# 医療情報システムの安全管理に関するガイドライン

第 7.0 版

Q&A

# 目次

## 概説編　Q&A


ガイドラインの使い方　（Q1～Q3）……1
適用範囲　（Q4～Q7）……2
利用時の基本的な安全管理　（Q8～Q10）……2


## 経営管理編　Q&A


経営層の責任・法令遵守　（Q1～Q4）……4
委託先管理・責任分界　（Q5～Q7）……5


## 企画管理編　Q&A


基本方針・リスク管理　（Q1～Q4）……6
責任分界・契約　（Q5～Q11）……6
第三者提供・共同利用　（Q12～Q15）……8
委託先・外部保存　（Q16～Q25）……10
医療情報の持出し・提供・破棄　（Q26～Q31）……12
非常時対応・BCP　（Q32～Q33）……13
本人確認・電子署名　（Q34～Q40）……14
紙媒体・スキャン　（Q41～Q45）……16


## システム運用編　Q&A


標準化・相互運用性　（Q1～Q4）……17
保存・見読性　（Q5～Q12）……17
マルウェア・保守　（Q13～Q20）……19
非常時対応・バックアップ　（Q21～Q25）……21
ネットワーク・VPN・無線 LAN　（Q26～Q32）……21
ID・利用者認証　（Q33～Q35）……24
真正性・電子署名　（Q36～Q43）……24

## 保守委託機関編　Q&A

保守委託機関編の適用対象　（Q1～Q3）…… 28
MDS/SDS・別紙　（Q4～Q7）…… 28

# 概説編　Q&A

## ガイドラインの使い方

**Q1**　本ガイドラインは、医療機関等の関係者のみを対象としたものか。医療情報システムに関係する事業者も理解する必要はあるのか。また、事業者が遵守すべきガイドラインには、他にどのようなものがあるのか。

**A**　事業者も本ガイドラインを理解し、2 省ガイドラインを遵守する必要があります。

医療機関等は安全管理の一次的な責任を負いますが、事業者と役割・責任を分担して対策を実施してください。事業者は、総務省・経済産業省の「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」も遵守し、医療機関等との協働に必要な情報を提供してください。

（参照：概説編 3.1.1～3.1.5、4.4・4.5／企画管理編 1 章 遵守事項②）

**Q2**　旧版の本ガイドラインの本編や別冊や別添等、全て理解する必要があるか。

**A**　旧版を読む必要はなく、最新版を参照してください。

旧版の内容は、最新版で変更又は削除等されている場合があるため、最新版をお読みください。

（参照：概説編 1 章・3 章）

**Q3**　本ガイドラインの説明会や研修会等についての情報はどこで確認できるのか。

**A**　ガイドライン全体像についての説明会はありません。一方で、ガイドラインに関連した研修は、厚生労働省の研修ポータルで実施しています。

受講方法は、医療情報セキュリティ研修ポータル（https://mist.mhlw.go.jp/）で最新情報を確認してください。

（参照：経営管理編 3.2.2、3 章 遵守事項⑨）

## 適用範囲

**Q4**　介護事業者は本ガイドラインを遵守する必要があるか。

**A**　介護事業者が医療情報を情報システムで扱う場合は対象です。

介護事業者は「医療機関等」に含まれ、医療情報を含む文書は保存義務の有無を問わず対象となるためです。

（参照：概説編 2.1・2.2）

**Q5**　他の医療機関等から提供された電子化された情報を取扱う場合は、本ガイドラインの対象となるのか。

**A**　他の医療機関等から提供された情報を取り扱う場合も、その情報が医療情報であれば対象です。

対象かどうかは情報の作成元ではなく、医療に関する患者情報を電子的に扱うかで判断してください。

（参照：概説編 2.2・2.3）

**Q6**　電子保存が認められている文書とは具体的に何か。

**A**　電子保存できる文書は、関係法令ごとに確認する必要があります。

対象文書は、e-文書法、厚生労働省令、関係通知等で定められています。本ガイドラインは、保存義務の有無を問わず医療情報を含む文書全般を対象としています。

（参照：概説編 2.2･4.3／企画管理編 1.1.2）

**Q7** 「医療情報システム」とは具体的に何を示すのか。

**A** 医療情報を扱うシステム・端末・ネットワーク全般を指します。

電子カルテ、レセコン、部門システムのほか、医療情報を保存・閲覧する端末や、その情報が流れる院内外のネットワークも含まれます。

（参照：概説編 2.3）

## 利用時の基本的な安全管理

**Q8** オンライン資格確認や電子処方箋の導入において、どのような留意事項があるか。

**A** 公式の導入資料と本ガイドラインの双方に従う必要があります。

接続する端末、ネットワーク、認証、ログ、委託先との責任分界等について本ガイドラインを満たす必要があります。公式情報は「オンライン資格確認について」及び「電子処方箋」の厚生労働省ページで確認してください。

・厚生労働省 オンライン資格確認について（医療機関・施術所等、システムベンダ向け）
https://www.mhlw.go.jp/stf/newpage_08280.html

・厚生労働省 電子処方箋
https://www.mhlw.go.jp/stf/denshishohousen.html

（参照：概説編 4.3･4.6／システム運用編 13 章 遵守事項①～⑬）

**Q9** 医療情報を電子的に保存するに当たって定められた要件は何か。また、情報セキュリティの 3 要素（機密性・完全性・可用性）との違いはあるか。

**A** 医療情報を電子的に保存する場合は、真正性、見読性及び保存性を確保する必要があります。これは e 文書法令に基づき、適切に電子保存するための要件となります。

・真正性：保存された情報が作成者の意思どおりに作成され、その後不正に作成・改ざん・消去されていないことを確認できること。

・見読性：必要なときに人が読める形で表示又は出力できること。

・保存性：法令等で定められた保存期間を通じて、情報を復元可能な状態で保存できること。

一方、情報セキュリティの 3 要素は「機密性・完全性・可用性」であり、情報セキュリティ全般の原則となります。

・機密性：権限のない者に情報を閲覧・利用されないこと。

・完全性：情報が正確かつ完全であり、不正又は意図しない改ざんが行われていないこと。

・可用性：必要なときに情報やシステムを利用できること。

本ガイドラインでは、情報セキュリティの三要素を踏まえた安全管理措置を講じることが求められており、両者は対立するものではなく、相互に補完する関係にあります。

（参照：概説編 4.2･4.3／企画管理編 1.1.2）

**Q10** SNS 等の Web サービスを利用して医療情報をやり取りする場合、考慮するべきことはあるか。

**A** SNS 等の Web サービスは利用可能ですが、医療情報システムとして安全性を評価する必要があります。

一般向け SNS を安易に利用せず、利用前に認証、アクセス制御、通信・保存時の暗号化、ログ、保存・削除、事故対応及び責任分界を確認してください。MDS/SDS やサービス仕様適合開示書等を事業者から入手し、リスク評価の上で採否を決めます。

特に、SNS の場合、セキュリティが十分に確保されていないサービスもあることから、一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）が公表している「医療情報連携において、SNS を利用する際に気を付けるべき事項」（https://hispro.or.jp/open/pdf/SNS_RiyouCheckJikou_20160126.pdf）を参考に、適切な対策を講じてください。

また、第 7.0 版では、医療情報システムの安全管理上のリスク評価・管理を実施するに当たり、医療情報システム・サービス事業者から技術的対策等の情報を収集することの重要性が強調されています（４．５ リスク評価とリスク管理）。具体的には、厚生労働省標準規格（HS040）として定められた「MDS/SDS（製造業者/サービス事業者による医療情報セキュリティ開示書）」のチェックリストや、２省ガイドラインにおける「サービス仕様適合開示書」等の提供を事業者に求め、当該事業者とリスク管理に関する合意形成（リスクコミュニケーション）を図ることが求められています

（参照：概説編 4.5～4.7／企画管理編 2.1.4・7.4／システム運用編 4 章 遵守事項③）

# 経営管理編　Q&A

## 経営層の責任・法令遵守

**Q1**　電子的な医療情報を扱う責任を果たすうえで、経営層の人はどのようなことを理解すればよいか。

**A**　経営層が責任を持ち、安全管理を経営課題として統制する必要があります。

法令遵守、リスク評価、予算・人員、責任体制、委託先管理、インシデント対応を経営層が統制します。

第 7.0 版の経営管理編では、医療 DX の進展に伴いサイバー攻撃の脅威が一層深刻化していることを踏まえ、経営層に対して次の点が新たに強調されています。

・情報セキュリティインシデントが起きた場合、医療の提供が停止し患者の生命・身体に影響を与える可能性があること、行政処分の対象となるリスクや民事上の賠償責任を負うリスクがあること

・安全管理対策の実施を「コスト」と捉えるのではなく、質の高い医療の提供等に不可欠な「投資」と捉え、その実施に必要となる資源（予算・人材等）の確保に努めること

・サイバー攻撃の脅威に鑑み、医療法施行規則（昭和 23 年厚生省令第 50 号）第 14 条第 2 項において、病院・診療所・助産所の管理者がサイバーセキュリティの確保のために必要な措置を講じなければならないとされており、薬局の管理者についても同様の義務が定められていること

（参照：経営管理編 1 章 遵守事項①～⑰、2 章 遵守事項①～⑦、3 章 遵守事項①～⑲）

**Q2**　本ガイドラインに従い、システム構築等をしていたにも関わらず起こった情報セキュリティインシデントについて、責任のあり方をどのように考えるべきか。

**A**　本ガイドラインを遵守しても、法的責任が当然に免除されるわけではありません。

責任は、当時のリスクに応じた措置、運用実態、予見可能性、原因及び損害との因果関係等を踏まえて個別に判断されます。発生時は、状況を厚生労働省、都道府県警察、その他所管官庁等に報告のうえ、事業者と連携して原因究明、説明、被害拡大防止及び再発防止を行ってください。

厚生労働省へは下記ポータルサイトからインシデントの報告が可能です。必要に応じて専門家チームを派遣しての初動対応支援も実施しておりますので、早期のご報告をお願いします。

インシデントかも？ - 医療機関向けセキュリティ教育支援ポータルサイト

（参照：経営管理編 1.1.2・1.2.2、1 章 遵守事項⑨～⑬）

**Q3**　本ガイドラインを遵守しなかった場合、罰則はあるのか。

**A**　本ガイドライン自体に独立した罰則はありません。

ただし、本ガイドラインに反する状態は、e-文書法、個人情報保護法、医療法その他の関係法令上の義務を満たしていないと評価される可能性があります。適用される処分・罰則は、違反した法令と事実関係により異なります。

