「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」概要

本資料の位置づけ

- 本資料は、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（以下、「本ガイドライン」という）に関する概要説明資料です。

本ガイドラインの目次

本ガイドラインの策定方針

- **本ガイドラインは、総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（以下、「クラウド事業者ガイドライン」という。）、および経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」（以下、「情報処理事業者ガイドライン」という。）が定める要件を整理・統合したガイドラインです。**

「1.2 本ガイドラインの策定方針」

クラウド事業者ガイドラインと情報処理事業者ガイドラインが求める要件を、以下の方針に従い整理・統合した。

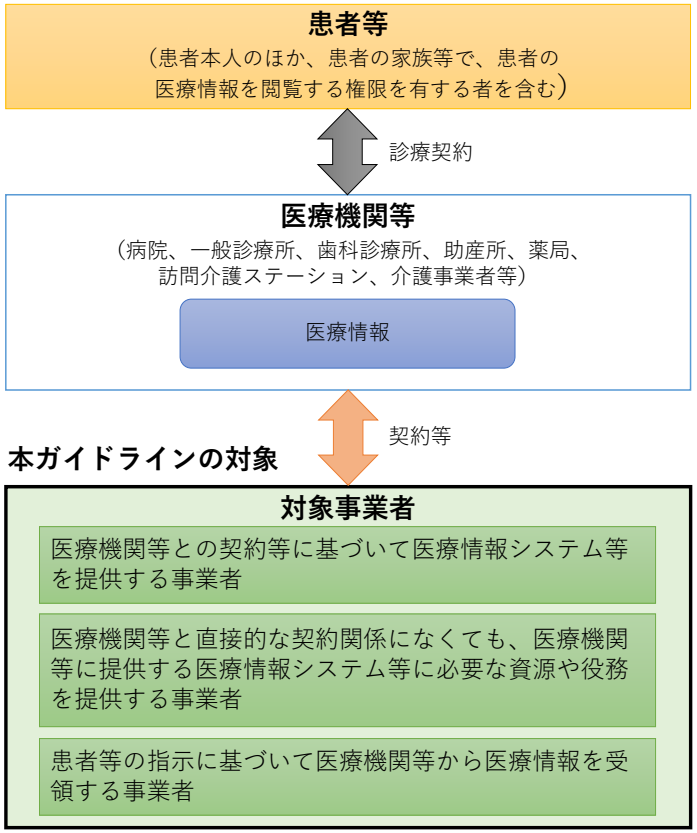
- 他の規格・ガイドラインとの整合性の確保に留意しながら、過去のガイドラインの要求事項と同等の安全管理水準が確保されるようにする
- 医療情報システム等の特性に応じた必要十分な対策を設計するために、一律に要求事項を定めることはせず、リスクベースアプローチに基づいたリスクマネジメントプロセスを定義する
- セキュリティ対策の妥当性と限界について、正しい共通理解と明示的な合意のもと医療情報システム等を運用するために、リスクコミュニケーションを実施できるようにする
- 医療情報システム等に関連する法令の求めに対して、セキュリティ対策の抜け漏れを防止するために、医療情報の取扱いにおいて留意すべき点や制度上の要求事項を明らかにする

本ガイドラインの対象範囲

- **本ガイドラインが対象とする事業者は、医療機関等との契約等に基づいて医療情報システムやサービス（以下、医療情報システム等）を提供する事業者です。**
  ※医療機関等と直接的な契約関係のない事業者も、医療情報システム等のサプライチェーンの一部としてシステムやサービスを提供している場合は、本ガイドラインの対象事業者となります。

「2.1 本ガイドラインが対象とする医療情報と事業者」

本ガイドラインが対象とする事業者は、医療機関等との契約等に基づいて医療情報システム等を提供する事業者（以下、「対象事業者」という）である。ただし、医療機関等と直接的な契約関係になくても、医療機関等に提供する医療情報システム等に必要な資源や役務を提供する事業者や、患者等の指示に基づいて医療機関等から医療情報を受領する事業者は本ガイドラインにおける対象事業者となる。

