医療情報システムの安全管理に関するガイドライン

第 6.1 版(案)

企画管理編

[Management]

目次

【はじめに】

＜企画管理編が想定する読者＞

企画管理編は、主に医療機関等において医療情報システムの安全管理（企画管理、システム運営）の実務を担う担当者（企画管理者）を対象にしている。

本編では、組織体制や情報セキュリティ対策に係る規程の整備等の統制等の安全管理の実務に当たり具体的に遵守が必要な事項、医療情報システムの実装・運用に関する適切な対応をシステム運用担当者に指示、管理するために必要な事項を示す。

１．管理体系

【遵守事項】

① 医療情報システムの管理に関する法令等について理解し、医療機関等の組織全体として法令等を遵守できるよう、必要な措置を講じること。

② 委託先の医療情報システム・サービス事業者（以下「委託先事業者」という。）等に対しても①に関して必要な措置を講じるよう契約において求め、その対応状況を定期的に把握すること。委託先事業者が再委託を用いる場合も同様の対応をすること。

③ 医療機関等内における法令の遵守状況について経営層に報告し、経営層の確認を取ること。また、遵守状況に応じて必要な改善措置を講じること。

④ 医療情報システムの安全管理に係る法令等が求める内容を把握した上で、対応策を整理すること。必要に応じて、システム運用担当者と具体的な対策について検討を求めて、その結果を反映すること。

⑤ 組織における情報セキュリティ方針、医療情報の取扱いや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を策定し、経営層の承認を得ること。

⑥ ⑤で経営層の承認を得た方針を実行するために必要な体制、規程、技術的措置等の整備を行うこと。またこれらが適切に運用されているか確認すること。

⑦ 患者等からの照会に対応するために必要な医療情報システムの安全管理に関する窓口等を整備すること。

１．１　安全管理に関連する法制度等

１．１．１　医療機関等における医療情報の取扱いに関する法令の遵守

➢ 医療情報の取扱いに関しては、さまざまな法令が関係する。例えば、医療情報は患者の個人情報であることから、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）を遵守する必要がある。さらに、医療情報は基本医療従事者や医療機関等が作成することから、医師法等の各種医療関係の法令の規定を遵守する必要があり、医療従事者や医療機関等には法律上の責任が生じる。（表１－１）

表１－１　医療情報の取扱いに関する法律上の責任

責任分野	関連法	情報に対する責任の内容の例
行政法上の責任	個人情報保護法	個人情報取扱事業者責任
	各種医療関係法※	医療従事者・医療機関等における業法責任
刑事上の責任	刑法等	秘密漏示罪など
民事上の責任	民法（契約）	診療契約（準委任）及びこれに関する安全配慮義務

※　医師法、歯科医師法、薬剤師法、医療法等を想定

- このように、医療機関等における医療情報システムの安全管理に関する責任は、業法責任（行政法上の責任）が中心となる。それと同時に、医療機関等で業務に従事する職員や関係する医療情報システム・サービス事業者（以下「システム関連事業者」という。）等による秘密漏えいや医療情報の漏えい等による損害賠償を防ぐ責任もある。
- 企画管理者は、このような医療機関等が負う責任の根拠となる各種法令等（ガイドライン等を含む。）が、医療機関等の組織全体として遵守されるよう管理すること。
- そのため、企画管理者には、医療情報の取扱いに関する法令等の内容を理解した上で、医療機関等や医療機関等で業務に従事する職員や関係するシステム関連事業者等が遵守すべき内容を整理し、必要な措置を行うことが求められる。
- また、医療機関等内における法令遵守状況の管理は、当該医療機関の経営層の責務でもあることから、企画管理者はその遵守状況について、経営層に適宜報告し、必要に応じて改善策を講じること。

１．１．２　医療情報システムに関係する法令

- 医療機関等が遵守すべき法令の中には、特に医療情報システムで取り扱うデータ等に関係するものが含まれている。例えば、個人情報保護法では、利用目的や第三者提供に関する適切な同意取得のない利用等の禁止等の個人情報の保護に関する必要な対応のほか、安全管理措置義務や委託先の監督等の個人データの保護に関する必要な対応を求めている。
- また、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（平成 16 年法律第 149 号。以下「e-文書法」という。）により電子化して保存することが認められる文書については、e-文書法及びその関係法令に従うことが求められる。
- なお、関係する法令に従って医療従事者が作成する文書（例えば医師法における診療録）の電子媒体による保存については、「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 17 年３月 31 日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知。平成 28 年３月 31 日最終改正。以下「施行通知」という。）第二の２（３）に掲げる３条件を満たす必要がある。

（参考：施行通知第二の２（３））

① 見読性の確保

必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、及び書面を作成できるようにすること。

（ア）情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。

（イ）情報の内容を必要に応じて直ちに書面に表示できること。

② 真正性の確保

電磁的記録に記録された事項について、保存すべき期間中における当該事項の改変又は消去の事実の有無及びその内容を確認することができる措置を講じ、かつ、当該電磁的記録の作成に係る責任の所在を明らかにしていること。

（ア）故意又は過失による虚偽入力、書換え、消去及び混同を防止すること。

（イ）作成の責任の所在を明確にすること。

③ 保存性の確保

電磁的記録に記録された事項について、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。

- また、診療録等を病院又は診療所等以外の場所に外部保存する場合は、「診療録等の保存を行う場所について」（平成 14 年 3 月 29 日付け医政発第 0329003 号・保発第 0329001 号厚生労働省医政局長、保険局長連名通知。平成 25 年 3 月 25 日最終改正。以下「外部保存通知」という。）に従うことが求められる。
- さらに、医療従事者等が作成する医療情報を含むデータに対して電子署名を施す必要がある場合には、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。以下「電子署名法」という。）等に従うこと。
- サイバー攻撃の脅威が近年増大していることに鑑み、医療法施行規則（昭和 23 年厚生省令第 50 号）第 14 条第 2 項は、「病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（略）を確保するために必要な措置を講じなければならない。」とし、医薬品、医療機器の品質、有効性及び安全性の確保等に関する法律施行規則（昭和 36 年厚生省令第 1 号）第 11 条第 2 項第 1 号は、薬局の管理者が遵守すべき事項として「保健衛生上支障を生ずるおそれがないように、その薬局に勤務する薬剤師その他の従業者を監督し、その薬局の構造設備及び医薬品その他の物品を管理し、その薬局の業務に係るサイバーセキュリティ（略）の確保のために必要な措置を講じ、その他その薬局の業務につき、必要な注意をすること。」としている。
- 本ガイドラインでは、これらの法令で規定している内容を前提として、遵守が必要な事項を示している。
- 企画管理者は、これらの法令等の内容を把握、整理した上で、必要な措置を講じることが求められる。具体的な方法については、医療情報システムに関する運用やシステム仕様の検討等に関わるシステム運用担当者に検討を求める必要がある。その上で、担当者の検討結果を踏まえて、講ずる措置の中に盛り込むことが求められる。

表１－２　医療情報システムに関係する法令

法令名	概要
個人情報保護法	個人情報及び個人データ（検索性のある個人情報）の管理に関する内容（安全管理措置義務、漏えい等の報告義務、第三者提供の制限等）を規定。
e 文書法省令[1] 施行通知	e-文書法を踏まえ、厚生労働省の所管する法令の規定に基づく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の要件等を規定。（対象となる書面（文書）は、表１－３のとおり。）
外部保存通知	診療録等の外部保存を行う際の基準や電子媒体により外部保存を行う際の留意事項等を規定。（対象となる記録等は表１－４のとおり。）
電子署名法	電磁的記録として作成される情報に行われる電子署名に関する要件等を規定。 医療情報を含む情報に関しては、電子署名を行うものについて電子署名法に基づく電子署名の要件に加え、署名者の資格確認に係る要件もあわせて満たす必要がある。

表１－３　　電磁的記録の保存、作成及び交付等を行うことができる文書

[1] 厚生労働省の所管する法令の規定に基づく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省令（平成 17 年 3 月 25 日厚生労働省令第 44 号）