また、医療法 25 条第 1 項の規定に基づく立入検査要綱において、「必要な措置」については本ガイドラインやサイバーセキュリティ対策チェックリストを参照することとされているため、立入検査の中で本ガイドラインに基づいた指摘を受ける可能性があります。

001711282.pdf

（参照：経営管理編 1.1.2、1 章 遵守事項①）

**Q4** 通常時の医療情報システムの運用状況等に関する患者からの問い合わせについて、医療機関等は、どのような受付体制を整備する必要があるか。

**A** 医療機関等は医療情報の保存・利用方針を含む運用状況等に関する問い合わせ方法を明確にしてください。

具体的には、医療情報を適正に保存・利用する方針を公表し、患者からの質問や苦情に対応できる窓口を設けてください。公表については、例えば院内掲示や Web ページでの公表が考えられます。窓口については、院内の相談窓口を設けること（専用窓口である必要はありません。）や、問い合わせ Web ページを設けることでも受付体制を整備できていると考えられます。

（参照：経営管理編 1.2.1、1 章 遵守事項④）

## 委託先管理・責任分界

**Q5** 委託している事業者において、情報漏えい等の情報セキュリティインシデントが発生した場合、事業者に対応をさせればよいのか。

**A** 事業者任せにはできず、医療機関等も対応責任を負います。

医療機関等は患者への説明と善後策を担い、事業者は技術的な原因調査・対策に協力します。また、早急に状況を厚生労働省、都道府県警察、その他所管官庁等に報告することが求められます。

厚生労働省へは下記ポータルサイトからインシデントの報告が可能です。必要に応じて専門家チームを派遣しての初動対応支援も実施しておりますので、早期のご報告をお願いします。

インシデントかも？ - 医療機関向けセキュリティ教育支援ポータルサイト

（参照：経営管理編 1.2.2・1.3.1、1 章 遵守事項⑨～⑭／経営管理編 3 章 遵守事項⑱・⑲）

**Q6** 委託先の事業者の対応にあたり、「個人情報保護の責任者」を選定する要件や考慮すべきこと（「個人情報の保護について一定の知識」など）はあるか。

**A** 法令上の一律要件はなく、管理者が適任者を選任します。

個人情報保護と電子情報の漏えいリスクを理解し、必要な権限と実行能力を持つ者を選任します。

（参照：経営管理編 3.1.1、3 章 遵守事項③～⑤／経営管理編 5 章 遵守事項④・⑥）

**Q7** 委託と第三者提供の情報管理責任上の違いは何か。

**A** 委託の場合は委託元、第三者提供の場合は、提供後は原則として提供先が管理責任を負います。

「委託」とは、医療機関等が自らの利用目的を達成するために、医療情報の取扱いの全部又は一部を外部事業者に行わせることをいいます。委託先は、委託された業務の範囲内でのみ医療情報を取り扱うことができ、自らの業務や目的のために利用することはできません。

一方、「第三者提供」とは、医療機関等が保有する医療情報を、提供先が自らの業務や目的のために利用できる状態にすることをいいます。

例えば、外部検査事業者に検体検査を行わせる場合は一般に「委託」に該当し、紹介先の医療機関が自ら診療を行うために診療情報を提供する場合は「第三者提供」に該当します。

委託元は委託先を監督する必要があります。第三者提供後も、提供元に残る情報の管理責任は引き続き提供元に残ります。

（参照：経営管理編 1.3.1・1.4、1 章 遵守事項⑭～⑰）

# 企画管理編　Q&A

## 基本方針・リスク管理

**Q1**　部門系で発生し、部門システムに保管する記録等は、本ガイドラインの適用を受けるのか。

**A**　部門システムで作成・保存される記録であっても、診療のために作成され、診療録又は診療に関する諸記録に該当するものは、本ガイドラインの対象となります。また、これらに限らず、医療情報を含む文書や医療情報を扱う情報システムも、本ガイドラインの対象となります。

（参照：概説編 2.2・2.3／企画管理編 1.1.2）

**Q2**　「医療情報システムに対する情報セキュリティ方針（ポリシー）や患者の医療情報の保護に関する方針及び医療情報システムの安全管理に関する方針」とあるが、具体的にはどのようなものが想定されているのか。

**A**　個人情報保護方針と情報システムの安全管理に関する方針が想定されます。

前者には利用目的、法令遵守、漏えい防止、苦情対応等を、後者には情報セキュリティ目標、責任、継続的改善等を含め、経営層の承認を得ます。

【個人情報保護方針】

「JIS Q 15001:2023（個人情報保護マネジメントシステム－要求事項）」に示す内部向け・外部向け個人情報保護方針の要件を踏まえ、利用目的の達成に必要な範囲での適切な取扱い、法令等の遵守、漏えい等の防止及び是正、苦情・相談への対応、並びに継続的改善に関する事項を含め、経営層の承認を得た上で策定してください。外部向けには制定年月日・最終改正年月日及び問合せ先を追加し、一般の人が入手可能な状態に置く必要があります。

【情報システムの安全管理に関する方針】

「JIS Q 27001:2023（情報セキュリティマネジメントシステム－要求事項）」に基づき、組織の目的に適切であり、情報セキュリティ目的の設定のための枠組みを示し、関連法令等への遵守及び ISMS の継続的改善へのコミットメントを含む方針を策定することが求められます。なお、JIS Q 27001:2023 においては PDCA という明示的な表現は使われなくなりましたが、ISMS を確立・実施・維持・継続的に改善することが引き続き求められます。

（参照：企画管理編 1.2、1 章 遵守事項⑤・⑥）

**Q3**　医療情報システム導入に際して規程等を作成する場合、どのように整備したらよいか。

**A**　自施設の規模・リスクに応じた運用管理規程等を整備する必要があります。

本ガイドラインの規定項目を参考に、自施設の実態に応じた運用管理規程を整備してください。

（参照：企画管理編 4.1・4.2、4 章 遵守事項①～④）

**Q4**　リスク分析で想定する脅威について、どのようなものがあるか。

**A**　自然災害、人為的脅威、サイバー攻撃、委託先リスクを想定する必要があります。

情報資産ごとに機密性・完全性・可用性への影響と発生可能性を評価し、対策、残存リスク及び受容判断を文書化してください。リスク評価では、脅威だけでなく対象資産の脆弱性、患者安全・診療継続への影響、残存リスクの受容者も記録してください。

（参照：企画管理編 6.1、6 章 遵守事項②～⑧）

## 責任分界・契約

**Q5** 委託したクラウド型の電子カルテサービス業者から自院の患者に関するデータが漏えいした場合、自院にはどのような責任が問われるのか。

**A** 委託したクラウド型電子カルテサービス事業者から患者情報が漏えいした場合であっても、医療機関等は医療情報の管理主体としての責任を負います。

一方、漏えいの原因が委託先にある場合には、委託先も契約や関係法令に基づき、原因究明、復旧及び再発防止等の責任を負います。いずれの場合も、早急に状況を厚生労働省、都道府県警察、その他所管官庁等に報告することが求められます。

厚生労働省へは下記ポータルサイトからインシデントの報告が可能です。必要に応じて専門家チームを派遣しての初動対応支援も実施しておりますので、早期のご報告をお願いします。

インシデントかも？ - 医療機関向けセキュリティ教育支援ポータルサイト

（参照：企画管理編 2.1.2・2.1.3・2.2.2、2 章 遵守事項①～⑤）

**Q6** 第三者提供における責任分界をどのように考えればよいか。

**A** 提供後の情報は提供先が、提供元に残る情報は提供元が管理する必要があります。

医療機関等が負う責任が「通常時における責任（説明責任・管理責任・定期的な見直しと必要な改善を行う責任）」と「非常時における責任（情報セキュリティインシデントの原因・対策等に関する説明責任・善後策を講ずる責任）」として体系的に整理されています（企画管理編「２． １ 運用管理における責任分界」）。第三者提供を行う際には、技術的内容と手続的部分の役割分担を含めた責任分界を取り決めることが求められます（２． 責任分界 遵守事項⑥）。責任の空白が生じないよう、情報の受領確認方法や事故発生時の対処も含めて事前に合意しておくことが重要です。

（参照：企画管理編 2.1.1～2.1.3・2.2.3、2 章 遵守事項⑥）

**Q7** 地域医療連携で暗号化を用いて第三者提供等を行う際、これに係る医療機関等と医療情報システム・サービス事業者における責任分界において、どのような留意事項があるか。

**A** 暗号化の実施主体ごとに、情報保護の責任を契約で分ける必要があります。

医療機関側で暗号化する範囲と、事業者が通信経路を保護する範囲を分け、改ざん・侵入・可用性への責任を明記してください。

（参照：企画管理編 2.2.3、2 章 遵守事項②・⑥／システム運用編 13.3、13 章 遵守事項⑦～⑫）

**Q8** 医療機関等の施設外から医療情報システムにアクセスする場合に、接続する者と医療機関等との間での責任分界において、どのような留意事項があるか。

**A** テレワーク・遠隔保守ともに、医療機関等の管理責任は残ります。

接続端末、利用者、認証、通信経路、操作ログ、保守時間帯を管理し、事業者から報告を受けて監督する必要があります。

（参照：企画管理編 2.1.1・8.2、8 章 遵守事項⑧／システム運用編 7.2.1・7.2.3、7 章 遵守事項⑫・⑬）

**Q9** 地域医療連携における第三者提供等で、外部保存を受託する事業者が介在する場合、これに係る医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。

**A** 医療機関間と外部保存事業者の三者で、責任分界を明確にしてください。

医療機関同士は提供・利用の責任を、外部保存事業者とは保存・障害対応の責任を、規約や契約で定めてください。

（参照：企画管理編 2.2.2・2.2.3、2 章 遵守事項④～⑥／企画管理編 7.4）

**Q10** レセプトのオンライン請求のように、第三者提供が法令に定められている場合、医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。

**A** 法令に基づく第三者提供であっても、本人同意が不要となるだけであり、安全管理責任が免除されるものではありません。

提供先が医療情報を利用可能な状態となり、第三者提供が成立するまでの送信過程は、医療機関等の管理責任の下にあります。事業者を利用する場合も、委託に該当するときは、医療機関等が必要かつ適切な監督を行う必要があります。

