメールクライアント等の業務処理において想定しない外部アプリケーションが明示的な確認なしに起動されないよう設定を行うことが望ましい。

【7.6.6 ネットワークセキュリティ管理】

実施すべき安全管理策

(3) ルータ等のネットワーク機器は、安全性が確認できる機器を利用すること。

(4) ネットワーク機器及びサーバ、端末の利用していないネットワークポートへの物理的な接続を制限すること。

(9) 医療情報システムにおいて、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定すること。他に必要なサービスがある場合には、医療機関等の合意を得てから利用すること。

- 外部からの医療情報システムの稼働監視･遠隔保守
- セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード
- オペレーティングシステム及び利用アプリケーションのセキュリティパッチファイル等のダウンロード
- 電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認証局へのアクセス
- ファイアウォール、IDS･IPS などのセキュリティ機器に対する不正アクセス監視
- 時刻同期のための時刻配信サーバへのアクセス
- これらのサービスを利用するために必要なインターネットサービス（ドメインネームサーバへのアクセス等）
- その他の医療情報システムの稼動に必要なサービス（外部認証サーバ、外部医療情報データベース等）

(14) VPN 接続を行う場合には以下の事項に従うこと。

- 接続時に VPN 装置間で相互に認証を行うこと。
- 傍受、リプレイ等のリスクを最小限に抑えるために、「7.6.11 暗号による管理策」に従い、適切な暗号技術を利用すること。
- インターネット上のトラフィックが VPN チャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しないこと。
- 複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるため VPN チャンネルを医療機関等別に構築する等の対策を実施すること。

【7.6.8 情報交換に関するセキュリティ】

実施すべき安全管理策

(2) 情報交換手順では搬送の形態によらず次の事項を確実にすること。

- 発送者、受領者を識別し記録すること。
- 発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止対策を行うこと。

● 交換する情報の機密レベルに関して合意すること（受領側で機密レベルが低くならないこと）。
● 交換された情報に悪意のあるコードが含まれていないことを確実とすること。

(4) 電子的に情報を転送する際には以下の対策を実施すること。
● 送信者、受信者は相互に電子的に認証を行って相手の正当性を検証すること。認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。
● 送受信する経路は適切な方法で傍受のリスクから保護されていること。
● 受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。
● 送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。

【7.6.11　暗号による管理策】

実施すべき安全管理策

(1) 暗号アルゴリズムは十分な安全性を有するものを使用すること。選択基準としては電子政府推奨暗号リスト 等を用いること。
(2) 暗号鍵が漏洩した場合に備えた対応策を策定しておくこと。
(3) 電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。
(4) 暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。
(5) 医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリント と比較して、真正性を検証すること。

推奨される安全管理策

(1) 暗号モジュールが外部のソースコードやライブラリを利用する場合には、その真正性を、製造元による電子署名等による完全性の検証を行った上で利用することが望ましい。
(2) 暗号鍵の生成は耐タンパー性を有する IC カード、USB トークンデバイスといった安全な環境で実施することが望ましい。
(3) 暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うことが望ましい。
(4) 電子署名法にもとづき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できることが望

ましい。

(イ) 保守における通信上の安全管理対策

① リモートメンテナンスにより保守を行う場合、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置を講じる。

(ウ) 医療機関等との責任分界に関する取り決め

1.通信経路に関する責任分界	**① 通常運用時及び非常時の医療機関等と事業者との起点から終点までの通信手順、その他厚生労働省ガイドライン第5版6.11 C項の6で定めるネットワーク経路及びこれに関連する機器等に係る責任の所在を明確にし、事業者の負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。** **② 交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、サービス仕様適合開示書に基づき、医療機関等と合意する。** **③ 医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、事業者が負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。**
2.患者等が閲覧する場合の手続・責任分界	**① サービスにより管理する医療情報を患者等の閲覧に供する場合に、クラウドサービス事業者において対応すべきセキュリティ上の措置の条件、内容等について、サービス仕様適合開示書に基づき、医療機関等と合意する。** **② 医療情報を患者等の閲覧に供する場合に、医療機関等及び患者等の閲覧環境において対応すべきセキュリティ上の対応に係る情報の提供条件、内容等について、サービス仕様適合開示書に基づき、医療機関等と合意する。** **③ 患者等が情報を閲覧する情報システムのセキュリティに関する説明責任等におけるクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。**

なお、医療機関等との責任分界に関する取り決めに関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.3 悪意のあるコードに対する管理策】

実施すべき安全管理策

(1) 最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅

威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。

(2) 悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。

- リアルタイムスキャン（ディスク書き出し･読み込み、ネットワーク通信）
- リスク評価の結果として必要であれば定期的にスキャンを実施
- 電子媒体へのデータ書き出し･読み込み時におけるオンデマンドスキャン
- 定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新
- 管理者以外による設定変更やアンインストールの禁止

(3) 一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止または隔離措置をとるといった対策が行われていること。

【7.6.4 ウェブブラウザを使用する際の要求事項】

実施すべき安全管理策

(1) ウェブブラウザの接続するサーバを業務上必要なサーバに限定すること

(2) ウェブブラウザの設定で、認可していないサイトから、ActiveX、Java アプレット、Flash 等のプログラムコードをダウンロード及び実行することができない設定になっていること（管理ソフトウェアが実行されるサーバのみを認可する）。

(3) 認可したサイトからダウンロードされるコードについても「7.6.3 悪意のあるコードに対する管理策」に即して検査されること。

推奨される安全管理策

(1) ウェブブラウザからメールクライアント等の業務処理において想定しない外部アプリケーションが明示的な確認なしに起動されないよう設定を行うことが望ましい。

【7.6.8 情報交換に関するセキュリティ】

実施すべき安全管理策

(1) 次の情報交換方法について予め合意しておくこと。

- 情報を電子媒体に記録して交換する際の手順
- 情報をネットワーク経由で文書ファイル形式にて交換する際の手順
- 情報をネットワーク経由でアプリケーション入力にて交換する際の手順
- 情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順

３．２．１０ 法令で定められた記名･押印を電子署名で行うことについての安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、法令で定められた記名･押印を電子署名で行うことについての安全管理対策を、6.12 章に記述している。そこでは、法令上、電子署名等を付することが認められた医療情報に対して求められる要件等を挙げている。具体的な対策として規定されている内容を以下に示す。

6.12 C.最低限のガイドライン

(1) 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局若しくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと	
	1. 保健医療福祉分野 PKI 認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。従ってこの保健医療福祉分野 PKI 認証局の発行する電子署名を活用することが推奨される。 ただし、当該電子署名を検証しなければならない者の全てが、国家資格を含めた電子署名の検証が正しくできることが必要である。
	2. 電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくても A の要件を満たすことは可能であるが、同等の厳密さで本人確認を行い、さらに監視等を行う行政機関等が電子署名を検証可能である必要がある。
	3. 「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成 14 年法律第 153 号）に基づき、平成 16 年 1 月 29 日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者が全て公的個人認証サービスを用いた電子署名を検証できることが必要である。
(2) 電子署名を含む文書全体にタイムスタンプを付与すること	
	1. タイムスタンプは、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの安全な長期保存のために－」（総務省　平成 16 年 11 月）等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能であること。
	2. 法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。

	3.　タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を講じる必要がある。
(3)　上記タイムスタンプを付与する時点で有効な電子証明書を用いること	
	1.　当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば電子署名を含めて改変の事実がないことが証明されるため、タイムスタンプ付与時点で電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策が必要である。

（２） クラウドサービス事業者への要求事項

厚生労働省ガイドライン第５版では、法令で定められた記名･押印を電子署名で行うことについての安全管理対策について

・医療情報の作成において付与する電子署名で用いる電子証明書
・タイムスタンプの付与
・タイムスタンプと電子証明書の関係

を規定しており、これに対応する必要がある。

そこで上記の分類に従い、クラウドサービス事業者への要求事項を以下に示す。

(ア)電子証明書による電子署名

① 法令で署名又は記名･押印が義務付けられた文書等において、記名･押印を電子署名に代える場合に、保健医療福祉分野 PKI 認証局の発行する署名用電子証明書へ対応することの可否を、医療機関等に対して明らかにする。 ② 保健医療福祉分野 PKI 認証局の発行する電子証明書以外の、電子署名法における認定認証事業者が発行する電子証明書を用いて、法令で定められた記名･押印を電子署名で行うサービスを提供する場合には、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、電子署名法の規定に基づく認定認証事業者の発行する電子証明書を用いなくても「電子署名及び認証業務に関する法律（平成 12 年法律第 102 号)」 第 2 条 1 項の要件を満たすことは可能であることから、同等の厳密さで本人確認を行い、さらに監視等を行う行政機関等が電子署名を検証可能であることを担保して、認定認証事業者以外が発行する電子証書書を利用する場合には、上記要件を担保できることを示して、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 公的個人認証サービスにおける署名用電子証明書を利用して、法令で定められた記名･押印を電子署名で行うサービスを提供する場合には、当該サービスにおける公的個人認証サービスに係る電子証明書の検証方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、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に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.8 情報交換に関するセキュリティ】

実施すべき安全管理策

(1)　次の情報交換方法について予め合意しておくこと。

- 情報を電子媒体に記録して交換する際の手順
- 情報をネットワーク経由で文書ファイル形式にて交換する際の手順
- 情報をネットワーク経由でアプリケーション入力にて交換する際の手順
- 情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順

【7.6.11　暗号による管理策】

実施すべき安全管理策

(3)　電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。

推奨される安全管理策

(3)　暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うことが望ましい。

(4)　電子署名法にもとづき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できることが望ましい。

(イ) タイムスタンプの付与

①　電子署名を施す情報に対しては、タイムスタンプを付与する。この場合には、タイムスタンプの内容･検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。

②　タイムスタンプを付与した情報を取り扱う場合に、法定保存年限内における当該タイムスタンプの有効性を検証する方法、対応方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

③　タイムスタンプを付与した情報を取り扱う場合に、当該情報を長期保存する場合に講じる対策等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、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に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.8　情報交換に関するセキュリティ】

実施すべき安全管理策

(1)　次の情報交換方法について予め合意しておくこと。

- 情報を電子媒体に記録して交換する際の手順
- 情報をネットワーク経由で文書ファイル形式にて交換する際の手順
- 情報をネットワーク経由でアプリケーション入力にて交換する際の手順
- 情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順

(ウ) タイムスタンプを付与する時点で有効な電子証明書の使用

① タイムスタンプを付与した情報を取り扱う場合に、電子証明書の失効前の電子署名の有効性を担保するためのタイムスタンプの付与方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、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に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.11　暗号による管理策】

実施すべき安全管理策

(3)　電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。

(4)　暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。

(5)　医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証すること。

３．３ 外部保存に関する要求事項

３．３．１ 外部保存に関する要求事項の趣旨

厚生労働省ガイドライン第 5 版では、医療情報の外部保存を行うための指針等を「8 診療録及び診療諸記録を外部に保存する際の基準」に示しており、クラウドサービス事業者が医療情報を取り扱う際もこれを満たすことが求められる。

またクラウドサービスによる外部保存は、電子保存であり、この場合には厚生労働省ガイドライン第 5 版「7 電子保存の要求事項について」に示される真正性、見読性、保存性を満たすことが求められる。

以下、医療情報を外部保存する場合にクラウドサービス事業者が対応すべき事項について記述する。

３．３．２ 外部保存に関する要求事項が求められる文書

外部保存の要求事項が求められる文書は、厚生労働省ガイドライン第 5 版の 3.2 章に示されているとおり、外部保存改正通知で定められた表 1 に示す文書が対象となる。

また、表 1 に示す文書等がその法定保存年限が経過した等の事由によって、施行通知[26]や外部保存改正通知の対象外となった場合にも、外部保存を実施（継続）する場合には、第 7 章～第 9 章に準じて取り扱うことが求められる（厚生労働省ガイドライン第 5 版 3.4 章）。

[26] 本ガイドラインで「施行通知」とは、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成 28 年 3 月 31 日付け医政発 0331 第 31 号・薬生発 0331 第 11 号・保発 0331 第 27 号・政社発 0331 第 2 号厚生労働省医政局長、医薬・生活衛生局長、保険局長、政策統括官（社会保障担当）連名通知をいう。

表 1　外部保存改正通知の対象となる医療関係文書等

文書等
医師法（昭和 23 年法律第 201 号）第 24 条に規定されている診療録
歯科医師法（昭和 23 年法律第 202 号）第 23 条に規定されている診療録
保健師助産師看護師法（昭和 23 年法律第 203 号）第 42 条に規定されている助産録
医療法（昭和 23 年法律第 205 号）第 46 条第 2 項に規定されている財産目録、同法第 51 条の 2 第 1 項に規定されている事業報告書等、監事の監査報告書及び定款又は寄附行為、同条第 2 項に規定されている書類及び公認会計士等の監査報告書並びに同法第 54 条の 7 において読み替えて準用する会社法（平成 17 年法律第 86 号）第 684 条第 1 項に規定されている社会医療法人債原簿及び同法第 731 条第 2 項に規定されている議事録
医療法（昭和 23 年法律第 205 号)第 21 条、第 22 条及び第 22 条の 2 に規定されている診療に関する諸記録及び同法第 22 条及び第 22 条の 2 に規定されている病院の管理及び運営に関する諸記録
診療放射線技師法（昭和 26 年法律第 226 号）第 28 条に規定されている照射録
歯科技工士法（昭和 30 年法律第 168 号)第 19 条に規定されている指示書
薬剤師法（昭和 35 年法律第 146 号）第 27 条に規定されている調剤済みの処方せん
薬剤師法（昭和 35 年法律第 146 号）第 28 条に規定されている調剤録
外国医師等が行う臨床修練に係る医師法第 17 条等の特例等に関する法律（昭和 62 年法律第 29 号）第 11 条に規定されている診療録
救急救命士法（平成 3 年法律第 36 号）第 46 条に規定されている救急救命処置録
医療法施行規則（昭和 23 年厚生省令第 50 号）第 30 条の 23 第 1 項及び第 2 項に規定されている帳簿
保険医療機関及び保険医療養担当規則（昭和 32 年厚生省令第 15 号）第 9 条に規定されている診療録等
保険薬局及び保険薬剤師療養担当規則（昭和 32 年厚生省令第 16 号）第 6 条に規定されている調剤済みの処方せん及び調剤録
臨床検査技師等に関する法律施行規則（昭和 33 年厚生省令第 24 号）第 12 条の 3 に規定されている書類
歯科衛生士法施行規則（平成元年厚生省令第 46 号）第 18 条に規定されている歯科衛生士の業務記録
高齢者の医療の確保に関する法律の規定による療養の給付の取扱い及び担当に関する基準（昭和 58 年厚生省告示第 14 号）第 9 条に規定されている診療録等
高齢者の医療の確保に関する法律の規定による療養の給付の取扱い及び担当に関する基準第 28 条に規定されている調剤済みの処方せん及び調剤録

３．３．３ 真正性の確保に関する要求事項

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、真正性の確保の安全管理対策について、7.1 章に記述している。

真正性の確保にかかる安全管理対策では、

・医療機関等に保存する場合

・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 2 つのケースについて、それぞれ対応策を整理している。

医療機関等に保存する場合では、さらに、

・入力者及び確定者の識別及び認証

・記録の確定手順の確立と、作成責任者の識別情報の記録

・更新履歴の保存

・代行操作の承認機能

・機器･ソフトウェアの品質管理

等の対策が示されている。

また、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については、

・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

・ネットワーク上で「改ざん」されていないことを保証すること

・リモートログイン機能を制限すること

の 3 点について対策が示されている。

具体的な対策として規定されている内容を以下に示す。

【医療機関等に保存する場合】

7.1 C.最低限のガイドライン

(1)　入力者及び確定者の識別及び認証	
a. 電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合	1.　入力者及び確定者を正しく識別し、認証を行うこと。
	2.　システムへの全ての入力操作について、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）を定めること。また、権限のある利用者以外による作成、追記、変更を防止すること。
	3.　業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止すること。

b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合	1.　装置の管理責任者や操作者が運用管理規程で明確にされ、装置の管理責任者、操作者以外による機器の操作が運用上防止されていること。
	2.　当該装置による記録は、いつ･誰が行ったかがシステム機能と運用の組み合わせにより明確になっていること。
（2）　記録の確定手順の確立と、識別情報の記録	
a. 電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合	1.　診療録等の作成･保存を行おうとする場合、システムは確定された情報を登録できる仕組みを備えること。その際、入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時が含まれること。
	2.　「記録の確定」を行うに当たり、内容の十分な確認が実施できるようにすること。
	3.　「記録の確定」は、確定を実施できる権限を持った確定者が実施すること。
	4.　確定された記録が、故意による虚偽入力、書換え、消去及び混同されることの防止対策を講じておくこと、また原状回復のための手順を検討しておくこと。
	5.　一定時間後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを策定し運用管理規程に明記すること。
	6.　確定者が何らかの理由で確定操作ができない場合、例えば医療機関等の管理責任者が記録の確定を実施する等のルールを運用管理規程で定め、記録の確定の責任の所在を明確にすること。
b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合	1.　運用管理規程等に当該装置により作成された記録の確定ルールが定義されていること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時が記録に含まれること。
	2.　確定された記録が、故意による虚偽入力、書換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。
（3）　更新履歴の保存	

	1. 一旦確定した診療録等を更新した場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合せることができること。
	2. 同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること。
(4) 代行入力の承認機能	
	1. 代行入力を実施する場合、具体的にどの業務等に適用するか、また誰が誰を代行してよいかを運用管理規程で定めること。
	2. 代行入力が行われた場合には、誰の代行が誰によっていつ行われたかの管理情報が、その代行入力の都度記録されること。
	3. 代行入力により記録された診療録等は、できるだけ速やかに確定者による「確定操作（承認)」が行われること。この際、内容の確認を行わずに確定操作を行ってはならない。
(5) 機器･ソフトウェアの品質管理	
	1. システムがどのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかが明らかにされており、システムの仕様が明確に定義されていること。
	2. 機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスが規定されていること。
	3. 機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。
	4. システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施すること。

【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】

7.1 C.最低限のガイドライン

（1） 通信の相手先が正当であることを認識するための相互認証を行うこと	
	診療録等のオンライン外部保存を受託する機関と委託する医療機関等が、互いに通信目的とする正当な相手かどうかを認識するための相互認証機能が必要である。
（2） ネットワーク上で「改ざん」されていないことを保証すること	
	ネットワークの転送途中で診療録等が改ざんされていないことを保証できること。なお、可逆的な情報の圧縮･解凍並びにセキュリティ確保のためのタグ付けや暗号化･平文化等は改ざんにはあたらない。
（3） リモートログイン機能を制限すること	

	保守目的等、どうしても必要な場合を除いて行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。
なお、これらの具体的要件については、「6.11 外部と診療情報等を含む医療情報を交換する場合の安全管理」を参照されたい。	

（２） クラウドサービス事業者への要求事項

厚生労働省ガイドライン第 5 版では、外部保存の対象となるデータについて、院内に保存する場合よりも多くの要求事項を設けている。一方で、クラウドサービスでは、外部保存は原則としてどのサービスでも生じうることから、本ガイドラインでは一般的な技術的対応策等として規定することとした。

また、本ガイドラインでは、真正性の確保について複数の箇所に分けて記述している。具体的な記述箇所を以下に示す。

【医療機関等に保存する場合】

7.1 C.最低限のガイドライン

厚生労働省ガイドライン第 5 版の項目	クラウドサービス事業者の要求事項で本ガイドラインでの記述箇所
（1）入力者及び確定者識別及び認証	３．２．３（２）（ウ）
（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	３．２．３　（２）（ケ）

【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】

7.1 C.最低限のガイドライン

厚生労働省ガイドライン第 5 版の項目	クラウドサービス事業者の要求事項で本ガイドラインでの記述箇所
（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おこなうこと	３．２．９（２）（ア）
（2）ネットワーク上で「改ざん」されていないことを保証すること	３．２．９　（２）
（3）リモートログイン機能を制限すること	３．２．６（２）（イ） ３．２．９（２）（ウ）

３．３．４ 見読性の確保に関する要求事項

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、見読性の確保の安全管理対策について、7.2 章に記述している。

見読性の確保の安全管理対策では、

・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
・医療機関等に保存する場合
・ネットワークを通じて外部に保存する場合

の 3 つのケースについて、それぞれ対応策を整理している。

また、どちらの場合にも対応すべき対策として

・情報の所在管理
・見読化手段の管理
・見読目的に応じた応答時間

等の対策が示されている。

具体的な対策として規定されている内容を以下に示す。

7.2 C.最低限のガイドライン

（1）情報の所在管理	
	紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者ごとの情報の全ての所在が日常的に管理されていること。
（2）見読化手段の管理	
	電子媒体に保存された全ての情報とそれらの見読化手段は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。
（3）見読目的に応じた応答時間	
	目的に応じて速やかに検索表示若しくは書面に表示できること。
（4）システム障害対策としての冗長性の確保	
	システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするために、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意すること。

【医療機関等に保存する場合】

7.2 D.推奨されるガイドライン

（1）バックアップサーバ	
	システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。
（2）見読性確保のための外部出力	
	システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力することができること。
（3）遠隔地のデータバックアップを使用した見読機能	
	大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップし、そのバックアップデータと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。

【ネットワークを通じて外部に保存する場合】

医療機関等に保存する場合に推奨されるガイドラインに加え、次の事項が必要となる。

7.2 D.推奨されるガイドライン

（1）緊急に必要になることが予測される診療録等の見読性の確保	
	緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しても複製又は同等の内容を医療機関等の内部に保持すること。
（2）緊急に必要になるとまではいえない診療録等の見読性の確保	
	緊急に必要になるとまではいえない情報についても、ネットワークや外部保存を受託する機関の障害等に対応できるような措置を行っておくこと。

（２） クラウドサービス事業者への要求事項

厚生労働省ガイドライン第 5 版においては【医療機関等に保存する場合】を基本としつつ【ネットワークを通じて外部に保存する場合】は追加の安全管理対策を求めている。クラウドサービスを利用する際には【ネットワークを通じて外部に保存する場合】に該当するケースが中心であることから、本ガイドラインにおいては厚生労働省ガイドライン第 5 版の【ネットワークを通じて外部に保存する場合】を踏まえた安全管理対策を規定することとする。

また、本ガイドラインでは、見読性の確保について複数の箇所に分けて記述している。具体的な記述箇所について以下に示す。

【保存する場所について共通する内容】

7.2 C.最低限のガイドライン

厚生労働省ガイドライン第 5 版の項目	クラウドサービス事業者の要求事項で本ガイドラインでの記述箇所
（1）情報の所在管理	３．２．３（２）（イ）
（2）見読化手段の管理	３．２．３（２）（ク）
（3）見読目的に応じた応答時間	３．２．３（２）（キ）
（4）システム障害対策としての冗長性の確保	３．２．３（２）（ク）

【医療機関等に保存する場合】

7.2 D.推奨されるガイドライン

厚生労働省ガイドライン第 5 版の項目	クラウドサービス事業者の要求事項で本ガイドラインでの記述箇所
（1）バックアップサーバ	３．２．３（２）（ク） ３．２．８（２）（ア）
（2）見読性確保のための外部出力	３．２．８（２）（ア）
（3）遠隔地のデータバックアップを使用した見読機能	３．２．８（２）（ア）