1．医師法（昭和 23 年法律第 201 号）第 24 条の診療録
2．歯科医師法（昭和 23 年法律第 202 号）第 23 条の診療録
3．保健師助産師看護師法（昭和 23 年法律第 203 号）第 42 条の助産録
4．医療法（昭和 23 年法律第 205 号）第 51 条の財産目録及び貸借対照表並びに損益計算書
5．歯科技工士法（昭和 30 年法律第 168 号）第 19 条の指示書
6．薬剤師法（昭和 35 年法律第 146 号）第 28 条の調剤録
7．外国医師又は外国歯科医師が行う臨床修練に係る医師法第十七条及び歯科医師法第十七条の特例等に関する法律（昭和 62 年法律第 29 号）第 11 条の診療録
8．救急救命士法（平成 3 年法律第 36 号）第 46 条の救急救命処置録
9．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 項の帳簿
10. 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 条の診療録等（作成については、同規則第 22 条）
11. 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 条の調剤録（作成については、同規則第 5 条）
12. 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 の書類（作成については、同規則第 12 条第 14 号及び第 15 号）
13. 医療法第 21 条第 1 項の記録（同項第 9 号に規定する診療に関する諸記録のうち医療法施行規則第 20 条第 10 号に規定する処方せんに限る。）、第 22 条の記録（同条第 2 号に規定する診療に関する諸記録のうち医療法施行規則第 21 条の 5 第 2 号に規定する処方せんに限る。）、同法第 22 条の 2 の記録（同条第 3 号に規定する診療に関する諸記録のうち医療法施行規則第 22 条の 3 第 2 号に規定する処方せんに限る。）及び同法第 22 条の 3 の記録（同条第 3 号に規定する診療及び臨床研究に関する諸記録のうち医療法施行規則第 22 条の 7 第 2 号に規定する処方せんに限る。）※
14. 薬剤師法第 26 条及び第 27 条の処方せん※
15. 保険薬局及び保険薬剤師療養担当規則第 6 条の処方せん※
16. 医療法第 21 条第 1 項の記録（医療法施行規則第 20 条第 10 号に規定する処方せんを除く。）、同法第 22 条の記録（医療法施行規則第 21 条の 5 第 2 号に規定する処方せんを除く。）、同法第 22 条の 2 の記録（医療法施行規則第 22 条の 3 第 2 号に規定する処方せんを除く。）及び同法第 22 条の 3 の記録（医療法施行規則第 22 条の 7 第 2 号に規定する処方せんを除く。）
17. 麻薬及び向精神薬取締法（昭和 28 年法律第 14 号）第 27 条第 6 項の処方せん※
18. 歯科衛生士法施行規則（平成元年厚生省令第 46 号）第 18 条の歯科衛生士の業務記録
19. 医師法第 22 条の処方せん※
20. 歯科医師法第 21 条の処方せん※
21. 健康保険法施行規則（大正 15 年内務省令第 36 号）第 54 条の処方せん※
22. 船員保険法施行規則（昭和 15 年厚生省令第 5 号）第 45 条第 1 項の処方せん※
23. 保険医療機関及び保険医療養担当規則第 23 条第 1 項の処方せん※
24. 国民健康保険法施行規則（昭和 33 年厚生省令第 53 号）第 25 条の処方せん※
25. 高齢者の医療の確保に関する法律施行規則（平成 19 年厚生労働省令第 129 号）第 30 条の処方せん※

26. 診療放射線技師法（昭和 26 年法律第 226 号）第 28 条第 1 項の規定による照射録
※ 処方せんについては、施行通知第二の２（４）の要件を充足する必要がある。

また、介護事業者が取り扱う文書等のうち、下記文書等は、e-文書法の対象範囲であり、かつ当該文書の内容には医療情報が含まれることがある。

1．指定居宅サービス等の事業の人員、設備及び運営に関する基準（平成 11 年厚生省令第 37 号）第 73 条の 2 第 2 項の規定による訪問看護計画書及び訪問看護報告書
2．指定居宅サービス等の事業の人員、設備及び運営に関する基準第 154 条の 2 第 2 項（第 155 条の 12 において準用する場合を含む。）の規定による短期入所療養介護計画
3．指定居宅サービス等の事業の人員、設備及び運営に関する基準第 191 条の 2 第 2 項及び第 192 条の 11 第 2 項の規定による特定施設サービス計画
4．指定介護老人福祉施設の人員、設備及び運営に関する基準（平成 11 年厚生省令第 39 号）第 37 条第 2 項の規定による施設サービス計画
5．介護老人保健施設の人員、施設及び設備並びに運営に関する基準（平成 11 年厚生省令第 40 号）第 38 条第 2 項の規定による施設サービス計画
6．健康保険法等の一部を改正する法律の一部の施行に伴う厚生労働省関係省令の整備に関する省令（平成 24 年厚生労働省令第 10 号）による廃止前の指定介護療養型医療施設の人員、設備及び運営に関する基準（平成 11 年厚生省令第 41 号）第 36 条第 2 項の規定による施設サービス計画
7．指定訪問看護の事業の人員及び運営に関する基準（平成 12 年厚生省令第 80 号）第 30 条第 2 項の規定による訪問看護記録書、訪問看護指示書、特別訪問看護指示書、精神科訪問看護指示書、精神科特別訪問看護指示書、在宅患者訪問点滴注射指示書、訪問看護計画書及び訪問看護報告書
8．指定介護予防サービス等の事業の人員、設備及び運営並びに指定介護予防サービス等に係る介護予防のための効果的な支援の方法に関する基準（平成 18 年厚生労働省令第 35 号）第 73 条第 2 項の規定による介護予防訪問看護計画書及び介護予防訪問看護報告書
9．指定介護予防サービス等の事業の人員、設備及び運営並びに指定介護予防サービス等に係る介護予防のための効果的な支援の方法に関する基準第 194 条第 2 項（第 210 条において準用する場合を含む。）の規定による介護予防短期入所療養介護計画
10. 指定介護予防サービス等の事業の人員、設備及び運営並びに指定介護予防サービス等に係る介護予防のための効果的な支援の方法に関する基準第 244 条第 2 項及び第 261 条第 2 項の規定による介護予防特定施設サービス計画
11. 指定地域密着型サービスの事業の人員、設備及び運営に関する基準（平成 18 年厚生労働省令第 34 号）第 3 条の 40 第 2 項の規定による定期巡回・随時対応型訪問介護看護計画及び訪問看護報告書
12. 指定地域密着型サービスの事業の人員、設備及び運営に関する基準第 40 条の 15 第 2 項の規定による療養通所介護計画
13. 指定地域密着型サービスの事業の人員、設備及び運営に関する基準第 128 条第 2 項の規定による地域密着型特定施設サービス計画
14. 指定地域密着型サービスの事業の人員、設備及び運営に関する基準第 156 条第 2 項（第

169 条において準用する場合を含む。）の規定による地域密着型施設サービス計画

15. 指定地域密着型サービスの事業の人員、設備及び運営に関する基準第 181 条第 2 項の規定による居宅サービス計画、看護小規模多機能型居宅介護計画及び看護小規模多機能型居宅介護報告書

16. 介護医療院の人員、施設及び設備並びに運営に関する基準（平成 30 年厚生労働省令第 5 号）第 42 条第 2 項（第 54 条において準用する場合を含む。）の規定による施設サービス計画

なお、法令等によって作成や保存が定められている文書等のうち、e-文書法の対象範囲でない医療関係文書等については、たとえ電子化したとしても、その電子化した文書等を法令等による作成や保存が定められた文書等として取り扱うことはできないため、別途紙媒体による作成・保存が必要となる。

表１－４　外部保存を認める記録等

1．医師法第 24 条に規定されている診療録

2．歯科医師法第 23 条に規定されている診療録

3．保健師助産師看護師法第 42 条に規定されている助産録

4．医療法第 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

5．医療法第 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

6．診療放射線技師法第 28 条に規定されている照射録

7．歯科技工士法第 19 条に規定されている指示書

8．薬剤師法第 27 条に規定されている調剤済みの処方せん

9．薬剤師法第 28 条に規定されている調剤録

10. 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

11. 救急救命士法第 46 条に規定されている救急救命処置録

12. 医療法施行規則第 30 条の 23 第 1 項及び第 2 項に規定されている帳簿

13. 保険医療機関及び保険医療養担当規則第 9 条に規定されている診療録等

14. 保険薬局及び保険薬剤師療養担当規則第 6 条に規定されている調剤済みの処方せん及び調剤録

15. 臨床検査技師等に関する法律施行規則第 12 条の 3 に規定されている書類

16. 歯科衛生士法施行規則第 18 条に規定されている歯科衛生士の業務記録

17. 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

18. 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

１．２　医療情報システムの安全管理に関する方針の策定

１．２．１　情報セキュリティ方針等の策定

- 医療機関等の組織全体として医療情報システムの安全管理に対する共通の認識を有し、適切な安全管理を行うためには、一組織としての方針を定める必要がある。
- この方針は、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）[4]、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に分けられる。企画管理者は、このような情報セキュリティ方針等の方針を策定した上で、経営層の承認を受けて、組織の方針として定めることが求められる。なお、医療機関等が所属する法人等において情報セキュリティ方針等が別に定められている場合には、当該医療機関等に特有の事項等について検討し、必要に応じて補則等を整備すること。

１．２．２　個人情報保護に関する方針の策定

- 医療機関等における個人情報保護に関する方針としては、いわゆるプライバシーポリシー等があるが、これは、医療機関等が行う個人情報の保護に関する措置の透明性の確保と対外的な明確化を目的としており、「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」（個人情報保護委員会、厚生労働省（平成 29 年４月 14 日））（以下「ガイダンス」という）においても求められているものである。企画管理者は、医療情報システムに関する情報セキュリティ方針等と併せて、個人情報保護に関する方針についても策定の上、経営層による承認を得て、組織の方針とすることが求められる。

[4] 情報セキュリティ方針（ポリシー）には、セキュリティ対策の目的や方向性や、関係主体等からの要求事項への対応を含むことが求められる。

2．責任分界

【遵守事項】

① 医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。また、重要な委託等に関する責任分界については、取決めに当たり、事前に経営層の承認を得ること。

② 取決めを行う責任分界のうち技術的な部分に関しては、その具体的な内容を検討するようシステム運用担当者に指示を行い、その結果を責任分界の取決めに反映させること。

③ 責任分界を取り決める際には、あらかじめ必要な情報を収集した上で、医療機関等におけるリスク管理を踏まえた仕様の適合性に関する調整を委託先事業者等と行うこと。

④ 委託先事業者等と責任分界の取決めを行う際には、委託先事業者が提供する医療情報システム・サービスの内容を踏まえて、安全管理に関する役割分担についても取り決めること。