このため、送受信の境界、暗号化、送信先の確認、障害・事故時の対応等について責任分界を明確にしてください。第三者提供の成立後は提供先が管理責任を負いますが、医療機関等が保有する情報については、引き続き医療機関等が責任を負います。

（参照：企画管理編 2.2.3、2 章 遵守事項⑥）

**Q11** 「２．１．１ 医療機関等における責任と責任分界」の「運用管理においては、医療機関等と情報システム・サービス事業者事業者との間で決定された責任分界を、契約書や SLA（Service Level Agreement：サービス品質保証、サービスレベル合意書）などの形で双方の拘束力ある合意文書として明らかにしたうえで、具体的に責任分界を踏まえた運用を行うことが求められる。」とあるが、契約書の記載方法を教えてほしい。

**A** 「２．責任分界」に掲げている事項に関し、個別に責任範囲及び共同対応範囲を定めて、誰が何をどのタイミングで行うかを文書化してください。

また、通信サービスを提供する事業者等に対しては、SLA（Service Level Agreement）を確認し、SLA に記載されていない若しくは不足する部分があれば、その部分について SLA の修正を要請する又は個別契約を結ぶことで対応してください。

（参照：企画管理編 2.1.1・2.1.5、2 章 遵守事項①～⑤／経営管理編 5.2.1・5.3、5 章 遵守事項④・⑥）

## 第三者提供・共同利用

**Q12** 第三者提供は、どの時点で成立するか。

**A** 個人データが第三者に提供された時点で第三者提供が行われたものと整理されます。提供先による受領確認をもって、初めて成立するものではありません。

一方、安全管理上の責任分界を明確にする観点からは、提供先による受領確認の方法をあらかじめ定め、送信したものの提供先が受領していないといった責任の空白が生じないようにすることが重要です。

（参照：企画管理編 2.2.3）

**Q13** 企画管理編２．２．３では第三者提供で責任分界を定める例が示されている。地域医療連携において、医療機関間での第三者提供の責任分界を定める際、どのような留意事項があるか。

**A** 送信元・通信経路・受信先の責任範囲と事故対応を明確にしてください。

受領確認、不達・誤送信、障害、漏えい時の対応を契約又は運用規程に定めてください。

**【「医療情報システム・サービス事業者の提供するネットワーク」を通じて医療情報の提供元医療機関等と提供先医療機関等で医療情報を交換する場合の責任分界】**

ここでいう「医療情報システム・サービス事業者の提供するネットワーク」とは、医療情報システム・サービス事業者の責任でネットワーク経路上のセキュリティを担保する場合をいいます。提供元医療機関等と提供先医療機関等は、ネットワーク経路における責任分界点を定め、不通時や事故発生時の対処を含め、契約等で合意してください。

その上で、自らの責任範囲において、医療情報システム・サービス事業者との管理責任の分担について責任分界点を定め、医療情報システム・サービス事業者の管理責任の範囲及びサービスに何らかの障害が起こった際の対処主体を明らかにしてください。

ただし、通常運用における責任及び事後責任は、委託の場合、原則として提供元医療機関等にあり、第三者提供の場合、適切に情報が提供される限り原則として提供先医療機関等にある。医療情報システム・サービス事業者に過失がない場合、医療情報システム・サービス事業者に生じるのは、あくまで管理責任の一部に留まることに留意する必要があります。

**【提供元医療機関等と提供先医療機関等が独自に接続する場合の責任分界】**

ここでいう「独自に接続」とは、接続しようとする医療機関等同士がルータ等の接続機器を自ら設定して 1 対 1 や 1 対 N で相互に接続する場合や電話回線等の公衆網を使う場合を言います。

そのうち、あらかじめ提供先又は提供先となる可能性がある医療機関等を特定できる場合は、委託又は第三者提供の要件に従って両医療機関等が責務を果たすこととなります。

このような場合、医療情報システム・サービス事業者には管理責任は発生せず、通信の品質確保の責任は発生するとしても、医療情報システム・サービス事業者が提示する約款に示されるような一般的な責任に限られます。

一方、提供先又は提供先となる可能性がある医療機関等が特定できない場合は、法令で定められている場合等の例外を除いて、原則として医療情報を提供できません。

**【共同利用により他の医療機関等が収集した医療情報を利用する場合の責任分界】**

地域医療連携で医療情報を交換する際、個人情報保護法上の共同利用により他の医療機関等が収集した情報を利用できます。この場合、医療機関等の間での責任分界などを規約や契約などで明確にすることが必要です。

（参照：企画管理編 2.2.3、2 章 遵守事項⑥）

**Q14** 地域連携のための医療情報システムとして、医療情報の所在だけを管理するレジストリと、各医療機関等が共有のために確保するリポジトリを設置する形態をとっている。利用者は、レジストリにアクセスして所在を知り、リポジトリにアクセスして実際の情報を利用する方式をとることができる（IHE XDS 統合プロファイル※）。この場合、各医療機関等は互いに保管された医療情報を共有する形となるので、共同利用という形と考えてよいか。

**A** 共同利用は、法定要件を満たす場合に認められ、当該要件を満たさない場合は第三者提供に該当します。

法定要件を満たすためには、共同利用をする旨、共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名について、あらかじめ本人に通知し、又は本人が容易に知り得る状態に置く必要があり、これらの要件を満たさない場合は、第三者提供として取り扱われます。

本ケースの場合は、これらの要件が不明確ですので、共同利用の要件を満たしていない可能性があります。共同利用の要件を満たしてない場合、他の施設での診療情報の利用は第三者提供に当たります。

（参照：企画管理編 1.1.1、1 章 遵守事項①／企画管理編 2.2.3、2 章 遵守事項⑥）

**Q15** 医療情報連携ネットワークにおける情報連携に際して、共同利用型の場合、どのような留意事項があるか。

**A** 個人情報保護法上の共同利用要件（対象データ、共同利用者の範囲、利用目的、管理責任者等を、事前に本人へ通知又は公表）を満たす必要があります。
（参照：企画管理編 2.2.3、2 章 遵守事項⑥）

## 委託先・外部保存

**Q16** 安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約）として「原則、患者が受診している医療機関等と患者との間での同意に基づいて実施すること。」とあるが、どのように患者へ説明を行うべきか。

**A** 外部保存の目的・保存先・安全性を、原則として事前に説明してください。
説明方法は院内掲示に限られず、ウェブサイトや説明文書等を組み合わせ、患者が事前に確認できるようにしてください。
（参照：企画管理編 7.6）

**Q17** クラウド型の電子カルテサービスを行う業者に認定制度のようなものはあるのか。もしなければ、業者を選定する際に３省２ガイドライン※に準拠していることは、どうやって確認すればよいのか。

**A** 2026 年 3 月末に厚生労働省にて、中小病院向け及び医科診療所向け「電子カルテ及びレセプトコンピュータ標準仕様（基本要件）」を策定しております。また、2026 年度中に認証制度を創設する方針を示しており、制度の詳細は今後公表される予定です。
中小病院向け電子カルテ及びレセプトコンピュータ標準仕様書（基本要件）、医科診療所向け電子カルテ及びレセプトコンピュータ標準仕様書（基本要件）｜厚生労働省
また、事業者から MDS/SDS を提出していただき３省２ガイドラインへの適合状況を確認してください。特に、保守委託機関編の「別紙」において、すべて「はい」または「対象外」が選択されていることが重要です。
「対象外」の項目は医療機関の責任で対応する必要があるのでご留意ください。
（参照：企画管理編 2.1.4・7.4、7 章 遵守事項⑤・⑥／システム運用編 4 章 遵守事項③／保守委託機関編【別紙】MDS/SDS におけるセキュリティ確認事項）

**Q18** 生成 AI サービスのプロンプトとして医療情報を入力する場合、入力情報が「AI の学習等のために保存されないこと」が、契約等において担保されていれば、生成 AI サービスのサーバが国内法の適用を受けている必要はないと考えて良いか？

**A** この場合、国内法の適用を受けていることは必須ではありません。企画管理編「7. 安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約」の【遵守事項】⑤において、「保存された情報を格納する情報機器等が、国内法の適用を受けることを確認すること。」としていますが、医療情報が保存されないことが、契約等において担保されている場合は国内法の適用を受けていないサーバを利用可能です。
（参照：企画管理編 7 章 遵守事項⑤）

**Q19** ISMS 認証を取得している事業者に対して、根拠資料を求めることはできるのか。

**A** 可能です。

ただし、認証は組織や適用範囲に対する評価であり、利用するサービスの安全性を直接保証するものではないことに留意してください。

（参照：企画管理編 7.4、7 章 遵守事項⑤・⑥／経営管理編 5.1.2）

**Q20** ７．安全管理のための人的管理⑥ｇの「適切な外部保存に求められる技術及び運用管理能力の有無」とは、「政府情報システムのためのセキュリティ評価制度（ISMAP）」や「JASA クラウドセキュリティ推進協議 会 CS ゴールドマーク」等で公開されたサービスリストやマーク取得サービス一覧などに掲載されていることを確認することでよいか。

**A** 認証・登録だけでは足りず、サービス固有の対策を確認する必要があります。

公開リストへの掲載は選定材料の一つであり、医療情報システム固有の要件と契約上の責任まで代替するものではありません。認証の適用範囲、対象サービス、医療情報に固有の対策、契約上の責任分界を資料で確認してください。