【ネットワークを通じて外部に保存する場合】

7.2 D.推奨されるガイドライン

厚生労働省ガイドライン第 5 版の項目	クラウドサービス事業者の要求事項で本ガイドラインでの記述箇所
（1）緊急に必要になることが予測され	３．２．８（２）（ア）

る診療録等の見読性の確保	
（２）緊急に必要になるとまではいえない診療録等の見読性の確保	３．２．８（２）（ア）

３．３．５ 保存性の確保に関する要求事項

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、保存性の確保の安全管理対策について、7.3 章に記述している。

保存性の確保の安全管理対策では、

・医療機関等に保存する場合

・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 2 つのケースについて、それぞれ対応策を整理している。

医療機関等に保存する場合では、さらに、

・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

・不適切な保管･取扱いによる情報の滅失、破壊の防止

・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

・媒体･機器･ソフトウェアの整合性不備による復元不能の防止

等の対策が示されている。

具体的な対策として規定されている内容を以下に示す。

【医療機関等に保存する場合】

7.3 C.最低限のガイドライン

(1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止	
	1. いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊･混同が起こらないように、システムで利用するソフトウェア、機器及び媒体の管理を行うこと。
(2) 不適切な保管･取扱いによる情報の滅失、破壊の防止	
	1. 記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと。
	2. システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること。
	3. 記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を施すこと。
	4. 電子的に保存された診療録等の情報に対するアクセス履歴を残し、管理すること。
	5. 各保存場所における情報がき損した時に、バックアップされたデータを用

	いてき損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと。
(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	
	1.　記録媒体が劣化する以前に情報を新たな記録媒体または記録機器に複写すること。記録する媒体及び機器ごとに劣化が起こらずに正常に保存が行える期間を明確にして、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体又は記録機器については、そのデータを新しい記録媒体又は記録機器に複写すること。これらの一連の運用の流れを運用管理規程にまとめて記載し、関係者に周知徹底すること。
(4)　媒体･機器･ソフトウェアの不整合による情報の復元不能の防止	
	1.　システム更新の際の移行を迅速に行えるように、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること。
	2.　マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えていること。

7.3 D.推奨されるガイドライン

(1)　不適切な保管･取扱いによる情報の滅失、破壊の防止	
	1.　記録媒体及び記録機器、サーバの保管は、許可された者しか入ることができない部屋に保管し、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存すること。
	2.　サーバ室には、許可された者以外が入室できないように、鍵等の物理的な対策を施すこと。
	3.　診療録等のデータのバックアップを定期的に取得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備えること。
(2)　記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止	
	診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1 若しくは RAID-6 相当以上のディスク障害に対する対策を行うこと。

【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】

医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。

7.3 C.最低限のガイドライン

(1)データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと	
	保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又

	は変更されることが考えられる。その場合、外部保存を受託する機関は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持しなくてはならない。
（2）ネットワークや外部保存を受託する機関の設備の劣化対策を行うこと	
	ネットワークや外部保存を受託する機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策を行うこと。

7.3 D.推奨されるガイドライン

（1）ネットワークや外部保存を受託する機関の設備の互換性を確保すること	
	1.回線や設備を新たなものに更新した場合、旧来のシステムに対応した機器が入手困難となり、記録された情報を読み出すことに支障が生じるおそれがある。従って､外部保存を受託する機関は、回線や設備の選定の際は将来の互換性を確保するとともに、システム更新の際には旧来のシステムに対応し､安全なデータ保存を保証できるような互換性のある回線や設備に移行すること。

（２） クラウドサービス事業者への要求事項

厚生労働省ガイドライン第 5 版においては【医療機関等に保存する場合】を基本としつつ【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】は追加の安全管理対策を求めているが、クラウドサービス事業者においては【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】に該当するケースが中心であることから、本ガイドラインにおいては【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】を踏まえた安全管理対策を規定することとする。

また、本ガイドラインでは、保存性の確保について複数の箇所に分けて記述している。具体的な記述箇所について以下に示す。

【医療機関等に保存する場合】

7.3 C.最低限のガイドライン

厚生労働省ガイドライン第 5 版の項目	クラウドサービス事業者の要求事項で本ガイドラインでの記述箇所
（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	３．２．３（２）（カ）
（2） 不適切な保管･取扱いによる情報の滅失、破壊の防止	３．２．２（２）（ア） ３．２．３（２）（エ）（ク） ３．２．７（２）（ア）
（3） 記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止	３．２．３（２）（ク）
（4） 媒体･機器･ソフトウェアの整合性不備による復元不能の防止	３．２．６（２）（エ）

7.3 D.推奨されるガイドライン

厚生労働省ガイドライン第 5 版の項目	クラウドサービス事業者の要求事項で本ガイドラインでの記述箇所
（1） 不適切な保管･取扱いによる情報の滅失、破壊の防止	３．２．３（２）（ク）
（2） 記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止	３．２．３（２）（ク）

【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】

7.3 C.最低限のガイドライン

厚生労働省ガイドライン第 5 版の項目	クラウドサービス事業者の要求事項で

	本ガイドラインでの記述箇所
（1）データ形式及び転送プロトコルのバージョン管理と継続性の確保をおこなうこと	３．２．６（２）(エ)
(1) ネットワークや外部保存を受託する機関の設備の劣化対策をおこなうこと	３．２．６（２）(エ)

7.3 D.推奨されるガイドライン

厚生労働省ガイドライン第 5 版の項目	クラウドサービス事業者の要求事項で本ガイドラインでの記述箇所
(1) ネットワークや外部保存を受託する機関の設備の互換性を確保すること	３．２．６（２）(エ)

３．３．６ 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、外部保存を受託する機関の選定基準及び情報の取扱いに関する基準について、8.1.2 章に記述している。

外部保存を受託する機関の選定基準及び情報の取扱いに関する基準では、

・病院、診療所、医療法人等が適切に管理する場所に保存する場合
・行政機関等が開設したデータセンター等に保存する場合
・医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合[27]

の 3 つのケースについて、それぞれ対応策を整理している。

本ガイドラインは、クラウドサービス事業者を対象とすることから、3 つ目の「医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」を考える。

具体的な対策として規定されている内容を以下に示す。

【医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合】

8.1.2 C.最低限のガイドライン

(ア) 医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取扱いに対して監督を行えること。
(イ) 医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること。
(ウ) 受託事業者が民間事業者等に課せられた経済産業省の「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」や総務省の「ASP･SaaS における情報セキュリティ対策ガイドライン」及び「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」等を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。
(エ) 保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。なお保守に関しては、「6.8 情報システムの改造と保守」を遵守すること。

[27] 民間の医療機関等が他の医療機関等に対して、クラウドサービスを提供する場合には、「医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」に含まれる。

(オ) 外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること。
(カ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないようにさせること。
(キ) 医療機関等において（ア）から（カ）を満たした上で、外部保存を受託する事業者の選定基準を定めること。少なくとも以下の 4 点について確認すること。 (a) 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 (b) 医療情報等の安全管理に係る実施体制の整備 (c) 実績等に基づく個人データ安全管理に関する信用度 (d) 財務諸表等に基づく経営の健全性

8.1.2 D.推奨されるガイドライン

(ウ) 「②行政機関等が開設したデータセンター等に保存する場合」及び「③医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」では、技術的な方法として、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保すること。
(エ) 外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつこと。具体的には、「暗号化を行う」、「情報を分散管理する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を併せ持つこと。

（２） クラウドサービス事業者への要求事項

厚生労働省ガイドライン第５版が示す対策のうち、契約に盛り込むべき内容（守秘義務違反への対応、各種ガイドライン遵守義務等）については、本ガイドライン３．２．１における契約内容に対する項目で示す。

本項で示すクラウドサービス事業者への要求事項については、

・医療機関等によるサービス選択のための事業者情報の提供
・受託医療情報の無断閲覧禁止
・受託情報の解析及び第三者提供の制限

等について整理する。

(ア) 医療機関等によるサービス選択のための事業者情報の提供

① サービスの提供に係る契約に際して、医療機関等の求めに応じて、以下の情報の提供を行う。

・医療情報等の安全管理に係る基本方針･取り扱い規程等の整備状況
・医療情報等の安全管理に係る実施体制の整備状況
・実績等に基づく個人データ安全管理に関する信用度[28]
・財務諸表等に基づく経営の健全性

なお、医療機関等によるサービス選択における事業者情報の提供に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.1.1 ISMS 認証取得時の考慮事項】

推奨される安全管理策

(1) 認証取得あるいは更新の際に ISMS の安全管理策として、本ガイドライン「7 医療情報を受託管理する情報処理事業者における安全管理上の要求事項」にて提示する安全管理策を盛り込むことが望ましい。

(2) 受託管理する医療情報の入り口から出口まで包括的に ISMS の適用範囲とすることが望ましい。

(3) 安全管理措置が適切に適用されていることを、医療機関等が委託先事業者を選定する際に確認できるよう、医療機関等の要請に応じて適用宣言書の閲覧を即座に行うことができるよう準備を行っておくことが望ましい（適用宣言書には医療情報を取り扱うために特別に配慮している管理策を明確にすること）。

[28]個人データ安全管理に関する信用度は個人情報の流出事故がない旨の実績やこれに基づく認証の取得のほか、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などが想定される。

【7.3 組織的安全管理策（体制、運用管理規程)】

実施すべき安全管理策

(1) 医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。

(2) 個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。

(イ) 受託情報に対する閲覧制限

1. 保守・運用における受託情報の閲覧制限	① 受託した医療情報を保守･運用を行うために閲覧するのは必要最小限とする。 ② ①の閲覧が必要な場合には、緊急時を除き、システム管理者の事前･事後の承認により実施する。 ③ 受託した医療情報を緊急時に閲覧した場合には、閲覧した受託情報の範囲及び緊急で閲覧が必要な理由等を示して、システム管理者の承認を得る。 ④ ①～③における閲覧に係る範囲、手順等について、サービス仕様適合開示書に基づき、医療機関等と合意する。また②、③により医療情報を閲覧した場合に、速やかに医療機関等にその旨の報告を行う。
2. 受託情報の閲覧制限のための機能	① 予定された保守･運用等を行う際に受託した医療情報を許可なく閲覧できないようにするために、権限設定等の対策を講じる。 ② システム管理者、運用担当者、保守担当者等が、意図しない閲覧を行わないことを担保するための措置（データベースの暗号化等）を講じる。

(ウ) 受託情報の解析及び第三者提供制限

1. 受託情報の解析等の制限等	① 受託した医療情報の解析･分析は、サービス提供に係る契約とは独立した契約に基づいて医療機関等からの委託を受けた場合を除いて行わない。 ② 受託した医療情報を匿名加工した情報も、医療情報に準じて取り扱う。
2. 受託情報の解析等の第三者提供制限	① 受託した医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わない。 ② ①の内容を、サービス提供に係る契約に含める。 ③ 医療機関等の指示に基づき、受託した医療情報の第三者提供（閲覧）を行う場合には、医療機関等が許諾した者以外が閲覧･取得できないように、３．２．３及び３．２．９に示す対応策を講じる。 ④ ③により、第三者提供（閲覧）を行う場合には、閲覧･取得が可能な者のID及び利用権限について、医療機関等又はその委託を受けた者（医療情報連携ネットワーク等）の指示に基づき、速やかに変更･削除できる対応を行

	う。 ⑤　医療機関等の指示に基づいて受託した医療情報の第三者提供を行った場合には、医療機関等に対してその内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告を行う。 ⑥　①～⑤により第三者提供及びその報告を行うための条件、範囲等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

３．３．７ 個人情報の保護についての安全管理対策

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、個人情報の保護についての安全管理対策について、8.1.3 章に記述している。そこでは、

・診療録等の外部保存委託先の事業者内における個人情報保護

・外部保存実施に関する患者への説明

の 2 つのケースについて、それぞれ対応策を整理している。具体的な対策として規定されている内容を以下に示す。

8.1.3 C.最低限のガイドライン

（1） 診療録等の外部保存委託先の事業者内における個人情報保護	
	① 適切な委託先の監督を行うこと 診療録等の外部保存を受託する事業者内の個人情報保護については、本ガイドライン 6 章を参照し、適切な管理を行う必要がある。
（2）外部保存実施に関する患者への説明 診療録等の外部保存を委託する施設は、あらかじめ患者に対して、必要に応じて患者の個人情報が特定の外部の施設に送られ、保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得る必要がある。	
	① 診療開始前の説明 患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を、院内掲示等を通じて説明し理解を得た上で診療を開始すること。
	② 患者本人に説明をすることが困難であるが、診療上の緊急性がある場合 意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明を行い、理解を得る必要がある。
	③ 患者本人に説明することが困難であるが、診療上の緊急性が特にない場合 乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得ること。 ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。

（２） クラウドサービス事業者への要求事項

個人情報の保護に関する要求事項は、３．２．１ないし３．２．７、及び３．２．９においてそれぞれ示しているが、厚生労働省ガイドライン第５版に従い、それらの要求事項に加えて、クラウドサービス事業者に求める事項を以下に示す。

(ア) 診療録等の外部保存委託先の事業者内における個人情報保護

① 個人情報保護対応策を、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお、診療録等の外部保存委託先の事業者内における個人情報保護に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.3 組織的安全管理策（体制、運用管理規程)】
実施すべき安全管理策
(3) 個人情報保護に関しては、医療機関等の監督の下に行うこと。

(イ) 外部保存実施に関する患者への説明

① 医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

３．４ クラウドサービスの利用終了に関する要求事項

３．４．１ クラウドサービスの利用終了における対応

（１） 厚生労働省ガイドラインの記述

厚生労働省ガイドライン第 5 版では、外部保存を終了する場合の対応についての考え方を 8.4.2 章で示している。そこでは、医療機関等において外部保存の終了に関して委託先事業者と取り決めるべきこと等についての考え方を示している。その内容を以下に示す。

8.4.2　B 項

診療録等が機微な個人情報であるという観点から、外部保存を終了する場合には、医療機関等及び受託する事業者双方で一定の配慮をしなくてはならない。

診療録等の外部保存を委託する医療機関等は、受託する事業者に保存されている診療録等を定期的に調べ、外部保存を終了しなければならない診療録等は速やかに処理した上で、当該処理が厳正に執り行われたかを監査しなくてはならない。また、外部保存を受託する事業者も、医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を医療機関等に明確に示す必要がある。

これらの廃棄に関わる規定は、外部保存を開始する前に委託契約書等にも明記をしておく必要がある。また、実際の廃棄に備えて、事前に廃棄プログラム等の手順を明確化した規定を作成しておくべきである。

これらの厳正な取扱い事項を双方に求めるのは、同意した期間を超えて個人情報を保持すること自体が、個人情報の保護上問題になり得るためであり、そのことに十分に留意しなければならない。

ネットワークを通じて外部保存する場合は、外部保存システム自体も一種のデータベースであり、インデックスファイル等も含めて慎重に廃棄しなければならない。また電子媒体の場合は、バックアップファイルについても同様の配慮が必要である。

また、ネットワークを通じて外部保存している場合は、自ずと保存形式が電子媒体となるため、情報漏えい時の被害は、その情報量の点からも甚大な被害が予想される。従って、個人情報保護に十分な配慮を行い、確実に情報が廃棄されたことを、外部保存を委託する医療機関等と受託する事業者とが確実に確認できるようにしておかなくてはならない。

（２） クラウドサービス事業者への要求事項

医療機関等がクラウドサービスの利用による医療情報の外部保存を終了するケースとしては、

・クラウドサービス事業者側の都合による終了

・医療機関等側における都合による利用の終了

の２つが考えられる。前者の場合には、医療機関等においては、必ずしも利用中のサービスが停止することは予定していないため、委託していた医療情報の利用が不能になるリスクが生じる。そのため、事前の取り決めを十分に行うことが求められる。

いずれの場合にも、クラウドサービス事業者は、

・受託したデータの返却

・受託したデータの削除

についての対応策を講じる必要がある。

また、クラウドサービス事業者の都合により、サービス内容の大きな変更が生じる場合も考えられる。

その場合には、クラウドサービス事業者は、医療機関等に対して、十分な告知期間の設定することや、終了等に伴う移行支援等の内容について、予め医療機関等に示し、医療情報の利用の停止を防止するための対応策を講じることが求められる。クラウドサービス事業者への要求事項を以下に示す。

① サービスの一部又は全部の停止やサービス変更の場合（軽微なバージョンアップは含まない）には、サービスを利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。
② ①の場合、受託した医療情報を、医療機関等に返却する。返却するデータの範囲（データ種類、期間等）、データ形式（データ項目、項目の詳細、ファイル形式）、返却方法、条件については、サービス仕様適合開示書に基づき、医療機関等と合意する。また医療機関等のサービス利用開始後に、サービス仕様適合開示書の内容を変更する場合には、①に準じた対応策を講じる。
③ ②におけるデータの返却については、厚生労働省ガイドライン第5版「5 情報の相互運用性と標準化について」に従って行うこととし、その内容について医療機関等と合意する。なお、返却するデータに、クラウドサービス事業者において実施した不可逆的な圧縮（画像データ等）や変換（パスワード等）によるデータが含まれる場合があるので、その旨も合わせて、サービス仕様適合開示書に基づき、医療機関等と合意する。
④ ①においてサービスの変更を含むサービスの一部又は全部の停止（軽微なバージョンアップは含まない）が生じる場合の医療機関等への対応の内容（移行支援等で、②の対応は除く）、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
⑤ 医療機関等の都合により医療機関等のサービス利用が終了する場合も、②、③に示す対応策を講じる。
⑥ サービス提供の停止又は医療機関等におけるサービス利用停止が生じた場合は、速やかに、記録の削除、媒体の廃棄等を行う。記録の削除、媒体の廃棄等を行った場合には、これを証明する資料を医療機関等に対して提出する。
⑦ ⑥に関して、医療機関等へのサポート（所管官庁への情報提供含む）等に関連して必要最低限の範囲で、記録を保持し続ける場合には、その目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
⑧ ①～⑦についての手順等を、運用管理規程等に含める。

なお、クラウドサービスの利用終了における対応に関して、経済産業省ガイドラインで規定している内容を参考に示す。

【参考】経済産業省ガイドラインにおける当該安全管理対策の記述内容

【7.6.7 電子媒体の取扱】

実施すべき安全管理策

(9) 電子媒体を廃棄する場合には、物理的な破壊措置（高温による融解、裁断等）を適用し、情報の読み出しが不可能であることを確認すること。

３．５　オンライン診療システム提供事業者における安全管理対策

３．５．１ オンライン診療におけるセキュリティ上の要求事項

オンライン診療指針では、医療機関がオンライン診療システムと電子カルテシステム等を接続し、医師がシステム内の医療情報を確認しながら診療を実施する場合や、患者側に検査結果等を表示しながら診療を行う場合など、医療情報システムにオンライン診療システムが接続する等の場合には、オンライン診療システムについても、医療情報安全管理関連ガイドラインに沿った対策を行うことが必要であるとされている[29]。

なお、オンライン診療指針では、患者側の端末を通じた医療情報システムへの不正アクセス等を防止する観点から、オンライン診療システムの機能として、患者側端末を医療情報システムと接続させないような措置を講ずることとしている。

３．５．２ オンライン診療システム提供事業者における要求事項

３．５．１で示した医療機関に対するオンライン診療におけるセキュリティ情報の要求事項を踏まえ、オンライン診療システムを提供するクラウドサービス事業者の要求事項を以下に示す。

① オンライン診療システムにおいて、医療情報システムとの接続がある場合には、本ガイドラインの「３．２」～「３．４」の要求事項を、オンライン診療システムを提供するクラウドサービス事業者にも適用する。

② 患者側端末で利用するオンライン診療システムの機能には、オンライン診療の実施中に医療情報システムと接続する機能等を含まないこと、及びこれに関する情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

③ 医師が利用するオンライン診療システムを提供するクラウドサービス事業者と患者との間の責任分界について、サービス仕様適合開示書に基づき、医療機関等と合意する。

[29] オンライン診療指針 P22

３．６ PHR サービス事業者における安全管理対策

３．６．１ PHR サービス事業者への要求事項

本ガイドラインでは、医療機関等が管理していた医療情報で、医療機関の管理を離れ、患者等の管理にある情報を取り扱うクラウドサービスを提供する事業者（PHR サービス事業者）における安全対策に関する要求事項を、第３章「３．６」に示している。

本ガイドラインの「３．２」～「３．４」では、医療機関等が管理する医療情報を取り扱うクラウドサービス事業者が対応すべき要求事項を示している。これらの要求事項については、PHR サービス事業者が医療情報を取り扱う際にも、基本的には同様のものが必要と考えられる[30]が、他方、医療機関等での医療情報の利用と PHR での医療情報の利用を比較した場合に、医療情報の機密性への要求水準は同じでも、医療機関等での利用の方が患者の身体や生命に直接関わることから、完全性や、特に可用性への要求水準が高いと考えられる。このため、①完全性や可用性を確保するために要求されている事項については、PHR サービス事業者に同水準で適用することは過度な要求となることから、PHR サービス事業者を適用対象から外すことが適当である。また、②法令で医療機関等に作成や保存等が義務付けられていることに起因する要求事項や、③医療機関等が行政機関等に報告を行うために必要な記録の管理を要求している事項、④医療機関等への適用しか想定されない要求事項（医療機器からのデータ取得等）についても、同様に PHR サービス事業者を適用対象から外すことが適当である。（３．６．３）

[30] ただし、PHR サービスの場合、医療機関等が医療情報を取り扱うクラウドサービスを利用する場合と異なり、患者等が取り扱う医療情報は自らの情報に限られることから、PHR サービス事業者における要求事項は、それに応じた水準・内容となる。

① PHR サービス事業者については、３．２．１～３．２．９、３．３．６～３．３．７に示す要求事項を以下のとおり読み替えるものとする。
・「医療情報」→「PHR で利用する医療情報[31]」
・「医療機関等」→「患者等」
・「クラウドサービス事業者」→「PHR サービス事業者」

② PHR サービス事業者については、３．２．９（２）（イ）2.の①の要求事項における「TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行う」とある部分を、「TLS の設定は 1.2 に限定し、信頼性の高い機関によって発行されたサーバ証明書を用いるとともに、本人性の確認を確実に実施する」と読み替えるものとする。

③ PHR サービス事業者については、３．２．３（２）（ア）4.の③の要求事項における「なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン 第 5 版の公表（平成 29 年 5 月）から約 10 年後を目途に 2 要素認証について「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。」とある部分を削除するものとする。

④ PHR サービス事業者については、３．３．６（２）（ウ）2. の①の要求事項における「患者本人を含め」とある部分を削除するものとする。

⑤ PHR サービス事業者については、３．２．１～３．２．９、３．３．６～３．３．７に示す要求事項のうち、３．６．３に掲げる要求事項を適用対象外とする。

⑥ PHR サービスの提供に際しては、以下の内容を含む手順を策定し、その手順に基づいて実施したことを確認する。
・登録時の ID 申請者である患者等の本人確認（実在性の確認）
・利用時の患者等の認証（利用者の本人確認）
・新たに受領した医療情報の患者等の ID への紐づけ（患者本人の情報であることの確認）