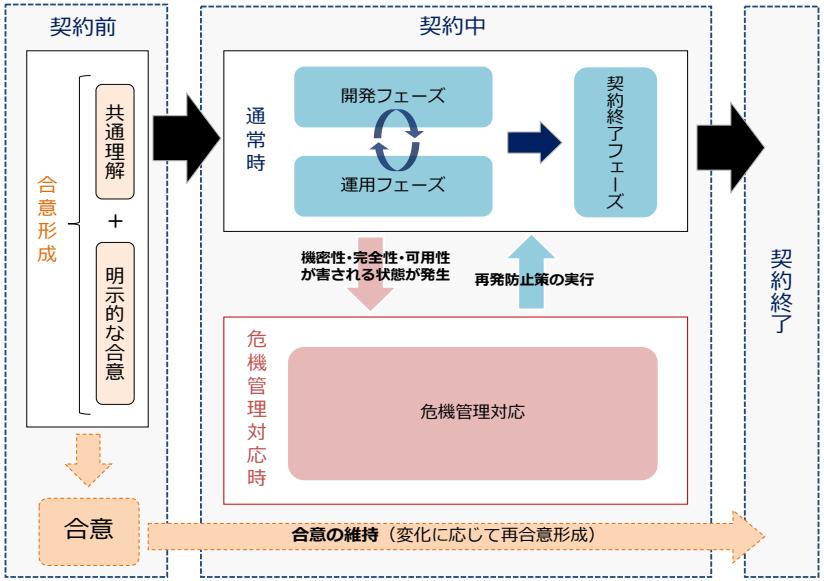


医療情報システム等のライフサイクルにおける義務と責任

- **本ガイドラインの対象となる事業者は、提供する医療情報システム等について、医療機関等と義務や責任についての合意形成が重要となります。合意形成にあたっては、医療機関等との間で「共通理解」と「明示的な合意」の形成が求められます。**

3.2. 医療情報システム等のライフサイクルにおける義務と責任

対象事業者が前節で記載した義務や責任に対応するにあたって、全ての医療情報システム等に共通な一律の要求事項を定めることは難しい。そのため、対象事業者は自らが提供する医療情報システム等を対象とし、リスクマネジメントのプロセスとリスクベースアプローチに基づいて対策をとりまとめ、医療機関等との間で合意を形成することとする。



3.2.1. 契約前の合意形成及び契約中の合意の維持

対象事業者は説明義務を果たすために、医療機関等との間で「共通理解」と「明示的な合意」の形成を行うこと。

合意形成にあたり医療機関等へ情報提供すべき項目

- **対象事業者は、医療機関等との合意形成にあたり、以下の項目についての情報を提供し、医療機関等と共通理解を形成する必要があります。**

4.1 医療機関等へ情報提供すべき項目

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

情報提供を行う際の文書例

- **情報提供を行う際の文書例として、別紙１「ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例」があります。本開示書の作成・提供は必須ではありませんが、対象事業者は医療機関等に対して、本開示書等と同等の内容について情報提供した上で、適切な共通理解に基づく合意形成を図ることが求められます。**

別紙1　ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例

１．　本参考例の目的

本参考例は、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（以下、「提供事業者ガイドライン」という）に基づいて、対象事業者が医療機関等に対してサービスの提供を行う際に求められる合意事項等を整理し、サービス仕様適合開示書　及びサービス・レベル合意書（SLA）参考例という形でまとめたものである。