（参照：企画管理編 7.4、7 章 遵守事項⑥）

**Q21** 外部保存を委託する場合のデータ閲覧権限はどのように設定すべきか。

**A** 閲覧権限は業務上必要な者に限定し、付与・変更・削除を管理する必要があります。

原則として委託元だけが閲覧できるようにし、事業者の例外アクセスは緊急時等に限定して記録してください。

緊急保守等で例外アクセスを認める場合は、事前又は事後承認、対象範囲、操作ログ、終了後の権限解除等を定めてください。

（参照：企画管理編 7.4、7 章 遵守事項⑤／システム運用編 10 章 遵守事項②・③・⑦）

**Q22** 外部保存の委託を終了する際、どのような留意事項があるか。

**A** 全データの返却・移行・消去を確認し、証跡を残してください。

契約終了前に、返却形式、移行期間、バックアップを含む消去範囲、消去証明、契約終了後の責任を確認してください。

バックアップや複製データも消去対象に含め、消去証明又は同等の証跡を取得してください。

（参照：企画管理編 7.5・8.3、8 章 遵守事項⑪・⑫）

**Q23** 医療情報の外部保存に関して、院内掲示以外の患者等への周知方法はどのようなものがあるか。

**A** 院内掲示に加え、ウェブサイト、説明書、口頭説明等で周知できます。

複数の方法を組み合わせ、患者が診療開始前に外部保存の事実を確認できるようにしてください。

周知日、周知方法、説明内容を記録しておくと、説明責任を果たしたことを確認しやすくなります。

（参照：企画管理編 7.6）

**Q24** 事前の確認時と状況が変わり、請負事業者が倒産する等してソフトウェアの保証がなくなった場合、見読性は確保されていないことになるのか。

**A** 直ちに見読性未確保とはなりませんが、代替手段を確保する必要があります。

事業者の倒産やサポート終了に備え、標準形式での出力、代替ソフトへの移行、契約終了時の支援をあらかじめ確保する必要があります。

事業者の倒産・製品終了を想定し、平常時に標準形式による出力と代替環境での読出し試験を行ってください。
（参照：企画管理編 7.5／システム運用編 5.2、5 章 遵守事項①・③・④）

**Q25** 保守要員の専用アカウントの不正使用を防止するためにどのような方法があるか。また保守作業にあたってどのような作業を求めるとよいか。

**A** 個人アカウント、最小権限、事前承認、作業ログで管理する必要があります。

保守要員の専用アカウントについては、管理者権限の付与は最小限の対象者にのみ行うこと（最小権限の原則）が 13 章遵守事項⑤において明示されています。保守要員の離職・担当替え等に応じて速やかにアカウントを削除または無効化できるよう、医療情報システム・サービス事業者に報告を義務付けるとともに、対応できるアカウント管理体制を整備してください。

保守作業に際しては、作業前に作業申請をさせ、終了後速やかに作業報告をさせることが求められます。これらの書類は医療情報システム安全管理責任者が承認することとし、事前承認が困難な保守については事業者との合意の上で事後承認とすることも可能です。
（参照：企画管理編 13.1.2・13.1.3、13 章 遵守事項⑤～⑦、15 章 遵守事項⑧・⑨／システム運用編 10.1、10 章 遵守事項③・⑤）

## 医療情報の持出し・提供・破棄

**Q26** 情報及び情報機器の持ち出しを認める場合、どのような留意事項があるか。

**A** 持ち出しは必要最小限とし、承認・暗号化・記録を行ってください。

持ち出しの方法としては、①記録媒体・情報機器等による物理的持ち出し（8.2.2）、②クラウドサービス等のネットワークサービスを通じた持ち出し（8.2.3）、③外部からのリモートアクセスによる参照・利用（8.2.4）のいずれも想定する必要があります。

リスク評価に基づき、持ち出し可能な情報・機器の範囲、持ち出し手順及び管理方法を情報管理規程等に明確に定めることが必要です。また、BYOD（個人所有端末）の利用についても利用条件・範囲・管理方法を規程等に含め、台帳管理を行う必要があります。

持ち出した記録媒体等の紛失・盗難が発生した際の対応手順もあらかじめ規程に定めておくことが求められます（8.2.5）。
（参照：企画管理編 8.2、8 章 遵守事項⑤～⑦／企画管理編 9 章 遵守事項⑦／システム運用編 7.1、7 章 遵守事項①・③～⑦・⑮）

**Q27** 「リスク評価に基づいて、医療情報の持ち出しに関する方針や、持ち出す情報、持ち出し方法に関する手順や管理方法を情報管理に関する規程で定めること。」とあるが、具体的にどのような基準で判断をすればよいか。

**A** 情報の重要度、持出し目的、経路、端末、利用場所から判断してください。

医療情報を保存する機器は原則持ち出さず、必要性がリスクを上回る場合に限り、承認と防護措置を講じる必要があります。

判断結果は、持出しの必要性、残存リスク、承認者、期限を含めて記録してください。
（参照：企画管理編 8.2、8 章 遵守事項⑤～⑦／システム運用編 7.1）

**Q28** 患者等に医療情報を提供する場合、どのような留意事項があるか。

**A** 本人確認と受領確認を行い、安全な方法で医療情報を提供してください。

この際、患者に対して情報提供の目的や情報セキュリティ上のリスクを説明するとともに、医療機関等と患者等それぞれの責任範囲を明確にしてください。患者への情報提供を事業者に委託する場合には、医療機関等と事業者との責任分界を明確にし、事業者は契約等で定められた範囲において情報提供を行う必要があります。

患者ポータル等を用いる場合も、本人確認、誤送信防止、受領確認及びアクセス期限等を設ける必要があります。

（参照：企画管理編 8 章 遵守事項⑨／システム運用編 7.2.2、7 章 遵守事項⑭）

**Q29** 「医療情報の破棄に関する手順等を定める際は、情報種別ごとに破棄の手順を定めること」の手順において、医療機関側の立ち会いは必要か。

**A** 立ち会いは必須ではなく、消去証明等で確認できれば足ります。

証跡を取得できない場合は、事業者の消去手順を事前確認し、医療機関等の手順に適合させて契約に定めてください。

消去証明を用いる場合は、対象媒体、消去方式、実施者、日時、バックアップの扱いが確認できるものにしてください。

（参照：企画管理編 8.3、8 章 遵守事項⑪・⑫／システム運用編 7.3、7 章 遵守事項⑨～⑪）

**Q30** 「８．情報管理（管理、持出し持ち出し、破棄等）③において医療情報が保存されている場所等については、記録・識別、入退室の制限等の管理を行うこと。また医療情報の保管場所には施錠等の対応を行うこと。」とあるが、例えば外来やナースステーション等では、それらの措置は困難ではないか。

**A** 一律の専用区画は不要で、場所のリスクに応じた管理を行ってください。

外来やナースステーション等、専用区画を設けにくい場所では、端末配置、画面ロック、のぞき見防止、施錠、入室管理を組み合わせてください。

（参照：企画管理編 8.1、8 章 遵守事項③、15 章 遵守事項①・②／システム運用編 12.1、12 章 遵守事項①～③）

**Q31** 外部の医療機関等から持ち込まれた X 線写真（コピー）や画像データを当院での診療に用いた場合、保存義務は生じるのか。

**A** 原本の保存義務は元の医療機関等にありますが、持ち込まれた医療情報を診療に利用した場合は、当該医療機関等においても保存義務が生じます。

（参照：概説編 2.2・4.3／企画管理編 1.1.2）

## 非常時対応・BCP

**Q32** BCP（Business Continuity Plan：事業継続計画）の内容を検討する上で、参考になる内容はあるか。

**A** BCP には、指揮命令、代替業務、復旧、連絡、訓練を盛り込みます。

災害、サイバー攻撃、システム障害を想定し、定期的に訓練して実効性を確認してください。

また、厚生労働省の公開している

・サイバー攻撃を想定した事業継続計画（BCP）策定の確認表

https://www.mhlw.go.jp/content/10808000/001261299.pdf

・医療情報システム部門等における BCP のひな形

https://www.mhlw.go.jp/content/10808000/001261302.pdf
等を参照してください。
（参照：企画管理編 11.1～11.3、11 章 遵守事項①～⑨／システム運用編 11 章 遵守事項①）

**Q33** 災害等で医療情報システムが運用できない場合で、一時的に運用した紙データを後から電子システムに反映させることは、真正性の観点から問題にならないか（システムへの入力時のタイムスタンプが有効になるのではないか）。

**A** 適切な安全管理が実施されていれば問題ありません。紙での作成者・時刻と後日入力を追跡できるようにしてください。
紙の記録を原本として保存し、後日入力の入力者・日時・元記録との対応を記録して確定してください。
（参照：企画管理編 11.2・13.2、13 章 遵守事項⑧／システム運用編 11.2・14.3、14 章 遵守事項⑨）

## 本人確認・電子署名

**Q34** 本人確認の方法として eKYC を採用する場合、どのような留意事項があるか。

**A** eKYC の保証レベルを、利用目的とリスクに合わせて選定してください。
electronic Know Your Customer（eKYC）の方式、本人確認書類、なりすまし耐性、証跡、委託先の管理を確認してください。
身元確認については、高い強度の確認が必要であり、対面又はこれに準じた方法が求められます。第 7.0 版では、NIST SP 800-63-4 の IAL（Identity Assurance Level）を参照し、個人の安全への影響に鑑みると IAL Level 3 が望ましく、一定程度の情報セキュリティレベルが担保された環境下で管理されている医療機関等であれば IAL Level 2 以上が望ましいとされています。レベル区分は「行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン」を参照してください。
（参照：企画管理編 13.1.2、13 章 遵守事項②）

**Q35** 一枚一枚の文書にリアルタイムにタイムスタンプを付与することは、実装が困難ではないか。
また、どのような文書にタイムスタンプの付与が必要か。

**A** タイムスタンプの付与が想定されるのは、
・法令で署名又は記名・押印が義務付けられた文書について、電子署名の長期的な検証を確保する必要がある場合
・医療情報の作成時刻又は変更時刻を証明する必要がある場合
です。
その他の文書における真正性は、確定者、確定時刻、変更履歴を追跡できる仕組みで確保できます。採用する確定方法を運用管理規程に定めてください。リアルタイムにタイムスタンプを付与するべき文書についても、その必要性を医療機関等において判断し、運用管理規程に定めることになります。
また、複数のスキャン画像ファイルなどにまとめてタイムスタンプを伏すことも想定されますが、個別ファイルを検証することができなくなることがあるため留意が必要です。
この場合も、個々のファイルのハッシュ値を束ねて階層化した上で、頂点のハッシュにタイムスタンプを付す ERS（Evidence Record Syntax）等の技術の利用により個別ファイルの検証が可能となり得ます。
（参照：企画管理編 14.2、14 章 遵守事項①／システム運用編 15.1、15 章 遵守事項①）

