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

本 FAQ はガイドラインに記載されている内容をより理解しやすくするため、基本的な考え方をまとめたものです。

目次

1.　ガイドラインの対象範囲（基本的な考え方）

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）を提供する事業者としています。基本的に、医療機関等から医療情報を受け取り、加工や保存等の処理に関連する医療情報システム等を提供している場合が対象範囲となります。具体的には、医療情報（電子カルテ、レントゲンや CT 画像等）の外部保存サービス、クラウド型電子カルテサービス、医療機関の医療情報システム等と接続されたオンライン診療システム等が該当します。

1.1.　医療機関等自らが医療情報を処理するシステムはガイドラインの範囲か？

医療機関等が、その医療機関等内において、対象事業者に委託等することなく、自ら医療情報を取り扱っている場合は本ガイドラインの対象範囲外となります。例えば、放射線科情報システム（RIS）や医療用画像管理システム（PACS）等のシステム製品販売事業者が、契約に従った製品の納入をもってその後の保守管理もなく売買契約が完了し、その後は購入した医療機関等の責任において管理・運用される場合、本ガイドラインの対象範囲外となります。

2.　医療情報システム等の提供形態（基本的な考え方）

本ガイドラインでは、医療情報システム等は、サプライチェーン全体を通して、適切に運用されるべきというのが基本的な考え方です。本ガイドラインは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機能している場合、本ガイドラインの適用範囲と考えます。例えば、事業者 A が病院にクラウド型電子カルテサービスを提供し、事業者 A はアプリケーションとプラットフォームを事業者 A が選定した事業者 B のインフラ上で稼働させる場合、事業者 A は事業者 B のインフラが、医療情報システム等のサプライチェーンの一部として、本ガイドラインに沿ったサービスを提供しているか確認すべきであるというのが基本的な考え方です。

近時、ネットワークシステムの高度化により、機能分化、専門化が進んでいます。SaaS、PaaS、IaaS という言葉に代表されるように、アプリケーション、プラットフォーム、インフラをそれぞれ異なった事業者が提供することも珍しくありません。それぞれの事業者がサービスを提供することで高度なセキュリティが期待される一方で、ある一つの機能のセキュリティ上の欠陥から問題が生じることもあり得ます。例えば、医療機関等がクラウド型電子カルテサービスの導入を検討しており、SaaS 事業者と導入について話し合いを進める際、その医療機関等や SaaS 事業者が PaaS や IaaS 事業者の選定に注意を払わなかった場

合、医療情報の漏洩をはじめとしたセキュリティ上のリスクは高まります。

本ガイドラインでは「2.2. 医療情報システム等の代表的な提供形態」において、医療情報システム等の代表的な提供形態を示し、システム全体がガイドラインの適応範囲であり、サプライチェーン全体を考慮しながら、医療情報システム等は運用されるべき旨を記述しています。

2.1. 複数関係者のリスクマネジメントはどうすべきか？

医療情報システム等がマルチクラウドやマルチベンダーで運用される場合があります。具体例として、ガイドラインの「2.2.2. 複数の事業者が提供するケース」と「2.2.3. 医療機関等が複数社と契約するケース」が挙げられます。

「2.2.2. 複数の事業者が提供するケース」のケース 1 では、事業者 A が他の事業者 B を選定した上で直接契約し、事業者 B の構成要素を含めてリスクマネジメントを行い、医療機関等と合意形成を行います。

一方、「2.2.3. 医療機関等が複数社と契約するケース」では、事業者 A は、事業者 B の選定に関与しておらず、事業者 AB 間で直接的契約がなされていません。「2.2.2. 複数の事業者が提供するケース」とは異なり、事業者 A は事業者 B に対してリスクマネジメントを行うことはできず、医療機関等は事業者 B に対してリスクマネジメントを確認する必要があります。