⑦ PHR サービス事業者については、３．２．１～３．２．９、３．３．６～３．３．７に示す要求事項のうち、上記①による読み替え後に「サービス仕様適合開示書に基づき、患者等と合意する」となる要求事項は適用対象外とし、それらの要求事項に代えて以下の対応を行うこととする。
・PHR サービスで取り扱う個人情報に関して、患者等からの同意の取得方法について運用管理規程を策定する。その運用管理規程には、本ガイドラインを遵守して個人情報を取り扱う旨を含める。
・PHR サービスの提供終了時又は契約終了時における患者等に関する医療情報の返却の範囲、方法、条件について、患者等とあらかじめ合意する。

・患者等の指示により、医療機関等が（自ら管理する）医療情報を患者等が契約する PHR サービス事業者へ送付する場合において、PHR サービス事業者と医療機関等との責任分界について、あらかじめ患者等に示す。
・PHR サービスの提供に関する患者等との合意においては、この情報が個人情報保護法上の要配慮個人情報であることや消費者保護法等の適用を受ける可能性があることを勘案して、免責事項等の内容を定める。

[31] 医療機関等が管理していた医療情報で、医療機関等の管理を離れ、患者等の管理にある情報をいう。

３．６．２ PHR サービス事業者を適用対象とする要求事項

本ガイドラインにおける医療機関等が管理する医療情報を取り扱うクラウドサービス事業者に対する要求事項のうち、読み替えて PHR サービス事業者に適用する要求事項を下記に示す。

（１） 組織的安全管理対策（３．２．１（２）の読替え）

項番	内容
（ア）	① サービスの提供についての管理責任を有する責任者を設置する。 ② 情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者）を設置する。 ③ サービスの提供に係る情報システムの運用に関する事務を統括する責任者を設置する。 ④ ①から③に掲げた責任者の任命･解任等のルールを策定する。
（イ）1	① サービスに係る情報及び受託した情報に関する守秘義務について、サービス提供に係る契約に含める。契約には、守秘義務に違反した PHR サービス事業者にはペナルティが課されること、及び委託した情報の取扱いに対する患者等による監督に関する内容を含める。
（イ）2	① サービス提供に係る契約において、次項（ウ）1. に定める運用管理規程等の内容、その他最新の関連法令等を遵守し、安全管理措置を実施する旨を明らかにする。
（ウ）1	① 経営者は、自社における個人情報保護指針、プライバシーポリシー等について明確にする。 ② ①の指針等には個人情報保護法及び個人情報保護委員会のガイドラインに定める安全管理措置等を実施する旨を含める。 ③ ①の指針等には、個人情報保護法の対象外の情報（死者に関する情報等）であっても、PHR で利用する医療情報の特殊性から個人情報保護法における運用に準じて取り扱う旨を含める。 ④ 情報セキュリティに関する基本方針、運用管理規程等の情報セキュリティポリシーを策定する。 ⑤ 情報セキュリティポリシーの遵守を担保する組織体制の構築とその文書化を行う。
（ウ）2	① サービスの提供に係る体制を、緊急時の対応も含めて明確にする。
（ウ）3	① 情報セキュリティに関する基本方針や運用管理規程等、重要な文書の作成や管理に関する規程を策定し、これに基づき文書の管理を行う。

	② サービスの運用や資源管理に関して、適切に文書化を行い、セキュリティ情報として管理する。
（ウ）4	① サービスに係るリスクの分析を行い、必要な対応措置等を講じる旨を定める。
（ウ）5	① 機器等の管理方法について、文書化を行う。 ② 機器等について、台帳管理等により所在確認等を行う旨を定める。
（ウ）6	① 個人情報を記録した媒体の管理等に関する運用規程を策定する。
（ウ）8	① サービスを提供する情報システム、組織体制、運用等に関する監査の方針、内容等について明文化を行う。 ② 第三者が提供するクラウドサービスを利用する場合については、これに対する監査又は代替する対応についての方針、内容を明確にする。 ③ 監査実施について記録し、当該記録の保存･管理方法を明確にする。
（ウ）9	② 自社で契約した第三者が提供するクラウドサービスを利用してサービスを提供する場合でも、患者等からの問合せ窓口を一元化する。
（エ）1	① PHR サービス事業者における情報システムへのアクセス権限、アカウント管理、認証及びアクセス等に対する記録の収集と保存、並びにアクセス管理の運用状況に関する定期的なレビューの実施等を内容とするアクセス管理規程を策定する。 ② サービスの提供に係るアクセス記録（外部からのアクセス、利用者によるアクセス等を含む）の保存、記録の定期的なレビューと改善を実施する旨を内容とするアクセス管理規程を策定する。
（エ）2	① PHR で利用する医療情報の取扱いに関する委託契約に、以下の内容を含める。 ・個人情報に関して、他の情報と区別して適切に管理を行う。 ・PHR で利用する医療情報は、死者に関する情報についても個人情報に準じて取り扱う旨を明確にする。

（２） 物理的安全管理対策（３．２．２（２）の読替え）

項番	内容
（ア）1	① サービスに供する機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。 ② サービスに供するサーバ等を格納するラック等について、施錠管理を行う。 ③ サービスに供する媒体等を格納するキャビネット等について、施錠管理を行う。
（ア）2	① サービスに供する機器や媒体の設置場所については、許可された者のみが入退できるように制限する。 ② サービスに供する機器や媒体の設置場所への入退状況の管理（入退記録のレビュー含む）は定期的に行う。 ③ サービスに供する機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じる。 ④ サービスに供する機器や媒体の設置場所への不明者の入退を発見するために、入退者に名札等の着用を義務付ける。 ⑤ サービスに供する機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。 ⑥ サービスに供する機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。 ⑦ ①～⑥につき、運用管理規程等に規定する。
（ア）3	① サービスに供する機器や媒体を物理的に保存するための施設は、災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能･構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置する。
（ア）4	① サービスに供する機器等が保存されている建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等を設置する。 ② 防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる。 ③ サービスに供する機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、状況を確認することで、不正な入退者がないことを確認する。

（イ）1	① 個人情報の表示中の覗き見を予防するために、運用端末に覗き見対策のシートを貼る等の対策を行う。 ② 運用中の画面が、運用者以外の者の視野に入らないような対応等を行う。
（ウ）1	① 個人情報が物理的に保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。 ② 個人情報が存在する PC 等の重要な機器には、盗難防止用チェーンを取り付ける。 ③ 受託する個人情報を運用や保守に用いる端末に保存しない旨、自社の運用管理規程等に定める。

（３） 技術的安全管理対策（３．２．３（２）の読替え）

項番	内容
（ア）1	① 情報システムの利用者を特定し識別できるように、アカウントの発行を行う（複数の利用者による ID の共同利用は行わない。ただし当該情報システムが他の情報システムを利用するための ID（non interactive ID）は除く）。 ② 利用者のなりすまし等を防止するための認証を行う。 ③ 利用者には、患者等においてサービスを利用する者のほか、情報システムの運用若しくは開発に従事する者又は管理者権限を有する者も含める。 ④ 情報システムの運用若しくは開発に従事する者又は管理者権限を有する者に対する ID の発行は必要最小限とし、定期的な棚卸しを行う。
（ア）2	① 本人の識別･認証に、ユーザ ID とパスワードを組み合わて用いる場合には、それらを、本人しか知り得ない状態に保つよう対策を行う。具体的には以下のような対策を行う。 ・利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと情報システムにアクセスできないにようにする。 ・初期パスワード以外のパスワードは、利用者本人が設定し、本人しか知りえない内容に限定する。 ・パスワードの設定に際しては、複数の文字種（英数字･大文字･小文字･記号等）を用い、また、8 文字以上等、十分に安全な長さの文字列等から構成されるルールとする。 ② パスワード認証に係る以下のルールを実現する措置を講じる。 ・パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定する。 ・パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない仕組みとする。 ③ パスワードには十分な安全性を満たす有効期間を設定する。ただし、利用者が患者等である場合には、他のサービスで利用しているパスワードを使わないよう特に促すだけでなく、サービス提供側から患者等に対して定期的なパスワードの変更を要求しないようにする。 ④ 認証に際して ID 及びパスワードによらない場合でも、上記と同等以上の安全性を確保する。
（ア）3	① 利用者のパスワードは、ハッシュ値での保存を行う等、暗号化して管理する。 ② サービスを提供する製品等の導入に際しては、初期パスワードを変更するだけでなく、アカウントの棚卸しを行い、不要なものについては削除を行う。 ③ 利用者が ID やパスワードを失念した場合には、予め策定した手順（本人確認

	を含む）に則り、本人への通知又は再発行を行う。 ④　パスワード等の情報の漏洩が生じた場合（不正な第三者からの攻撃による場合を含む）には、直ちに当該 ID を無効化し、予め策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知する。 ⑤　パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知した上で、当該パスワードを無効化し、変更できるような対応を講じる。 ⑥　利用者が設定するパスワードについては、第三者から容易に推定されにくい内容を含む品質基準を策定し、これに基づく運用を行う。 ⑦　利用者のパスワードの世代管理を行い、パスワード変更に際して、安全性を確保するために必要な範囲で、過去に設定したパスワードを設定できないような運用を行う。
（ア）4	①情報システムの運用若しくは開発に従事する者又は管理者権限を有する者の情報システム利用に係る認証は、2 要素認証以上の認証強度のある方法による。 ③　利用者の認証において、固定式の ID･パスワードによる認証方式を採用している場合には、固定式の ID･パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。 ④　利用者の認証に際して、何らかの物理的な媒体･身体情報等を必要とする場合に、例外的にそれらの媒体等がなくても一時的に認証するための代替的手段･手順を事前に定める。 ⑤　代替的手段･手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差が最小となるようにする。 ⑥　代替的手段･手順により、情報システム利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理する。
（イ）1	①　PHR で利用する医療情報とそれ以外の情報を区分できる措置を講じる。 ②　PHR で利用する医療情報については、情報区分に従ってアクセス制御を行えるようにする。 ③　仮想化技術を用いた資源をサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じる。
（イ）3	①　サービスには、受託する PHR で利用する医療情報を患者等ごとに管理できる機能を含める。
（エ）1	⑥　情報システムの運用若しくは開発に従事する者又は管理者権限を有する者によるアクセスの記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。
（エ）2	①　アクセス記録が保存されている資源に対して、アクセス制限を行い、不正なアクセスを防止する。

	② アクセス記録の保存に必要な容量を十分確保し、可用性、完全性の確保を図る。 ③ アクセス記録を暗号化する、あるいは定期的に追記不能な媒体への記録を行う等、改ざん防止の措置を講じる。
（エ）3	① アクセス記録の時刻の信頼性を確保するために、情報システムの時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で行う。
（オ）1	① サービスの運用･保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。 ② サービスの運用･保守端末等を設置している区域は監視カメラ等により適切に監視を行う。 ④ 端末又はセッションの乗っ取りのリスクを低減するため、利用者のログオン後に一定の使用中断時間が経過したセッションを遮断する、あるいは強制ログオフを行うことができるようにする。
（カ）1	① 情報システムの構築に際しては、ウイルスやマルウェア等の混入が生じないようにするための手順を策定し、これに則って構築する。 ② ウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新する。 ③ 情報システムの構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新のウイルス対策ソフト等の導入を行う。また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。 ④ サービス利用環境がウイルス等による攻撃を受けた場合に、サービス提供に係る影響について、速やかに患者等に周知し、必要な対応等を求める。 ⑤ 情報システムの脆弱性に関する情報は、JPCERT コーディネーションセンター（JPCERT/CC)、内閣サイバーセキュリティセンター（NISC)、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得し、確認する。
（カ）2	① 外部のネットワークと PHR で利用する医療情報を格納する機器との接続に際しては、セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行う。 ② 患者等との接続ネットワーク境界には、侵入検知システム（IDS)、侵入防止システム（IPS）等を導入してネットワーク上の不正なイベントを検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じる。

	③　侵入検知システム等が、常に最新の攻撃･不正アクセスに対応可能なように、シグネチャ･検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行う。 ④　ホスティングの利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行う。
（ク）2	①　３．２．１（２）（ウ）4. ①において実施するリスク分析結果に基づき情報システムのバックアップを取得する。バックアップの取得対象、取得頻度、保存方法･媒体、管理方法等を定め、その内容を運用管理規程等に含める。 ②　①に従い取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、記録内容の改ざん･破壊等がないことを確認する。 ③　記録媒体に格納するバックアップについては、その媒体の特性（テープ／ディスクの別、容量等）を踏まえたバックアップ内容、使用開始日、使用終了日を明らかにして管理する。 ④　③の対象となるバックアップの記録媒体につき、使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複写する。 ⑤　①～④の手順を運用管理規程等に含め、従業者等及び再委託業者に対して必要な教育を行う。
（ケ）1	①　情報システムにおける機器及びソフトウェアの構成図を作成する。 ②　情報システムのネットワーク構成図を作成する。 ③　①、②で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。 ④　情報システムを構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。
（ケ）2	①　サービスに供する機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等に含める。 ②　サービスに供する機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う。 ③　サービスに係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。 ④　システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等に含める。

（４） 人的安全管理対策（３．２．４（２）の読替え）

項番	内容
（ア）1	① サービスの提供に従事する要員（被用者、派遣従業者等）については、守秘義務に関する内容を、雇用契約又は派遣契約に含めるか、就業規則等に含める。
（ア）2	① サービスの提供に従事する要員に対して、個人情報保護ポリシー及び個人情報の安全管理に関する教育･訓練を行う。 ② この教育･訓練は就業開始時及び就業後定期的に行う。
（ア）3	① サービスの提供に従事する要員が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等に含める。 ② サービスの提供に従事する要員が業務上管理していた個人情報については、離職時（内部の異動含む）に返却を求め、システム管理者が返却されたことを確認する。 ③ サービスの提供に従事する要員の退職時又は契約終了時以降の守秘義務について、上記 2.における教育･訓練に含める。
（ア）4	① 上記 1.～3.に違反した被用者、派遣事業者等に対して、適切なペナルティを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。
（イ）1	② 再委託先には、自社と同等の個人情報保護指針等を遵守させる。 ③ 再委託に係る契約に、委託業務に係る守秘義務を含める。 ④ 再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。 ⑤ 再委託先が、本ガイドラインに規定する安全管理対策を行っていることを確認する。

（５） 情報の破棄に関する安全管理対策（３．２．５（２）の読替え）

項番	内容
（ア）2	① 運用管理規程に以下の内容を定める。 ・管理する個人情報又はこれを格納する媒体等について、サービス提供上の要否の確認を定期的に行うこと。 ・サービス提供上不要とされた個人情報及びこれを格納する媒体についての破棄手順。 ・サービス提供上不要とされた個人情報及びこれを格納する媒体の破棄に際して、患者等が不測の損害を被らないようにするための措置(事前に破棄の基準等を告知する等)。

（６） 情報システムの改造と保守に関する安全管理対策（３．２．６（２）の読替え）

項番	内容
（ア）1	① 情報システムの保守に従事する者及び管理者権限を有する者が、その業務の目的で当該情報システムにアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。 ② ①で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。
（ア）2	① 情報システムの保守に従事する者及び管理者権限を有する者は、業務上用いるアカウントが漏洩しないよう厳重に管理する。
（イ）1	① リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、情報システムへの不正な侵入が生じないよう安全管理措置を講じる。 ② リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認する。
（イ）2	① 情報システムの保守において実施した操作結果について、操作ログ等により記録し、管理する。 ② 取得した操作ログ等により、アクセスされたPHRで利用する医療情報についての状況をレビューする。
（ウ）1	① 情報システムの動作確認に際しては、原則として受託した個人情報を含むデータを使用せず、テスト用のデータを使用する。 ② 情報システムの動作確認に際し、受託した個人情報を含むデータをやむを得ず使用する場合には、３．２．４で示す守秘義務が課された要員･委託先等により動作確認を行う旨を含めた手順を定める。
（ウ）2	① PHRで利用する医療情報を格納する機器等を、保守（例えば機器の修理等）の目的で、患者等又はPHRサービス事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、その手順を策定する。

（７） 情報及び情報機器の持ち出しについての安全管理対策（３．２．７（２）の読替え）

項番	内容
（ア）1	① サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（委託元からの持ち出しを含む）に関する方針及び規則等を、運用管理規程に定める。 ② ①における「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。
（ア）2	① サービスに供する記録媒体･記録機器に関し、以下の内容を運用管理規程に含める。 ・管理体制及び管理方法 ・記録媒体･記録機器の取扱い ・サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等（「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。） ・サービスに関する情報を持ち出した場合で、当該情報を格納する機器･媒体等の盗難･紛失（持ち出し時の機器･媒体等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等（第三者による悪意の送信、従業者等における誤送信等を含む。））が起きた場合の対応 ・外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改ざんが生じないようにするための具体的な措置（マルウェア対策、暗号化、ファイアウォール導入等)）
（ア）3	① 「2.サービスに供する記録媒体･記録機器に関する対応」に示した内容に関する教育を従業員等に対して行う。 ② 上記の運用管理規程については、再委託先に対しても遵守等を求める。
（イ）	① サービスに関する情報を格納する機器･媒体等については、台帳管理等を行い、定期的に所在確認を行う。
（ウ）1	① サービスに供する機器等については、起動パスワードの設定を行う。 ② 起動パスワードは、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じる。 ③ サービスに関する情報を格納する情報機器へのログイン及びアクセスについては、複数の認証要素を組み合わせて行う。

項番	内容
（ウ）2	①　サービスに関する情報を格納する機器･媒体等を持ち出す場合の手順には、機器･媒体自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる、パスワードを設定する等の事項を含める。
（ウ）3	①　サービスに関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。 ②　サービスに関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。
（ウ）5	①　業務上、サービスに関する情報を格納するモバイル端末を持ち出す場合には、公衆無線 LAN への接続は行わない。

（８） 災害等の非常時の対応についての安全管理対策（３．２．８（２）の読替え）

項番	内容
（イ）1	① サービスに係るBCP及びコンテンジェンシープランの策定を行う。 ② ①で策定するBCP及びコンテンジェンシープランには、非常時における体制及びサービス回復手順等の内容を含める。
（イ）3	① サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。 ② ①の場合において、サービスに生じている障害の状況及び復旧に関する見通し等について、患者等に速やかに報告を行う。
（イ）4	① 非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定･検証方法の規定等）を講じる。

（９） 個人情報を含む医療情報を外部と交換する場合の安全管理対策（３．２．９（２）の読替え）

項番	内容
（ア）1	① ネットワークにおいて、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）を行う。 ② アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐのに必要な措置(サーバ証明書の導入等）を行う。
（ア）3	① ルータ等のネットワーク機器は、ISO15408 で規定されるセキュリティターゲット又はそれに類する文書が、本ガイドラインに適合しているものを選定する。
（ア）4	① 送信元と送信先の間で、暗号化等の情報そのものに対するセキュリティ対策を実施する。 ② サービスの提供において SSL/TLS を用いる際には、TLS1.2 に対応した措置を講じる。
（ア）5	① オープンなネットワークを介して HTTPS を利用した接続を行う際は、TLS の設定は 1.2 に限定し、信頼性の高い機関によって発行されたサーバ証明書を用いるとともに、本人性の確認を確実に実施する。 ② SSL-VPN は、原則として使用しない。 ③ サービス提供に際して、ソフトウェア型の IPsec 又は TLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃について、適切な対策を実施する。
（イ）	① リモートメンテナンスにより保守を行う場合、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置を講じる。

（１０） 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準（３．３．６（２）の読替え）

項番	内容
（イ）1	① 受託したPHRで利用する医療情報を保守･運用を行うために閲覧するのは必要最小限とする。 ② ①の閲覧が必要な場合には、緊急時を除き、システム管理者の事前･事後の承認により実施する。 ③ 受託したPHRで利用する医療情報を緊急時に閲覧した場合には、閲覧した受託情報の範囲及び緊急で閲覧が必要な理由等を示して、システム管理者の承認を得る。
（イ）2	① 予定された保守･運用等を行う際に受託したPHRで利用する医療情報を許可なく閲覧できないようにするために、権限設定等の対策を講じる。 ② システム管理者、運用担当者、保守担当者等が、意図しない閲覧を行わないことを担保するための措置（データベースの暗号化等）を講じる。
（ウ）2	① 受託したPHRで利用する医療情報は、法令による場合又は患者等の指示に基づく場合を除き、第三者への提供は行わない。 ② ①の内容を、サービス提供に係る契約に含める。 ③ 患者等の指示に基づき、受託したPHRで利用する医療情報の第三者提供（閲覧）を行う場合には、患者等が許諾した者以外が閲覧･取得できないように、３．２．３及び３．２．９に示す対応策を講じる。 ④ ③により、第三者提供（閲覧）を行う場合には、閲覧･取得が可能な者のID及び利用権限について、患者等又はその委託を受けた者（医療情報連携ネットワーク等）の指示に基づき、速やかに変更･削除できる対応を行う。 ⑤ 患者等の指示に基づいて受託したPHRで利用する医療情報の第三者提供を行った場合には、患者等に対してその内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告を行う。

３．６．３ PHR サービス事業者を適用対象外とする要求事項

適用対象外とする項番	
３．２．１（２）	（イ）3.
	（ウ）7.
３．２．３（２）	（イ）2.
	（ウ）
	（エ）1. ①～⑤
	（キ）
	（ク）1.
	（ク）3. ～5.
	（コ）2.
３．２．４（２）	（イ）1.①
３．２．５（２）	（ア）1.
３．２．６（２）	（イ）4.
	（エ）
	（オ）
３．２．７（２）	（ウ）4.
３．２．８（２）	（ア）
	（イ）2.
	（イ）3.④
３．２．９（２）	（ア）2.
	（ウ）
３．２．１０（２）	
３．３．６（２）	（ア）
	（ウ）1.