**Q36** クラウド型の電子カルテサービスを行う場合、利用者によるトランザクションごとに電子署名が必須となるのか。

**A** トランザクションごとの電子署名は、一律には必須ではありません。

ただし、電子署名を省略する場合も、利用者識別、確定時刻、変更履歴及び監査ログ等で真正性を確保する必要があります。

（参照：企画管理編 13.2・14.1、13 章 遵守事項⑧、14 章 遵守事項①／システム運用編 14.3・15.1）

**Q37** １４．法令で定められた記名・押印のための電子署名① １⑵の「法令で医師等の国家資格を有する者による作成が求められている文書については、以下の(a)～(c)のいずれかにより、医師等の国家資格の確認が電子的に検証できる電子署名等を用いること」とあるが、要件を満たす具体的な手段は何か。

**A** 令和８年７月 31 日時点で存在している、「法令で医師等の国家資格を有する者による作成が求められている文書」に対し、医師等の国家資格の確認が電子的に検証できる電子署名としては、１４．法令で定められた記名・押印のための電子署名　遵守事項①1(2)(a)「保健医療福祉分野 PKI 認証局の発行する電子証明書」

・日本医師会 電子認証センターが発行する「医師資格証」
・日本薬剤師会 認証局が発行する「薬剤師資格証」
・医療情報システム開発センター(MEDIS-DC) 電子認証局が発行する「HPKI 電子証明書」

があります。なお、今後、(a)の「監査基準」を満たす新たな「保健医療福祉分野 PKI 認証局」や、

（ｂ）の「適切な外部からの評価」を受けた事業者、電子的な資格確認に対応した（ｃ）の「公的個人認証サービス」による電子証明書が発行された場合、適宜、追加も考えられます。

（参照：企画管理編 14.1、14 章 遵守事項① 1(2)(a)～(c)）

**Q38** １４．法令で医師等の国家資格を有する者による作成が求められている文書の電子署名の要件のうち、①1(2)（ｂ）にある「医療機関等の管理者」とは、具体的には施設単位で考えればよいか。

**A** 原則として、病院・診療所・薬局等の施設単位の管理者です。

同一法人に複数施設がある場合も、各施設の管理者が資格確認の実施・記録・保存及び監査に関する責任を負う体制を明確にしてください。

（参照：企画管理編 14.1、14 章 遵守事項① 1(2)(b)）

**Q39** タイムスタンプはパソコンの時間と同じでよいか。

**A** パソコンの時計による時刻は第三者による検証可能性が担保されないため、利用することはできません。端末時計はずれや改変の影響を受けるため、組織で管理する信頼できる時刻源と同期させる必要があります。認定事業者が提供するタイムスタンプを利用し、法定保存期間中にわたってタイムスタンプの有効性が維持されるよう必要な対策を講じてください。

（参照：企画管理編 14.2／システム運用編 15.1・17.1、17 章 遵守事項③）

**Q40** 暗号化を行うための適切な鍵管理を行うために、どのような対応が考えられるか。

**A** 鍵の生成から廃棄までのライフサイクルを管理する必要があります。

生成、保管、利用権限、バックアップ、更新、失効、廃棄、事故時対応を規程化し、鍵へのアクセスを最小限にしてください。SSL/TLS・電子署名・通信機器認証等の用途に応じてそれぞれ必要な共通鍵・秘密鍵を保護する機能を具備することが求められています。電子証明書を利用する認証については、認証局が定める「証明書ポリシー」（CP）等に従って鍵を管理することが必要です。

暗号モジュールに関するセキュリティ要件については、米国連邦標準規格 FIPS 140（最新版は FIPS 140-3）が参照されます。利用する暗号モジュールについて当該規格で求められる要件を具備することが望まれます。

（参照：企画管理編 14.1・14.2／システム運用編 15.1）

## 紙媒体・スキャン

**Q41** 「情報が作成されてから又は情報を入手してから一定期間以内にスキャンを行うこと。」とあるが、一定期間以内とはどれぐらいをいうか。外来診療の場合、1 日の診療が終わった後にまとめて行う等の運用でもよいか。

**A** 原則は 1 日以内です。ただし、深夜に来院し、次の日が休診である場合等は営業日として 1 日以内となります。

（参照：企画管理編 16.2、16 章 遵守事項⑤）

**Q42** 電子カルテを導入した場合、それまでの旧カルテ（紙カルテ）について保存義務があるか。あるとすれば何年か。

**A** 旧紙カルテにも法定保存期間が適用されます。

ただし、電子カルテの導入により、以前の紙の診療録がスキャナ等で適切に電子化されており、管理責任者によって保存義務の対象が電子化された診療録であると認められていれば、紙の診療録に法定上の保存義務はありません。このような処理を行わない場合は、 法定の保存義務があります。

（参照：企画管理編 16.1・16.3、16 章 遵守事項①～⑥／システム運用編 16.1、16 章 遵守事項①）

**Q43** 診療録等をスキャナで電子化した場合、原本の取扱いはどのようにすべきか。

**A** 要件を満たして電子化すれば原本は廃棄できます。

ただし、法令上原本保存が必要な文書や、スキャンにより有用な情報が画像で失われる場合は、原本を残すか別の記録手段を用いる必要があります。

（参照：企画管理編 16.1・16.3、16 章 遵守事項①～⑥／システム運用編 16.1、16 章 遵守事項①）

**Q44** 電子化して保存した紙の調剤済み処方箋を修正する場合、修正前の電子署名を検証できる状態で残した上で、保存済みのデータを一度印刷し、紙上で訂正したものを再度電子化して、薬剤師の電子署名を付して保存する運用でもよいか。

**A** プリント後に訂正して再電子化する運用は、適切ではありません。

電子データ上で修正し、元の電子署名を検証できる状態で、修正前後と修正者を記録してください。

（参照：企画管理編 16.4、16 章 遵守事項⑦）

**Q45** 紙媒体等をスキャナ等で電子化保存する場合は、どの程度の解像度がいいか。

**A** 保存目的に必要な解像度を確保する必要があります。

文字、画像、色調等を保存目的に支障なく再現できることを確認し、規格を運用管理規程に定めてください。放射線フィルム等の情報をスキャンする場合、どの程度の解像度を求めるべきかについては、日本医学放射線学会電子情報委員会が公表した「デジタル画像の取り扱いに関するガイドライン」等を参考にしてください。

（参照：企画管理編 16.1、16 章 遵守事項①～④／システム運用編 16.1、16 章 遵守事項①）

# システム運用編　Q&A

## 標準化・相互運用性

**Q1**　相互運用性と標準化を行うことのメリットは何か。標準仕様等を実装しなかった場合、どのような不利益が想像されるか。

**A**　相互運用性と標準化は、データ交換・移行・継続利用を容易にします。

標準仕様等を実装しないと、他システムとの交換、更新時の移行、長期保存後の利用が困難になりうるほか、事業者のロックイン（技術的、経済的もしくは運用上、他社製品への切替えが困難となり、その事業者と継続的に契約せざるを得なくなる状態）にもつながります。

（参照：システム運用編 5.1、5 章 遵守事項①・③）

**Q2**　基本データセットを利用し、一般財団法人医療情報システム開発センター（MEDIS-DC）の標準マスタを組み合わせた場合、医療情報システムのリプレイス時の相互運用性は保証されるか。

**A**　基本データセット及び標準マスタを活用することは、相互運用性の確保を容易にしますが、保証はされません。なお、基本データセットに含まれない項目や標準が定められていない用語・コードも存在します。

基本データセットや標準マスタは、概ね重要あるいは実装頻度の高いものを対象にしており、採用することによって、相互運用性を確保するためのコストを大幅に下げることができます。

（参照：システム運用編 5.1・5.2、5 章 遵守事項①～③）

**Q3**　データ交換のための国際的な標準規格については、どのようなものがあるか。

**A**　HL7 FHIR、DICOM 等があります。用途に応じて、これらの標準規格を採用してください。

Health Level Seven Fast Healthcare Interoperability Resources（HL7 FHIR）、Digital Imaging and Communications in Medicine（DICOM）等があります。

規格名だけでなく、用途、バージョン、実装ガイド及び適合性試験の有無を確認してください。

また、以下の URL から JAHIS により標準規約化されたものが確認可能です。

https://www.jahis.jp/standard/contents_type=33

（参照：システム運用編 5.1・5.2、5 章 遵守事項①・③）

**Q4**　外字の使用について注意すべき点は何か。

**A**　外字は可能な限り使用せず、標準文字へ置換又は対応付けてください。

外字を使用したシステムでは、あらかじめ使用した外字のリストを管理しておき、システムを変更した場合又は他のシステムと情報を交換する場合に、表記に齟齬のないよう対策する必要があります。

（参照：システム運用編 5.1・5.2、5 章 遵守事項①・③）

## 保存・見読性

**Q5**　診療情報等が復元できなくなることが生じないように、どのような対応をすべきか。

**A**　互換形式での出力、媒体移行、バックアップ、復元試験を行ってください。

警察庁の公表している「令和７年における サイバー空間をめぐる脅威の情勢等について（p129-130）」ではランサムウェア被害にあった事業者の８割近くがバックアップを復元できず、その原因のおよそ 1/4 が運用不備であったことが報告されています。

R07_cyber_jousei.pdf

ランサムウェア攻撃に対しては、オフラインバックアップを確保することも有効な対策となります。さらに複数の媒体でバックアップを確保することも重要です。例えば、HDD と RDX（Removable Disk Exchange system）、クラウドサービスと NAS（Network Attached Storage）など複数の媒体でバックアップを保存することなどが考えられます。

また、製品・事業者のサービス終了も想定し、定期的な読み出し確認と移行計画を定めてください。

（参照：システム運用編 5.2、5 章 遵守事項①・③・④）

## Q6 見読性を確保するために、どのような対応が必要か。

**A** 必要時に速やかに表示・印刷できる状態を維持する必要があります。

保存情報と表示・印刷に必要なソフトウェア、マスタ、設定を対応付け、定期的に見読性を確認してください。

また、ソフトウェアやマスタのサポート終了も見読性リスクとなります。システム・ネットワーク障害等に備え、BCP に基づき、冗長化、バックアップ、代替手段及び復旧・復帰手順を整備し、復元した情報を見読できることを確認してください。