事業者 A が事業者 B のシステムについて医療機関等を通じて把握できれば良いのですが、事業者 A は事業者 B のシステムについて不明である場合があります。その場合、事業者 A がアプリケーション及びプラットフォームを医療機関等に提供する際には、事業者 B の構成要素を含めた上で、つまり不明なインフラ上で事業者 A のシステムが利用される場合には、どのようなリスクがあるのか医療機関等に対して伝え、事業者 A の負う責任の範囲を明確化し、合意形成した上で、事業者 A のシステムを医療機関等に提供することになります。

また、事業者 A が事業者 B を調達しても、契約上は、医療機関等と事業者 B が直接契約する場合もあります。その場合、事業者 A は事業者 B の構成要素は不明ではなく、具体的に把握しているため、「2.2.2. 複数の事業者が提供するケース」と同様、事業者 A は事業者 B の構成要素の内容を含めてリスクマネジメントを行い、医療機関等と合意形成を行います。

医療情報システム等がマルチクラウドやマルチベンダーで運用される場合、ある事業者の提供サービスや契約の変更が、他の事業者の提供サービスに影響を及ぼすことがありま

す。関係者間でサービスや契約変更に関する通知などの責務について検討、合意形成が重要と考えられます。

2.2. 地域医療連携ネットワークの取扱いはどうなるのか？

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」では、医療情報連携ネットワークが対象範囲となる場合がある旨を記述していました。本ガイドラインでも同様の扱いとなります。

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対象事業者として位置づけられると考えられます。例えば、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す。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ます。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役割分担を契約等により合意した上で対応する必要があります。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、委託先の事業者を監督し、管理責任を果たすことが求められます。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対象事業者とはなりません。

3. 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（基本的な考え方）

ガイドラインの「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」は、医療機関等と対象事業者間における義務と責任についての合意形成の重要性を示しています。当該箇所は、医療機関等と対象事業者間の合意形成に焦点を当てて書かれていますが、本 FAQ の「2 医療情報システム等の提供形態」で述べているサプライチェーン全体においても適応可能なものです。例えば、事業者 A のアプリケーションを事業者 B のプラットフォームとインフラ上で利用する場合の事業者 AB 間の義務と責任の合意形成を考える際にも適応できます。

3.1. 運用フェーズと開発フェーズで事業者が異なる場合があるのではないか？

医療情報システム等のライフサイクルは、運用フェーズだけでなく、運用開始前もしくは

運用開始後の開発フェーズがあります。医療情報システム等の運用と開発が別事業者になる場合があり、そのような複数社が関与する場合においても、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について関係者間で合意形成しておく必要があります。例えば、事業者 A が運用を担当し、事業者 B が開発を担当し、医療機関等は事業者 A のみとの契約関係にある場合です。医療機関等は事業者 A との間で運用と開発に関する義務と責任について明確化し、合意形成しておく必要があります。事業者 A は事業者 B との間で開発に関する義務と責任について明確化し、合意形成しておく必要があります。

4. 対象事業者と医療機関等の合意形成（基本的な考え方）

医療情報システム等を適切に利用・運用するためには、対象事業者と医療機関等で適切な合意形成が必要です。適切な合意形成のために、両者で必要な安全管理のための情報の共有、役割分担の明確化、医療情報システム等の安全管理に係る評価の共有等がなされる必要があります。

4.1. 医療機関等へ情報提供すべき項目以外の情報提供は必要ないのか？

本ガイドライン「4.1. 医療機関等へ情報提供すべき項目」は、対象事業者と医療機関等で適切な合意形成のために必要となる情報を掲載しています。両者で適切な合意形成ができる程度まで情報共有が必要なので、ここで記載されていない項目についても、必要があれば情報共有することが望ましいと考えます。

また、表 4-1 は、①「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」と②「医療機関等との共通理解を形成するために情報提供すべき項目」の２つの目的で分類していますが、例えば、①の項目は合意形成過程の初期段階における情報提供項目として、②の項目は契約に向けて具体的な話が進んだ段階で合意形成の内容を深めるための情報提供項目として利用することが考えられます。