２．サービス仕様適合開示書について

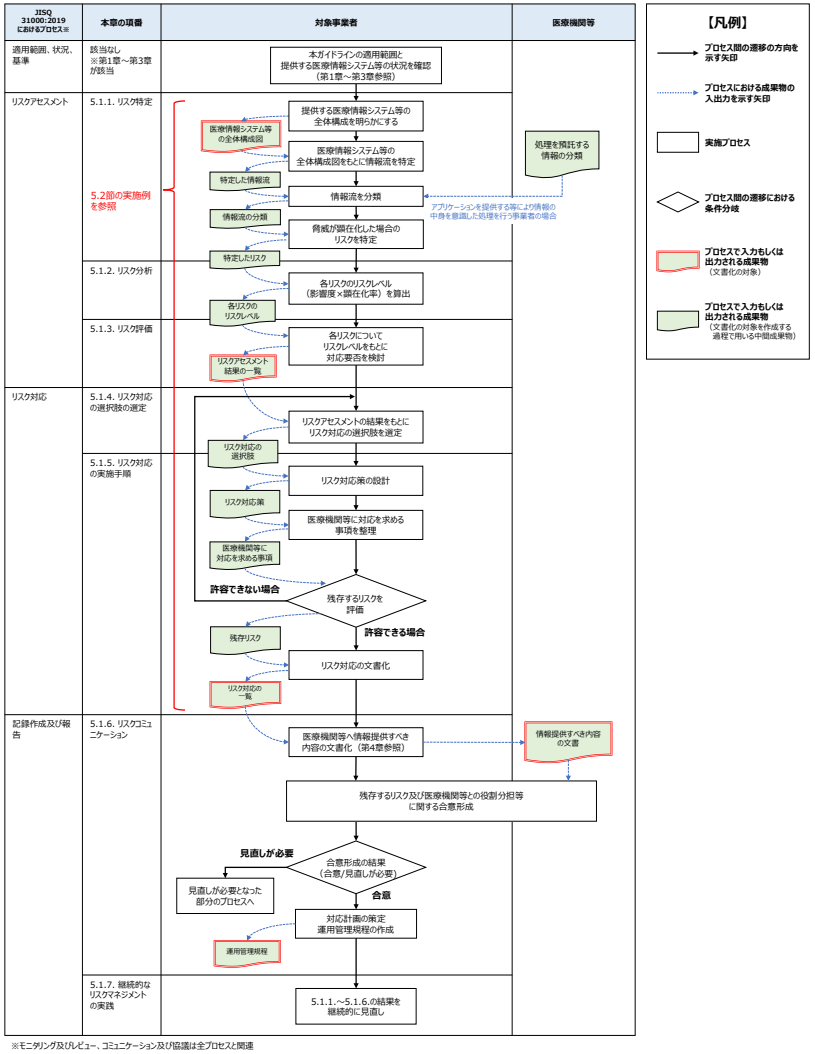
対象事業者と医療機関等が容易に合意形成することができるよう、情報提供すべき内容として記載すべき項目の参考例であり、対象事業者はサービス仕様適合開示書を医療機関等に提供し、医療機関等はこれに基づいて医療情報システム等の選択を行い、両者はその内容を踏まえた形でサービス内容の合意を図ることを想定している。なお、本開示書はその一つの例示であり、本開示書の作成・提供は必須ではないが、対象事業者は、このような開示書等を用いて、医療機関等に対して対応状況を開示・説明した上で、合意形成を図ることが求められる。

安全管理のためのリスクマネジメントプロセス

- 対象事業者は、医療情報システム等を提供する際には、本ガイドラインで定めるリスクマネジメントプロセスに基づき、想定されるリスクを洗い出し、必要な対策を導出します。
- リスクマネジメントプロセスは、大きく以下の3つのプロセスに分類されます。
  1. リスクアセスメント
  2. リスク対応
  3. 記録作成及び報告