その他、共通して「サービス仕様適合開示書」に係る項番は、適用対象外である。

第４章　安全管理の実施における医療機関等との合意形成の考え方

第３章では、クラウドサービス事業者が医療情報を取り扱うクラウドサービスを提供するにあたり、安全管理の観点から対応すべき項目についてまとめた。これらの項目は、医療機関等がクラウドサービス事業者に対して「対応済み」であることを期待しているものである。

ただし、医療機関等が求める責任分担やサービスレベルに幅があるため、提供コストも考慮しつつ、選択と合意形成を要する事項も含まれる。具体的には、第３章で対応すべき内容として「合意する」とした項目がこれにあたる。

本章では、このように医療機関等が求める責任分担やサービスレベルに幅がある内容に関し、医療機関等がどのようにサービスの選択を行い、クラウドサービス事業者と医療機関等が「何について合意しなければならないか」、「合意形成した事項をどのようにして遵守するか」について記述する。

４．１ サービス仕様適合開示書による情報提供

クラウドサービス事業者と契約等の合意をするのに先立ち、医療機関等は、クラウドサービス事業者からサービスについての詳細な情報の提供を受けた上で、サービス内容が本ガイドラインに適合しているか検証を行うことが求められる。このような対応を行うためには、情報システムに関する深い知見を要することが多く、医療機関等によっては、過大な負担となることが懸念される。

他方、クラウドサービスにおいては、必ずしも１対１のサービス提供ではなく、１対多の形で多くの医療機関等に対して同時にサービス提供を行うモデルが主流である。このようなモデルでは、契約者（医療機関等）に対して個々に対応するのではなく、可能な限り同一のサービスを提供することにより、サービス提供価格を抑えながら、安全なサービス提供を実現する仕組みを設けている。したがって、個別の契約交渉等を行うことは、実質的には困難であることが多い。

そこで、医療機関等が、サービスの本ガイドラインへの適合状況を容易に確認することができるとともに、クラウドサービス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なスキームが求められる[32]。厚生労働省ガイドライン第５版では、医療情報システムの製造業者が作成する「製造業者による医療情報セキュリティ開示書」[33]が医療機関等におけるリスクアセスメントや運用管理において参考になることを示してい

---

[32] 厚生労働省ガイドライン第５版は、医療機関等の管理者に対して、「委託先事業者の管理の実態を理解し、その監督を適切に行う仕組みを作る必要があり、契約事項に含める」ことを求めているため、その点でも、医療機関等が、サービス内容の本ガイドラインへの適合状況を容易に確認することができるようにすることが重要である。

[33] ＪＡＨＩＳ「「製造業者による医療情報セキュリティ開示書」ガイド Ver.3.0a」（2017 年 7 月　一般社団法人 保健医療福祉情報システム工業会医療情報システム部会 セキュリティ委員会 開示説明書 WG）、JESRA TR-0039*B「「製造業者による医療情報セキュリティ開示説明書」ガイド Ver.3.0a」（2018 年 1 月　一般社団法人日本画像医療システム工業会医用画像システム部会セキュリティ委員会 JIRA-JAHIS 合同開示説明書 WG）

るが[34]、医療機関等が医療情報を取り扱うクラウドサービスを選定するに当たっても、このコミュニケーション方法が参考になる。

医療情報システム機器では下の＜「製造業者による医療情報セキュリティ開示書」の目的＞に示すように、製造業者は標準化された書式を用いることで製品に係るセキュリティ情報を一律に医療機関等に提供している。これにより医療機関等は、製造事業者におけるセキュリティ情報の比較やレビュー、ガイドラインへの適合状況の確認を容易に行い、機器等の選定を行うことができる。

＜「製造業者による医療情報セキュリティ開示書」の目的＞

> 本書の意図は、医療機関が医療情報システムによって送信され維持される健康情報に関するリスクアセスメントおよびリスクマネジメントを行うとき、それを支援できる重要な情報を提供することにあります。製造業者は、標準化された書式を使用することにより、自らが製造する医療情報システムのセキュリティ関連機能に関して、医療機関から情報提供を要求されたとき迅速に答えることができます。一方、医療機関は、標準化された書式の記載により、製造業者によって提供されるセキュリティ関連情報のレビューを行い易くなります。

クラウドサービスも、上述のように、1 対多型のサービス提供モデルであり、製品の提供と類似するところがあることから、このような手法を用いることで、医療機関等は少ない負担で本ガイドラインに適合したサービスを選択できるようになる。同時にクラウドサービス事業者にとっても、効率的な情報提供を行うことが可能になると考えられる。

本ガイドラインでは、このような観点から、クラウドサービス事業者は「クラウドサービス仕様における『クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン』への適合性の開示書」（サービス仕様適合開示書）を医療機関等に提供し、医療機関等はこれに基づいてサービスの選択を行い、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。

サービス仕様適合開示書を用い、クラウドサービス事業者が、自社のサービスに関する本ガイドラインへの適合性や、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、役割の範囲等を制約事項として表示することにより、サービスの品質や内容を示すことが可能となる。

医療機関等によるサービス選択後は、医療機関等とクラウドサービス事業者は、サービス仕様適合開示書の内容を踏まえて契約することとなる。

---

[34] 厚生労働省ガイドライン第 5 版　P 40、P 162

４．２ サービス仕様適合開示書により情報提供される内容

ここでは、第３章に示した要求事項のうち、サービス仕様適合開示書により情報提供すべき項目を示す。

（１） 組織的安全管理対策

サービス仕様適合開示項目
組織的取組における基本方針
サービス提供に係る体制等に関する情報の開示
医療情報の管理状況に関係する資料の提供
サービス提供に係る運用管理規程の開示等の有無、範囲、条件等
受託する医療情報に係るリスク分析の結果と対応措置
リスク等に対する予防措置及び事故等の発生時の対応等（自社の規程）
機器の管理等の運用（自社の規程）
個人情報を記録した媒体の運用
自社において実施するシステム監査等の状況及びその記録の提示条件･範囲等
医療機関等の管理者側からの問合せ窓口における受付の時間帯等

（２） 物理的安全管理措置

サービス仕様適合開示項目
サービス提供に使用する機器等が格納されている建物種別（建物名）･地域
上記建物における物理的安全管理措置の概要（耐災害のための措置（火災対策、水害対策、落落雷対策、熱対策等）、入退管理等）

（３） 技術的安全管理対策

サービス仕様適合開示項目
パスワードポリシー
利用者の認証で採用する認証手段･方式、一時的な利用者の認証方法
医療機関等による情報資産の区分の設定、アクセス制御の設定の状況
利用者の職種等に応じたアクセス制御の設定の可否及びその仕様、提供の範囲･条件等
運用管理規程に基づくアクセス管理状況に関する資料･提供の可否等
アクセス記録の取得（有無、対象（時間、データ、利用者等）取得方法）、取得していない場合の代替措置

システム管理者･運用者･保守担当者等におけるアクセス管理の状況等の情報開示、運用状況の開示
受託した医療情報の法定年限経過後の保存期間･対応･管理方法
法定年限が定められていない医療情報の保存期間･対応･管理方法
医療機関等における利用者端末に対するクリアスクリーン等の対策の責任関係
医療機関等における利用者端末に対するセッションの遮断、強制ログオフ機能の有無、対応状況、責任関係
サービス提供に際しての利用者側の応答速度等
サービス利用に際して利用可能な保存可能量(サイズ･利用可能期間)、リスク、バックアップ頻度、バックアップ方法等
バックアップルール
サービス継続性を保証するための水準･冗長化対策の状況
障害時等でも診療等を継続するための代替措置等
障害等により毀損した情報に関する責任の範囲、免責条件等
システムに関するドキュメントの提供の有無･範囲･条件等
医療機関等が無線 LAN を導入する場合のセキュリティ上の責任関係、情報提供
IoT 機器の利用を含むサービスを提供する場合の医療機関等との責任分界
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、PC 等の汎用入力端末を利用するサービスにおける以下の仕様 ・医療機関等の職務権限等に応じたアクセス制御の可否を含め、作成者の識別及び認証に関する仕様 ・確定された登録情報（作成責任者の氏名等の識別情報、信頼できる時刻源を用いた作成日時）に係る仕様 ・入力された内容についての記録確定前における作成責任者による確認の可否等についての仕様 ・確定した記録に関する追記･削除の機能等に関する仕様 ・確定した記録の原状回復の機能等に関する仕様 ・記録の自動確定の機能等に関する仕様 ・代替的な確定権限の機能等に関する仕様 ・一旦確定した診療録等を更新した場合、更新前と更新後に係るデータの保存、若しくは更新履歴等の保存を行うことにより、更新前後の内容を照らし合せられる機能に関する仕様 ・一旦確定した診療録等を更新した場合、更新履歴を保存し、更新の順序性が識別できる機能に関する仕様

・提供するサービスに関連する臨床検査システム、医用画像ファイリングシステム等との連携におけるインタフェースの構築に関し、事業者の役割、範囲

（４） 人的安全管理対策

サービス仕様適合開示項目
教育･訓練の実施状況や、守秘義務等への対応状況等に関する資料の提供

（５） 情報の破棄に関する安全管理対策

サービス仕様適合開示項目
情報の廃棄に関する手順･消去方法等の情報提供･廃棄証明の提供の条件

（６） 情報システムの改造と保守に係る安全管理対策

サービス仕様適合開示項目
システムのリモートメンテナンスに関する事項
医療機関等施設内でサービス提供に必要な保守業務を行う際の対応等
受託した個人情報をやむを得ず保守･動作確認で使用する場合の対応
医療情報を組織外に持ち出す手順及びこれに関する情報提供の条件
標準形式を採用していない項目の場合のデータ項目の形式、標準形式への変換等への対応
マスターテーブルの変更におけるレコード管理方法･移行対応への支援
データ形式の変更等における互換性確保への方針･対応支援措置
機器･ソフトウェアのバージョンアップ等に伴うサービス提供の一部停止･終了時の対応方針･支援措置
保守体制の変更における報告の有無、範囲等

（７） 情報及び情報機器の持ち出しについての安全管理対策

サービス仕様適合開示項目
クラウドサービス事業者における運用管理規程に示す情報の社外持ち出しのルール、従業員等における対応
医療機関等における利用者が個人所有する機器によりサービス利用する場合の責任分界、必要な対応策に関する情報提供

（８） 災害等の非常時の対応についての安全管理対策

サービス仕様適合開示項目
障害等が生じた場合の責任分界、稼動を保証するサービスの品質
障害時における見読性確保のための、医療機関等側で講じうる方策に関する情報提供
障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容
遠隔地に保存するバックアップデータにつき、その利用方法のための機能、利用に必要な情報の提供、条件等
緊急時の医療機関等における診療録等の見読性の確保を支援する機能(例えば画面の印刷機能、ファイルダウンロードの機能等)
BCP 及びコンテンジェンシープランに基づくサービス内容
非常時に用いる利用者のアカウント及び非常時用機能の有効化のための措置
サイバー攻撃的等が生じた際に医療機関等が行う必要のある、所管官庁への連絡・報告について、医療機関等への提出資料の範囲、条件等

（９） 個人情報を含む医療情報を外部と交換する場合の安全管理対策

サービス仕様適合開示項目
経路の安全性確保のための措置（IPSec＋IKE への対応や閉域ネットワークへの対応)、情報提供等（閉域性の範囲等）
改ざんに対する防止措置（ウイルスや不正なメッセージの混入等への対応措置)、情報提供
チャネル・セキュリティの確保のための閉域ネットワークの範囲に関する情報の提供
医療機関等が採用する通信方式認証手段の厚生労働省ガイドラインとの適合性に関する確認
医療機関等の施設内のルータにより経路設定されている場合のサービス提供上の責任分界・必要な対応措置、条件等
メール・ファイルに対する暗号化措置への対応の可否、対応可能な暗号化手法、条件等
ソフトウェア型の IPsec 又は TLS1.2 への対応における医療機関等側に対する、クラウドサービス事業者からの要請事項、責任分界等
サービスを提供する際に用いる回線の管理責任、品質等に対する事業者の責任の範囲、役割等
サービス利用に際して医療機関等の利用者が利用する仮想デスクトップ等におけるクラウドサービス事業者の役割・責任分界等
医療機関等からクラウドサービス事業者に至る通信経路に関する責任分界の考え方、クラ

ウドサービス事業者の責任の範囲、医療機関等における責任の内容
医療機関等とクラウドサービス事業者において交換する情報の機密レベル
医療機関等の管理者において発生する患者等に対する説明責任、管理責任等、各種責任におけるクラウドサービス事業者の対応方針等、対応措置、条件等
サービス提供上想定されるネットワーク上の脅威に対する責任分界の考え方、クラウドサービス事業者の責任･対応の範囲
医療情報を患者（患者の家族等、患者が閲覧を同意した等の者を含む）の閲覧に供する場合のセキュリティ条件、情報提供の範囲等

（１０） 法令で定められた記名･押印を電子署名で行うことについての安全管理対策

サービス仕様適合開示項目
電子署名法における認定特定認証事業者が発行する電子証明書を用いないで、法令で定められた記名･押印を電子署名で行うサービスを提供する場合の本人確認･検証方法
公的個人認証サービスにおける署名用電子証明書を利用して、法令で定められた記名･押印を電子署名で行うサービスを提供する場合の、公的個人認証サービスに係る電子証明書の検証方法等
タイムスタンプの付与に関する内容･検証方法等
法定保存年限内の期間におけるタイムスタンプの有効性検証の方法等
タイムスタンプを付した情報の長期保存における対応措置
タイムスタンプを付した場合の電子証明書の執行前の有効性担保にかかる対応等

（１１） 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

サービス仕様適合開示項目
受託した医療情報の閲覧に係る範囲、手順等
受託情報の第三者提供及びその報告範囲、条件等

（１２） 個人情報の保護についての安全管理対策

サービス仕様適合開示項目
クラウドサービス事業者における個人情報保護対応策
医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供

とその範囲、役割分担等

（１３） クラウドサービスの利用終了における対応

サービス仕様適合開示項目
サービス提供終了時の医療機関等へのデータ返却におけるデータの範囲（データ種類、期間等)、データ形式（データ項目、項目の詳細、ファイル形式)、返却方法、条件
返却するデータに、クラウドサービス事業者において実施した不可逆的な圧縮（画像データ等）や変換（パスワード等）によるデータが含まれる場合の対応
サービス提供終了時における医療機関等へのデータ返却以外の対応内容（移行支援等)、条件等
サービス終了後にクラウドサービス事業者が管理する情報の範囲等

（１４） オンライン診療システム提供事業者における安全管理対策

サービス仕様適合開示項目
患者側端末において提供されるオンライン診療システムの機能において、医療情報システムへの接続がないこと及びこれに関する情報提供
オンライン診療システムを利用する場合の医療機関とオンライン診療システムを提供するクラウドサービス事業者との責任分界

４．３ 契約、SLA 等の文書による合意

サービス仕様適合開示書では、クラウドサービス事業者が提供するサービスの仕様や、その前提となる免責内容、責任分界などが示される。上述のように、医療機関等とクラウドサービス事業者は、この内容を踏まえて、サービス利用契約等を締結することになる。

サービス利用契約においては、契約書のほかに、提供するサービス内容についてのSLA が策定され、合意文書を構成する。SLA には、サービス仕様適合開示書で示されるサービス仕様やその前提条件などのほか、サービス提供にあたって必要な安全管理措置等に関する一般的な対応や、サービスレベル確保のための対応措置等、提供されたサービスレベルの評価等を含むことが想定される。

SLA の策定形式については、さまざまであり、本ガイドラインで示すサービス仕様適合開示書などを活用して策定することも想定される。

なお、医療機関等とクラウドサービス事業者との合意内容については、本ガイドラインの内容を満たすものであることが求められる。サービス仕様適合開示書には、クラウドサービス事業者が提供するサービス仕様等に加えて、必要に応じて医療機関等に実施していただきたい役割についても記載することが必要である。

このように、クラウドサービスでは契約書、SLA 等の文書化により、両当事者において遵守する対象を明確化することが可能となる。

４．４ 合意における注意点

４．２で示した各項目について、契約、SLA 等により合意するに際して、以下の点に留意する必要がある。

４．４．１　サービスレベルとコストに見合った提案

医療情報の取扱いに際しては高い安全性が求められる。機微な個人情報を取り扱うため、高度なセキュリティ確保が求められると同時に、診療の継続に支障を来たさないようにするための可用性等も求められる。

したがって、第一にクラウドサービス事業者は、情報セキュリティ対策ガイドライン及び本ガイドラインを遵守しながらサービスを提供することが求められ、医療機関等との協議により合意する契約、SLA 等の内容もこれを満たすものであることが必要である。

その上で、一定水準以上のサービス品質を実現しようとする場合は、医療機関等のリスクに対する考え方に従って、クラウドサービス事業者と医療機関等とで協議することが必要になる。その際、クラウドサービス事業者には、ICT や情報セキュリティ対策の専門家として、医療機関等に対し、コストとサービスレベルのバランスが取れた提案を行うことが求められる。

４．４．２　医療機関等との責任分界の明確化

クラウドサービスの安全性確保のためには、クラウドサービス事業者側の対応だけではなく、医療機関等においても適切な運用管理を行なうことが求められる。例えば、クラウドサービスが堅牢なアクセス制御機能を持っていたとしても、医療機関側の利用者がパスワードを利用端末に貼っていたり、アカウントを複数で共有していたりしていれば、サービスの安全は守ることができない。

従って、クラウドサービス事業者は、医療機関等と契約、SLA 等について協議するにあたり、医療機関等の側における運用管理対応等も踏まえた形で、責任分界を定めることが必要である。これにより、事故が発生した場合等のクラウドサービス事業者と医療機関等との責任分担が明確になり、事後の対応を円滑に行うことができる。

４．５ サービスレベルマネジメントの実践

締結された契約、SLA 等の内容については、締結後、一定のサイクルで見直すことが求められる。情報通信技術は日進月歩であり、情報セキュリティ対策等の内容によっては数年で陳腐化してしまうケースも予想される。

クラウドサービス事業者が提供するサービスのレベルについても、サービス運用状況を計測、分析、評価した上で、技術環境の変化等も踏まえながら、継続的な改善を行っていく必要がある。

サービスレベルマネジメントの実践にあたっては、医療機関等とクラウドサービス事業者が協力してこれに当たることが望ましい。特に、クラウドサービス事業者は、情報システムの専門家として、サービスレベルの向上に主体的に取り組む姿勢が求められる。

（別添）

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

総務省

平成３０年７月

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

内容

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 2
Ⅱ. 参考例編(サービス仕様適合開示書) 3
1. サービス仕様適合開示書の作成について 3
2. サービス仕様適合開示書参考例 5

（1）組織的安全管理対策（3.2.1）
（2）物理的安全管理対策
（3）技術的安全管理対策
（4）人的安全管理対策
（5）情報の破棄
（6）情報システムの改造と保守
（7）情報および情報機器の持ち出し
（8）災害等の非常時の対応
（9）医療情報を外部と交換する場合の安全管理対策
(10) 法令で定められた記名・押印を電子署名で行うことについての安全管理対策
(11)個人情報の保護
(12)クラウドサービスの利用終了

Ⅲ. 参考例編(SLA) 38
1. 本サービスの目的と対象 38
1.1 本サービスの目的 38
1.2 本サービスの提供範囲 40
1.3 本サービスの提供時間 41
2. 本 SLA について 42
2.1 本サービスにおけるサービスレベル合意書の意義 42
2.2 本サービスにおけるサービスレベル適用の考え方 43
2.3 本 SLA の適用期間 44
2.4 本 SLA の改定 45

3. 前提条件 46
3.1 リスク評価 46
3.2 サービス利用環境 47
3.3 サービス提供環境・運用に係る前提条件 48
3.4 機器・ソフトウェアの品質 50
3.5 準拠する法令・ガイドライン等 51
3.6 守秘義務等 52
3.7 監査 54
4. 役割分担 55
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) 55
4.2 甲の業務上の役割分担と責任 60
4.3 再委託事業者・連携クラウドサービス事業者等 62
4.4 連絡体制 64
5. サービス仕様 66
5.1 ネットワークセキュリティに関するサービス仕様 66
5.2 受託情報に関するサービス仕様 68
6. 運用内容 81
6.1 運用組織・規程等 81
6.2 受託情報の取り扱い 85
6.3 運用仕様及びその指標 90
6.4 非常時の対応 95
6.5 報告事項・事前連絡 96
6.6 サポート 104
7. サービスレベルに関する合意事項 108
7.1 サービスレベルの評価方法 108
7.2 サービスレベルマネジメント 112

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、「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第１版」（総務省　平成 30 年７月　以下、「クラウドサービス医療ガイドライン」という）に基づいて、クラウドサービス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、サービス仕様適合開示書[1]及びサービス・レベル合意書（SLA）参考例という形でまとめたものである。

クラウドサービス事業者は、サービス仕様適合開示書及びサービス・レベル合意書（以下「SLA」という）により、提供するサービス内容を明らかにし、医療情報が安全に取り扱われていることを医療機関等に示すことが可能となる。

本参考例のサービス仕様適合開示書及び SLA の参考例は、クラウドサービス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。

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、クラウドサービス事業者が、自社のサービスに関するクラウドサービス医療ガイドラインへの適合状況や、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しており、これにより提供するサービスの品質や内容を示すことが可能となる。サービス仕様適合開示書で記載されるサービス内容は、各クラウドサービス事業者が任意で記載するものであるが、前提としてクラウドサービス医療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。

クラウドサービス医療ガイドラインでは、クラウドサービス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。

①クラウドサービス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クラウドサービス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

これらの要求事項のうち、②については、クラウドサービス事業者が、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示し、その上で当該項目に関する合意を行うこととしている。

---

[1]「クラウドサービス仕様における『クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン』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）

また、これに加え、医療情報の安全管理を確実にする観点から、サービス仕様適合開示書には、必要に応じて医療機関等に実施を求めることが必要となる事項についても記載している。サービス仕様適合開示書の内容は、契約後はSLAを定めるために活用することも想定している（必要に応じて、より詳細なサービス品質に関する内容を記載することもある)。

３．SLA参考例について利用方法及び利用上の留意点

SLAは、クラウドサービスにおいて、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、クラウドサービス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、医療情報を取り扱うクラウドサービスにおいて合意すべき具体的な内容を、クラウドサービス医療ガイドラインに則して、診療所向け診療録の作成・保存等のサービスを想定したひとつのサンプルとして条項案を提示している。従って、提供するサービスの内容や医療機関等とクラウドサービス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ことに留意されたい。また、クラウドサービス事業者が提供するサービスの態様（ASP・SaaS、PaaS、IaaSなど）によっては、必要な条項についてのみ提供することも想定される。

本参考例のSLAでは、各項目において「【本項を定める上での考え方】」を記述した。これは本参考例を記述する際に想定した内容や、本参考例を変更・加除する際に念頭に置くべき考え方を概説するものである。本参考例を踏まえて、実際にSLA等を作成する際には、「【本項を定める上での考え方】」の内容を理解の上、利用されたい。

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

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の作成について

サービス仕様適合開示書は、クラウドサービス事業者が、クラウドサービス医療ガイドラインに基づいて実施している内容を、サービス利用者である医療機関等に示すことを目的として作成するものである。

サービス仕様適合開示書には、以下の内容が含まれることが想定される。

① クラウドサービス医療ガイドラインにおいて、医療機関等と、サービス仕様適合開示書を通じて合意するとされている事項

② クラウドサービス医療ガイドラインにおける要求事項で、サービス提供に際して実施している事項、あるいは具体的な対応内容

③ サービス仕様適合開示書に基づくサービス提供に際して、医療機関等に求める対応事項、責任分界等

①について、クラウドサービス事業者において、医療機関等と、サービス仕様適合開示書を通じて合意するとされている事項については、その具体的な内容はクラウドサービス事業者によって異なるため（例えば提供に際しての費用の有償・無償の別や、提供に際しての機密保持契約の締結の要否等)、各クラウドサービス事業者がその内容を示すことを想定している。

②は、クラウドサービス医療ガイドラインにおいて、各事業者が遵守すべきとされる要求事項について、改めてその遵守状況を表明する趣旨で記載することを想定している。また要求事項においては、一般的な対応のみを記述しており、具体的な内容は各サービスに委ねているものもある(例えばサービス利用における認証方法)。このようなものについては、各クラウドサービス事業者が具体的に採用している措置を記載し、医療機関等に示すことが求められる。