4.2. プライバシーマーク認定/ISMS 認証の取得と本ガイドラインとの関係の考え方は？

本ガイドラインにおいては、医療情報を取り扱う対象事業者に対して、情報セキュリティに係る公的な第三者認証として、プライバシーマーク認定または ISMS 認証の取得を求めています。しかし、これらの認証は、医療情報に限らず、個人情報の取扱いに関し、適切な体制を整備していることを示すものであり、あくまで最低限の適格性を医療機関等へ示す

手段として捉えています。本ガイドラインの求める医療情報の適切な取扱いとは位置づけや求める内容も異なり、これらの認証の取得をもって、本ガイドラインの安全管理水準を満たすわけではありません。

5. 安全管理のためのリスクマネジメントプロセス（基本的な考え方）

厚生労働省「医療情報システムの安全管理に関するガイドライン」の第 4 章にある通り、医療情報の最終的な管理者としての責任は医療機関等にあります。その責任を完遂させるため、医療情報システム等を提供する事業者は、医療情報の適切な利用と保護を目的に安全管理のためのリスクマネジメントを実施し、その結果をもとに医療機関等と適切な合意形成を図るべきというのが、本ガイドラインの基本的な考え方です。

5.1. 対象事業者はリスク移転とリスク保有を行ってよいのか？

本ガイドラインは、一般的なリスクマネジメント手法をもとに、リスク対応の選択肢として、「リスク低減」、「リスク回避」、「リスク移転」、「リスク保有」の 4 つを提示しています。本ガイドラインは、医療情報の安全な管理を目的としているため、安易にリスク移転やリスク保有を採用することは適当ではなく、推奨していません。しかし、どれほどリスク低減を行ったとしても、リスクはゼロにならず、最終的にリスク移転またはリスク保有を選択せざるを得ない場合もあり得ます。安全管理のためのリスクマネジメントは、本 FAQ の「5 安全管理のためのリスクマネジメントプロセス（基本的な考え方）」で述べている通り、医療情報の適切な利用と保護のため、リスクマネジメントの結果をもとに医療機関等と適切な合意形成を図って、医療情報システム等を適切に運用していくためのものです。対象事業者の判断のみによってリスク移転やリスク保有を選択することは適当でなく、医療機関等への説明や合意形成の上、これを選択することが必要です。

5.2. 残存するリスクをどのように考えるべきか？

残存するリスクの対応は、「5.1.5. リスク対応の実施手順、(3) 残存するリスクの評価」に記述されています。残存するリスクについては、対象事業者は（定期的に）再評価し、医療機関等と合意形成していく必要があります。

ガイドラインの「5.1. リスクマネジメントの実践」では、対象事業者が実施すべきリスクマネジメントのプロセスを解説しています。対象事業者は、「リスク特定」、「リスク分析」、「リスク評価」、「リスク対応」等を実施し、継続的なリスクマネジメントをしていきます。

一例として、事業者がクラウド型カルテサービスを医療機関等に提供する場合の医師のログイン認証（ID と 4 桁のパスワード認証）について考えてみます。対象事業者は不正ログインというリスク特定をし、機微性の高い患者情報と 4 桁というパスワードを考慮して影響度と顕在率の高さからリスクレベルは極めて高いとリスク分析し、リスクレベルの高さから対応が必要とリスク評価し、パスワードの桁数を増やすというリスク低減策でリスク対応を図ります。リスク対応は対象事業者だけで完結するものではなく、医療情報システム等を利用する医療機関等にも対応を求めることもあります。例えば、様々な患者やスタッフが行き交う診察室の端末にパスワードを貼り付けておかないなどです。パスワードの桁数を増やすという対応は、その時点において、対象事業者は残存リスクとして許容できたとしても、情報技術の進展によるセキュリティの危殆化から、対象事業者として多要素認証を用いるべきであると判断する場合が出てきます。その場合、対象事業者はリスク対応方法について再度検討し、医療機関等とあらためて合意形成を図ることになります。