5. 安全管理のためのリスクマネジメントプロセス

対象事業者は、図5-1のプロセスに従い、医療情報システム等を提供する際に想定されるリスクを洗い出し、必要な対策をとりまとめること。

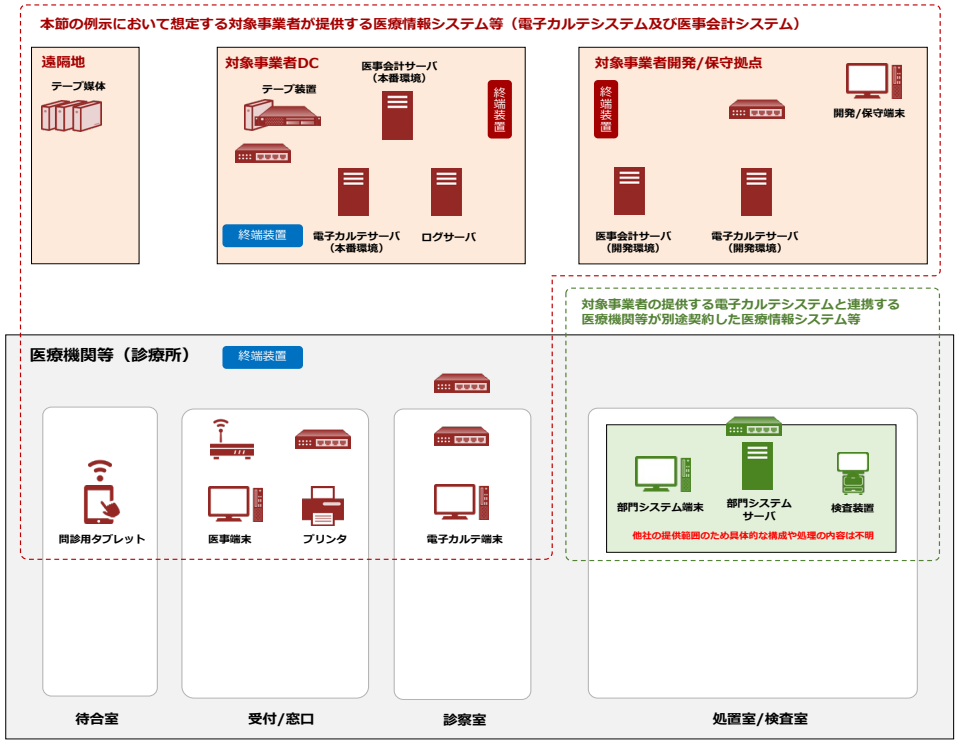


リスクアセスメントの実施手順

- 「リスクアセスメント」は、「リスク特定」→「リスク分析」→「リスク評価」の流れで実施します。当該作業の結果、以下の成果物が作成されることを想定します。
  - （１）リスク特定における医療情報システム等の全体構成図
  - （２）リスク特定における情報流
  - （３）リスク特定・リスク分析・リスク評価の結果

5.2.1 リスクアセスメント

(1)リスク特定における医療情報システム等の全体構成図（例）



(2)リスク特定における情報流（例）

Who（誰が）	Where（どこの/どこを）	Which（どの機器で/どの媒体で）	What（何を/何が）	How（どうするか/どうされるか）
患者が	待合室の	問診用タブレットで	患者情報等を	閲覧・操作する
医療事務/看護師等が	受付/窓口の	医事端末で		
		プリンタで	レセプト等を	帳票出力する
医師/代行入力者等が	診察室の	電子カルテ端末で	患者情報/オーダ/検査結果/診療録/診療諸記録等を	閲覧・操作する
医師/看護師/臨床検査技師等が	処置室/検査室の	電子カルテシステムと連携する他社が提供するシステムで	オーダ/検査結果等を	処理する
―	対象事業者DCの	電子カルテサーバ（本番環境）で	オーダ/検査結果/診療録/診療諸記録等が	作成や保存される
		医事会計サーバ（本番環境）で	レセプト/処方箋/患者情報等が	
		ログサーバで	アプリケーションのログが	保存される

(3)リスク特定・リスク分析・リスク評価の結果（例）

リスク特定					リスク分析			リスク評価
情報流	分類	関連する脅威	特定したリスク		影響度	顕在化率	リスクレベル	対応要否
医療事務/看護師等が受付/窓口の医事端末で患者情報等を閲覧・操作する	患者個人情報	不正な閲覧・操作	受付/窓口の医事端末において	正当な者以外による患者個人情報の不正な閲覧や作成、更新が行われる	5	3	A	要
				・・・				
		情報の改ざん・破壊		故意又は過失による虚偽入力、書き換えにより患者個人情報の改ざん・破壊が行われる	5	3	A	要
				・・・				
		医療情報システム等の停止		アプリケーション停止により、患者個人情報が見読不可となる	5	3	A	要
				・・・				
		技術的脆弱性の混入		アプリケーションに混入した脆弱性の悪用により患者個人情報の漏えい・改ざん・破壊が行われる	5	3	A	要
				・・・				
		・・・						
・・・								

リスクアセスメントにおける留意点

- **「リスク特定」における情報流の洗い出しにおいて、特にクラウドサービスで医療情報システム等を提供する際には、ICTサプライチェーン全体を含めて情報流を洗い出します。**