また、クラウドサービス医療ガイドラインにおいて示す要求事項には、クラウドサービス事業者が提供するサービスによっては、対応が求められないものも含まれている（例えばIaaS事業者においては、医療情報の閲覧可能端末に関する要求事項は、一般的には想定されない)。そこで、提供するサービスの内容に応じて、求められる要求事項とその対応状況を示すことになる。本例では、診療録作成・外部保存を行うASP・SaaSを想定して、遵守している要求事項を示す形として示している。

なお、クラウドサービス医療ガイドラインに示す要求事項については、対象となるものはすべて遵守することが前提となっている。従ってサービス仕様適合開示書で記載されるサービス内容も、クラウドサービス医療ガイドラインの内容に適合するよう示されることが求められる。

③については、②で示す要求事項の対応をクラウドサービス事業者において実施する際に、その要求事項への対応の前提として、サービス利用者である医療機関等における対応が不可欠なものなどを示すことを想定している。例えば認証において ID・パスワード方式を採用する場合、パスワードの品質を高いものにした場合でも、医療機関側のパスワード自体の管理が杜撰であれば、意味をなさないことがある。そこで、医療機関等の利用者において、一定の管理を実施することを、サービス仕様の前提として記載することを示している。

なお、本サービス仕様適合開示書には、利用の便利を図る観点から、記入例を示しているものがある。この場合には、斜体で示した上で、文末に「(例)」と示している。

２．サービス仕様適合開示書参考例

（１） 組織的安全管理対策（3.2.1）

① 組織的取組における基本方針

(a) 情報セキュリティに関する組織体制（3.2.1(2)（ｱ）①-③）

情報セキュリティに関する役職	役職及び氏名
管理責任者	
本サービスに関するシステム管理者	
本サービスのシステムに関する 運用管理責任者	

(b) 個人情報保護指針、プライバシーポリシー等について（3.2.1(2)（ｳ）1.①）

文書名	内容の開示の可否 (開示可能の場合)開示方法	個人情報保護指針、プライバシーポリシー等の遵守上、顧客側に求める対応

(c) 個人情報保護法及び個人情報保護委員会が定めるガイドライン等の遵守状況
(3.2.1(2)（ｲ）3.）

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）* *・クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン第1版【総務省】（例）* *・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」第2版【経済産業省】（例）* *※ なお、下記のガイドライン、ガイダンスについても、クラウドサービス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【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）*

(d) 情報セキュリティに関する基本方針、運用管理規程等の情報セキュリティポリシーの策定状況（3.2.1(2)（ウ）1.④-⑥、3.①）[2]

文書名	開示の可否及び開示条件、提供方法
情報セキュリティ基本指針(例)	
……	

② サービス提供に係る体制等

再委託先の有無・事業者名・再委託先との契約種別（3.2.1（2）(ウ)2.②）

(a) サービス提供体制（3.2.1(2)（ウ）2.）

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）*

※ *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（3.2.1(2)（ウ）2.②）

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

③ 運用管理規程の開示等の有無、範囲、条件等（3.2.1(2)（ウ）3.③）

文書名	内容の開示の有無及び開示する場合の開示方法・条件・範囲

④ 医療情報の管理状況に関係する資料の提供（3.2.1(2)（ウ）3.④）

資料提供の可否	開示する場合の開示方法・条件・範囲

[2] 本項で定める運用管理規程等には、クラウドサービス医療ガイドライン 3.2.1(2)(ウ)4.①、5.①、6.①、8.①-②に示す内容を含めることを想定する。

⑤ 受託する医療情報に係るリスク分析の結果と対応措置

(a) サービスに係るリスク分析の概要（3.2.1(2)（ｳ）4.①）

リスク分析の結果、脆弱性に関する開示情報	脆弱性に対する対応の概要
OS における未知のセキュリティホールによる攻撃リスク(例)	*不正侵入防止システムにより、不正な通信を遮断しております。(例)*
・・・・・	

(b) サービスに係る脆弱性について、お客様側において対応していただく措置（3.2.1(2)（ｳ）4.②）

脆弱性に関する開示情報	脆弱性に対する対応の概要
利用端末の OS 等における適切なアップデートがなされないことによる攻撃リスクへの対応(例)	*OS、ブラウザ等、ベンダーが提供するアップデートプログラムへ対応いただくことが必要となります。(例)*
・・・・・	

(c) セキュリティ上の事故が生じた際の対応（3.2.1(2)（ｳ）4.②、3.2.8(2)（ｲ）4.①）

- *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)*

⑥ 自社で定める機器の管理等の運用（3.2.1(2)（ｳ）5.③）

運用状況に係る資料提供の可否	開示する場合の開示方法･条件･範囲

⑦ 個人情報を記録した媒体の運用（3.2.1(2)（ｳ）6.②）

運用状況に係る資料提供の可否	開示する場合の開示方法･条件･範囲

⑧ 患者等への説明および同意を得る方法（3.2.1(2)（ｳ）7.①）

本サービスの利用に係る患者等への説明および同意については、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)

⑨ 自社において実施するシステム監査等の状況、監査記録等の開示等の範囲、条件等（3.2.1(2)（ｳ）8.④-⑤）

実施しているシステム監査の種類	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

⑩ 医療機関等の管理者側からの問合せ窓口における受付の時間帯等（3.2.1(2)（ｳ）9.①）

【乙サポートセンター】　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）

(2) 物理的安全管理対策 (3.2.2))

① 本サービスの提供に供する機器等が格納されている建物種別（建物名）・地域
(3.2.2(2) (ｱ) 3.)

建物に関する情報	内容
データセンタの所在	*東京都及び北海道等（例）*
建物種別	*鉄筋コンクリートによるビルディング内（例）*

② ①に示す施設における災害対策の状況 (3.2.2(2)(ｱ)3.)

災害種別等	具体的な対応(複数ある場合には代表的な対応)
地震への対応	*免震構造による建築（例）*
水害への対応	*機器類については3階のフロアに設置（例）* *窓類のない構造での専用室に設置（例）*
落雷対策	*誘導雷対策を実施（例）*
火災対策	*サーバルーム内において二酸化炭素消火装置を設置* *その他の区画についてはスプリンクラーによる消火設備を設置（例）*
停電対策	*建物に3日間運用可能な非常電源を設置しているほか、サーバルーム専用の非常電源についても設置（例）* *複数の給電ルートを確保して電力を利用（例）*
熱対策及び結露対策	*非常時において温度湿度を適切に管理できるよう、サーバルーム内温度計を設置し、専用空調設備により室温及び湿度を管理（例）*
その他の対策	*海岸線及び原子力発電所から 30km 以上はなれたところに設置（例）*

③ 入退管理に関する状況 (3.2.2(2)(ｱ)2.①-③、4.、(ｲ)1.①-②、3.2.3(2))

弊社で実施している対応については、下表に示している項目です。

入退記録の管理（データセンタおよび医療情報が保存されている区画）
監視カメラの設置および監視
サーバルーム等への個人認証システム

④ その他クラウドサービス医療ガイドラインで定める物理的対策の実施状況

(3.2.2(2)(ｱ)1.、(ｲ)1.、(ｳ) 1.、3.2.3(2)(ｵ)1)

弊社で実施している対応については、下表に示している項目です。

サーバルーム及びラック等の鍵管理の対応項目
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
個人情報を格納する記録媒体等の鍵管理の実施
受託する個人情報を参照可能な弊社内事務室等における入退管理の実施及び記録の作成（3.2.2(2)(ｲ)1.）
個人情報データの記録媒体の保管場所に関する弊社の入退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できる者の制限
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参照できる端末に対する、覗き見予防措置の実施（3.2.2(2)(ｲ)2.）
受託する個人情報を格納する機器・媒体等の所在確認等・施錠

⑤ 物理的対策実施上、お客様に実施していただく対応(3.2.2(2)(ｱ)2.)

弊社のサーバルーム施設への入館等に際しては、事前にご来訪いただく方を登録していただき、入館時に本人確認をさせていただきます。また、館内では弊社運用管理規程に従っていただくこととしております。(例)

(3) 技術的安全管理対策 (3.2.3)

① 本サービスに関する情報の区分設定及び管理 ((２) (イ))

(a) 本サービスに関する情報の区分設定(3.2.3(2)(イ)1.①、④)

当サービスの提供に係る情報については、以下の区分で管理しております。(例)

- *受託する医療情報 (例)*
- *サービス提供に必要なシステム運用上の個人に関する情報 (ID、パスワード、システム利用記録等) (例)*
- *その他サービス提供に係るシステム及び運用に関する情報 (例)*

(b) 本サービスに関する情報の区分設定及び管理(3.2.3(2)(イ)1.②-④)

弊社で実施している対応については、下表に示している項目です。

対応項目
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) の設定
本サービスで採用する仮想化技術を利用した資源において、受託情報の所在等について、論理的に管理できる措置を講じている。

(c) 医療情報の管理(3.2.3(2)(ｴ)1.2)

医療情報については、クラウドサービス医療ガイドラインに基づき以下のように管理しております。

法定保存義務の保存年限内の医療情報の管理	*・常時参照可能なサーバ上で管理するほか、バックアップについては弊社内所定の保存区域において管理します。 (例)*
法定保存義務の保存年限を越えた医療情報の管理	*・弊社運用管理規定に基づき、サービス提供用サーバから削除の上、バックアップについては、年次で取得し、弊社契約の外部倉庫に、弊社運用管理規程に基づいて管理します。 (例)*
法定保存義務のない医療情報	*・記録後 3 年間は参照可能なサーバ上で管理し、3 年経過後はサービス提供用サーバから削除の上、バックアップのみを保管対象とし、弊社契約の外部倉庫で、弊社運用管理規程に基づいて管理します。 (例)*

② アクセス制御等

(a) お客様の利用時における対応可能な認証方法（3.2.3(2)(ア)1.②、2.①、3.⑧、4.②）

弊社では以下の認証方法に対応しております。

【認証に用いる ID】

・本サービスでは、ご登録いただきました各利用者のメールアドレスを、各利用者のサービス利用 ID とさせていただきます。（例）

【認証方法】

認証方法	対応の有無(有りの場合○)	備考
パスワード認証	○	*英数字記号８桁以上（例）*
生体認証		
物理媒体認証	○	HPKI による認証
その他（具体的内容　　）		

お客様が利用される認証に関する対応措置として、下表に示している項目を実施しています。((2)(ア)1.①、2.①-④、3.⑧)

対応項目
お客様の利用を特定するために、各利用者[3]に ID を発行する。
各利用者に発行する初期パスワードは、最初のログインの際に変更しないと、以降のサービス利用ができない対策を講じる。
お客様の認証に ID･パスワード方式を採用する場合には、パスワード入力に失敗した場合には、一定の不応時間を設定するとともに、失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構を採用する。
パスワードには有効期限を定め、サービス利用に鑑みて十分な安全性を満たす期間を設定する。
認証に際して ID 及びパスワードによらない場合でも、上記 3 項目と同等以上の安全性を確保する。

[3] ここでの利用者は、医療機関等において実際にサービスを利用する者(エンドユーザ)を想定する。

(b) 一時的な認証に関する取扱い（3.2.3(2)(ア) 4.④-⑦）[4]

お客様の利用者が、HPKI を格納する IC カードを所持していない場合で、業務の必要性から本サービスの利用のための認証を行う必要がある場合には、お客様の管理者に事前に代替的な認証手段に関する情報を提供しますので、それに基づいて一時的なサービス利用を行うことが可能です。(例)

(c) お客様が利用する認証情報に対する管理（(２)（ア）3.①、③-⑧）

お客様の認証に用いる情報については、下表に示している項目を実施しています。

対応項目
サービスの利用者が設定したパスワードについては、ハッシュ値で保存を行うなど、利用を本人しか知り得ないよう管理を行う。
サービスの利用者が ID･パスワードを失念した場合には、本人確認のうえ、弊社運用管理規程に基づいて、ID の通知を行い、または初期パスワードの再発行を行う。
サービスの利用者のパスワード等の情報の漏洩が生じた場合（不正な第三者からの攻撃による場合を含む）には、直ちに当該 ID を無効化し、本開示書(8)(C)に所定の対応を実施する。

(d) 認証情報管理上のお客様に実施していただく対応（(２)（ア）3.⑧）

初期パスワードについては、サービスのご利用者ご自身で変更して頂くこととし、その他、お客様における認証情報（パスワード等）の管理につきましては、アクセス制御によるセキュリティ確保の観点から、弊社が定めるサービス利用規約に基づいて実施していただく必要があります。これに依らない管理により生じた損害等については免責とさせていただきます。(例)

(e) 本サービスをご利用いただく利用者のアクセス権限の設定に関する対応状況

(3.2.3(2)(イ) 2.①、3.）

医療機関等のお客様が利用される認証に関する対応措置として、下表に示している項目を実施しています。

対応項目
本サービスにおいて、医療従事者、関係職種ごとにアクセス権限・範囲等のアクセス制御が可能な機能を含んでいる。
本サービスにおいて取り扱う医療情報について、患者等ごとに管理できる機能を有している。

[4] 提供サービスにおいて、対象外である場合には省くことができる。

(f) 権限設定に関してお客様に実施していただく対応(3.2.3(2)(イ) 2.③)

お客様における各利用者様のアクセス権限の設定については、お客様ご自身の責任において実施していただく必要があります。権限設定は、弊社が定めるサービス利用マニュアルに基づいて実施していただくようお願いします。(例)

(g) 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 (3.2.3(2)(ウ))

(対象 ／ 対象外) [5]

本サービスにおけるe-文書法の対象となる医療情報を含む文書等の作成における機能の対応状況は以下のとおりです。

対応項目
システムが端末を管理することによって、権限を持たない者からのアクセスを防止する機能がある。
医療機関等の職務権限等に応じた作成者の識別及び認証のための機能がある。
確定情報に、作成責任者の識別情報、信頼できる時刻源を用いた作成日時を含む。
「記録の確定」を行うにあたり、作成責任者による内容確認の機能がある。
確定された記録に対して、故意による虚偽入力、書き換え、消去及び混同を防止する機能がある。
確定された診療録等が更新された場合、更新履歴を保存し、更新前後の内容を参照する機能がある。
同じ診療録等に対して更新が複数回行われた場合、更新の順序性を識別できる機能がある。
代行操作の承認機能がある。
代行操作が行われた場合、代行者、被代行者、代行日時、対象となる記録等の管理情報を、その代行操作の都度、記録する機能がある。
代行操作により記録された診療録等を、作成責任者による「確定操作（承認）」を行う機能がある。

(h) 本サービス提供に従事する運用・開発担当者（管理責任者含む）におけるアクセ

[5]提供するサービスに応じて選択する。

ス制御に関する対応（3.2.3(2)(ｱ)1.①、②、④、 4.①）

本サービス提供に従事する運用・開発担当者（管理責任者含む）における本サービスに関する業務実施に際しては、担当者を一意に特定できる ID を発行し、

・ID･パスワード認証及び物理媒体認証の二要素認証

によるアクセス制御を実施しております。（例）

その他、本サービス提供に係る運用・開発担当者（管理責任者含む）のアクセス制御に関する対応措置として以下の対応をしております。(3.2.3(2)(ｱ)1.、4.①-②)

対応項目	
運用・開発担当者の ID は必要最小限の範囲で発行し、定期的に棚卸しを行い、不要な ID 等の削除を行う。	
運用・開発担当者の認証に ID･パスワード方式を採用する場合には、本人しか知り得ない状態に保つよう対策を講じる。	
運用・開発担当者の認証に ID･パスワード方式を採用する場合には、パスワード入力に失敗した場合には、一定の不応時間を設定するとともに、失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構を採用する。	
パスワードには有効期限を定め、サービス利用に鑑みて十分な安全性を満たす期間を設定する。	
認証に際して ID 及びパスワードによらない場合でも、上記 4 項目と同等以上の安全性を確保する。	
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を実施する。	
下記の内容について、運用管理規程に含めている。	
	本サービスの提供においてメンテナンスを実施するために、作業員がサーバに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
	保守業務に携わる従業員の雇用が終了又は変更となる場合のアカウント削除の手順

③ アクセス記録に関する機能

(a) アクセス記録の取得（3.2.3(2)(ｴ)1.①-②,⑥、2.、3.）

本サービスで実施しているアクセス記録に関する対策への対応として、下表に示している項目を実施しています。

対応項目
医療情報を取り扱うサービスに供するシステムへのアクセスについて記録している。
アクセス記録には、アクセスした ID、アクセス時刻、アクセス時間、アクセス対象（情報主体単位）等を含む。
システムの運用または開発に従事する者、管理者権限を有する者によるアクセスの記録については、定期的にレビューを行い、不正なアクセス等がないことを確認する。
アクセス記録が保存されている資源に対して、アクセス制限を講じている。
アクセス記録の機密性、完全性、可用性を保証する措置を講じている。
アクセス記録の改ざん防止措置を講じている。

アクセス記録に用いられる時刻の信頼性を確保するための措置を講じている。

(b) アクセス記録の保存期間 (3.2.3(2)(ｴ)1.④-⑤)

受託する医療情報の利用に係るアクセス記録は、本開示書(3)①(c)（医療情報の管理）に準じて保存します。(例)

(c) アクセス記録の提供 3.2.3(2)(ｴ)1.⑦)

本サービスの提供において取得するアクセス記録は、セキュリティの観点から、お客様には提供しておりません。但し、受託している医療情報漏洩の発生、あるいはなりすましによる医療情報の不正な作成、改ざん、破壊等などが生じた場合には、協議の上、アクセス記録の提供あるいはこれに代わる対応を行います。(例)

④ 情報漏洩対策への対応

(a) マルウェア等への対策 (3.2.3(2)(ｶ)1.①-③、⑤)

本サービスで実施しているマルウェア等への対策として、下表に示している項目を実施しています。

対応項目
本サービスの提供に係るシステムに対しては、ウイルスあるいはマルウェア対策ソフトウェアを導入し、最新の攻撃への対策を講じている。
本サービスの提供に係るシステムにマルウェアあるいはウイルスが混入しないよう手順を策定し、開発・運用を実施している。
ウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新している。
情報システムの構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新のウイルス対策ソフト等の導入を行う。またシステム情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。
情報システムの脆弱性に関する情報は、JPCERT コーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得し、確認する。

(b) 外部からの攻撃等への対策 (3.2.3(2)(ｶ)2.)

本サービスで実施している外部からの攻撃等への対策として、下表に示している項目を実施しています。

対応項目

受託する医療情報を格納する機器と、サービス提供に必要な外部ネットワークの間には、セキュリティゲートウェイ等を設置して、確立されたポリシーに基づいて、アクセス制御を行っている。
不正侵入検知システム（ＩＤＳ）または不正侵入防止システム（ＩＰＳ）等を導入し、不正な攻撃に対するトラフィックの遮断等がとれるような措置を講じている。
侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行っている。

その他、外部からの不正な攻撃への対応として以下の対策を講じています。

DDoS 攻撃への対策として、アクセス監視結果に基づいて、異常なアクセスに対する遮断等を行っています。（例）

(c) お客様の端末等に表示される医療情報の情報漏洩対応（3.2.3(2)(ｵ)1.④-⑤）

本サービスで実施しているお客様の端末等に表示される医療情報の情報漏洩対策については、下表に示している項目です。

対応項目
本サービス利用に際して、お客様の要望に基づき、一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを行える措置を講じる機能を有している。

(d) 情報漏洩対策に関して、お客様に実施していただく対応（3.2.3(2)(ｵ)1.③）

情報漏洩対策として、お客様における実施していただきたい内容を以下に示します。

- *本サービス利用環境がウイルス等による攻撃を受けた場合に、サービス提供に係る影響について、速やかにお客様に周知すると共に、お客様において対応して頂く必要のある対策をご連絡しますので、対策をお願いします。（例）*
- *上記以外のお客様の利用者が本サービスを利用する端末等に係る外部からの攻撃への対策は、お客様の責任において実施していただきます。（例）*
- *お客様の利用者が本サービスを利用する端末におけるクリアスクリーン等の対策は、お客様の責任において実施していただきます。（例）*

⑤ バックアップ等の対策

(a) バックアップの取得と管理等（3.2.3(2)(ｶ)2.）

本サービスで実施しているバックアップの取得及び管理等については、下表に示している項目です。

対応項目
運用管理規程等に基づき、複数の間隔（例：随時と日次）でバックアップを取得している。
取得するバックアップの期間等に応じて、複数の種類の媒体により、バックアップを保管している。
取得したバックアップ媒体に関しては、クラウドサービス医療ガイドラインの定めるところにより、ラベル管理、定期的な可読管理を行う等により、適切に管理している。
お客様の運用管理規程を策定する目的で、バックアップに関する情報（取得間隔、取得メディア等）の提供が可能である。

なお、法定保存義務がある医療情報について、本サービスで実施しているバックアップ対策は下表において示している項目です。(なお本開示書(3)①(c)参照)

(3.2.8(2)(ア)4.)

対応項目
医療機関等内において医療情報を保存する場合、そのバックアップを遠隔地に保存し、障害時等に医療機関等が利用できる対策が講じられおり、お客様の求めに応じて必要な情報提供が可能である。

(b) 冗長化対応（3.2.3(2)(ク)3.、5.②)

本サービスで実施している冗長化対応については、下表に示している項目です。

対応項目
医療情報を取り扱うサービスに供するシステム、ネットワーク等に関し、通常の診療等に影響が生じないよう、サービスの継続に必要な冗長化対応を講じている。
診療録等の情報を格納するハードディスク等については、RAID-1 又は RAID-6 相当以上のディスク障害への対応策を講じている。
障害時等でも診療等が継続できるための代替措置等として、医療機関等の側における対応策（紙出力、ファイル出力等）が可能となっている。

(c) 毀損したデータの取扱い（3.2.3(2)(ク)4.)