⑤ 委託先事業者等において複数の関係者が関与する場合には、その関係を整理し、医療機関等が直接責任分界を取り決める相手方を特定すること。また、関与する関係者への管理なども責任分界の取決めに含めること。さらに、責任分界の取決めに際しては、委託先事業者間での役割分担なども含めて、取決め内容に漏れがないよう留意すること。

⑥ 第三者提供を行う際の責任分界については、技術的な内容と手続的な部分の役割分担を含めて取り決めること。

2．1 運用管理における責任分界

2．1．1 医療機関等における責任と責任分界

- 医療機関等の医療情報システムの安全管理に関する責任として、通常時における責任と非常時における責任がある。
- 医療機関等がシステム関連事業者に委託を行い、医療情報システムの実装や運用を図る場合には、この委託契約に基づいて、医療機関等とシステム関連事業者との間で、医療情報システムの実装や運用に関する責任の分担（責任分界）を決める必要がある。従って責任分界の設定においては、通常時における責任を果たすための責任分界と、非常時における責任を果たすための責任分界の二つが想定される。
- また、このような責任分界の設定に際しては、医療機関等とシステム事業者等において、それぞれ医療情報システムに根差すリスクに関する共通の理解を得た上で、それぞれがどのリスクに対してどのような対応を行うかを決めることにより、具体的な責任分界の内容を決めることができる。このようなリスクに関する合意を図るためのリスクコミュニケーションを行うことも、委託においては重要である。
- 運用管理においては、医療機関等とシステム関連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上で、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。

２．１．２ 通常時における責任

- 医療機関等が負う通常時における責任としては、
  ・説明責任
  ・管理責任
  ・定期的な見直し、必要に応じて改善を行う責任
  がある。

（１）説明責任

- 説明責任とは、医療情報システムの運用状況等が適切に行われていること等を患者等に説明する責任である。医療情報システム・サービスの運用等についてシステム関連事業者に委託している場合には、委託している範囲の医療情報システム・サービスの運用状況等について、医療機関等において直接把握することが難しい。そこで医療機関等は、委託先事業者に対して、提供を受ける医療情報システム・サービスが本ガイドラインを遵守した仕様や運用となっていることの説明を求めることができるよう、委託先事業者と取決めを行う必要がある。
- 例えば、医療情報システム・サービスの採用に際しては、システム関連事業者からサービス仕様適合開示書等の提供などを受けることになるが、当該文書の中に本ガイドラインを遵守している旨（あるいは遵守できていない部分がある場合はその旨）を記載することのみならず、委託決定後も必要に応じて当該遵守状況を示す資料の提供を求めることができる旨の取決めを行うことが求められる。（なお、このような説明責任に関する分担の取決めがない場合には、医療機関等は自ら委託している医療情報システム・サービスの運用状況に関する説明のための資料を用意することが必要となる。）

（２）管理責任

- 医療機関等における管理責任とは、医療情報システムの運用管理を医療機関等が適切に行う責任である。これも医療情報システム・サービスを委託している場合には、委託している範囲の医療情報システム・サービスの運用状況等について医療機関等において直接把握することが難しいため、委託先事業者に適切な運用管理の実施を委ねるとともに、医療機関等は適宜委託先事業者において適切な運用がなされていることを管理することで、責任の分担を図る必要がある。
- 特に委託先事業者が再委託を行う場合、再委託先事業者において生じた漏えい等の情報セキュリティインシデントの責任も、委託元の医療機関等の責任となりうることから、再委託先事業者の管理だけではなく選定などについても、委託先事業者と適切に分担することが求められる。また、医療機関等が購入した機器等については、別途、事業者と当該機器についての保守契約を締結しない場合には、原則、管理責任は医療機関等にあり、事業者との間での管理責任の分担は生じない。
- 以上の内容を踏まえながら、企画管理者は、管理責任を全うするため、委託先事業者に対して、委託先事業者の運用状況の報告資料の提供や、委託先事業者による再委託が行われる場合には再委託先事業者も含めた責任分界についての取決めを行うことが求められる。

（３）定期的な見直し、必要な改善を行う責任

- 医療機関等において定期的な見直しを実施し、必要な改善を行う責任は、基本的には医療機関等が自ら負うものである。ただし、医療情報システム・サービスを委託している場合には、委託先事業者から、適宜、情報提供や提案等を求め、医療機関等における見直しの参考とすることなどが想定される。
- また、サイバーセキュリティ対策の観点から、委託先事業者に対して、委託している医療情報システム・サービスに関して、自発的な見直し対応を求めることも想定される。企画管理者は、委託先事業者に対して、委託しているサービスの特徴に応じて、必要であれば自発的な対策の見直しを求める項目などを、SLA 等に含めるなどの対応を行うことが求められる。

２．１．３　非常時における責任

- 医療機関が負う非常時における責任としては、
  ・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
  が挙げられる。

（１）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

- 医療情報に関して、例えばサイバー攻撃などで、医療情報が破壊されたり、漏えいしたりした場合には、対策を講じるために、原因を特定し、その上で対策の検討、それらに関する対外的説明などを行う必要がある。
- 対外的な説明に関しても、専門的な見地からの対応が求められることもあるため、医療機関等とシステム関連事業者との間での分担等の取決めを行うことが求められる。
  - 企画管理者は、対外的説明の範囲や内容などをあらかじめシステム関連事業者と取り決めておく必要がある。

（２）善後策を講ずる責任

- 医療機関等が果たすべき善後策を講ずる責任の中には、「情報セキュリティインシデントの原因を究明する責任」、「再発防止策を講ずる責任」がある。
- 医療情報システム・サービスを委託している場合には、情報セキュリティインシデントの原因が直ちに判明しない場合が想定されることから、医療機関等と委託先事業者とで協力して対応する必要があり、これらの責任分界についても医療機関等と委託先事業者とであらかじめ取り決めておく必要がある。具体的には、情報セキュリティインシデント発生後から収束に至るまでの期間の対応における分担や協力の内容に関して、あらかじめ委託先事業者と取り決めておくことで、的確かつ迅速な原因究明が可能となるとともに、究明された原因に応じた再発防止策を講じる際の分担や協力についても取り決めておくことで、情報セキュリティインシデントの発生後、システム関連事業者への医療情報システム・サービスの委託を継続する場合に、再発防止策を含むインシデントを踏まえた委託内容の更新を的確かつ迅速に行うことが可能となる。
- 以上のとおり、企画管理者はこれらの責任を適切に果たすことができるよう、システム関連事業者との間での役割分担を含む責任分界を定める必要がある。

２．１．４　リスク分析を踏まえた要求仕様適合性の確認への対応

- 医療機関等とシステム関連事業者との間で、役割分担、当該事業者が受容したリスクの内容等について合意形成を図るため、医療情報システムについて、医療機関等におけるリスクアセスメントを踏まえた医療機関等の要求仕様への適合性を確認する必要がある。

- 医療機関等によるリスクアセスメントの結果、一部のリスクを委託先事業者で負うことになることが想定される。その際に、委託先事業者が想定していたリスクの内容とリスクアセスメントを踏まえたリスクの内容に不一致があると、リスク管理が不十分となり得る。そこで、医療機関等が責任分界を定めるに際しては、その前提としてそれぞれが負うことが想定されるリスクの内容について、合意を得るための調整を行うことになる。
- 実際には、システム関連事業者が提供する情報やサービス仕様適合開示書等の内容を踏まえて、遵守している対策項目等の状況が医療機関等で求める内容と乖離があるかどうかを把握すること。乖離がある場合には対応を両者で協議し、合意した上で、医療情報システム・サービスの提供を受けることが想定される。
- 企画管理者は、このような要求仕様適合性の調整・確認に必要な情報をシステム関連事業者から収集し、必要な調整を行った上で、責任分界に関する取決めを行うことが求められる。

2．1．5　医療情報システム等提供事業者との取決めにおける留意点

- 医療情報システム等提供事業者との間で取決めを行う場合、事業者が提供するシステム・サービスの内容や、その契約形態などに応じて、具体的なコミュニケーションについて留意する必要がある。例えば、個々に契約内容等の調整を行うことを想定した医療情報システム等の提供と、パブリッククラウドサービスのように約款契約による画一的な契約内容による場合では、コミュニケーションの進め方は異なる。特に約款契約による場合には、個々の契約内容の調整が難しいことから、医療機関等は対象事業者に対して、より丁寧にサービス内容やリスクについて、わかりやすい情報提供を求めること。具体的には、以下のような対応を事業者に求めることが挙げられる。
  - リスク判断に必要な基礎資料の提供（MDS/SDS[6]等の提供、主なセキュリティ事項に関するチェック結果の提供等）
  - 医療機関等側が説明を求めた場合の対応の表示
  - 約款契約におけるリスクの表示（民法第 548 条の 2 関係）
  - 医療機関等が、リスクや役割分担等を確認した上でサービス利用する旨を明示することを求め、合意すること

2．2　責任分界の決め方

2．2．1　委託と第三者提供における責任分界

- 医療機関等が責任分界を取り決める場面として大きく 2 つの場面が想定される。
- 一つが医療情報システムに関連して、委託を行う場合に委託先事業者との間で取り決める責任分界である。
- もう一つは、医療機関等が保有する医療情報を、第三者に提供する際に、提供元の医療機関等と提供先の第三者との間で取り決める責任分界である。