5.3. 別紙 2 の取扱いをどう考えれば良いか？

本ガイドラインは、リスクベースアプローチを採用しています。医療情報システム等のリスク特定、リスク分析、リスク評価、リスク対応といったプロセスをもとに、リスクマネジメントを継続的に実施し、医療情報システム等の適切な運用を図っていきます。言い換えれば、ある特定の要求事項を最低限満たすことを目的としていません。

別紙 2 は、従前の経済産業省「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」及び総務省「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」の要求事項を、厚生労働省ガイドラインとの対応関係も踏まえ対策項目として整理・統合したものです。別紙 2 は、医療情報システム等の運用が適切であるか、リスクマネジメントを通じて、最低限確認するためのものと位置づけています。リスク分析の結果、適切であるならば、別紙 2 に記載されていない対策（代替策を含む）、記載されていること以上の対策の実施を妨げるものではありません。別紙 2 は ISMS の附属書 A 管理策に近い位置づけと考えることができます。

ただ、基本的に、適切なリスクマネジメントを実施していれば、別紙 2 で求められている対策項目と同等又はそれ以上の対策は実施されるものと考えています。別紙 2 で求められる対策を採用しない場合は、合理的な理由（例：当該医療システムとは関係のない事項である、要求事項の代替措置がある等）が必要です。

5.4. 医療情報システム等特有の考慮事項はどう考えるべきか？

ガイドライン「5.1.5. リスク対応の実施手順、(1) リスク対応策の設計、(イ) 医療情報システム等特有の考慮事項」では、現行の厚生労働省「医療情報システムの安全管理に関するガイドライン」（第 5 版）も踏まえつつ医療情報システム等特有の考慮事項をまとめています。しかし、この考慮事項は当該厚生労働省ガイドラインの改訂等とともに、変更される可能性（例えば、VPN や無線 LAN の技術的な項目）があります。対象事業者は医療情報システム等を医療機関に提供する場合、最新の厚生労働省ガイドラインの内容について考慮し、リスクマネジメントの結果にもとづいて、適切な対策を実施する必要があります。

6. 対象事業者と医療機関等とのリスクコミュニケーション（基本的な考え方）

対象事業者にとって、自らが提供する医療情報システム等やそのリスクについて医療機関等に説明することは、対象事業者と医療機関等との共通理解を深め、互いの役割について合意形成する上で有効であると考えます。ガイドラインの第 4 章での対象事業者として医療機関等に対して情報提供すべき内容を示したり、第 5 章でのリスク対応一覧や運用管理規程に定められた事項を情報共有したりすることは、対象事業者と医療機関等との間のリスクコミュニケーションにおいて役立つものと考えられます。

6.1. 文書や規程にどこまでの内容を記載すべきか？

ガイドライン「5.1.6. リスクコミュニケーション、(2) 文書・規程の作成」では、対象事業者が安全管理義務を果たすために、医療機関等と合意形成した結果を文書化し、運用管理規程を定めるように求めています。運用管理規程に含める項目の最低限の具体例として、(ア)～(コ)を挙げていますが、これに限るわけではありません。内容については、リスクコミュニケーションを通じて、両者が納得できる程度にまで、記載されている必要があります。例えば、「(エ) 機器等を用いる場合の機器等の管理方法」では、機器等の管理方法について台帳管理等による所在確認を行う旨を運用管理規程に含めることを求めています。対象事業者が医療機関等にクラウド型電子カルテサービスを提供し、それへのアクセスのために専用の PC 端末またはタブレットを配布する場合、台数の確認や利用場所を限定について、必要な範囲で運用管理規定に記載する必要があります。

7. 制度上の要求事項（基本的な考え方）

本ガイドラインは、リスクベースアプローチを採用しており、リスクに応じて適切な安全

管理措置を選択して実施するように求めています。一方で、法令等で義務付けられている項目があり、それらについては一律に対応する必要があります。

7.1. 制度上の要求事項はどのようなものがあるか？

制度上の要求事項は本ガイドラインの第 6 章において整理しています。例えば、e-文書法や電子署名及び認証業務に関する法律に係る対応があります。それらの要求事項は、本ガイドライン（別紙を含む）のみによることなく、各文書を参照の上対応する必要があります。