本サービスの提供に際して、受託したデータの毀損が生じた場合に実施している対応は、下表に示している項目です。

対応項目
運用管理規程に則り、データが毀損した場合でも、速やかに回復できるよう、バックアップ対応および冗長化対応を講じるとともに、その回復手順を定めている。
毀損したデータの回復が困難である場合には、毀損したデータに最も近いデータの回復を、回復手順に基づき行う。

※データの毀損等に対する免責

サービス提供に際して、受託データが毀損した場合において、本項で定める措置を行ったうえで、なお回復が困難であった場合、弊社の故意・重過失があった場合を除き、免責とさせていただきます。(例)

⑥ サービス品質

(a) サービス品質の内容（3.2.3(2)(ｷ)、(ｸ)①、②）

本サービスの品質に関する対応策およびその内容については、下表に示しているものです。

対応項目
本サービスの利用を行う際の、サービス仕様上の応答時間（一般的な表示速度、検索結果の表示時間等）を示している。 *検索結果の表示にかかる時間　：　最大 10 秒（平均 2 秒）(例)* *確認画面の表示にかかる時間　：　最大 5 秒　(平均 1 秒)（例）*
本サービスを利用する際の、契約上利用可能な資源に係る情報（保存可能容量（利用可能期間）など）が提供されており、サービス利用に際して、随時、利用者が確認できる措置が講じられている。 *※確認可能な情報の概要（例）* *・最大利用可能容量(例)* *・残存利用可能容量(例)* *・保存データ件数(例)*

(b) サービス品質に係る免責（3.2.3(2)(ｷ)）

本サービスの品質に関して、以下の免責事項を設けています。(例)

・サービス仕様上の応答時間は、お客様側で利用する回線等、通信環境の状況のほか、サービス利用の集中状況に大きく影響を受けます。従って必ずしも応答時間に示す数値を保証するものではありません。(例)

⑦ 機器・ソフトウェア等の品質管理（3.2.3(2)(ｹ)1.、2.）

本サービスの提供に際して実施しているソフトウェア・機器等の品質管理については、下表に示している項目です。

対応項目

運用管理規程等に基づき、医療情報を取り扱うシステムにおける機器及びソフトウェア等についての構成および所在等に関する文書化を行い、運用・保守が適切に行えるよう管理している。
運用管理規程等において、医療情報を取り扱うシステムにおける機器及びソフトウェア等の品質管理に関する規程、手順などを定めて、実施している。
品質管理に係る従業員等及び委託先において手順等の遵守がなされる措置を講じている。
運用管理規程等において、情報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に関する規程、手順等を定めて実施している。

⑧ お客様が利用する無線 LAN・IoT 機器に関する免責

(a) 無線 LAN に関する免責(3.2.3(2)(ｺ) 1.)

医療機関等の施設、その他の施設において既に設置されている無線 LAN を通じて、本サービスを利用する場合、無線 LAN の装置の稼働やセキュリティ対策については、お客様の責任において対応していただくものとし、これに起因して本サービスの利用に支障が生じた場合には、本サービスのサポート対象外とさせていただきます。

(例)

(b) IoT 機器に関する免責(3.2.3(2)(ｺ) 2.)

本サービスを利用する際にお客様の責任で IoT 機器を使用する場合、IoT 機器の稼働やセキュリティ対策については、お客様の責任において対応していただくものとし、これに起因して本サービスの利用に支障が生じた場合には、本サービスのサポート対象外とさせていただきます。(例)

⑨ 本項で定める管理対策に係る資料の提供等について(3.2.3(2)(ｲ)1.④、2.③、(ｳ)、(ｸ)2.⑥、(ｹ)1.⑤)

「技術的安全管理対策」において示す本サービスの管理対策に関する資料については、原則として本サービスのサポートページで提供するもの、及び各項で定める場合を除き、提供の対象外とさせていただきます。但し、お客様の申請に基づき、弊社で必要性を認めた場合には、弊社が定める情報開示規程に基づいて、お客様と必要な条件について合意の上、提供いたします。(例)

(4) 人的安全管理対策

① サービス提供に従事する要員が遵守する義務(3.2.4(2)(ｱ)1.、3.、(ｲ)②-⑤)

本サービスの提供に従事する要員（弊社従業員・派遣従業者・委託先）が遵守する義務等について、下表に示している項目を弊社就業規程・契約等に定めています。

対応項目
要員における弊社個人情報保護指針遵守に関する規定
要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
クラウドサービス事業者において要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
本サービス提供に係る要員におけるその他の遵守規程 具体的に（　　）

② サービス提供に従事する要員に対する教育（3.2.3(2)(ｸ)1.⑤、2.⑤、3.2.4(2)(ｱ)2.、3.、(ｲ)②-⑤、3.2.7(2)(ｱ)3.）

本サービスの提供に従事する要員（弊社従業員・派遣従業者・委託先）に行う教育について、下表に示している項目を、弊社就業規程・契約等に定めています。

対応項目
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
サービスの提供に従業者の退職時又は契約終了時以降の守秘義務についての教育･訓練
受託した医療情報の保存に関する業務に従事する者に対する教育・訓練の実施
サービスに供する機器、ソフトウェアの品質管理についての従業員への教育・訓練の実施
本書「Ⅱ(7) 情報および情報機器の持ち出し」に規定する内容の従業員等への教育の実施
その他、本サービス提供に際し、従業者に対して実施する教育 具体的に（　　）

③ 本項で定める管理対策に係る資料の提供等について

「人的安全管理対策」において示す本サービスの管理対策に関する資料については、原則として本サービスのサポートページで提供するもの、及び各項で定める場合を除き、提供の対象外とさせていただきます。但し、お客様の申請に基づき、弊社で必要性を認めた場合には、弊社が定める情報開示規程に基づいて、お客様と必要な条件について合意の上、提供いたします。(例)

(5) 情報の破棄

① 情報の破棄に関する安全管理対策(3.2.5(2)(ｱ)1.①、2.①)

本サービスの提供に情報機器等の破棄等における安全管理対策について、下表に示している項目を実施しています。

対応項目
本サービスの提供に際して用いる弊社保有の情報機器、本サービスの提供に係る情報を格納した媒体等を破棄する際には、弊社運用管理規程に基づき、データに不可逆的な破壊・抹消等を行い、復元を不可能にする措置を実施。
本サービスの提供に際して用いる弊社保有の情報機器、本サービスの提供に係る情報を格納した媒体等の破棄を第三者に委託した場合には、弊社運用管理規程に基づき、破棄にかかる方法の確認及びその方法に基づき破棄したことの証跡等を取得。
本サービスの提供に際して個人情報の格納に用いる他社保有の情報機器、本サービスの提供に係る情報を格納した他社保有の媒体等の破棄を委託する際には、弊社運用管理規程に基づくものと同等の措置を委託先の義務とする。また情報機器等の破棄を行う場合には、弊社運用管理規程に定める内容と同等の手法により、実施する旨を委託契約書に含めている。
管理する個人情報又はこれを格納する媒体等について、サービス提供上の要否についての定期的な確認。
個人情報の削除をサービス提供上不要として削除する基準（例えば古くなった情報を削除とする等）および削除実施に関する事前の通知。

② 情報破棄の手順(3.2.5(2)(ｱ) 2.②)

本サービス提供に関して保存した情報もしくはその媒体に関し、①に示す対策を踏まえて、弊社運用管理規程に基づき、不要と判断したものの破棄を行います。(例)

③ 本項で定める管理対策に係る資料の提供等について(3.2.5(2)(ｱ)1.②-③)

「情報の破棄」において示す本サービスの管理対策に関する資料については、原則として本サービスのサポートページで提供するもの、及び各項で定める場合を除き、提供の対象外とさせていただきます。但し、お客様の申請に基づき、弊社で必要性を認めた場合には、弊社が定める情報開示規程に基づいて、お客様と必要な条件について合意の上、提供いたします。(例)

(6) 情報システムの改造と保守

① 情報システムの改造と保守に関する安全管理対策（3.2.6(2)(ｲ)１.、2.、(ｳ)2.、3.2.9(2)(ｲ)）

本サービスの提供に際して実施する改造と保守業務における安全管理対策のうち、下表に示している項目について弊社運用管理規程等に定めています。

対応項目
リモートメンテナンスの実施手順及びシステム管理者による保守業務実施時のアクセス記録等の確認手順
リモートメンテナンスにより保守業務を行う場合における、適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置に関する設定手順等
医療情報を取り扱うサービスに供するシステムの保守において実施した操作結果についてのアクセス記録の取得とレビューの実施
医療情報を格納する機器等を、保守（例えば機器の修理等）の目的で、医療機関等もしくはクラウドサービス提供事業者等（再委託事業者含む）の組織外に持ち出す際の手順

なお、保守業務行う際における個人情報の取扱いについて、下表に示している項目は本サービスで実施しております。(3.2.6(2)(ｳ)1).

対応項目
システムの動作確認には、原則として受託した個人情報を含むデータを使用せず、テスト用のデータを使用する。
受託した個人情報を含むデータをやむを得ず使用する場合※には、「人的安全管理対策」の項で示す守秘義務が課されている要員･委託先等により行う。 *※やむを得ず使用する場合については、サービス提供に供する機器、システムの正常動作を確認するのに、必要不可欠な場合を想定しています。(例)*

② 本サービスの提供に際して行う保守業務における技術的対応（3.2.6(2)(ｴ)1～4.）

本サービスの提供に際して行う保守業務における技術的対応について、実施しているのは、下表に示している項目です。

対応項目
医療情報を取り扱うサービスにおける診療録等のデータ項目で、厚生労働省における保健医療情報分野の標準規格が定められているものについては、厚生労働省標準規格を採用

<table>
<tr><td colspan="2">対応項目</td></tr>
<tr><td></td><td>厚生労働省標準規格が定められていない項目については、変換容易なデータ形式を採用
具体的に

<table><tr><td>項目名</td><td>データ形式</td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table></td></tr>
<tr><td></td><td>上記以外のデータ項目及びその形式

具体的に
<table><tr><td>項目名</td><td>データ形式</td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table></td></tr>
<tr><td colspan="2">マスターテーブルの変更に際しての、影響を与えないレコード管理方法・とるべき措置等についての機能及び検証方法を採用</td></tr>
<tr><td></td><td>上記が困難な場合に採用するお客様のシステム等におけるシステム更新・移行するための手順
具体的に
（　　）</td></tr>
<tr><td colspan="2">サービスの利用に影響がないことを確認した上で、データ形式や転送プロトコルをバージョンアップもしくは変更を実施</td></tr>
<tr><td></td><td>上記において、既に提供するサービスの利用に影響があると認められる場合の変更等に係る告知期間

具体的に
（　　）以上前から告知</td></tr>
<tr><td></td><td>上記について、お客様が利用するサービスとの互換性確保に係る情報の提供

具体的に提供する情報の概要
（　　）</td></tr>
<tr><td colspan="2">機器・ソフトウェア等の劣化や提供事業者におけるサポート終了等により、サービスの一部又は全部の提供が困難となる場合には、お客様への影響を最小とするための措置</td></tr>
<tr><td colspan="2">機器・ソフトウェア等の劣化や提供事業者におけるサポート終了等、変更（軽微なバージョンアップは含まない）、他のクラウドサービス事業者が提供するクラウドサービスの停止・変更により、サービスの一部又は全部の提供が困難となる場合の告知期間

具体的に
（　　）以上前から告知</td></tr>
</table>

対応項目	
	上記におけるお客様への影響を最小とするための措置 （　　）
ネットワークに関する機器についての、定期的に劣化状況に関する検査	
ネットワーク等に係る機器、ソフトウェアの、将来的な互換性確保を視野に入れた採用。およびサービス提供後の標準仕様等の変更が生じたときのリスクの検討	
他のクラウドサービス事業者が提供するクラウドサービスを用いてサービスを提供する場合において、他のクラウドサービス事業者がサービスを停止した場合でもサービス提供に支障が生じないようにするための対応策の実施	

③ 本項で定める管理対策に係る資料の提供等について

「情報システムの改造と保守」において示す本サービスの管理対策に関する資料については、原則として本サービスのサポートページで提供するもの、及び各項で定める場合を除き、提供の対象外とさせていただきます。但し、お客様の申請に基づき、弊社で必要性を認めた場合には、弊社が定める情報開示規程に基づいて、お客様と必要な条件について合意の上、提供いたします。（例）

また本項でお客様に提供する旨を示した技術情報につきましては、弊社が定める情報開示規程に基づいて、お客様と必要な条件について合意の上、提供いたします。

（例）

(7) 情報および情報機器の持ち出し

① 情報および情報機器の持ち出しに関する運用管理規程(3.2.7(2)(ｱ)1.2.、(ｲ))

本サービスの提供に際して実施する情報および情報機器の持ち出しにおける安全管理対策のうち、下表に示している項目について弊社運用管理規程等に定めています。

対応項目
持ち出しに関する方針
管理体制及び管理方法
記録媒体・記録機器の取扱い
本サービスに関する情報(受託情報、システムに関連する情報等)を格納する機器・媒体等の持ち出し(委託元からの持ち出し含む)に関する方針及び規則等(「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。)
本サービスに関する情報を持ち出し、当該情報を格納する機器・媒体等の盗難・紛失が発生した時の対応(持ち出し時の機器、媒体等の物理的な盗難、紛失のほか、管理者が承認しない外部への送信等(第三者による悪意の送信、従業者による誤送信等)を含む。)
外部のネットワークに接続する場合の接続条件、安全管理措置等、接続に係る手順(格納された情報の漏洩や改ざんが生じないようにするための具体的な措置(マルウェア対策、暗号化、ファイアウォール導入等)
医療情報を取り扱うサービスに関する情報を格納する機器・媒体等についての、台帳管理等の実施、定期的な所在確認の実施

② 情報および情報機器の持ち出しにおける漏洩対策に関する安全策(3.2.3(2)(ｱ)3.②、3.2.7(2)(ｳ))

本サービスの提供に際して実施する持ち出しにおける漏洩対策については、下表に示している項目を実施しています。

対応項目
本サービスに供する機器について、出荷時のパスワード以外の起動パスワードの設定の実施。パスワード設定については、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないための対策の実施
サービスに関する情報を格納する情報機器(PC 等)におけるログイン及びアクセスにおける、複数要素認証の採用
本サービスに関する情報を格納する機器・媒体等を持ち出す場合、運用管理規程等に従い、機器・媒体自体に暗号化等の措置を実施
本サービスに関する情報を格納する機器にインストールするアプリケーションについては、必要最小限に限定
本サービスの提供に係る目的(開発、保守、運用含む)での、従業員等の個人所有の機器の利用は禁止
サービス提供に関する業務上、医療情報を取り扱うサービスに関する情報を格納するモバイル端末を持ち出す場合、弊社が運用管理規程等により、安全性を認めたネットワーク以外の当該端末の接続禁止(公衆無線 LAN への接続禁止含む。)

③ 各利用者の個人所有の端末について(3.2.7(2)(ｳ)4.)

本サービスを、各利用者様が個人で所有する端末で利用する場合（BYOD)、BYOD の可否の決定およびその状況に関する管理は、本サービスの対象外でございます。従いまして、各利用者様が個人所有の端末を利用し、これに起因して発生した漏洩事故等に関しては、免責とさせていただきます。

なお、本サービスが利用できる環境につき、仮想化技術を用いた環境での利用に関する情報の提供については、次項「④ 本項で定める管理対策に係る資料の提供等について」に基づいて提供します。(例)

④ 本項で定める管理対策に係る資料の提供等について(3.2.7(2)(ｱ)1.、4.、(ｳ)4.)

「情報および情報機器の持ち出し」において示す本サービスの管理対策に関する資料については、原則として本サービスのサポートページで提供するもの及び各項で定める場合を除き、提供の対象外とさせていただきます。但し、お客様の申請に基づき、弊社で必要性を認めた場合には、弊社が定める情報開示規程に基づいて、お客様と必要な条件について合意の上、提供いたします。

また本項でお客様に提供する旨を示した技術情報につきましては、弊社が定める情報開示規程に基づいて、お客様と必要な条件について合意の上、提供いたします。

（例）

(8) 災害等の非常時の対応についての安全管理対策

① 障害に関する対応

(a) 障害に対する対応 (3.2.9.(2)(ア) 6.)

本サービスの提供に際して、障害対応を速やかに行うための対策として、下表に示している項目を実施しています。

対応項目
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を踏まえた定期的なリスク分析・評価及び劣化等への対策
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監視、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
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

(b) 障害時における見読性確保のための機能(3.2.8.(2)(ア)3.、4.)

障害時における見読性確保のための機能について、下表に示している項目に対応しています。

対応項目
・障害時の見読性を確保するために必要な外部ファイル等の出力機能 具体的な対応内容 (　　)
・障害時の診療録等の見読性の確保を支援する機能(例えば画面の印刷機能、ファイルダウンロードの機能等) 具体的な対応内容 (　　)
・障害時の見読性を確保するために遠隔地に保存するバックアップデータを利用する機能 具体的な対応内容 (　　)

(c) 障害時の責任分界(3.2.8.(2)(ア)1.)

本サービスのシステム等のトラブルにより生じた障害については、弊社において調査を行い、その原因及び回復状況等に関する情報を、本サービス HP において速やかに公表いたします。但し災害等、不可抗力により生じた障害につきましては、可及的

速やかに調査いたしますが、調査結果の公表の時期について、災害等が沈静化以降に実施することとします。

本サービスのシステム等のトラブル以外で生じた本サービス提供上の障害につきましては、その調査結果及び対応に関しては免責とさせていただきます。(例)

② 非常時の対応(3.2.8.(2)(ｲ).1.2.3.)

(a) 非常時の対応に関する運用管理規程

非常時における本サービスの提供に際して実施する安全管理対策のうち、下表に示している項目について弊社運用管理規程等に定めています。

対応項目	
医療情報を取り扱うサービスに係る BCP 及びコンテンジェンシープランの策定	
	上記で策定する BCP 及びコンテンジェンシープランに、非常時における体制及びサービス回復手順等の内容を含む。
サービス回復後のデータ整合性の確保	
	上記に正常復帰後の対応との間に齟齬が生じないための整合性確保のための対応策を含む。
非常時に用いる利用者のアカウント発行に関する規定	
	上記アカウント発行管理者に関する規定を含む。
	上記に非常時に用いる利用者のアカウントの定期的レビューを実施する旨を含む。
	上記に正常復帰後のアカウントの無効化に関する規定を含む。
	上記アカウントの平常時の利用状況に関する確認を含む。

(b) 弊社における BCP およびコンテンジェンシープラン(3.2.8.(2)(ｲ).3.)

非常時に備えた本サービス提供に関する BCP およびコンテンジェンシープランについては、弊社 HP の下記の URL にて公表しています。

【http://+++.****.jp/----/】*(例)*

(c) 非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置

(3.2.8.(2)(ｲ).3.)

非常時が生じた場合に、セキュリティ確保の観点から、通常利用しているお客様の ID については、一時的に無効とさせていただき、代わりに利用できる ID 及びパスワードについて、お客様の管理者を通じて、ご連絡させて頂くことがあります。その際には、上記「非常時に用いる利用者のアカウント発行に関する規定」に基づいて、非常時における運用をさせていただきます。(例)

(d) サイバー攻撃等への対応

サイバー攻撃等の非常時に対する本サービスの安全管理対策については、下表において○を示している項目を実施しています。(3.2.8.(2)(ｲ).4.)

対応項目	
サイバー攻撃により、本サービスの提供が困難、もしくは大きな支障が生じた場合の原因探査に必要なログ等の記録を確保している。	
	上記の場合、サービス提供が困難等になっている旨、及び復旧に関する見通し等について、お客様に速やかに告知を行う。 具体的な告知手段 (　　)
本サービスの提供に用いる全てのアプリケーション、プラットフォーム、サーバ・ストレージ等は日本国の法令の執行が及ぶ場所に設置されている。	

③ 本項で定める管理対策に係る資料の提供等について(3.2.8.(2)(ｱ)、(ｲ)4.)

「災害等の非常時の対応についての安全管理対策」において示す本サービスの管理対策に関する資料については、原則として本サービスのサポートページで提供するもの、及び各項で定める場合を除き、提供の対象外とさせていただきます。但し、お客様の申請に基づき、弊社で必要性を認めた場合には、弊社が定める情報開示規程に基づいて、お客様と必要な条件について合意の上、提供いたします。(例)

(9) 医療情報を外部と交換する場合の安全管理対策

① ネットワークに関する安全管理対策

(a) ネットワークに対する安全管理対策(3.2.9.(2)(ｱ)1.①-③、2.①-③、3.①、4.①-②、5.①-③、(ｳ)1.②)

本サービスの提供に用いるネットワーク経路の安全管理対策について、下表に示している項目を実施しています。[6]

対応項目
ネットワークにおける、情報の盗聴、改ざん、誤った経路での通信、破壊等への対抗措置として通信の暗号化の実施
弊社サーバにおけるなりすまし防止のためのサーバ証明書の導入等
本サービス利用における IPSec + IKE の導入
誤った経路での通信を防止するため、送受信の拠点の出入り口から弊社の送受信の拠点までのネットワーク経路につき、情報機器ごとに、接続する相手方の確認を実施
お客様の外部接続サーバ等と弊社サーバ間における相互認証の実施
本サービス提供に供するルータ等のネットワーク機器は、ISO15408 で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書によりクラウドサービス医療ガイドラインに適合していることを確認できるものを使用
TLS1.2 に対応した暗号化措置(「SSL/TLS 暗号設定ガイドライン」に基づいた「高セキュリティ型」に準じた設定)
SSL-VPN の不採用
TLS1.2 接続における、セッション間の回り込み(正規のルートではないクローズドセッションへのアクセス)等による攻撃対策の実施
本サービスにおいて利用する他社のクラウドサービスの接続においても、本項で規定する対応を行うほか、弊社サーバと他社サーバの接続においても、同水準のセキュリティを確保する。

(b) お客様の施設内におけるルータ等の設定に関する免責(3.2.9.(2)(ｱ)3.②)

お客様が本サービスを利用するネットワークで用いるお客様の施設内のルータについて、これを経由して施設間を結ぶ VPN の間で送受信ができないように経路を設定する場合には、お客様の責任で実施していただき、この設定に伴う本サービスの障害等については、免責させていただきます。

なおルータの設定に必要な技術情報は、「③ 本項で定める管理対策に係る資料の提供等について」に基づいて、提供いたします。(例)

---

[6] 本例では S/MIME などの採用を前提としていないため記述していないが、S/MIME などのメール暗号化やファイル暗号化措置をサービス提供上、講じている場合には、クラウドサービス医療ガイドライン 3.2.9(2)(ｱ)4.③に基づく対応も併せて記載する。

(c) お客様の機器の設定に関する免責(3.2.9.(2)(ｱ)7.)