2．2．2　委託における責任分界（複数事業者が関与する場合を含む）

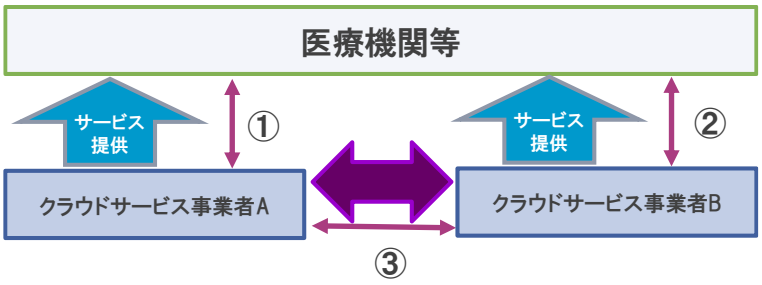
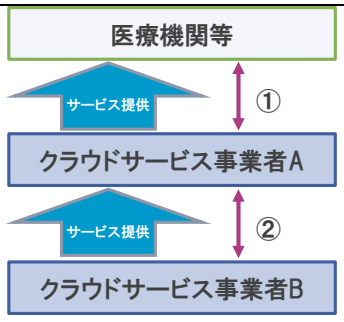
- 医療機関等の医療情報システム・サービスが一事業者のみから提供されたもので構成されている場合には、2.1 に示す内容で責任分界を決定することになる。
- しかし実際には、医療機関等が利用する医療情報システム・サービスは複数の事業者が提供するサービスから構成されており、医療機関等と各事業者との関係を考慮した上で、責任分界を取り決めることになる。
- システム関連事業者が提供するサービスの類型により、医療機関等が直接管理する医療情報システムに関する情報機器やソフトウェアなどの範囲が異なるため、サービス類型に応じた責任分界を取り決めること。

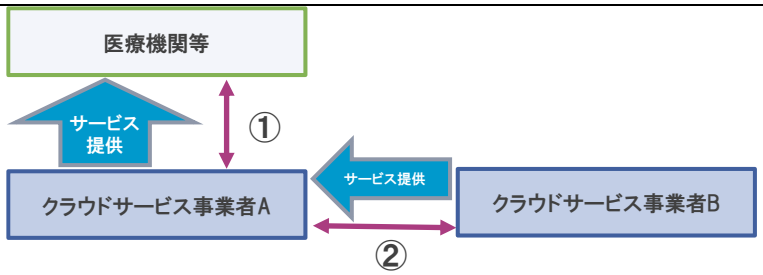
[6] 厚生労働省標準規格 「HS040「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド」参照

（１）複数のシステム関連事業者に対する委託を含む場合の責任分界

- 医療情報システム・サービスを委託する場合、複数のシステム関連事業者が関わる場合があり、具体的には医療機関等が複数のシステム関連事業者の提供するサービスを組み合わせて利用する場合と、一システム関連事業者が複数のサービスを組み合わせて提供するサービスを利用する場合などが想定される。
- 前者の場合は、基本的には医療機関等が各事業者と責任分界を取り決めることになるが、複数のシステム関連事業者のサービスの連携部分についても併せて取決めを行うことが求められる。これには、技術的な仕様等に関する取決めだけではなく、非常時におけるシステム関連事業者間での対応なども含めて取り決めることが求められる。
- 後者の場合には、基本的には医療機関等は最終的に医療情報システム・サービス等を取りまとめて提供するシステム関連事業者との間で責任分界を定めることになる。この場合、当該事業者が利用する他の事業者のサービスとの関係では、委託先事業者による再委託の関係になることが多いため、医療機関等は、取りまとめを担うシステム関連事業者との間で、当該事業者が再委託や提携に当たり他のシステム関連事業者との間で責任分界が整理されていることを確認した上で、取決めを行う。
- 前者はシステム関連事業者間の責任分界の取決めにも医療機関等が関与していく必要があり、システム関連事業者の数だけ対応が必要となることから、一般的には後者の形態でのサービスの利用を行い、責任分界を定めることが望ましい。
- 企画管理者はこれらの場合について、各事業者に必要な対応を依頼できるよう、責任分界について契約や SLA などにおいて取り決めることが求められる。
- VPN 機器をはじめとする外部ネットワークとの接続点となる機器については、脆弱性の管理が適切に行われず、サイバー攻撃の起点となる事案が頻発している。脆弱性の管理等について保守契約の範囲を明確にし、確実に管理可能な体制を整備すること。

表２－１　クラウドサービスの提供パターンと責任分界

パターン	概要
医療機関等が複数のシステム関連事業者の提供するサービスを組み合わせて利用	 ・　医療機関等が事業者 A、B をそれぞれ別に契約してサービスを利用（①、②） ・　A、B の連携が取れるように③の部分についても各①、②の契約内容に盛り込む必要がある。
一システム関連事業者が複数のサービスを組み合わせて提供するサービス	 ・　医療機関等は利用する事業者 A と取り決め（①）、A が他のサービス B を利用（②：別の

	階層サービスを利用）  ・　医療機関等が利用する事業者 A と取り決め(①)、A が他のサービス B を利用（②：別の機能のサービスを利用）

出所：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３版）より作成

（２）医療機関等が利用するサービスの類型による責任分界

- 医療機関等が利用するサービス類型により、医療機関等が直接管理できる医療情報システムの範囲が異なる場合がある。
- クラウドサービスの場合、医療情報システムが利用するソフトウェア・ミドルウェア・ハードウェアなどのクラウドサービスのリソースの層により、SaaS、PaaS、IaaS などの類型に分類される。このうち SaaS では、医療情報システムのアプリケーションの層、PaaS では、医療情報システムが利用するミドルウェアの層、IaaS では医療情報システムが利用するサーバやネットワークなどのインフラの層がサービスとして提供されることになる。
- 従って、例えば SaaS を利用する場合には、医療情報システムのうち、アプリケーション部分の管理や責任をシステム関連事業者に委ねることになるため、アプリケーション部分に関する安全管理ガイドラインの遵守状況を確認するに当たって、システム関連事業者との責任分界の検討は必要となる。
- このように、利用するサービスの内容により、それぞれが負うべき責任の内容が異なるため、企画管理者は、委託により医療機関等が行うべき安全管理のうちどの部分の責任をどちらが負うのかといった責任分界を取り決めるとともに、それぞれが対応する安全管理の具体的な内容についてシステム関連事業者と取り決めることが求められる。
- クラウドサービスなどを利用する場合には、利用者側でもルールの策定や設定等の役割などを果たすことが求められる。このような役割分担については、「クラウドサービス提供・利用における適切な設定に関するガイドライン」[7]などでも示されている。システム運用担当者は、このような資料を参考にして、システム関連事業者との技術的な役割分担についても調整することが求められる。

２．２．３　第三者提供における責任分界

- 医療機関等が管理する医療情報を第三者に提供する場合には、医療機関等と提供先の第三者との間で責任分界を取り決めることになる。この場合、医療情報データの送信、受信に係る責任分界など技術的対策に関する内容のほか、医療情報の提供に係る法律上の義務への対応（第三者提供に関する手続等）の分担なども確認する必要がある。
- 責任分界を定めるのは、例えば
  ・医療情報連携ネットワークにおける医療情報の提供
  ・個々の医療機関等間での医療情報の提供
  ・患者の依頼に基づく、医療機関等から特定の場所（患者宅、患者が利用するサービスを提供する事業者等）

[7] 総務省　令和４年 10 月 31 日

への当該患者の医療情報の送付
・その他法令に基づく第三者提供
等の場面が想定される。

3．安全管理のための体制と責任･権限

【遵守事項】

① 情報システム管理委員会等の組織が構成されている場合には、その業務内容、権限等の運営に関する規程等を策定し、経営層の承認を得ること。委員会等が設置されない場合も、情報システムの導入や変更に当たっては、経営層や医療情報システム安全管理責任者等の承認を必要とする仕組みを構築すること。

② 非常時の対応を想定して、安全管理に必要な体制を構築すること。特に医療機関等において発生した情報セキュリティインシデントに対処するための体制として情報セキュリティ責任者（CISO）や CSIRT などの要否を検討し、必要な措置を講じ、その結果を経営層に報告し、承認を得ること。

③ 法律上の対応を含め医療情報の漏えい等が生じた際の必要な体制の構築や手順の策定等の必要な措置を講じ、その結果を経営層に報告し、承認を得ること。

④ 医療機関等内における医療従事者や職員等に対して、医療情報の安全な取扱いに必要な教育や訓練を講じるための体制を整備すること。

⑤ 医療情報の取扱いに関して委託等を行う場合には、委託先事業者を含めた安全管理に関する体制を整備すること。

⑥ 医療情報の取扱いの安全性が確保できるよう、内部検査及び監査等の体制を構築すること。

⑦ 患者等からの相談や苦情への対応を行うための体制を構築すること。

⑧ 医療情報システムの安全管理の責任を担う者としての位置付け、その業務範囲と権限を明確にし、その内容について経営層の承認を得ること。

⑨ 安全管理に関する技術的な対応を行う担当者を任命し、その業務内容、権限、業務上の義務等を明確にし、経営層の承認を得ること。

⑩ ①～⑨までの対応においては、整備した内容を可視化できるようにすること。

3．1　医療情報システムの安全管理体制の構築

3．1．1　医療情報システムの安全管理のための企画管理者の設置

- 企画管理者とは、医療情報システムの安全管理を行うために必要な運用管理の管理責任者を指す。ここでいう「運用管理」には、安全管理のうち「組織的な対応」と「技術的な対応」のいずれをも含んだものである。