（参照：システム運用編 5.2・9.2、5 章 遵守事項④、9 章 遵守事項④）

## Q7 汎用性が高く、見読するソフトウェアに困らない形式にはどのようなものがあるのか。

**A** PDF/A、CSV、DICOM 等、仕様が公開された標準形式を用いてください。

用途に応じ、文書は PDF/A、表形式は CSV、医用画像は DICOM 等を選択してください。

参考：形式の選定時は、仕様の公開性、長期保存性、文字・画像・署名情報の保持可否を確認してください。

（参照：システム運用編 5.2、5 章 遵守事項①・③・④）

## Q8 X 線 CT の検査で、オリジナルの画像のほかに、オリジナル画像から生成した３Ｄ画像も使って診断している。電子保存を行う際に、オリジナル画像さえ保存しておけば、診断に使用した３Ｄ画像は消去してしまっても構わないか。

**A** 施行通知において、保存性の要件として、「保存すべき期間中において復元可能な状態で保存することができる措置を講じていること」が求められています。

診断にあたり、３Ｄ画像を用いている場合は、原画像のみでは、この保存性の要件を満たせない場合も想定されるため、3D 画像又は再現に必要な処理条件を保存する必要があります。

（参照：システム運用編 5.2・14.3、5 章 遵守事項③・④、14 章 遵守事項⑨）

## Q9 3D 画像処理を行った場合、処理を行う元となった画像は保存しなければならないか。

**A** 3D 画像を生成するためだけに用いた thin slice 画像等で、診断の根拠として使用していない中間画像を保存する必要はありません。

診断に用いた 3D 画像については、当該画像そのものを保存するか、保存した元画像及び処理条件から完全に再現できる状態を確保する必要があります。完全に再現できない場合は、診断に用いた 3D 画像を保存してください。

（参照：システム運用編 14.3、14 章 遵守事項⑨）

**Q10** 確定保存された画像に関し、診断や患者説明のために一時的に医師が表示方法（濃度の変更、拡大など）のみを修正した場合、この画像を保存する必要があるか。

**A** 表示方法の一時的な変更だけであれば、原則として保存不要です。
濃度の変更、拡大といった程度の処理ならば、改めて保存する必要はありません。
（参照：システム運用編 14.3、14 章 遵守事項⑨）

**Q11** 検像において、検像前の画像情報、検像後の画像情報のいずれを保存対象とすべきか。

**A** 原則として、検像後に確定した画像を保存する必要があります。
診断にもちいる検像後の画像を対象とすべきと考えられます。ただし、検像において情報の修正・削除といった行為により、照射記録と検像の後の画像情報が一致しない等のことが生じる場合には、修正履歴を保存しておく等、所定の措置が必要となります。検像で修正・削除を行う場合は、照射記録との対応と変更履歴を保持してください。
（参照：システム運用編 14.3、14 章 遵守事項⑨）

**Q12** 「緊急に閲覧が必要になったときに迅速に対応できるよう、保存している紙媒体等の検索性も必要に応じて維持すること。」とあるが、どのようなケースで、どれくらいの対応時間内で行う必要があるのか。

**A** 一律の時間規定はありません。緊急時の業務要件に基づき、必要時間内に検索できるようにしてください。
システム停止時や緊急診療時に必要となる情報を特定し、検索方法と保管場所を定めてください。
（参照：システム運用編 16.2、16 章 遵守事項②）

## マルウェア・保守

**Q13** 医療情報システム・サービス事業者がやむを得ず個人情報を含むデータを医療機関等外に持ち出さなければならない場合はどのような対応をすべきか。

**A** 原則として持ち出さず、やむを得ない場合は承認・暗号化・記録を行ってください。
持出しの目的、対象、件数、保存環境を示して承認を得ます。作業後はデータを消去し、結果報告を求めてください。
ただし、クラウドサービス等を利用し、契約に基づいて医療機関等の外部に医療情報を保存すること自体は、ここで想定する「持出し」とは区別して考える必要があります。契約で定められたクラウド等の保存環境については、保存場所や安全管理措置、事業者との責任分界等をあらかじめ確認し、適切に管理してください。
（参照：システム運用編 7.1、7 章 遵守事項②・③／システム運用編 10.1、10 章 遵守事項①）

**Q14** 情報機器の持ち出し又は外部利用をする場合どのような対策をすべきか。

**A** 承認済み端末に限定し、暗号化・認証・紛失対策等を行ってください。
例えば下記の様なものが考えられます。
①端末の起動時の認証は必須であり、認証ルールに沿った内容であることが求められます。
②医療情報が保存されている場合には記録媒体に暗号化を施すこと。
③タブレット PC 及びスマートフォンの持出しに際して、目的から不要なプログラム等はインストールしないこと、情報機器等に対する管理者権限等を原則付与しないこと。
④公衆無線 LAN の利用がなされた場合、利用後に端末の安全性が確認できる手順を策定すること。
⑤医療情報が格納された可搬媒体及び情報機器の所在を台帳等により管理し、定期的に棚卸を行うこと。
⑥取り扱う情報を最小限とし、不要な個人情報を利用させないこと。

⑦利用終了時の媒体からデータを削除すること。
（参照：システム運用編 7.1、7 章 遵守事項①・③～⑦・⑮）

**Q15** マルウェア対策ソフトの導入が求められているが、ホワイトリスト方式もマルウェア対策に含まれると考えてよいか。

**A** ホワイトリスト方式も、マルウェア対策に含まれます。

許可したプログラムだけを実行させる方式であり、実行プログラムが固定的な医療機器等では一定程度有効です。製造販売業者が十分に検証した方式を採用してください。

ただし、一般的なマルウェア対策ソフト同様、それのみでマルウェア対策が十分とは言えません、セキュリティパッチの適用や最小権限の原則、ログ監視などを組み合わせた多層防御が重要です。特に Living off the land 攻撃についてはホワイトリスト方式では効果がない場合があります。十分なリスク評価を実施の上導入してください。
（参照：システム運用編 8.1、8 章 遵守事項②・③）

**Q16** マルウェア対策等が大変なので、外部と遮断した環境を設定する方が望ましいのか。

**A** 外部との遮断だけでは不十分で、環境に応じた多層防御が必要です。

閉域網環境でも、VPN 装置の脆弱性を用いたサイバー攻撃が複数発生しています。持込媒体、保守接続、内部不正、脆弱性のリスクは残るため、更新、マルウェア対策、監視等を行ってください。
（参照：システム運用編 8.1・8.2、8 章 遵守事項①～④）

**Q17** 医療等分野における IoT 機器に対する安全対策を行う上で、どのような留意事項があるか。

**A** IoT 機器も、資産管理・認証・更新・監視の対象にする必要があります。

機器の一覧、接続先、初期設定変更、脆弱性・サポート期限、通信制御、異常時の隔離等を管理する必要があります。
（参照：システム運用編 8.2、8 章 遵守事項⑥）

**Q18** IoT 機器を含む医療情報システムの接続状況や異常発生を把握するためにはどのような方法あるか。

**A** IoT 機器・医療情報システム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してください。

7.0 版では、医療情報システムの稼働状況が正常であることを把握するため、パフォーマンス管理や死活管理を行い、パフォーマンスが低下した場合やシステムがダウンした場合に速やかに把握可能な状態とする必要があることが明記されています。医療機関等のみでの対応が困難な場合には、適宜、事業者からシステムのパフォーマンスの状況等で異常が発生した場合に速やかに連絡を受けられるような体制を設けることが求められます。
（参照：システム運用編 8.2・8.4、8 章 遵守事項⑥・⑦／システム運用編 11.1、11 章 遵守事項②）

**Q19** 医療情報システム・サービス事業者による保守対応が行われた場合に、診療録にアクセスした証跡を確認する方法はどのようなものがあるか。

**A** 個人別アカウントを付与し、アクセスログで、保守時の閲覧を確認してください。

ログには作業者、日時、対象患者・データ、操作内容を記録し、医療機関等が定期的に確認してください。作業申請・報告とログとの突号による確認も重要です。
（参照：システム運用編 10.1・17.1、10 章 遵守事項③・⑤・⑦、17 章 遵守事項①・②）

**Q20** 保守要員が外部機器を持ち込む場合、何を確認すべきか。

**A** 持ち込まれる外部機器の承認、マルウェア検査、接続範囲を確認してください。

保守作業に必要な接続先・経路のみを利用し、作業後は作業ログや接続ログを確認してください。

（参照：システム運用編 8.1、8 章 遵守事項①／システム運用編 10.1、10 章 遵守事項③・⑥）

## 非常時対応・バックアップ

**Q21** 「１１．１ 通常時における運用対策表１１－１ 平常通常時に対応すべき技術的対応の例の広域災害対策（遠隔地バックアップ等）とあるが」とあるが、「遠隔地」の定義はあるのか。

**A** 距離の一律基準はなく、同時被災しない場所を選定してください。

地震、水害、停電、通信障害等で本番環境と同時に失われないことを、リスク評価で確認してください。

（参照：システム運用編 11.1・12.2、11 章 遵守事項①(6)、12 章 遵守事項④）

**Q22** 非常時における利用に備えて、診療録等をどのように保存すべきか。

**A** 必要な診療情報を、非常時にも閲覧できる形で保存する必要があります。

患者の安全と診療継続に必要な情報を選定し、参照系システムの確保や、オフラインバックアップ等で確保することが想定されます。

例えば、クラウド上にオフラインバックアップを確保しておくことは災害等を含めた対策として有用です。クラウドサービスを利用したオフラインバックアップは以下のような場合となります。

① クラウドサービスから、専用アプリを用い抽出したデータを、ＲＤＸなど別の媒体で保管している場合

② クラウドサービスから外部の記録媒体（ＮＡＳ等）に自動でデータが転送される場合であって、常時（データ転送の際を除く。）ネットワークから切り離した状態でのバックアップを行っている場合

③ クラウドサービスから、当該クラウドサービス内の他の論理的に切り離されている領域にバックアップを取っている場合であって、災害時等に速やかにデータ復旧が可能な状態にある場合

なお、ネットワークから切り離したオフラインで保管していることについては、医療情報システム・サービス事業者との契約書等に記載されているかについても十分に確認してください。

また、非常時に必要な情報の範囲、更新頻度、閲覧権限、保管場所及び切替条件等を事前に検討してください。

（参照：システム運用編 11.1・11.2・12.2、11 章 遵守事項①(4)～(6)、12 章 遵守事項④）

**Q23** 障害等によるデータ保存時の不整合に備えて、どのような対応をすればいいか。

**A** 保存処理が正常に完了し、保存先でデータが正しく保存されたことを確認できる仕組みを設けてください。また、通信障害等により保存処理が中断した場合には重複や欠落が生じないよう整合性を確認した上で再送することができるようにしてください。不整合が生じた場合、バックアップからのリカバリーに関する手順を備えておくことも重要です。