5.1.1 リスク特定

対象事業者は、自らが提供する医療情報システム等の全体構成図を作成することで、医療情報システム等の全体構成を明らかにすること。その上で、医療情報システム等の全体構成図をもとに、医療情報システム等のライフサイクルにおけるフェーズ毎の情報流を特定すること。本ガイドラインでは、医療情報システム等の提供に関わる情報の流れを「情報流」と定義する。情報流にはネットワークを介した電子的な情報の流れだけでなく、記憶媒体の搬送により発生する情報の移動も含まれる。全体構成図をもとに情報の作成及び参照、更新、保存、移送、廃棄等の処理を洗い出すと、構成要素間で情報がどのように流れるのかが明らかになるため、結果として情報流が特定される。このとき、情報流を洗い出す範囲には、ICTサプライチェーン全体を含めること。特に、医療情報システム等をクラウドサービスとして提供するケースにおいては、ASP・SaaSとPaaS、IaaSをそれぞれ別の事業者が提供する等、ICTサプライチェーンが複雑となる傾向にあるため、抜け漏れがないよう十分留意すること。

リスク特定の実施手順

➢ 「リスク特定」は以下の手順で実施します。

5.2.1 リスクアセスメント

（１）リスク特定における医療情報システム等の全体構成図の作成

【手順1】どこにどのような機器や記憶媒体があるかを明らかにする

【手順2】機器同士の接続や記憶媒体の搬送を明らかにする

【手順3】人が扱う機器や記憶媒体における情報の処理を明らかにする

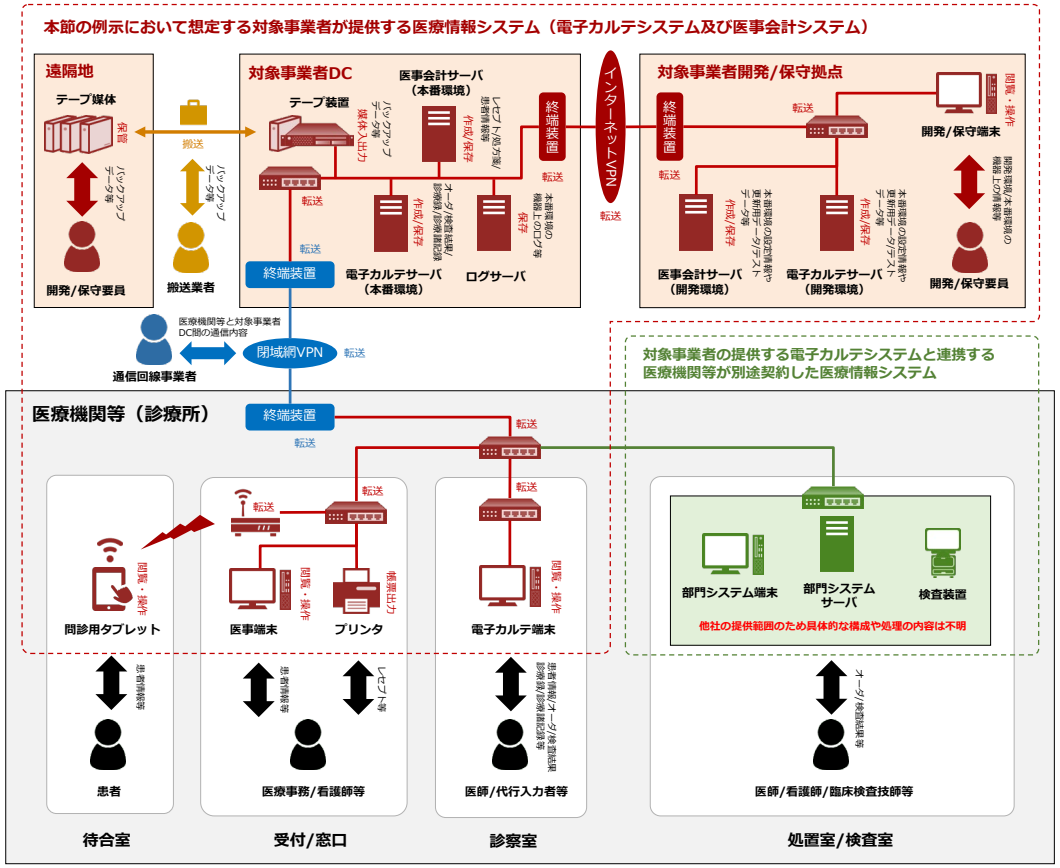
例）

- 患者が、待合室の、問診用タブレットで、患者情報等を、閲覧・操作する
- 医師/看護師/臨床検査技師等が、電子カルテシステムと連携する他社が提供するシステムで、オーダ/検査結果等を、処理する

【手順4】人が直接扱わない機器における情報の処理を明らかにする

例）

- 受託事業者DCの、医事会計サーバで、レセプト/処方箋/患者情報等が、作成・保存される



リスク対応の実施手順

- 「リスク対応」は、「リスク対応の選択肢の決定」→「リスク対応策の設計・評価」の流れで実施します。当該作業の結果、以下の成果物が作成されることを想定します。
  （１）リスク対応一覧表

5.2.2 リスク対応

リスク対応									
対応するリスク		対応	対策の観点	対象事業者が実施する対策	医療機関等へ対応を求める事項	残存するリスク			
							影響度	顕在化率	リスクレベル
受付/窓口の医事端末において	正当な者以外による患者個人情報の不正な閲覧や作成、更新が行われる	低減	人的・組織的対策	―	医療機関等の職員への内部不正防止のための教育や、患者等による画面の覗き見防止のための医事端末のレイアウト調整については、医療機関等にて実施をお願いいたします。	―			