本サービスを仮想デスクトップ等により利用する場合、当該の利用環境に関する管理は、本サービスの対象外でございます。従いまして、お客様が仮想デスクトップ環境を利用し、これに伴い発生した漏洩事故等に関しては、免責とさせていただきます。

なお、本サービスが利用できる環境につき、仮想化技術を用いた環境での利用に関する情報の提供については、「③ 本項で定める管理対策に係る資料の提供等について」に基づいて、情報提供します。(例)

② お客様とのネットワークに関連する責任分界

(a) 通信経路に関する責任分界について(3.2.9.(2)(ｳ)1.①)

本サービスの提供に際して利用されるネットワーク対策については、①に定める対策を講じた上で、弊社における責任の範囲については、以下のように定めさせていただきます。

・本サービスに係る弊社送受信の拠点から、弊社が利用する ISP までに生じた障害等に関する責任については、弊社側の責任とし、調査対応を行うほか、発生した障害による対応責任などを負うものとします。なお、弊社が利用する弊社以外のクラウドサービス事業者についても同様とします。(例)

・それ以外のネットワーク上において発生した障害等に関しては、弊社における責任外とします。この場合、可能な範囲で情報提供などを行います。(例)

(b) 本サービス利用に係る患者等へのセキュリティに関する説明について

(3.2.9.(2)(ｳ)1.③)

本サービスの利用に係る患者等へのセキュリティに関する説明については、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を範囲とした対応とさせていただきます。

なお、情報漏えい等のセキュリティ事故が生じた場合につきましては、別途お客様と協議の上、資料の提供や患者等への説明対応、問合せ対応を実施いたします。
(例)

(c) 患者等が閲覧する場合の対応について(3.2.9.(2)(ｳ)2)

本サービスで管理する情報につきましては、お客様の責任の下で、患者等の第三者の閲覧の用に供することとさせて頂きます。患者等の第三者の閲覧については、お客様が管理する環境下での閲覧を想定しており、併せて閲覧に必要な認証情報の管理についても、お客様の管理の下で、閲覧されることを想定しております。

従いまして、本開示書にあるお客様の対応事項を実施して頂いたうえで、患者等への閲覧を行って頂くほか、これにより生じた情報漏洩等に関しましては、お客様との関係で取り決めた責任の範囲で対応させて頂くこととします。

なお患者等が閲覧する場合の本サービスのセキュリティに関する説明につきましては、(b)項に準じて対応いたします。(例)

③ 本項で定める管理対策に係る資料の提供等について

「個人情報を含む医療情報を外部と交換する場合の安全管理対策」において示す本サービスの管理対策に関する資料については、原則として本サービスのサポートページで提供するもの、及び各項で定める場合を除き、提供の対象外とさせていただきます。但し、お客様の申請に基づき、弊社で必要性を認めた場合には、弊社が定める情報開示規程に基づいて、お客様と必要な条件について合意の上、提供いたします。

(例)

また本項でお客様に提供する旨を示した技術情報につきましては、弊社が定める情報開示規程に基づいて、お客様と必要な条件について合意の上、提供いたします。

(例)

(10) 法令で定められた記名・押印を電子署名で行うことについての安全管理対策

本サービスで作成するデータのうち、電子署名による記名・押印が法令で定められたものについて、下表において○を示している項目に対応しています。(3.2.10 (2) (ｱ)、(ｲ)、(ｳ))

対応項目		対応の有無(有りの場合○)
法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名について、保健医療福祉分野 PKI 認証局の発行する電子証明書への対応		
法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名について、保健医療福祉分野 PKI 認証局の発行する電子証明書以外の電子署名法における特定認証業務により発効された電子証明書への対応 具体的な認証機関(公的個人認証サービスに基づくプラットフォーム事業者制度を用いている場合には、総務大臣認定プラットフォーム事業者名) (　　)		
	上記につき、タイムスタンプの付与	
	上記につき、タイムスタンプの付与の時点での電子証明書の有効性確認	

【タイムスタンプの検証方法】(3.2.10 (2) (ｲ)、(ｳ))

本サービスでは、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの安全な長期保存のために－」(総務省、平成 16 年 11 月) 等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者である●●株式会社が提供する▲▲サービスを用いて、タイムスタンプの付与および有効性の検証を行っています。

また電子証明書の期限が切れた後のデータ保存については、「ｅ－文書法におけるタイムスタンプ適用ガイドライン」(タイムビジネス推進協議会、平成 17 年 10 月) に基づいて、長期保存対応策を講じております。(例)

(11) 個人情報の保護

① 受託情報に対する閲覧制限（3.3.6（2）(ｲ)）

お預かりしている医療情報の閲覧制限について、下表に示している項目を実施しています。なお閲覧に際しては、弊社運用管理規程に基づいて、実施します。

対応項目	
サービス提供に必要な保守・運用を行う際に、その目的のために必要最小限の範囲を超えた、受託医療情報の閲覧禁止。	
	受託した医療情報の閲覧が必要である場合、事前・事後のお客様側の管理者の了解の取得(非常時を除く)
	受託した医療情報を非常時に閲覧した場合の、閲覧した受託情報の範囲及び緊急性となる事由の提示。
	受託した医療情報を閲覧した場合の、報告の実施。 報告方法 (　　)
受託した医療情報の予期せぬ閲覧を防止するための技術的措置の実施	

② 受託情報の解析制限・第三者提供制限（3.3.6（2）(ｲ)、(ｳ)）

お預かりしている医療情報については、運用上の必要がある場合を除き、お客様の指示に基づかない限り、解析・第三者提供はいたしません。

指示に基づく解析・第三者提供を行った場合には、その内容を報告いたします。

(例)

③ 個人情報等の外部保存に関する患者等への説明について（3.3.7（2）(ｲ)）

お客様の患者に対する本サービスの説明については、原則として本サービスのサポートページで提供するものを除き、提供の対象外とさせていただきます。但し、お客様の申請に基づき、弊社で必要性を認めた場合には、弊社が定める情報開示規程に基づいて、お客様と必要な条件について合意の上、提供いたします。(例)

(12) クラウドサービスの利用終了

① 本サービスの提供停止等における対応（3.4.1（2）①～④）

本サービスの提供停止よる弊社の対応については、下表に示している項目です。

対応項目	
本サービスの提供の変更を含むサービスの一部もしくは全部を停止する場合（軽微なバージョンアップは含まない）に、影響を最小とするための措置の実施	
	上記において、サービスの提供の一部又は全部が困難となる場合、変更（軽微なバージョンアップは含まない）等の場合の告知期間 （　　）以上前から告知
本サービスの提供の変更を含むサービスの一部もしくは全部を停止する場合、お客様からお預かりした医療情報の返却希望に対応します。	
	上記において、返却するデータの範囲（データ種類、期間等）、データ形式(データ項目、項目の詳細、ファイル形式）、返却方法、条件について公開あるいは情報提供しています。 具体的な公開・情報提供の方法 （　　）
本サービスの提供の変更を含むサービスの一部又は全部を停止することにより、お客様が他のサービスあるいはシステムの利用に変更する場合の、移行の支援 具体的な移行支援の内容 （　　） 移行支援を行うための条件（費用、その他） （　　）	

② お客様都合による本サービスの利用停止等における対応（3.4.1（2）⑤）

お客様都合による本サービスの利用停止等による弊社の対応については、下表に示している項目です。

対応項目	
サービスの一部又は全部の利用を停止する場合の、受託した医療情報の返却対応	
	返却するデータの範囲（データ種類、期間等）、データ形式(データ項目、項目の詳細、ファイル形式）、返却方法、条件についての公開、情報提供の実施 具体的な公開・情報提供方法 （　　）

サービスの一部又は全部の利用を停止することにより、お客様が他のサービスあるいはシステムの利用に変更する場合の、移行の支援 具体的な移行支援の内容 (　　) 移行支援を行うための条件(費用、その他) (　　)

③ お預かりしている医療情報の削除等（3.4.1（2）⑥、⑦）

お客様の本サービスの利用停止が生じた際の、お預かりしている情報の削除等に関する弊社の対応については、下表に示している項目です。

対応項目	
お客様のサービス利用の停止が生じた場合の、受託した医療情報の、記録の削除、媒体の廃棄等の迅速な実施	
	記録の削除または廃棄等を行った場合の、証明資料等の提供 提供方法・手段等 (　　)
医療機関等へのサポート(所管官庁への情報提供含む)等に関連する必要最低限の範囲での記録の保持	
	記録保持の目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等について公開 具体的な公開方法・内容 (　　)

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

(2) 本サービスの対象

本サービスの対象は、診療所とする。

【本項を定める上での考え方】

・本項では、SLA により提供されるサービスの目的を明示する。
・本例では、サービスの目的を、診療所向け診療録の作成・保存等のサービスを想定して提供することを明示している。
・クラウドサービスの提供目的等により、医療機関等及びクラウドサービス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。
・クラウドサービス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、クラウドサービス事業者、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) クラウドサービス

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

(2) ネットワークサービス

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

(3) 使用機器等

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

(4) 本サービスの利用に供するソフトウェア

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

【本項を定める上での考え方】

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

１．３ 本サービスの提供時間

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

本サービスの提供に当たり、乙の通常業務時間は以下のとおりである。

【平日・土曜日】 8:00～21:00

【日曜・祝日】 8:00～17:00

【本項を定める上での考え方】

・本項では、本サービスの提供時間を明示する。
・サービス提供時間は、クラウドサービス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クラウドサービス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。クラウドサービス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、クラウドサービス事業者のサービス内容や、医療機関等の要請を勘案して変更されることを想定している。

２．本 SLA について

２．１ 本サービスにおけるサービスレベル合意書の意義

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

(1) クラウドサービスを利用する際の医療情報の安全性の確保を図る

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

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

(2) 医療業務等への影響の把握

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

(3) サービス品質とコストの妥当性を図る

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

(4) 各役割分担の明確化を図る

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

【本項を定める上での考え方】

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

２．２ 本サービスにおけるサービスレベル適用の考え方

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

(1) 電子カルテの利用に鑑みたサービスレベルの適用

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

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

等を念頭に置いたサービスレベルの設定や適用が求められる。

(2) 情報システムに関する管理業務についてのサービスレベル

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

【本項を定める上での考え方】

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

２．３ 本 SLA の適用期間

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

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

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

【本項を定める上での考え方】

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

２．４ 本 SLA の改定

(1) 改定の契機

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

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

(2) 変更の手続き

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

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

【本項を定める上での考え方】

・本項では、本 SLA の改定手続について示す。
・SLA の改定は定期的に実施する方法と、改定期間を示さずに必要に応じて実施する方法がある。本例では後者の方法を記述している。
・改定を定期的に実施する方式では、例えば、改定時期を毎年 4 月等に定めて実施することが想定される。
・「双方の合意事項に明確な変更があった場合」の例としては、例えば新たなサービスをクラウドサービスとして提供することになった場合等が挙げられる。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管理対策を講じることとされている。
・クラウドサービスを利用し、医療情報を取り扱う場合には、クラウドサービス事業者は、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、クラウドサービス事業者においても、医療情報を取り扱う際のリスク評価を行い、これに応じた安全管理対策が求められ、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、クラウドサービス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。
・なお、「Ⅱ.参考例編（サービス仕様適合開示書)」の（１）⑤、⑥では、サービス選択をするのに必要な範囲での、リスク分析の概要、評価を示している。リスク分析・評価の情報は、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)(機密保持契約の締結等)により、提供することになる。

３．２ サービス利用環境

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

別紙の内容は、予告の上、適宜変更を行う。

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

【本項を定める上での考え方】

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

・クラウドサービスの場合、多くはWebブラウザ等が使用されるが、動作の正確性や表示の正確性を確保する観点から、利用に供されるOSやブラウザの製品名、バージョン情報、アプリケーションによってはセキュリティパッチへの対応の有無等が動作保証の条件とされる場合がある。また、使用するPCに関する仕様や、ネットワーク回線の仕様等も動作保証条件、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、提供するクラウドサービス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、クラウドサービス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、クラウドサービス事業者のサービス提供環境・運用に係る前提条件について示す。
・具体的な内容として本項では、サービス提供に係る機器等の所在、データセンターの所在、運用管理に必要な受託情報等の利用等を前提条件として示す。
・サービス提供に係る機器等の所在につき、本例では委託先データセンターに格納する旨を示す。データの所在については、データセンターかそれ以外（例えば自社サーバルーム）か、データセンターが自社のものか委託先のものかを明示することが求められる。また委託先の場合、委託先会社名も併記することが求められる。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、（２）①にデータセンターの所在地を示している。
・運用等により、リモートアクセスを行う場合には、その有無を明記する必要がある。再委託事業者による場合も同様である。これらの所在については、再委託事業者の項（４．３)、運用組織の項（６．１(1)）において、明確にすることが望ましい。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、（６）①でリモートメンテナンスの実施状況を示している。
・医療情報を取り扱うクラウドサービスに供する機器等については、クラウドサービス医療ガイドラインにより、国内法の執行が及ぶ場所に設置することが求められる（ク

ラウドサービス医療ガイドライン 3.2.8)。本例の第 2 段落はこの内容を示すものである。

・本例の第 3 段落では、サービスの運用上不可欠なハードウェアや回線の利用状況の把握について記載している。

・本例の第 4 段落では、サービス提供上生じた個別の障害対応等に際して、受託する医療情報をやむを得ず参照する場合や、セキュリティ対応上、必要と考えられる受託情報へのアクセス状況やシステム負荷の状況等を例として示している。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(3) ⑦で実施している機器・ソフトウェア等の品質管理を示している。

・本例の第 5 段落では、クラウドサービス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、クラウドサービス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、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(3) ⑦で実施している機器・ソフトウェア等の品質管理を示している。
・品質管理については、クラウドサービス医療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クラウドサービス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。クラウドサービス事業者によっては、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

本サービスの提供に当たり、乙は、下記に示す法令及びガイドラインを遵守する。

・個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）
・クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第 1 版（総務省　平成 30 年 7 月　）
・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 第 2 版（経済産業省　平成 24 年 7 月）

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ダンス（厚生労働省　平成 29 年 5 月 31 日）
・医療情報システムの安全管理に関するガイドライン　第 5 版（厚生労働省　平成 29 年 5 月）
・クラウドサービスにおける情報セキュリティ対策ガイドライン　第 2 版（総務省　平成 30 年 7 月）

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

【本項を定める上での考え方】

・本項では、クラウドサービス事業者が遵守している法令及びガイドラインについて明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、（１）①(c)でサービス提供において遵守するガイドラインを示している。
・クラウドサービス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、死者の情報については、個人情報には当たらないとされている。しかし医療情報の重要性、機微性に鑑みると、死亡した患者に関する情報についても、生存する者の情報と同様に取り扱う必要があり、また、取り扱う個人情報の件数によって安全管理対策を講じる必要性は変わらない。クラウドサービス医療ガイドラインでは、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サービス提供に際して用いる他の事業者が提供するサービス（連携クラウドサービス）を提供する事業者（連携クラウドサービス事業者）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、クラウドサービス事業者の負うべき守秘義務に関して、クラウドサービス事業者が使用する従業員や再委託事業者、連携クラウドサービス事業者に対する具体的な守秘義務について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、（４）①で要員の守秘義務対応を示している。
・クラウドサービス事業者は、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、これをクラウドサービス事業者が使用する従業員や再委託事業者、連携クラウドサービス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、クラウドサービス医療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、クラウドサービス事業者が実施する監査について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、（１）⑨で実施しているシステム監査の概要を示している。
・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)。クラウドサービス医療ガイドラインにおいてもこれを受けて、クラウドサービス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(2))。
・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、クラウドサービス事業者が内部監査を年次で実施し、その結果を医療機関等に報告する旨を明示している。
・また、クラウドサービスの特殊性から、報告方法については、本 SLA 参考例６．５(1)②にしたがって実施することを想定し、医療機関等が個別により詳細な実施状況の資料等を求める場合には、別途資料提供を行うという形式としている。
・クラウドサービス事業者において、例えば、ISO27001 等の第三者認証制度を取得している場合には、当該認証に係る検査の結果をもって監査結果に代える等も想定される。

４．役割分担

４．１ システム構成上の役割分担と責任（各ベンダー間等の役割分担）

(1) 本サービス提供に対する責任

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

【本項を定める上での考え方】

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

(2) 本サービスの甲における利用環境に係る具体的な役割分担と責任

① 利用環境に関する役割分担と責任

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

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

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

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

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

【本項を定める上での考え方】

・本項では、利用者側の役割分担について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、例えば（3）②(a)でアクセス制御によるセキュリティ確保の観点から、医療機関等の利用者が行うべき対応を示している。
・クラウドサービスでは、事業者側が後述のように一定のサービス仕様に基づくサービスを提供し、そのために必要な運用を行うが、医療機関等においてもサービスを利用するために一定の役割を果たすことが求められる。
・本例では、本サービスの利用に当たり、利用者側で用意すべき機器やサービス（ネットワーク等）についての役割分担のほか、外部からの当該クラウドサービスの利用や、当該クラウドサービス事業者が関与しないクラウドサービスの利用に伴う設定についての役割分担を例示している。
・本項で示す内容は、あくまでも例であり、具体的な内容については、クラウドサービス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、クラウドサービス事業者は、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、クラウドサービスの提供において発生した障害につき、第一次対応については、クラウドサービス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、クラウドサービス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、クラウドサービス事業者は、専門的な知見からの協力を行うことが望ましい。

③ 甲が行う他の利用機関等との情報交換に関する障害についての役割分担と責任

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

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

【本項を定める上での考え方】

・本項では、医療機関等が他の医療機関等と医療情報の交換を行う際に生じた障害に関する役割分担と責任について明示する。
・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、クラウドサービス事業者が提供するサービスにおいて利用できない場合、若しくは逆にクラウドサービス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、クラウドサービス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、クラウドサービス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、クラウドサービス事業者は専門的な知見からの協力を行うことが望ましい。

４．２ 甲の業務上の役割分担と責任

(1) 甲のサービス利用に関する業務上の役割分担

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

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

上記に関し、乙は、甲に対して必要な情報提供等を行い、支援を行う。

(2) サービス利用開始及び利用終了における情報内容の確認

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

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

(3) 甲が患者に対して行う情報提供に関する業務上の役割分担

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

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

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

【本項を定める上での考え方】

・本項では、サービス提供上発生する手続等の業務について、医療機関等とクラウドサービス事業者との役割分担と責任について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、例えば（11）③で患者等に対して行う個人情報等の外部保存に関する説明についての対応を示している。

・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、医療機関等がクラウドサービス事業者に対して申請して、発行する形を想定している。クラウドサービス事業者によっては、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。クラウドサービス事業者のサービスによっては、クラウドサービス事業者が設定することも想定される。なお、いずれの場合においても、医療機関等において権限設定等の作業を行うことを想定する場合には、クラウドサービス事業者は、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)。クラウドサービス事業者は、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、この趣旨からクラウドサービス医療ガイドラインにおいてもクラウドサービス事業者に対しては、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、クラウドサービス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、クラウドサービス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、クラウドサービス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 データセンター業務

本サービスの提供において、乙は、下記の業務の一部再委託を行う。

【株式会社××データセンター】（以下、丙とする）

・乙の管理する受託情報を含むシステムに関する物理的安全管理対策の管理業務

・乙の管理する受託情報を含むシステムに関する運用業務

② 保守業務

本サービスの提供において、乙は、下記の業務の一部再委託を行う。

【株式会社××情報サービス】（以下、丁とする）

・乙の管理する受託情報を含むシステムに関する保守業務

(2) 連携クラウドサービス事業者

本サービスの提供において、乙は、その管理に基づくクラウドサービス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・連携クラウドサービス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・連携クラウドサービス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クラウドサービス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、クラウドサービス事業者が行う業務に関する再委託及び連携クラウドサービス事業者について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、（１）②(a)で再委託先の状況について、④で委託先の人的安全管理対策について示している。

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

る観点から行われる。なお、自らクラウドサービスの提供を行わず、自らは契約主体となるだけで、クラウドサービスの提供を専ら連携クラウドサービス事業者に委ねた場合でも、クラウドサービス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、クラウドサービス事業者においては、その情報を提供することが求められる。特に医療情報の場合には、高度な安全管理対策が求められることから、利用者である医療機関等においても、再委託先の安全管理対策について十分に考慮する必要がある。したがって、再委託の事実だけではなく、再委託先の安全管理対策の内容についても明示することが求められる。また、同様の観点から、再委託される業務の内容についても明示し、再委託が合理的な範囲であることを判断できるように配慮することが求められる。

・本例では、データセンター業務と保守業務の一部をクラウドサービス事業者が再委託した場合を例示している。再委託業務については、例えば、ヘルプデスク業務等の業務を行う場合も想定される。これらは、クラウドサービス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。

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

・本例では、クラウドサービス事業者が他のクラウドサービス事業者と連携を行わない場合を想定している。連携する事業者がある場合には、連携クラウドサービス事業者名のほか、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クラウドサービス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、すべてクラウドサービス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クラウドサービス事業者に対して、クラウドサービス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クラウドサービス事業者を用いる場合、それらの事業者の情報についても、クラウドサービス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、クラウドサービス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、クラウドサービス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： 【クラウドサービス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。

【クラウドサービス事業者側ヘルプデスク窓口】（通常業務時間）

【クラウドサービス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、医療機関等とクラウドサービス事業者との連絡体制について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(1) ①で組織体制を示している。

・本例では、医療機関等側の責任者とクラウドサービス事業者側の責任者のほか、ヘルプデスク窓口の連絡先を明示している。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(1) ⑩で問い合わせ窓口について示している。

・クラウドサービス事業者が提供するサービスにおいて、連携クラウドサービス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クラウドサービス事業者を直接の連絡先とすることが求められる。

(2) 障害時・非常時の連絡体制・告知方法

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

通常業務時間　　【連絡先】

上記以外の時間　　【連絡先】

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

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

【本項を定める上での考え方】

・本項では、障害時・非常時のクラウドサービス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。
・クラウドサービス事業者の用意する問合せ先については、電話による連絡先が通常である。しかし、日中等以外の時間帯における問合せ先としては、メール等による連絡の場合も想定される。ただし、医療機関等の業務によっては、障害時・非常時等のようなケースで、即時性や双方向性等が求められることもある。サービスを供する業務の性格や、必要性等に鑑みて合意することが求められる。

５．サービス仕様

５．１ ネットワークセキュリティに関するサービス仕様

(1) ネットワーク経路の安全管理対策（暗号化、盗聴対策、使用機器等）

本サービスの提供に際して乙が使用するネットワーク及びこれに関する機器につき、乙は「サービス仕様適合開示書」「(9) 外部と個人情報を含む医療情報を交換する場合の安全管理対策」「① ネットワーク経路に関する安全管理対策」に示す事項を実施することにより、ネットワーク経路の安全管理対策を実施する。

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

【本項を定める上での考え方】

・本項では、ネットワーク経路の安全管理対策（暗号化、盗聴対策、使用機器等）について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、（９）①で実施しているネットワーク経路の安全管理対策を示す。
・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（例えば、6.11 C 等)。医療機関等が医療情報をクラウドサービス事業者に寄託する場合、クラウドサービス医療ガイドラインではクラウドサービス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管理対策を講じることを求めている（例えば、3.2.9 等)。
・そこで、本 SLA では、上記の趣旨を反映した運用内容を「ネットワーク経路上の安全管理対策」に示し、クラウドサービス事業者は、これを運用管理規程に含めることとし、本例ではこれに基づいてネットワーク経路の安全管理対策の実施を行う旨を明示している。
・また、クラウドサービス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、クラウドサービス事業者は、一定の条件で資料提供を行う旨を明示している。

(2) 外部からの不正アクセス対策（不正アクセス防止、なりすまし防止等）

本サービスの提供に際して乙が使用するネットワーク及びこれに関する機器につき、乙は別添「サービス仕様適合開示書」の「(3) 技術的安全管理対策」、「④ 情報漏洩対策への対応」に示す事項を実施することにより、不正アクセス対策を実施する。

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

【本項を定める上での考え方】

・本項では、外部からの不正アクセス対策（不正アクセス防止、なりすまし防止等）について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(3) ④で実施している不正アクセス対策を示す。
・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クラウドサービス事業者に寄託する場合、クラウドサービス医療ガイドラインではクラウドサービス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、3.2.3 等)。
・そこで本 SLA では、上記の趣旨を反映した運用内容を「不正アクセス対策」に示し、これをクラウドサービス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、クラウドサービス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、クラウドサービス事業者は一定の条件で資料提供を行う旨を明示している。