3．1．2　非常時の体制･CSIRT 等の整備

- 医療機関等で情報セキュリティインシデントが発生した場合、この非常時対応として、迅速な判断や対応を要する。これに対応するための体制整備も必要であり、特にサイバー攻撃を受けた場合には、初動対応等専門的な対応が可能な体制を要する。企画管理者は、こうした体制の構築について、通常時からその内容について検討し、必要な措置を講じること。
- ここでいう非常時の体制における対応としては、
  ･影響範囲や損害の特定
  ･被害拡大防止を図るための初動対応
  ･復旧措置のための対応
  ･再発防止策の検討
  などがある。
- サイバー攻撃に対しては情報セキュリティ責任者（CISO：Chief Information Security Officer）の配置

や、CSIRT（Computer Security Incident Response Team）の構築が有効とされており、企画管理者はこれらの整備の要否や、必要な場合にはその構成や非常時の対応内容などについて検討し、経営層の承認を得ること。

- また、医療情報の漏えいが生じた場合も、法令上必要な対応（個人情報保護法に基づく漏えい等の報告など）や説明責任の実施等の必要な措置を講じる必要があるため、体制や手順等を整備して、経営層の承認を得ること。

３．１．３　医療機関等の内部における職員等に対する教育・訓練等の体制

- 医療情報システムの安全管理においては、医療機関等において医療情報システムに関与する全ての者において当該安全管理に対する知識と意識付けが求められる。そのため、企画管理者は、職員に対して安全管理に関する教育・訓練等を行うとともに、必要な体制を整備することが求められる。

３．１．４　委託等における安全管理の体制

- 医療情報システムの安全管理においては、何らかの形でシステム関連事業者が関与する場合が多く、運用等をシステム関連事業者へ委託することも多い。
- 個人情報保護法第 25 条において委託先の監督義務が示されているとおり、医療機関等においては委託先事業者の安全管理の体制も含めて把握することが必要となる。
- 企画管理者は、委託等における安全管理を行うため、委託先事業者については、委託先事業者の運用等の体制や連絡体制を明確にするほか、運用状況を定期的に把握するために必要な体制を整備すること。

３．１．５　監査体制の整備と監査責任者の設置

- 医療情報システムの安全管理が適切に行われていることを担保するためには、担当者による自己点検だけではなく、客観的な監査によることが重要である。監査は、担当者や企画管理者以外の医療機関等内の第三者による方法や、外部の第三者による方法などが挙げられる。
- 企画管理者は、安全管理が適切に行われていることを確認するために監査等の必要な体制を整備すること。

３．１．６　患者等からの苦情・質問の受付体制

- 「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」では、医療機関等が患者などに対して説明責任を果たすためには、個人情報の取扱いに関し患者等からの問い合わせや苦情への対応等を行う窓口機能等を整備することが必要とされている。
- 企画管理者は、患者等からの相談や苦情への対応を行うための受付体制の整備を行うこと。

３．１．７　体制整備の可視化

- 医療情報システムの安全管理の体制を明確にすることは、医療機関等内において医療情報を取り扱う者が滞りなく安全管理に関する対応を行うために必要であり、また非常時において迅速かつ適切な対応をとる上でも重要である。
- 企画管理者は、医療情報システムの安全管理に関して整備した体制に関する内容を文書化等によって可視化し、関係者に共有できるようにする必要がある。

３．２　安全管理の責任・権限

３．２．１　企画管理者の業務範囲と権限

- 経営層は医療情報システムにおける安全管理について医療機関としての最終的な管理責任を負うが、企画管理者はその経営層の判断をサポートし、医療機関等において円滑に安全管理を行うことができるようにすることが重要な業務である。
- 具体的な企画管理者の業務範囲としては、医療機関等の医療情報システムの安全管理について、
  ・経営層が行う管理をサポートするために必要な資料の作成や報告
  ・日常的な医療情報システムの安全管理
  が想定される。また、これらを行うのに必要な承認権限等を有することが想定される。

３．２．２　情報システム管理委員会の業務範囲と権限

- 複数の部門（担当する業務毎に区分された組織）が存在する医療機関等においては経営層の行う管理等の一部又は全部を担うものとして、情報システム管理委員会やセキュリティ委員会等の設置が求められる。委員会を設置する場合には、設置の根拠、目的、業務範囲、構成員の選定・任命方法、権限などを規程等で設け、これに基づいて運営すること。
- また、各部門に委員会に参加するセキュリティ担当者等を配置し、統制に実効性を持たせること。
- 企画管理者は、これらの規程等を策定の上、経営層の承認を得る必要がある。
- 昨今、各部門が独自に調達したシステムやそれに伴う回線が、管理不十分なシャドーIT となり、サイバー攻撃の起点となる事案が起きている。医療機関等の規模を考慮して、委員会が設置されない場合も、情報システムの導入や変更に当たっては、経営層や医療情報システム安全管理責任者等の承認を必要とする仕組みを構築すること。
- また、多数の外部接続点が存在することは、それ自体が管理を困難にし、VPN 装置等の脆弱性が放置されるリスクが増大する。新たに導入するシステムに保守回線が必要な場合は、医療機関側で集約した回線を利用可能な事業者を選定する等、管理の実効性を高めるための対策を講じること。

３．２．３　担当者の任命、業務範囲、権限

- 企画管理者は、医療情報システムの安全管理のうち特に技術的な対応を行う担当者を任命し、経営層の承認を得る必要がある。
- ここでいう技術的な対応の内容としては、
  ・技術的な対応に必要なリスクアセスメント
  ・採用すべき技術等の選定と実装、関連資料の作成
  ・医療情報システムの運用とそのための規則やマニュアル等の作成
  ・上記に対する企画管理者への報告や協議
  等が考えられる。
- 担当者の権限としては、技術的な対応のうち、通常時における運用に関する判断権限、非常時における一次対応の判断権限などが想定される。そのほか、技術的な対応のうち重要なものについては、企画管理者へ協議を行い、対応することが想定される。

４．医療情報システムの安全管理において必要な規程・文書類の整備

【遵守事項】

① 医療機関等が医療情報システムの安全管理に関して定める各種方針等を実現するために必要な規程等の整備を行い、経営層の承認を取ること。

② 規程等に基づいて、医療情報の取扱いや医療情報システムの構築、運用を行うために必要な規則類の整備を行うこと。規則類は必要に応じて見直しを行うこと。

③ 医療情報システムの構築、運用における通常時の対応に必要なマニュアル類や各種資料の整備を担当者に指示し、確認すること。

④ 非常時における医療情報システムの運用等に関するマニュアル類や各種資料の整備を担当者に指示し、整備状況を確認の上、経営層に報告すること。

４．１　運用管理において必要な文書の体系（方針、規程、規則、マニュアル等）

- 医療情報システムの安全管理が適切に行われるためには、組織内において明文化されたルールが必要である。医療機関等においては安全管理に関する方針を定めるが、これを実際に運用するためには、より詳細な規程等の整備が必要となる。
- 企画管理者は、必要な規程の内容を検討した上で、経営層に諮り、承認を得ることが求められる。安全管理の運用上特に重要なルール等は経営層の判断も必要であることから、規程として定めた上で、経営層において承認する必要がある。
- 整備した規程を踏まえて、細則を定めたり、通常時における対応の手順や内容をルールとして定めたりする必要がある。これらについては、内容に応じて企画管理者が策定、あるいはその策定権限を担当者に移譲するなどして整理することが求められる。

４．２　規程の整備（運用管理規程ほか）

- 規程は、医療機関等においても特に重要なルールが対象となる。規程の位置づけは組織ごとに異なるが、医療情報システムの安全管理に関するものとして、
  ・組織規程
  ・個人情報保護規程
  ・運用管理規程
  ・人事・権限規程（認証との関係で対応）
  などが挙げられるほか、
  ・情報管理に関する規程
  ・資産管理に関する規程
  ・監査に関する規程
  等についても組織の方針に応じて整備することが想定される。
- 企画管理者は、作成する規程の対象や重要度などを考慮した上で規程の整備を行う必要がある。また、整備を行った規程については、関係者に対して周知を図ること。

４．３　規則等の整備

- 規則類は、主に通常時における運用に必要なルールを明文化したものであり、規程を踏まえて具体的な内容を定めるものである。
- 規則のうち、組織的な対応に関するものは、企画管理者自ら策定し、技術的な対応に関するものは、担当者に策定権限を移譲することになる。規則についても、規程と同様、関係者に対して周知を図ること。

４．４　マニュアル等及び各種資料の整備

- マニュアル等は、医療情報システム・サービスの利用者が当該システム・サービスを適切に利用できるようにするためのものである。マニュアル等のうち、医療情報システムの利用の手続に関する内容（システム利用期間や利用権限の設定など）については、企画管理者と担当者とで分担して作成し、医療情報システムの操作等の利用に関する内容のシステム設定作業については、企画管理者が担当者に作業に係る権限移譲を行うなどして設定する。
- そのほか、医療情報システムに関する資料（仕様書、システムに関連するドキュメント（設計書、プログラム開発資料等）、システムの全体構成図、ネットワークの構成図、各システムの担当責任者（委託の場合には、委託先事業者の責任者等）など、運用等に必要な資料については、企画管理者が担当者に対して、適切に整備した上で最新の状態に更新をするよう指示することが求められる。