			物理的対策	―					
			技術的対策	医事端末のアプリケーション利用に際して、利用者を一意に識別するID/パスワード（8桁以上英数大文字小文字混合）による認証と静脈による多要素認証を実装する。					
				・・・					
	故意又は過失による虚偽入力、書き換えにより患者個人情報の改竄・破壊が行われる	低減	人的・組織的対策	誤操作防止のための医療機関等の利用者向けマニュアルを提供する。	医療機関等の職員への内部不正や誤操作防止のための教育については、医療機関等にて実施をお願いいたします。	―			
				・・・					
			物理的対策	―					
			技術的対策	患者個人情報の更新や削除に係る履歴を、ログとして取得する。なお、法定保存期間が定められた情報に関しては当該期間の間ログを保存し、それ以外の情報については1年間ログを保存する。					
				・・・					
・・・									

リスク対応時の留意事項

- **「リスク対応策の設計・評価」にあたっては、医療機関等が医療情報安全管理ガイドラインを遵守できるよう、医療情報システム等の特有の考慮事項も踏まえたリスク対応策の設計が必要です。**

5.1.5 リスク対応策の設計・評価

(1)リスク対応策の設計

対象事業者は、リスク対応策について、次に示す基本的な考え方と医療情報システム等特有の考慮事項を踏まえて設計すること。

(ア)基本的な考え方

対象事業者は、対策の設計にあたっては、医療機関等が医療情報安全管理ガイドラインを遵守できるような設計となっていることについて、3.1.2で述べた説明義務を有していることに留意しなければならない。ここで、対策の設計や、設計した対策の妥当性を判断するにあたっては、高度な専門性が要求されるが、従前の情報処理事業者ガイドライン及びクラウド事業者ガイドラインの要求事項を医療情報安全管理ガイドライン（第5版）との対応関係を踏まえ対策項目として整理・統合した別紙2を用い、その全ての対策項目についての確認をすることは、対象事業者による対策の設計や妥当性の判断、説明義務への対応において必須である。（中略）

(イ)医療情報システム等特有の考慮事項

対象事業者は、対策の設計にあたっては上記で示す基本的な考え方に加え、以下に記載する医療情報システム等特有の考慮事項を参照し、必要な対策を設計すること。

リスク対応策の設計時の参考資料

- **対象事業者は、リスク対応策の設計や、設計した対策の妥当性を判断するにあたって、別紙２に記載のある全ての対策項目について、対応しているかどうかを確認をする必要があります。**
- **別紙2に記載されている対策を採用していない（しない）場合は、合理的な理由（例：代替措置がある、スコープの対象外である等）を説明できるようにしておく必要があります。**