（参照：システム運用編 11.1・12.2、11 章 遵守事項①(6)、12 章 遵守事項④）

**Q24** 診療録等のデータのバックアップの管理や方法に関して、どのような留意事項があるか。

**A** バックアップを本番環境から分離し、定期的に復元試験を行ってください。

また、バックアップの設計に関しては、3-2-1 ルールを参考にしてください。データは 3 世代以上保持し、2 種類以上の異なる媒体に保存し、1 つ以上は本番環境と分離した場所に保管することが推奨されます。

（参照：システム運用編 11.1・12.2・18.1、11 章 遵守事項①(6)、12 章 遵守事項④、18 章 遵守事項①）

**Q25** 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りを防止するために、どのような対応が考えられるか。

**A** 媒体の寿命を管理し、期限前に新しい媒体へ移行してください。

保存環境、読出し確認、装置の互換性も管理し、移行履歴を残してください。

（参照：システム運用編 12.2・12.3.1、12 章 遵守事項⑤）

## ネットワーク・VPN・無線 LAN

**Q26** 専用線以外の回線サービスを利用する場合、どのような留意事項があるか。

**A** 原則として、専用線、IP-VPN 又は IPsec＋IKEv2 を利用してください。

オープンなネットワークを経由する場合、TLS のプロトコルバージョンを TLS1.3 以上に限定して、TLS クライアント認証（mutual-TLS）を用いる、又はこれと同等以上の安全性対策が求められます。システム・サービスの対応上困難な場合には、TLS1.2 の設定によることも可能ですが、いずれも「TLS 暗号設定ガイドライン」（IPA）に規定される「高セキュリティ型」の設定を適用することが必要です。

SSL-VPN を使用する場合は「クライアント型」を選択し、その場合も TLS 要件の遵守が必要です。また、VPN 機器の管理インターフェイスやログインページが外部から接続できないよう設定するとともに、VPN 機器の脆弱性対策としてクラウド型 VPN の採用や自動アップデートに対応した製品の選定が推奨されます。

（参照：システム運用編 13.1.1・13.1.2・13.3.1、13 章 遵守事項②～⑦）

**Q27** 「ルータ等のネットワーク機器について、安全性が確認できる機器を利用すること。」とあるが、どのようなものが安全性を確認できる機器として考えられるのか。

**A** 更新が継続され、安全機能と設定管理を確認できる機器を選ぶことが重要です。

安全性を確認する方法の一つとして、ISO/IEC 15408（Common Criteria）に基づく第三者評価・認証を受けた製品を選定することが考えられます。製品仕様書、セキュリティに関する技術資料、MDS/SDS、医療情報セキュリティ開示書等を用いて、本ガイドラインで求めるセキュリティ要件を満たしていることを確認してください。例えば、以下のような事項を確認することが考えられます。

- 製造事業者等によるセキュリティ更新やファームウェアの提供が継続されていること
- 脆弱性が判明した場合の情報提供及び修正プログラム等の提供体制が確保されていること
- 管理インターフェースへのアクセス制御、認証、通信制御、ログ取得等、必要なセキュリティ機能を備えていること
- 当該製品のサポート期間及び使用しているファームウェア等のバージョンが確認できること

（参照：システム運用編 13.1、13 章 遵守事項⑤）

**Q28** 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）とは、具体的にどのような事象を指すものか。

**A** 例えば、下図のように、医療情報連携ネットワークの Web サーバへのアクセス等のために、医療機関等の専用端末がソフトウェア型の IPsec や TLS1.2 以上によりオープンネットワークに接続している場合、攻撃者は開放された当該端末のポートを標的として、何らかの攻撃（典型的には標的型メール攻撃等）を試みることが想定されます。

この攻撃により、当該専用端末が遠隔操作型のマルウェア等に感染すると、攻撃者は本人になりすまして医療情報連携ネットワークの Web サーバとのセッションの立上げを試みることが可能になります。セッションの立上げに成功すると、外観

上は正規の権限によるアクセスが発生することになり、IPsec や TLS1.2 以上により適切に暗号化していても、攻撃者は医療情報連携ネットワークの Web サーバにアクセスできるようになります。

本ガイドラインでは、この一連の攻撃を「セッション間の回り込み」と称しています。対策として、適切な経路設定を実施することに加え、医療情報連携ネットワークへのアクセスに当たって、セッション確立時の利用者二要素認証を行うこと等が考えられます。

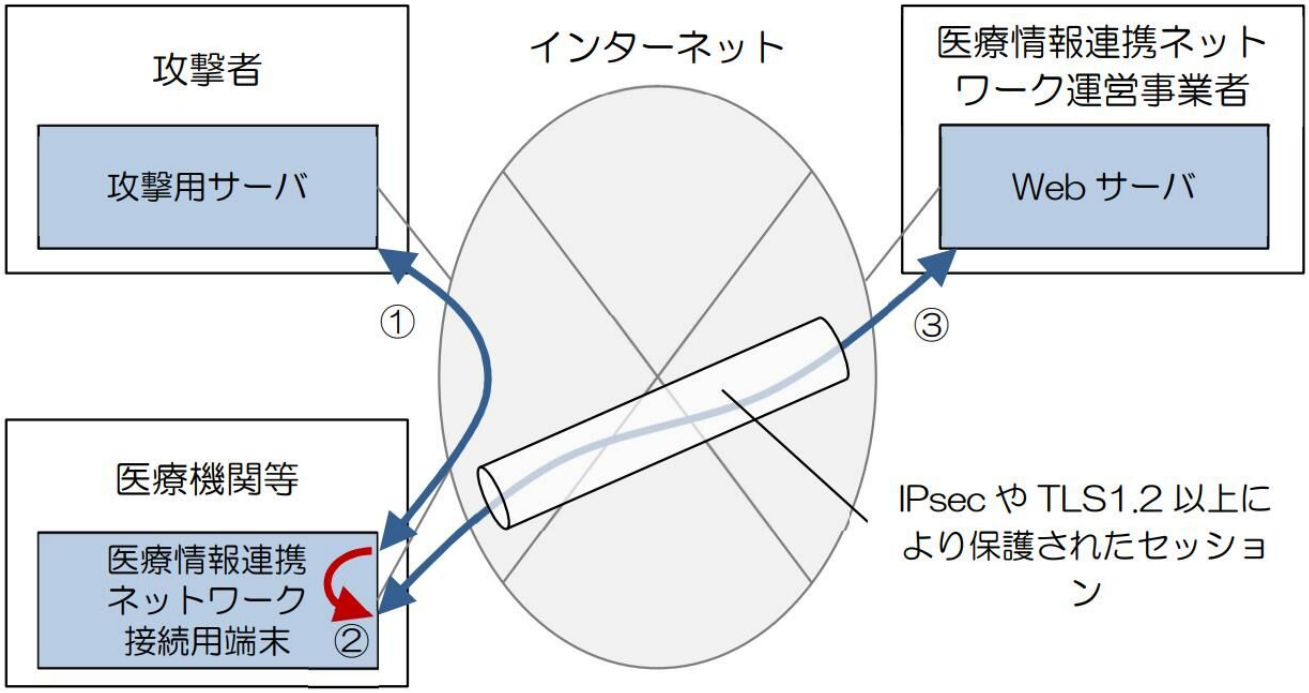


図　セッション間の回り込みのイメージ

（参照：システム運用編 13.3.1、13 章 遵守事項⑦）

**Q29** 「１３．ネットワークに関する安全管理措置 」⑥に「 SSL-VPN は利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと」とあるが、具体的にはどのように利用するのか。

**A** クライアント型 SSL-VPN を選び、サーバ証明書を検証してください。

クライアント型だけでは足りず、TLS の安全な設定、端末識別・認証、接続先制限、セッション管理を組み合わせてください。

（参照：システム運用編 13.1.2・13.3.1、13 章 遵守事項⑥・⑦）

**Q30** 無線 LAN の利用において、どのような留意事項があるか。

**A** 無線 LAN では、強固な暗号化・個別認証・不正アクセスポイント対策を行ってください。

共通の事前共有鍵は避け、WPA2-EAP 又は WPA3-Enterprise 等で利用者・端末ごとに認証してください。

無線 LAN の運用に関しては、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」を参考に対策を実施してください。

（参照：システム運用編 13.4、13 章 遵守事項⑬）

**Q31** 「改ざん」への対応として、どのような留意事項があるか。

**A** 改ざんには、電子署名、ハッシュ、システム上の変更履歴等を用いてください。受信側が内容の完全性と送信者を検証できるようにし、変更を検知・追跡してください。

（参照：システム運用編 13.3、13 章 遵守事項⑨・⑩）

**Q32** 許可された者以外の無線 LAN の利用を防止するためにはどのような対策が必要か。

**A** 802.1X 等で利用者・端末を認証し、無線 LAN への接続を制限してください。

MAC アドレス制限だけに依存せず、電子証明書等による認証と WPA2-EAP 又は WPA3-Enterprise 等を用いてください。

（参照：システム運用編 13.4、13 章 遵守事項⑬(1)～(3)）

## ID・利用者認証

**Q33** 医療情報システムに用いる ID について「不要なものは適宜削除すること。」とあるが、不要な ID を適切に無効化することも含まれるという理解でよいか。

**A** 不要な ID の無効化も含まれます。

（参照：システム運用編 14.2、14 章 遵守事項⑧）

**Q34** 利用者の識別・認証に IC カード等のセキュリティ・デバイスを配布する場合、どのような留意事項があるか。

**A** カード等を個人に紐付け、紛失・貸借・失効を管理する必要があります。

カード単独で認証せず、PIN 等と組み合わせてください。紛失時の停止、再発行、緊急時の代替手順も定めてください。

（参照：システム運用編 14.1.1、14 章 遵守事項③・⑤）

**Q35** 利用者の識別・認証で二要素認証を採用する際、指紋、虹彩等のバイオメトリクスを利用する場合、どのような留意事項があるか。

**A** 下記の様な生体情報の特性を踏まえ、誤認識・漏えい時の代替手段を用意してください。

・事故や疾病等による認証に用いる部位の損失等
・成長等による認証に用いる部位の変化
・一卵性の双子の場合における特徴値の近似
・赤外線写真等による“なりすまし” （IC カード等の偽造に相当）