5．安全管理におけるエビデンス

【遵守事項】

① 医療情報システムの安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要な対応を行うこと。

② 証跡の整備に当たっては、証跡により管理する安全管理の対象の目的や特性に応じたものとすることに留意すること。また証跡の改ざん等を防止する措置を講じること。

③ 収集した証跡に対するレビュー等を行い、医療情報システムの安全管理の状況を把握し、必要があれば証跡の整備に関する改善を行うこと。

④ 法令で求められる医療情報の管理に関する証跡を、必要に応じて、説明責任等を果たせるように管理すること。

5．1 証跡の整備の目的

- 医療情報システムの安全管理においては、医療機関等で策定した規程や規則などに基づく当該システムの適切な利用、運用が求められる。システムの利用又は操作の証跡（操作ログ、システムログ）を収集し、レビューすることで、医療情報システムが適切に利用・運用されているかどうか等を確認できる。
- 証跡のレビューでは、当該システムの利用、運用が規程や規則等に定めた内容のとおりに行われていることを確認するほか、本来想定されていない利用や不正な利用などを確認する目的で用いることができる。例えば、外部から侵入があった場合に、その痕跡を発見して、不正な攻撃を追跡する起点としたり、本来業務を行わない時間にもかかわらず、職員などが頻繁に医療情報システムを利用しているなどの事実を確認して、不正利用を探知するきっかけとしたりすることなどが想定される。
- 企画管理者には、このような観点から、医療情報システムに関連する証跡等の整備を行うことが求められる。

5．2 整備する証跡の種類

- 証跡については、あらかじめシステムの利用に際して必要な手続などが適切に行われていることを確認するためのものと、システムログのように、利用されている医療情報システム等が自動的に記録するものが挙げられる。
- 前者は、例えば ID の申請など、医療情報システム・サービスを利用するに際して必要な手続や判断が適切になされていることをあらかじめ確認するものである。こうした予防的な確認を行うことで、不適切な利用の防止が可能となる。
- 後者は、医療情報システムにおける利用者の操作やシステムの動作が自動的に記録されることで、システム障害やサイバー攻撃などが生じた際の原因の追跡、あるいは一見、正常に動作しているシステムが不適切に利用されていることをログのレビューから発見するなど、事後の発見に寄与するものが多い。
- なお、証跡に関しては、過大に収集することにより、運用上の負担が過大となり、結果として医療情報システムの運用に支障が出ることも想定される。
- 企画管理者は、このような特性を理解した上で、担当者と協議して、リスク評価などを踏まえて、適切な証跡を適宜選択して整備することが求められる。

5．3 証跡のレビュー

- 証跡には不正利用の探知の起点ともなるため、単に収集するだけではなく、適宜レビューを行うことが重要である。

そのため、企画管理者は、適宜証跡のレビューを行うことが求められる。

- また、証跡のレビューは、その周期が長すぎると発見までの間に不正な利用が継続してしまうリスクなどがある。一方で、レビュー対象が多いことで作業負担が過大になるため、リスクと負担のバランスを勘案すること。そのため企画管理者は、担当者と協議の上でレビューの対象や周期などを決定することが求められる。

５．４　証跡の管理

- 証跡は適切な安全管理を確認するための根拠（エビデンス）であり、改ざんや変更などがなされないように、適切な管理が求められる。システムログ等の管理に関する技術的な対応については、担当者と協議の上で必要な措置を講じること。

6．リスクマネジメント（リスク管理）

【遵守事項】

① 医療機関等内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討して必要な措置を講じること。

② 医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、常に最新の状態で管理すること。

③ 医療情報システムで取り扱う情報及び関連する情報に関するリストを作成し、必要に応じて速やかに確認できる状態で管理すること。

④ 安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。

⑤ ②～④を踏まえて、リスク分析やリスク評価を、担当者と協働して行うこと。

⑥ リスク評価を踏まえ、経営層がリスク判断をする際に必要な資料を整理すること。

⑦ リスク評価の結果、リスク管理の方針に関する説明責任に関する資料等を整理し、経営層が説明責任を果たすために必要な対応を行うこと。

⑧ リスク評価の結果を経営層に報告し、承認を得ること。また承認を踏まえて安全管理対策を講じること。

⑨ PDCA（Plan-Do-Check-Act）モデルに基づく ISMS（Information Security Management System：情報セキュリティマネジメントシステム）を構築し、管理すること。また、ISMS が適切に実施されていることを確認し、経営層にその状況を報告すること。

⑩ PDCA モデルの実施において不備等が認められる場合には、その原因を確認した上で改善策を講じ、経営層に報告し、承認を得ること。

6．1 運用管理におけるリスクマネジメント

6．1．1 リスクマネジメントの役割

- 医療情報システムにおける情報セキュリティ対策を講じるにあたっては、組織としてのマネジメントが必要なため、運用管理としてリスクマネジメントを適切に行うことが求められる。
- リスクマネジメントとしては、リスク分析とリスク評価、そしてこれらを踏まえたリスク管理を行う必要があるところ、運用管理において、この一連のリスクマネジメントサイクルが適切に行われるよう管理を行うことが求められる。
- リスク分析とリスク評価については、医療機関等における情報資産の状況などを把握しながら、医療機関等で利用する医療情報システム・サービスを踏まえて行うことから、情報システムの技術担当者などとも協働して行うことになる。その上で、リスクに対する判断は最終的には経営層に委ねられることになるが、運用管理上は、企画管理者において経営層による判断に必要な資料の整理などを行うことが求められる。
- サイバー攻撃など日々新しい形態の脅威が発生することから、医療情報システムにおけるリスク分析やリスク評価なども定期的に行うことが求められ、これら一連のマネジメントサイクルが適切に実施されるよう管理することが運用管理において求められる。
- 企画管理者は、経営層に対して、医療機関等内でリスクマネジメントが適切に実施されているかどうかを報告し、不備があれば改善策を講じることも求められる。

6．1．2 リスクアセスメント（リスク分析、リスク評価）の役割

- リスクアセスメントは、企画管理者と情報システムの技術担当者とで協働して実施することになるが、運用管理上

は、特に取り扱う情報の把握とこれに対するリスク評価を担当者と行うことが求められる。

- 取り扱う情報の把握は、医療機関等において取り扱う医療情報と、医療情報システムで扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認することである。そのため、取り扱う情報等に関するリストを作成し、企画管理者が必要に応じて速やかに確認できる状態で管理することが求められる。近年では、医療情報システムに係る外部委託先や製品供給などとのサプライチェーンに関するリスクも大きく、リスク分析の対象とすることが求められる。
- 安全管理上の重要度は、安全性が損なわれた場合の影響の大きさに応じて決める。少なくとも患者等の視点からみた影響の大きさと、業務継続の視点からみた影響の大きさを考慮する必要がある。このほかにも、医療機関等の経営上の視点、人事管理上の視点等の必要な視点を加えて重要度を分類する。例えば、医療情報の安全性に問題が生じた場合、患者等に極めて深刻な影響を与える可能性があるため、医療情報は最も重要度の高い情報として分類される。また、医療情報システムについても、医療サービスの提供継続性への影響の観点から重要度を判断して分類し、管理状況を把握する必要がある。
- リスク評価は、リスクの発現率と影響の大きさから算定することになる。そのため、リスクの影響の大きさに関する判断は企画管理者が行い、リスクの発現率に関する技術的な判断は担当者と協働して行うことが求められる。

6．2 ISMS（Information Security Management System：情報セキュリティマネジメントシステム）

- 医療情報システムの情報セキュリティを確保するために、ISMS を構築することが重要である。ISMS は、PDCA モデルに基づいて行われる（※）が、運用管理においては、このような PDCA モデルが適切に行われるよう ISMS を構築し、管理することが求められる。

  ※ JIS Q27001:2023 では PDCA との記述は使われていないが、「情報セキュリティマネジメントシステム」として「組織は、この規格の要求事項に従って ISMS を確立し、実施し、維持し、かつ、継続的に改善しなければならない。」と記述されている。継続的改善のモデルとして PDCA サイクルが理解しやすいため、旧版（JIS Q27001:2006）より引用している。
- ISMS の構築のために、JIS Q27001:2006 では下表のように PDCA モデルが規定される。運用管理においては、PDCA モデルを採用し、管理、確認をすることが求められる。

表６－１　ISMS プロセスに適用される PDCA モデルの概要

Plan－計画 (ISMS の確立)	組織の全般的方針及び目的に従った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連した、ISMS 基本方針、目的、プロセス及び手順の確立
Do－実行 (ISMS の導入及び運用)	ISMS 基本方針、管理策、プロセス及び手順の導入及び運用
Check－点検 (ISMS の監視及び見直し)	ISMS 基本方針、目的及び実際の経験に照らした、プロセスのパフォーマンスのアセスメント（適用可能ならば測定）、及びその結果のレビューのための経営陣への報告
Act－処置 (ISMS の維持及び改善)	ISMS の継続的な改善を達成するための、ISMS の内部監査及びマネジメントレビューの結果又はその他の関連情報に基づいた是正処置及び予防処置の実施

P（Plan）では、ISMS 構築の骨格となる文書（基本方針、運用管理規程等）により、ISMS 構築手順を確立する。

D（Do）では、P で準備した文書や手順を使って実際に ISMS を構築する。

C（Check）では、構築した ISMS が適切に運用されているか、監視と見直しを行う。

A（Act）では、改善すべき点が出た場合に是正処置や予防処置を検討し、ISMS を維持する。

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）

【遵守事項】

① 医療情報を取り扱う者を職員として採用するに当たっては、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含める等の安全管理対策を実施すること。

② 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。

③ 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、委託契約の契約書に守秘・非開示に関する内容を含めること。