別紙2 旧ガイドラインにおける対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
1. 人的・組織的対策								
1.1. 規程・手順の策定	①アクセス管理規定の策定	①-1	医療情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規定を作成し、医療機関等の求めに応じて提出できる状態にしておく。	◎	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	6.3 組織的安全管理対策（体制、運用管理規程）	C.最低限のガイドライン	3.情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。
		①-2	アクセス管理規定には以下の内容を含める。 ・アクセス権限、アカウント管理における登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセス ・認証及びアクセス等に対する記録の収集と保存 ・認証及びアクセス等に対する記録の定期的なレビュー ・アクセス管理の運用状況に関する定期的なレビューの実施	◎				
	②持ち出した機器の外部のネットワークに接続する場合の対策の策定	②-1	持ち出した機器を外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改竄が生じないようにするための具体的な措置（不正プログラム対策、暗号化、ファイアウォール導入等））を運用管理規程に含める。	◎	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	6.5 技術的安全対策	C.最低限のガイドライン	10.システム構築時、運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。運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運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。

従前の情報処理事業者ガイドライン及びクラウド事業者ガイドラインの要求事項を、「人的・組織的」・「物理的」・「技術的」の３つの対策の観点毎に整理・統合した内容

対策項目により対策可能となる、代表的なリスクシナリオを例示

関連する医療情報安全管理ガイドラインの要求事項

リスクコミュニケーションの実施内容

- **リスクコミュニケーションでは、「医療機関等とのリスクコミュニケーションの実施」及び「文書・規程の作成」を実施します。**
- **リスクコミュニケーションは、リスクアセスメントやリスク対応の内容を医療機関等に情報提供するといった限定的なものではなく、リスクマネジメントのあらゆるプロセスにおいて、その実効性を高めるために実施される活動である点に留意する必要があります。**

5.1.6 リスクコミュニケーション

(1)医療機関等とのリスクコミュニケーションの実施

対象事業者は、自らが提供する医療情報システム等の安全管理に係る説明義務を果たし、医療機関との共通理解を形成するために、医療機関等に対して第4章で情報提供すべき内容として示した事項を含む必要な情報を文書化して提供すること。具体的には、5.1.5で作成した「リスク対応一覧」や後述の運用管理規定に定められた事項に係る情報提供を通して、医療機関等との役割分担、対象事業者として受容したリスクの内容等について、医療機関等と合意形成を図ること。なお、その際には、対象事業者は、医療機関等が容易に理解可能となるよう内容を工夫する等、適切に共通理解を得ること 。

なお、医療機関等と合意に至らなかった場合は、対象事業者はリスク対応事項の見直し結果に基づく再協議、残存するリスクの共通理解に向けた再協議等、医療機関等と再度合意形成を図ること。

(2)文書・規定の作成

対象事業者は、医療機関等と合意したリスクへの対応を踏まえ、リスクに対する対応計画を策定すること。（以下略）

制度上の要求事項

- **医療機関等へ医療情報システム等を提供するにあたっては、リスクマネジメントに基づく対応とは別に、制度上の要求事項として、法令等の制度上の要求事項への遵守の観点から、一律の対応を求められる要求事項があります。**

6.制度上の要求事項

6.1. 医療分野の制度が求める安全管理の要求事項

6.2. 電子保存の要求事項

6.3. 法令で定められた記名・押印を電子署名に代える場合の要求事項

6.4. 取扱いに注意を要する文書等の要求事項

6.5. 外部保存の要求事項

ガイドライン関連文書

- 本ガイドラインでは、第4章に基づく医療機関等との情報提供と合意形成にあたって活用することを想定した「別紙1 サービス仕様適合開示書及びSLAの参考例」（以下、「別紙1」という。）及び第5章に基づくリスクマネジメントの実践において事業者が確認する内容として、「別紙2 旧ガイドラインにおける対策項目一覧と医療情報安全管理ガイドラインの対応表」（以下、「別紙2」という。）を用意しています。

- また、本ガイドラインの理解を深めるため「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドラインFAQ」を用意しています。