生体認証は ID 等と組み合わせた 1 対 1 照合を基本とし、身体変化や認証不能時の代替手段を定めてください。

（参照：システム運用編 14.1.1、14 章 遵守事項⑤）

## 真正性・電子署名

**Q36** 「虚偽入力、書換え、消去及び混同を防止する」ために、はどのように、どのような対応が求められるのか。

**A** 以下のような対応を行ってください。

・入力者及び確定者を識別・認証し、記録の確定を権限のある者に限定する。
・確定前に内容及び対象患者が正しいことを確認する。
・確定した記録に、入力者・確定者又は装置の識別情報と、信頼できる時刻源による作成日時を記録する。
・確定後に訂正等を行う場合は、更新前後の内容と更新の順序が分かる履歴を保存し、誤った変更等があった場合の原状回復手順を定める。

（参照：システム運用編 14.3、14 章 遵守事項⑨(1)(d)・(3)・(4)）

**Q37** 「作成の責任の所在を明確する」ために、はどのように、どのような対応が求められるのか。

**A** 以下のような対応を行ってください。

・入力者及び確定者を識別・認証し、記録の確定を権限のある者に限定する。

・確定前に内容及び対象患者が正しいことを確認する。

・確定した記録に、入力者・確定者又は装置の識別情報と、信頼できる時刻源による作成日時を記録する。

・確定後に訂正等を行う場合は、更新前後の内容と更新の順序が分かる履歴を保存し、誤った変更等があった場合の原状回復手順を定める。

（参照：システム運用編 14.3、14 章 遵守事項⑨(1)(a)～(c)）

**Q38** 医療情報システムにおいて、真正性の確保を求める場合、記載されている情報と確定者には具体的にどのような組み合わせがあるか。

**A** 情報と確定者の組み合わせとしては、例えば下記のような例があります。

例 1） 医師が患者の診察時にカルテに所見を記述する。

情報 ：所見

確定者 ：実際に診察を行った医師

例 2） 看護師が医師の指示に基づく処置を行った際に、実施状況を看護記録に記述する。

情報 ：処置実施記録

確定者 ：実際に処置を行った看護師

例 3） 読影担当医が放射線画像の読影レポートを作成する。

情報 ：読影レポート

確定者 ：読影を行った放射線科医師

例 4） 検査技師が検査ラインから出力された検査結果のバリデーションを実施し、システムに取り込む。

情報 ：検査結果

確定者 ：バリデーションと取り込み操作を行った検査技師

例 5） 夜間等で当直医が主担当医の電話での指示により、指定された薬剤のオーダ入力を行った。

情報 ：投薬指示

確定者 ：実際にオーダを実施した当直医

（参照：システム運用編 14.3、14 章 遵守事項⑨(1)・(2)）

**Q39** 「１４．認証・認可に関する安全管理措置」⑨(1) f において、「確定者が何らかの理由で確定操作ができない場合における記録の確定の責任の所在を明確にすること。例えば、医療情報システム安全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に定めること」とあるが、具体的にどのような場合を指すか。

**A** 確定者の不在や緊急対応等で、本人が確定操作できない場合を指します。

代替確定を認める条件、実施者、事後確認を運用管理規程に定めてください。

（参照：システム運用編 14.3、14 章 遵守事項⑨(1)(f)）

**Q40** 記録を確定する方法として、①入力者が入力画面を見ながら情報を入力して記録する場合、②外部機器等から確定されていない情報を取り込み記録する場合、③外部システムで確定された情報を取り込み記録する場合が考えられるが、それぞれどのように対応すべきか。

**A** 確定操作は、

・文書の責任者が誰かを明らかにする

・操作の時点で対象とする文書の記述に誤入力や改ざん等がないことを保証し、記載に対して責任を持つ

という意味合いがあります。

質問①～③の対応については下記のように考えられます。

①「入力者が入力画面を見ながら情報を入力し記録する場合」

この場合には、確定するという操作を行うことで、内容を確定者が保証することになります。文書の入力を確定者が自ら行う場合や代行入力による場合がありますが、いずれの場合も、確定者が確定したということになります。また、処理としては署名を施す等に該当します。

②「外部機器等から確定されていない情報を取り込み記録する場合」

この場合には入力者が、記述の改ざんや誤入力等がないことを確認した上で、スキャナ等による読み込みを行い、誰の記録であるかを関連付けして、①の確定操作を行うことになります。

③「外部システムで確定された情報を取り込み記録する場合」

改めて受け取り側で確定操作を行う必要はありませんが、外部システムで確定されていることを確認することが必要です。ただし、確定された情報しか取り込まれないようにシステムが構築されている場合、その限りではありません。

（参照：システム運用編 14.3、14 章 遵守事項⑨(1)・(2)）

**Q41** 画像の確定に当たっては明示的な確定操作が必要か。

**A** 必ずしも必要ではありません。例えば、①PACS が受信した時点、②PACS で受信してから一定時間経過した時点、③PACS で受信してから一定時刻を過ぎた時点をもって確定とすること等が考えられます。これらについては、各医療機関等において、運用管理規程に明記することが必要です。

（参照：システム運用編 14.3、14 章 遵守事項⑨(2)(a)）

**Q42** 法令で定められた署名又は記名押印のための電子署名における要件として暗号に関するものがあるが、具体的にはどのようなものを採用する必要があるか。

**A** 安全性が確認された電子署名方式と暗号アルゴリズムを採用してください。

関係法令や電子政府推奨暗号リスト等を確認し、危殆化した方式を更新できるようにしてください。

CRYPTREC 暗号リスト(電子政府推奨暗号リスト)

（参照：企画管理編 14.1、14 章 遵守事項①／システム運用編 15.1、15 章 遵守事項①）

**Q43** 共通鍵、秘密鍵を使用して情報を管理する場合どの程度のレベルのものが必要か。

**A** FIPS 140-3 Level 1 相当以上の暗号モジュールを使用してください。

当該暗号モジュールについては、その認証又は評価の対象となった製品、バージョン及び構成並びに所定の動作モードで使用するとともに、認証又は評価の対象となった暗号方式、動作モード、ハッシュ関数及び鍵長を使用してください。

また、共通鍵及び秘密鍵について、生成、保管、配布又は移送、利用権限、バックアップの要否及び方法、鍵更新、利用停止、廃棄並びに危殆化時の対応を適切に管理してください。

鍵が危殆化し、又はそのおそれがある場合には、当該鍵の利用を停止して鍵を更新するとともに、影響を受ける情報及びシステムの範囲を確認し、必要に応じて新しい鍵による再暗号化等を行ってください。また、危殆化した秘密鍵に対応す

る電子証明書がある場合には、当該電子証明書を速やかに失効させてください。

（参照：システム運用編 15.1、15 章 遵守事項①）

# 保守委託機関編　Q&A

## 保守委託機関編の適用対象

**Q1**　保守委託機関編は、どのような医療機関等を対象とするものですか。

**A**　すべてのサーバのセキュリティアップデート責任を事業者に委託している医療機関等を対象としています。クラウド型電子カルテの利用や保守契約等により、すべての医療情報システムのセキュリティアップデートを事業者が担うことが、契約書、約款、SLA 等で明確になっている場合に利用してください。

（参照：保守委託機関編 1 章（本編の対象））

**Q2**　小規模な医療機関のみが、保守委託機関編の対象ですか。

**A**　いいえ。医療機関等の規模だけで判断するものではありません。すべてのサーバのセキュリティアップデート責任を事業者に委託しているかを確認し、本編の対象判断フローチャートに沿って判断してください。

（参照：保守委託機関編 1 章（本編の対象））

**Q3**　事業者がセキュリティアップデートを実施しているようですが、契約書に記載がない場合も保守委託機関編の対象になりますか。

**A**　対象とは判断できません。事業者が責任を負うことが契約書、約款、SLA 等に明記されている必要があります。記載が不明確な場合は、事業者に確認し、責任の所在を書面等で明確にしてください。

（参照：保守委託機関編 1 章（本編の対象））

## MDS/SDS・別紙

**Q4**　MDS/SDS とは何ですか。また、誰に提出を求めればよいですか。

**A**　MDS/SDS は、医療情報システムやサービスのセキュリティ対応状況を事業者が開示するための資料です。一般社団法人保健医療福祉情報システム工業会が策定しており、厚生労働省標準規格となっています。

提出を求める対象は医療情報システムの製造、販売、保守又はサービス提供を行う事業者になります。

（参照：保守委託機関編 3 章 遵守項目②、10 章 遵守項目⑨、【別紙】MDS/SDS におけるセキュリティ確認事項）

**Q5**　保守委託機関編の別紙は、どのように利用すればよいですか。

**A**　事業者から提出してもらい、MDS/SDS のうち、本編別紙に示された項目が「はい」又は「対象外」となっていることを確認するために利用してください。医療情報システム事業者ではなく、MDS/SDS を提出していただけない場合は、契約書や製品仕様、事業者への問い合わせにより別紙の項目を確認してください。

（参照：保守委託機関編 10 章 遵守項目⑨、【別紙】MDS/SDS におけるセキュリティ確認事項）

**Q6** 別紙の項目に「いいえ」がある場合、そのシステムやサービスは導入できませんか。

**A** 原則として、本編別紙の項目がすべて「はい」又は「対象外」となっている事業者を選定してください。「いいえ」がある事業者を選定する場合は、不足する対策、代替措置を検討してリスクを医療機関等の責任で評価し、導入の可否を判断してください。

（参照：保守委託機関編 10 章 遵守項目⑨、【別紙】MDS/SDS におけるセキュリティ確認事項）

**Q7** MDS/SDS は導入時に一度確認すればよいですか。

**A** いいえ。セキュリティ対応状況は、製品の更新、サービス内容の変更、本ガイドラインの更新等により変化します。契約内容に基づき、サービスや規制の変化に併せて MDS/SDS 及び遵守事項への対応状況を確認してください。

（参照：保守委託機関編 3 章 遵守項目②、10 章 遵守項目⑨、【別紙】MDS/SDS におけるセキュリティ確認事項）