④ ③の委託契約の際に、当該委託先事業者の就業規則等に①及び②の対応を含めるよう求めること。

⑤ 外部の事業者との契約に基づいて医療情報を外部保存する場合、以下の対応を行うこと。重要度の高い委託の場合は、経営層に丁寧に報告し、承認を得ること。

- 保存した医療情報の取扱いに関して監督可能とするため、外部保存の委託先事業者及びその管理者、電子保存作業従事者等に対する守秘義務に関連する事項やその事項に違反した場合のペナルティを契約書等で定めること。
- 医療機関等と外部保存の委託先事業者を結ぶネットワークインフラに関しては、委託先事業者にも本ガイドラインを遵守させること。
- 総務省・経済産業省の定めた「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」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して遵守状況を確認すること。
- 外部保存の委託先事業者の選定に当たっては、システム関連事業者の情報セキュリティ対策状況を示した資料を確認すること。（例えば、「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」における「サービス仕様適合開示書」の提供を求めて確認することなどが挙げられる。）
- 外部保存の委託先事業者に、契約書等で合意した保守作業に必要な情報以外の情報を閲覧させないこと。
- 保存した情報（Cookie、匿名加工情報等、個人を特定しない情報を含む。本項において以下同じ。）を外部保存の委託先事業者が独自に提供しないよう、契約書等で情報提供のルールについて定めること。外部保存の委託先事業者に情報の提供に係るアクセス権を設定する場合は、適切な権限を設定させ、情報漏えいや、誤った情報閲覧（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）が起こらないよう求めること。
- 保存された情報を格納する情報機器等が、国内法の適用及び執行の及ぶ範囲にあることを確実にすること。

⑥ 外部保存の委託先事業者を選定する際は、少なくとも次に掲げる事項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・取扱規程等の整備状況

b 医療情報等の安全管理に係る実施体制の整備状況

c マルウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況

d 実績等に基づく個人データ安全管理に関する信用度

e 財務諸表等に基づく経営の健全性

f プライバシーマーク認定又は ISMS 認証の取得

g プライバシーマーク認定、ISMS 認証のいずれも取得していない場合は、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（令和７年５月 27 日デジタル社会推進会議幹事会決定）の「セキュリテ

ィクラウド認証等」に示す下記のいずれかの認証等により、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

・政府情報システムのためのセキュリティ評価制度（ISMAP）（ISMAP-LIU は含まない）
・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク
・米国 FedRAMP（LI-SaaS は含まない）
・AICPA SOC2／SOC3（又はこれに準じる公認会計士による監査報告書）

上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力の有無を確認すること

・システム監査技術者
・Certified Information Systems Auditor ISACA 認定
・「民間事業者による医療情報に係るクラウドサービスの評価」（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）

h　医療情報を保存する情報機器が設置されている場所(地域、国)

i　委託先事業者に対する国外法の適用可能性

⑦ 医療情報の外部保存の委託先事業者との契約には、以下の内容を含めること。

– 委託元の医療機関等、患者等の許可なく保存を受託した医療情報を分析等の目的で取り扱わないこと。
– 保存を受託した医療情報の分析等は正当な目的の場合に限り許可されること。
– 匿名化した情報であっても、匿名化の妥当性の検証を行う、及び院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱うこと。
– 保存を委託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存の委託先事業者に適切な利用者権限や閲覧の範囲を設定し、情報漏えいや、誤った情報閲覧が起こらないように配慮すること。
– 情報の提供は、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。

⑧ 委託先事業者が契約に基づいて必要な対応を行っていることを定期的に確認するため、委託先事業者に報告を求めること。当該報告の結果、必要に応じてその改善を求めること。また委託先事業者からの報告内容については、経営層に報告し、承認を得ること。

⑨ 委託契約終了に際し、医療情報の返却とその方法など、委託先事業者が行うべき内容についてあらかじめ契約により取り決めておくこと。

⑩ 外部保存の委託に当たり、あらかじめ患者に対して、必要に応じて個人情報が特定の外部の施設に送付・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、理解を得ること。

7．1　職員管理

- 医療機関等は、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管理対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育・訓練に関する事項が含まれる。
- 以下の者については、医療機関等の職員に対する人的安全管理の対象として整理される。

（a） 医師、看護師等の業務で診療に関わる情報を取り扱い、法令上の守秘義務のある者
（b） 医事課職員等、業務に携わることで医療情報を取扱い、守秘義務を負う者

- いずれも、医療情報を取り扱う者として、守秘義務や教育・訓練等を受ける義務を課す雇用契約等を締結することで、企画管理者は人的管理を行うことができる。なお、この場合、直接雇用する職員だけではなく、派遣雇用の者も対象となる。

- 守秘義務については、就業時はもちろん、退職後においても遵守される必要がある。医療機関等の職員に対して退職後を含めて医療情報に関する守秘義務を課すこと。

7．2　委託先事業者管理

- 医療情報システム等を委託する場合には、委託先事業者である法人だけではなく、実際にその業務にあたる者に対して、医療機関等の職員と同様の責任や守秘義務を課すことで、医療機関等としての人的管理を実現する必要がある。
- 企画管理者は、委託先事業者との契約に際して、委託先事業者と当該事業者で業務にあたる者との雇用契約等において、守秘義務等を含んでいることを確認し、委託先事業者において人的管理が適切に行われることを確認する必要がある。

7．3　教育・訓練

- 医療機関等の職員が医療情報の安全管理に関して遵守すべき内容を十分理解できるよう、教育を行うことが求められる。また、非常時などでも適切に行動できるよう、通常時における訓練の実施も求められる。
- 企画管理者は、職員に対する教育・訓練を定期的に行うことが必要である。また、就業時間内に実施すること。
- 医療情報システムの利用に関連する教育内容については、システムの担当者と協議の上、必要な事項を整理することが求められる。特に、近年、医療機関等におけるサイバー攻撃被害により、地域医療の安全性を脅かす事案も発生していることから、公表されている各種資料を参考に、職員への教育・育成を実施すること。
- 医療情報システムの安全管理やセキュリティ対策業務に従事する人材に対し、独立行政法人情報処理推進機構（IPA）の実施する「情報処理安全確保支援士」、「情報セキュリティマネジメント試験」等の資格取得[9]、演習・訓練への参加等を推進することが望ましい。
-

7．4　委託先事業者選定

- 適切な委託先事業者の選定は、個人情報保護法における委託先の監督（第 25 条）の一環として必要であるほか、医療情報を医療機関の外部に保存する場合に、「外部保存通知」（第２　1（2））にあるとおり安全が確保された場所に保存する観点からも必要である。
- 外部のシステム関連事業者との契約に基づいて、医療情報を外部保存する場合には、データセンター等の情報処理の委託先事業者が総務省・経済産業省の定めた「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」の要求事項を満たしていることを確認し、契約等においてもそれらを遵守することを明確に定めること。
- 委託先事業者の選定を法令等の要求に基づいて適切に行う必要があるほか、リスク評価を踏まえた観点からも適切に選定を行う必要がある。また、当該選定に際しては、担当者と協議し、技術的な観点からの妥当性なども加味すること。なお、選定時に認識されたリスク評価内容はその後変化しうる。特にサイバーセキュリティにおいては、攻撃方法の巧妙化に伴い、適宜、リスク対応の再検討を要する。対象事業者が行うリスクの管理体制や、リスクが選定時以降に上昇した場合の対応も想定することが望ましい。契約時の取決め内容においてもこれに関する随時の情報提供等を含めることが重要である。

---

[9] 資格については情報処理安全確保支援士以外にも、独立行政法人情報処理推進機構による情報処理技術者資格等や民間事業者が認定する医療情報の取扱いに関する資格が含まれる。

- 重要度の高い委託の場合は、経営層に丁寧に報告の上、承認を得ること。

７．５　外部保存･外部委託の終了

- 医療情報が機微な個人情報であることから、外部保存を終了する場合や外部保存の委託を終了する場合には、医療機関等及び委託先事業者の双方で適切な配慮が求められる。
- 外部保存の開始時に、保存の期限等の保存期間に関する条件が明確に示されている必要があり、外部保存の終了は、この条件に基づいて適切に実行されなければならない。期限には具体的な期日が指定されている場合もあれば、「一連の診療の終了後○○年」といった一定の条件が示されている場合も想定される。
- 医療機関等は、委託先事業者に保存されている医療情報を定期的に確認し、外部保存を終了すべき医療情報が、速やかかつ厳正に処理されているかを監査しなくてはならない。また、委託先事業者も、委託元の医療機関等の求めに応じて、保存している医療情報を厳正に取り扱い、保存の終了を適切に処理している旨を委託元の医療機関等に明確に示す必要がある。
- 外部保存の保存期間や委託の終了に伴う医療情報の破棄や返却に関する規定は、外部保存を開始する前に契約書にも明記をしておく必要がある。また、実際の破棄や返却に備えて、事前に破棄や返却等の手順を明確化した資料等を作成しておくこと。
- 委託する医療機関等及び委託先事業者の双方に厳正な取扱いが求められるのは、同意された期間を超えて個人情報を保持することが個人情報の保護上問題となり得るためであり、十分な留意が必要である。
- また、患者の医療情報に関する検索サービスを実施している場合は、検索のための台帳やそれに代わるもの、及び検索履歴等も厳正な取扱いの後に破棄されなければならない。
- 医療情報の破棄に関しては、可搬媒体で保存している場合でも責任を持って対応する必要がある。