５．２ 受託情報に関するサービス仕様

(1) 真正性に関するサービス仕様

① 利用者認証（利用者資格認証、電子署名等）

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

本サービスの提供に際して、乙は別添「サービス仕様適合開示書」巻末の「技術的安全管理対策」「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。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(3) ②(a)で採用する認証方法や講じている認証に関する措置を示している。
・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クラウドサービス事業者に寄託する場合、クラウドサービス医療ガイドラインでは、クラウドサービス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 等)。
・そこで本 SLA では、上記の趣旨を反映した運用内容を「アクセス制御」に示し、これをクラウドサービス事業者は運用管理規程に含めることとし、本例では、これに基づいて、アクセス制御の実施を行う旨を明示している。
・本例では ID･パスワードによる認証と IC カードを用いた認証の組み合わせによる利用者認証を採用している例を示している。実際の SLA ではクラウドサービス事業者が採用する認証方法（パスワード等の記憶要素、ハードウェアトークン又は IC カード等の物理媒体要素、指紋・顔などの生体情報(バイオメトリクス)要素等）を記載する。
・また、クラウドサービス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、クラウドサービス事業者は、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毎にアクセス権限を設定できること。
・甲が利用する、複数の担当業務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。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では（3）②で、実施しているアクセス制御の内容・機能を示している。
・医療情報を作成する場合、法令による職種等の身分要件や管理者等の役職要件が求められるものがある。特に本 SLA で想定する電子カルテについては、医師による作成が義務付けられている。
・このような観点から、法的保存義務のある文書を電子的に作成するために用いるクラウドサービスにおいては、サービス仕様として職種等に基づくアクセス制御が必要とされる（クラウドサービス医療ガイドライン 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ている。
・本例で示す項目に関しては、システム機能として実装できない場合でも、運用方法により代替することによって同程度の安全性を確保できる場合には、その内容を記述することが想定される。
・また、本サービスに係る職種等に基づくアクセス制御の状況等につき、医療機関等からの要請があった場合に、クラウドサービス事業者は、一定の条件で資料提供を行う旨を明示している。

③ 電子署名

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

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

【電子署名に係る要求事項】

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

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

【本項を定める上での考え方】

・本項では、電子署名を採用する場合の仕様等について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では（10）で、実施している法令で定められた記名・押印を電子署名で行うことについての安全管理対策を示している。

・「電子署名及び認証業務に関する法律」（電子署名法）では、書面における署名に代えて一定の要件を満たした電子署名により、署名と同様の証拠力を認めている。また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、情報の作成責任者を明らかにするに当たって、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 認証局発行の電子証明書または電子署名法の認定認証事業者が発効する電子証明書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、クラウドサービス事業者は、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、乙は別添「サービス仕様適合開示書」「技術的安全管理対策」「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。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では（３）②(d)で、ｅ-文書法の対象となる医療情報を含む文書等の作成を目的とするサービスにおける機能を示している。
・記録の確定については、クラウドサービス医療ガイドラインでは、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、クラウドサービス事業者は、一定の条件で資料提供を行う旨を明示している。

⑤ データの更新履歴管理

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

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

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

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

【本項を定める上での考え方】

・本項では、診療記録のデータの更新履歴管理の仕様等について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では（３）②(d)で、ｅ-文書法の対象となる医療情報を含む文書等の作成を目的とするサービスにおける機能を示している。
・診療記録のデータの更新履歴管理については、クラウドサービス医療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。クラウドサービス医療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、クラウドサービス事業者による運用上での対応も想定される。
・第２段落では、本項で定める機能の実装等により防止対策を講じたにもかかわらず、確定された記録が第三者により不正な書き換えや消去等がなされた場合に必要な対応をとることについて例示している。具体的な対応の内容としては、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、クラウドサービス事業者は、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 又は RAID-6 相当以上のディスク構成を採用し、障害対策を講じる。

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

【本項を定める上での考え方】

・本項では、見読性に関するサービス仕様等について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、応答時間の状況については（3）⑥(a)で、冗長性については（3）⑤(b)および（8）①(b)で示している。
・電磁的記録による場合には、「民間事業者等が行う書面の保存等における情報通信技術の利用に関する法律」(「e-文書法」）等により見読性の確保が求められる。すなわち電磁的記録においても、紙媒体による場合と同様の内容が完全に再現できることを確保することが求められる。
・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、クラウドサービス医療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、クラウドサービスの場合には、ネットワークのトラフィックの状況等により、応答速度にバラつきが生じることがある。そして責任分界等との関係においては、スループットタイムを保証するか等が論点となる。本 SLA ではクラウドサービス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、クラウドサービス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クラウドサービス医療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、その他クラウドサービス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、クラウドサービス事業者のサービス内容にしたがって記述することが求められる。電子カルテ等の重要システムにおいて、障害回復時間等をサービス内容として明確にしない場合には、医療機関等において障害発生時の代替的措置を講じることができるようにすることが望ましい。
・本サービスにおける見読性に関する仕様、対応等の情報については、医療機関等からの要請があった場合に、クラウドサービス事業者は一定の条件で資料提供を行う旨を明示している。

(3) 保存性に関するサービス仕様

① データの破壊防止対策（ウイルス等による攻撃対策等）

本サービスの運用に供する乙の施設において、乙は、別添「サービス仕様適合開示書」の「(3)技術的安全管理対策」「情報漏洩への対策」に示す内容を実施することにより、本サービスの運用におけるウイルス等によるデータの破壊防止対策を行う。

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

・ウイルス対策のためのパターンファイルの更新、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。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(3) ④(a)で外部からの攻撃への対策について示している。
・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、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)。クラウドサービス医療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では、クラウドサービス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、「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、クラウドサービス事業者は、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、クラウドサービス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、クラウドサービス事業者は、一定の条件で資料提供を行う旨を明示している。

② データの劣化、滅失対策

本サービスに供する乙の施設において、乙は、「サービス仕様適合開示書」「(8) 災害等の非常時の対応についての安全管理対策」「① 障害に対する対応」「(a) 障害に対する対応」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データの劣化、滅失対策に必要なモニタリングを行う。

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

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

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

【本項を定める上での考え方】

・本項では、データの劣化、滅失対策について明示する。なお、「Ⅱ.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（8）①(a)で、転送プロトコルの変更等については、(6)②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（7.3 B)。クラウドサービス医療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 では、クラウドサービス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、「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、クラウドサービス事業者はデータの劣化、滅失等によるデータの破壊防止の対策について明示している。
・併せて、本例では主にデータ形式や転送プロトコルの変更やバージョンアップが生じる場合には、旧方式のものとの互換性を確保することについて明示している。
・また、医療機関等がサービス利用中に、何らかの障害が発生し、データの転送が医療機関等からクラウドサービス事業者に対してデータの転送が完了していなかった場合に、その旨を表示する機能を実装する例を示している。本項では、データ転送中のトラブルへの対応方法について、各クラウドサービス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、クラウドサービス事業者は、一定の条件で資料提供を行う旨を明示している。

③ データ仕様について

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

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

【本項を定める上での考え方】

・本項では、データ仕様について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、 (6)②でデータ項目の規格等について示している。
・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（7.3 C)。クラウドサービス医療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、クラウドサービス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。クラウドサービス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若しくは手順を講じる等が想定される。
・本サービスにおけるクラウドサービス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、クラウドサービス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、クラウドサービス事業者の運用体制を明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(1) ②でサービス提供体制を示している。
・本例では、クラウドサービス事業者の運用体制図を示す形をとっている。
・医療情報を情報システムで取り扱う場合、医療機関等には、組織体制を含む運用管理規程の整備等が求められる（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、クラウドサービス事業者の運用管理体制を明示することが求められる。
・クラウドサービス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
  ✓連携クラウドサービス事業者がある場合には、その事業者

と、それぞれの役割を明示することが求められる。

(2) 運用に関する規程

① 本サービス提供上、根拠とする運用管理規程等

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

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

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

【本項を定める上での考え方】

・本項では、本サービス提供上、根拠とする運用管理規程等の考え方を明示する。
・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、クラウドサービス事業者においても、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。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クラウドサービス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、クラウドサービス事業者の運用管理規程等に定める内容を適用する
  ✓医療機関等の運用管理規程において規定が存在する場合で、クラウドサービス事業者の運用管理規程等と内容が異ならない部分は、クラウドサービス事業者の運用管理規程等に定める内容を適用する
  ✓医療機関等の運用管理規程において規程が存在する場合で、クラウドサービス事業者の運用管理規程等と内容が異なる部分は、医療機関等とクラウドサービス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の内容とクラウドサービス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、クラウドサービス事業者は、必要に応じて運用管理規程等の情報開示が求められる。

② 運用の方針となる規程

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

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

③ 運用管理を構成する規程・要領・手順等

乙規程等には、下記に定める規程・要領・手順等が含まれる。

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

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

④ 本項で示す運用管理規程類等の提供

本項で示す乙規程等については、６．６(3)に基づいて、乙は、甲に提供する。

【本項を定める上での考え方】

・本項では、クラウドサービス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。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(1) ①(d)で策定している規程類を示している。
・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。実際には各クラウドサービス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、各クラウドサービス事業者のセキュリティ対策等に関係する内容も含まれていることから、一般的には公開には馴染まない。ただし６．１(1) ①に示すように医療機関等の運用管理規程に代替するものとして取り扱われることも想定されることから、一定の条件等に基づいて、医療機関等に対して提供する旨を、本例では明示している。

(3) 運用における遵守事項

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

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

【本項を定める上での考え方】

・本項では、クラウドサービス事業者がサービス提供上の禁止事項を明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(11) ①(b)で受託情報の解析制限・第三者提供制限を示している。
・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、特にクラウドサービス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、クラウドサービス事業者は医療機関等に対して必要な説明を行う。

６．２ 受託情報の取り扱い

(1) 受託情報の取り扱い範囲

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

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

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

【本項を定める上での考え方】

・本項では、クラウドサービス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。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(11)①(a)で受託情報の閲覧制限を示している。
・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、原則としてクラウドサービス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
  ✓ただしクラウドサービス事業者において受託した医療情報の内容を参照できる者を限定し、その範囲でのみ参照権限を付与する
  ✓受託した医療情報を参照する場合には、原則として委託元の医療機関等に事前告知及び事後報告する。サービスの提供上、緊急性があり、事前連絡が困難な場合でも、参照後に委託元の医療機関等へ速やかに報告を行う

等の対応が求められる。本例は、上記内容について、例示しているものである。

(2) 受託情報の管理

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

【本項を定める上での考え方】

・本項では、サービス提供に際して、クラウドサービス事業者の実施する受託情報の管理について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、（１）①で受託情報の管理状況を示している。
・本 SLA では、クラウドサービス事業者が行うべき受託情報の管理について、「受託情報の管理」に示す内容を運用管理規程等で規定することとしている。本例では、これに基づいて、クラウドサービス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クラウドサービス事業者の受託情報の管理につき、具体的な対応内容や実施状況を把握する必要が生じうる。そこで本例では、医療機関等からの要請があった場合に、クラウドサービス事業者は一定の条件で受託情報の管理状況についての資料提供を行う旨を明示している。

(3) 受託情報の提供

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

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

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

・受託情報の提供に要する費用

本項につき、乙は、受託情報を甲に提供する際、下記の事項を実施する。

・「医療情報システムの安全管理に関するガイドライン　第５版」の「5 情報の相互運用性と標準化について」に従った実施
・提供される情報に、標準仕様に該当しない項目等の内容が含まれている場合には、甲において正確なデータの確認が可能となるために必要な説明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、医療機関等からクラウドサービス事業者に対して、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。
・クラウドサービス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。
・クラウドサービス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5版」の「5 情報の相互運用性と標準化について」に従った実施
・ 提供される情報に、標準仕様に該当しない項目等の内容が含まれている場合には、甲において正確なデータの確認が可能となるために必要な説明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、クラウドサービス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。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(12) でサービス利用停止に伴う受託情報の返却等について示している。
・サービス提供契約終了に際して、医療機関等とクラウドサービス事業者は、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、医療機関等とクラウドサービス事業者で協議して決める

旨を明記している。クラウドサービス事業者によっては、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、クラウドサービス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、乙はサービス仕様適合開示書の「物(2) 物理的安全管理対策」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。

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

【本項を定める上での考え方】

・本項では、クラウドサービス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。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、(2) で物理的安全管理対策について示している。
・医療機関等においては、厚生労働省ガイドラインにより物理的安全管理対策の実施が求められる（例えば、6.4 C 等)。そのため医療機関等が医療情報をクラウドサービス事業者に寄託する場合、クラウドサービス医療ガイドラインではクラウドサービス事業者の運用において必要な物理的安全管理対策を講じることを求めている（例えば、3.2.2 等)。
・そこで本 SLA では、上記の趣旨を反映した運用内容をサービス仕様適合開示書の「(2) 物理的安全管理措置」に示し、これをクラウドサービス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。
・またクラウドサービス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、クラウドサービス事業者は一定の条件で受託情報の管理状況についての資料提供を行う旨を明示している。

② セキュリティ管理

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

・乙の管理下にあるネットワーク及びサービス提供に係るシステムにおいてセキュリティが確保されていることの監視
・乙の管理下にあるネットワーク及びシステムの稼動状況（特に、通信容量とトラフィック変動が重要）の監視
・乙の管理するネットワーク及びシステム等に対するサイバー攻撃に対するネットワーク等に関する定期的な監視
・業務上、受託情報を外部に持ち出す際の適切なウイルス対策等の実施
・業務上受託情報の参照等を行う場合の覗き見予防措置の実施
・バックアップデータにつき、その内容の改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、クラウドサービス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。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、運用の機密性等について、（６)、（８）で示している。
・本例では、クラウドサービス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クラウドサービス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、さらにクラウドサービス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、クラウドサービス医療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。したがってクラウドサービス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。
・またクラウドサービス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、クラウドサービス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（４．１②参照）をする。

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

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

【本項を定める上での考え方】

・本項では、本サービスの可用性について明示する。

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

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

・本例では、診療録の作成、保存等のサービスを想定して、クラウドサービス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、クラウドサービス事業者に起因するサービスが障害により停止した場合に、サービス提供時間において、最大半日程度以内には回復できることを想定して設定している。

・本例で示した報告項目及び数値は、あくまでも例示であり、サービス稼働率、問題管理対応時間等及び問題検出のための手法（例えば、死活監視間隔やロードアベレージの検出等）について挙げている。実際の SLA においては、サービスの内容に応じてクラウドサービス事業者がサービス提供上必要とされる可用性の確保に必要な項目や指標について、追記することが想定される。なお、乙による感知若しくは甲からの連絡があった時刻から第一次対応を行うまでの時間については、医療機関等とクラウドサービス事業者の合意にしたがって記入されることを予定している。
・また、本例では、ネットワークに起因するサービスレベルの低下については明示していない。本例の想定では、クラウドサービス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。クラウドサービス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。
・クラウドサービス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、クラウドサービス事業者は、一定の条件で受託情報の管理状況についての資料提供を行う旨を明示している。

(3) 完全性

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

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

上記の記録につき、乙は法定保存年限経過後 5 年間保存する。

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

【本項を定める上での考え方】

・本項では、運用の完全性について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、アクセス記録の取得について（３）③で示している。
・本例では、運用の完全性を担保する観点から、クラウドサービス事業者が利用者及び運用者の受託情報へのアクセス状況を記録し、保存することを明示している。
・アクセス記録の保存期間として本例では法定保存年限経過後 5 年間としている。
・アクセス記録については、取得対象とするシステムや方法によって記録容量等が大きくなることも想定される。そのため、記録方法や保管形態、保管方法によりサービスコストの上昇につながりうる。またアクセス記録に対するレビュー等をサービス内容とする場合にも、サービスコストに大きく影響が生じる。クラウドサービス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、クラウドサービス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。クラウドサービス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。
・クラウドサービス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、クラウドサービス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「サービス仕様適合開示書」の「(8) 災害等の非常時の対応についての安全管理対策」「②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。

・【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。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、非常時の対応について（８）②で示している。
・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クラウドサービス事業者が定めて、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、クラウドサービス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。クラウドサービス事業者は、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、クラウドサービス事業者が行うものとして示している。クラウドセキュリティ医療ガイドラインでは、非常時のアカウント対応の判断者について、サービス仕様適合開示書を通じて、医療機関等が行うか、クラウドサービス事業者が行うかを決めて、合意するものとしている（3.2.8(2)(イ) 3.)。
・クラウドサービス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、クラウドサービス事業者は、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、クラウドサービス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。
・クラウドサービス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。したがってクラウドサービス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、クラウドサービス事業者において、月次報告を行う時期（例えば、毎月第一週目の火曜日等）等を定めることも想定される。

② 年次報告事項

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

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

【本項を定める上での考え方】

・本項では、クラウドサービス事業者が医療機関等に行う報告につき、年次報告の内容について明示する。
・医療機関等は、適切な委託先と契約をしていること、また、継続して委託してよいか確認する必要があることから、クラウドサービス事業者は、自身の運用状態に係る情報や、経営等に係る情報等についても定期的に報告をすることが望ましい。特に厚生労働省ガイドラインでは、契約開始段階で一定の条件を満たした事業者が外部保存を行うサービスを提供することを条件としており（8.1 3(c)）、契約の継続等を進める上でも、定期的に条件を満たしていることを確認する必要がある。
・上記の観点から、本例では、クラウドサービス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、クラウドサービス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、クラウドサービス事業者において、年次報告を行う時期（例えば、毎年契約更新時等）等を定めることも想定される。

③ 発生の都度に報告する事項

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

・本サービスに係る業務体制、管理体制、保守体制等の変更
・システムの動作確認において、乙が受託する医療情報を参照した際の作業結果
・リモートメンテナンスによる甲のシステム改造、保守作業の実施結果
・乙が業務上、受託情報を組織外に持出し、あるいは、再委託事業者へ保存した結果
・ウイルス混入や不正なメッセージの混入等による改ざん、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、クラウドサービス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、例外的にクラウドサービス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、クラウドサービス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、乙が受託する医療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している。

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

(3) 事前連絡及び承認等

① 保守業務に伴うサービスの停止の告知

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

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

【本項を定める上での考え方】

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

② 受託情報等に関する保守業務の事前連絡・承認

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

・システムの動作確認において、受託した個人情報の参照をする場合
・リモートメンテナンスによる甲側のシステム改造、保守作業を実施する場合
・乙が受託した情報を組織外に持出し、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。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」では、個人情報の閲覧に関する事前･事後の報告について（11）①で示している。
・第１段落では、保守業務を実施する上で、受託情報を参照したり、外部に持出したり、あるいは、医療機関等の管理するシステム（例えば、利用端末）をリモートメンテナンスする場合等について、事前の連絡と承認を受ける旨を明示している。
・受託する医療情報は、特に取扱いに注意を要する個人情報であることから、原則として受託するクラウドサービス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。
・またクラウドサービス事業者のサービス内容によっては、医療機関等がクラウドサービスの利用端末等の環境を保守する場合も想定される。この場合でも、利用者側の混乱や不測の影響を回避する観点から、事前連絡と承認が求められる。
・第１段落但し書きは、前段の原則に対する例外を明示している。
・クラウドサービス事業者が繰り返し事前連絡を行ったにもかかわらず、医療機関等側から合理的な理由がないまま承認がない、等の医療機関等の帰責事由によって承認が得られない状況が生じ、かつ保守業務との関係で速やかに受託情報を参照しなければならない等の要請がある場合の例外的な対応について明示している。
・第２段落では、事前連絡及び承認に基づいて、本項で定める保守業務を実施した場合に、事後の報告と承認を得る旨を明示している。
・本例で定めている事前連絡・承認の対象となる事項は、例示であり、クラウドサービス医療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、クラウドサービス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)。
・一方でクラウドサービスは、多数の利用者に対して同時にアプリケーションを利用できる環境を提供するサービスという性格を有している。そのため、すべての利用者が保守業務に対して事前承認を行わなければ着手できないとすると、かえって安全な利用環境の提供ができなくなる場合が生じることが懸念される。
・本例では、保守業務の内容により、ア)事後報告のみを要する保守内容、イ)事前告知及び事後報告を要する保守内容、ウ)事前承認及び事後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、クラウドサービスの特性から生じる要請を満たすことを目的としている。
・なお、本例では、上表ウ）に当たる実施内容においても、契約時に包括的事前承認を得ている保守業務については、例外として扱う旨を明示している。

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

６．６ サポート

(1) 利用者に対するサポート

① サポート内容

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

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

② サポート対応時間

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

【乙サポートセンター】　連絡先　（受付対応時間、曜日）

【本項を定める上での考え方】

・本項では、サポート対応時間等を明示する。なお、「Ⅱ.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（1）⑩で示している。
・サポート対応時間は、通常電話によるものが想定されるが、例えば、時間外や、急を要しない照会内容等は、メールによる受付を行うクラウドサービス事業者もある。このような場合には、本項で問合せ用の Web ページ等を併せて明示する。

(2) 技術情報提供について

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

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

【本項を定める上での考え方】

・本項では、技術情報提供について明示する。なお、「Ⅱ.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、技術情報の提供の可否や条件等を示している。
・本 SLA では、クラウドサービス事業者が講じるべき安全管理対策のうち、技術的な対応については、個別の対応措置の内容や方式、仕様等を明記せず、各項目において３．５に示す法令・ガイドラインの該当箇所を満たす対応を実施する、という規程振りを採用している。その上で、個別の対応措置の内容や方式、仕様等については、医療機関等の求めに応じてクラウドサービス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、クラウドサービス事業者は、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
  ✓クラウドサービス事業者は、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

  という規程振りをしている。
・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、クラウドサービス事業者はその旨も含めて、医療機関等の理解を得た上で合意を行うことが求められる。

(3) 運用状況に係る情報提供について

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

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

【本項を定める上での考え方】

・本項では、運用状況に係る情報提供について明示する。なお、「Ⅱ.参考例編（サービス仕様適合開示書)」ではそれぞれの項目で、運用状況の資料の提供の可否や条件等を示している。
・本例では、クラウドサービス医療ガイドラインに記述する各項目について、クラウドサービス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、
  ✓原則としてクラウドサービス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
  ✓クラウドサービス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
  という規程振りをしている。
・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、クラウドサービス事業者は、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クラウドサービス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クラウドサービス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、クラウドサービス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。クラウドサービス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。

■ 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、各項目について特に軽重を置かない形を例示しているが、例えば情報漏洩事故に強く関係する要求事項の不達成を重視して評価を定めるなどの考え方もある。

・本例は、あくまでも事例であり、どのような評価方法を採用するかについては、クラウドサービス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。クラウドサービス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、クラウドサービス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、クラウドサービス事業者、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。クラウドサービスの場合、複数のサービスを合わせることで利用される場合（例えば、通信サービスとクラウドサービス等）等が挙げられる。この点は、責任分界とも密接に関係する部分である。

・本例では、クラウドサービス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、クラウドサービス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。クラウドサービス事業者と医療機関等との協議の結果、変更されることを想定している。

７．２ サービスレベルマネジメント

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

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

【本項を定める上での考え方】

・本項では、サービスレベルマネジメントについて明示する。
・SLA の評価の結果、サービスレベルを維持するためにどのような対応をとるのかがサービスレベルマネジメントである。
・本例では、SLA の評価等により、サービスレベルの達成状況に問題がある場合の対応について示している。本例で示す対応のほか、クラウドサービス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、クラウドサービス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。クラウドサービス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。