７．６　患者への説明等

- 医療機関等は、患者から医療情報を預かっているという観点から、患者に対しては適切な説明と理解を得ることが求められる。医療情報の取扱いを医療機関等以外に委ねる場合には、患者の理解を得た上で行うこと。
- 外部保存の委託について、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、理解を得ること。

8．情報管理（管理、持ち出し、破棄等）

【遵守事項】

① 医療機関等において保有する医療情報の管理、医療機関等外への持ち出し、破棄等の方針と手順等を含む情報管理に関する規程等を定め、当該規程等に基づいて適切に医療情報を管理すること。

② 医療情報の管理において、各医療情報に関する管理責任者を定め、適切に管理するよう指示すること。また、管理責任者から管理状況に関する報告を受け、必要に応じて改善を指示すること。

③ 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。

④ 医療機関等における医療情報の管理状況を把握し、経営層の承認を得ること。管理状況の把握のため、医療機関等で保有する医療情報について定期的な棚卸や管理実態の確認を行うこと。特に患者に関する情報は、患者ごとに識別できるよう、管理すること。

⑤ 医療機関等外への医療情報の持ち出しに関する手順等を定める際は、リスク評価に基づいて、医療情報の持ち出しに関する対応方針や、持ち出す情報、持ち出し方法や管理方法について情報管理に関する規程で定めること。

⑥ 医療機関等外への医療情報の持ち出しに関する手順等を定める際は、医療情報を記録した媒体や情報機器を用いる持ち出しのほか、ネットワークを通じて外部に医療情報を送信し、又は外部から医療情報を保存する場所等にネットワークを通じて医療情報の閲覧や受信・取り込みを行う場合も想定すること。

⑦ 持ち出した医療情報を格納する（外部からアクセスして格納する場合を含む。）記録媒体や情報機器の盗難、紛失が生じた際の対応について情報管理に関する規程に定めること。

⑧ 医療機関等の外部からのアクセスについて、許諾対象者、許諾条件やアクセス範囲等、許諾を得るための手順等を定めること。

⑨ 患者等に情報を閲覧させるために医療情報システムへのアクセスを許可する場合には、患者等に対して、情報セキュリティに関するリスクや情報提供目的について説明を行い、それぞれの責任範囲を明確にすること。

⑩ 医療情報の持ち出し状況について定期的なレビューを行い、持ち出し状況の適切な管理を行うこと。

⑪ 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。当該手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。

⑫ 保存等を委託している医療情報を破棄する場合、委託先事業者に対して、医療情報の破棄等（格納する記録媒体・情報機器等の破壊含む）を行ったことについての証跡等の提出を求めること。システム関連事業者のサービス等の性格上、破棄等を行ったことの証跡の提出を求めることが困難な場合には、当該事業者における破棄等の手順等の提供を求め、委託先事業者における破棄の手順等が、医療機関等が定める破棄の手順等に適合するよう、事前に協議した上で、委託契約等の内容にも含めること。

8．1 情報管理

8．1．1 情報管理方針の整備

- 医療機関等が保有する情報の管理について、組織としての管理方針を定める必要がある。小規模な医療機関等であって、情報管理体制が明文化されていない場合でも、情報の持ち出しは想定されることから、リスク分析を実施して対策を検討しておくこと。
- 企画管理者は、情報管理方針を策定し、経営層による承認を得ること。

８．１．２　情報管理の手順

- 情報管理方針を踏まえて、具体的な情報管理の手順を定める必要がある。情報管理の手順等は、管理対象となる情報により異なる。各情報を主に管理する者を管理責任者として、それぞれで適切に管理できるよう手順の策定や管理方法などを定めること。
- 情報については、一般的には、作成、利用、保存、廃棄などのライフサイクルが想定される。それぞれの過程ごとに、セキュリティが確保できるよう、適切に管理すること。

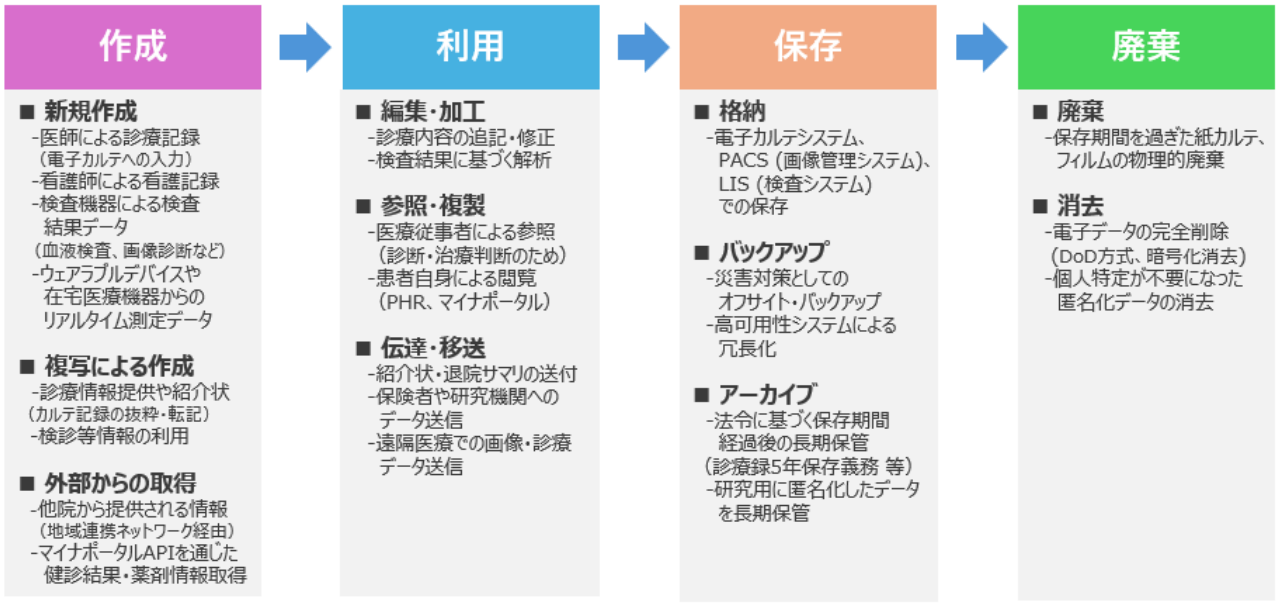


図８－１　情報のライフサイクル

- 企画管理者は、これらの管理手順等について、各情報の管理責任者から整備状況等の報告を受け、把握する必要がある。
- 漏えいや不正利用を防ぐ観点から、医療情報が保存されている施設、情報機器等へのアクセスを制限し、管理を行うための規則等を設ける必要がある。

８．１．３　情報の安全管理状況の報告

- 企画管理者は情報の管理状況の把握を行う必要がある。管理状況の把握対象は、医療機関等が保有している情報、特に医療情報の状況（どの程度の人数の情報が管理されているか、どのような情報が管理されているか）などと、それらに対する管理状況（システムによる管理か、紙媒体によるものか、内部管理か外部管理か）などについて定期的に把握し、経営層に対して報告を行うこと。
- 医療情報に関しては、患者の取り違い等の様々なリスクを避ける等の観点から、的確に各患者を識別し、適切に管理されるように運用する必要がある。

８．２　医療情報の持ち出し

８．２．１　医療情報の持ち出し手順等の策定

- 医療機関等が管理する情報又は情報機器の持ち出しには、漏えいのリスクが伴う。このリスクを低減するため、組織として情報又は情報機器の持ち出しに関する取扱いを整理した方針が必要である。当該方針は、物理媒体での持ち出しだけではなく、外部のクラウドサービスなどを用いたデータ等の持ち出しや、テレワークなどによる外部か

らの作業に伴う持ち出しなども想定した内容とすることが求められる。

- 特に可搬媒体や情報機器の盗難、紛失、置き忘れ等の人による不注意、過誤、誤送信等のリスクが大きいことから、人的安全管理対策と併せて対応する必要がある。
- これらのリスクを低減するため、医療情報の持ち出しに関する手順等を策定し、職員等の教育など周知を図ること。

８．２．２　記録媒体・情報機器等による持ち出し

- 医療機関等の外部に医療情報を持ち出す方法の一つとして、記録媒体や情報機器等への格納による持ち出しが想定される。持ち出し先での紛失や盗難のほか、外部の情報機器へ接続した場合にはマルウェアの混入なども想定されることから、持ち出す前だけではなく、持ち出した後の対応についても検討する必要がある。
- 記録媒体・情報機器等による医療情報の持ち出しに際しては、
  ・医療情報の持ち出しが可能となる記録媒体や情報機器等を限定
  ・医療情報の持ち出しに対する手続等を策定
  ・記録媒体・情報機器等を持ち帰った際の確認に関する手続等の策定
  等を行うことが求められる。
- 医療情報を持ち出す際の記録媒体や情報機器に関する安全性について、担当者と協議すること。
- ネットワークを通じて外部保存を行い、外部保存の委託先事業者においてこのデータを可搬媒体に保存する場合も、同様の対策を講じるよう委託先事業者に求めること。

８．２．３　ネットワークサービスを用いた持ち出し

- 医療機関等の外部に容易にデータを保管し、加工や共有もできるクラウドサービスなどが普及している。特に容量が大きいデータの外部との交換においては、ネットワークを通じたクラウドサービスを利用することも想定される。
- このようなクラウドサービスの中には、管理者の承認なく容易に外部への保存などが可能となるものもあることから、ネットワークを通じた医療情報の持ち出しについても、適切な対応を講じること。
- 医療情報の持ち出しが可能なネットワークサービスについては、企画管理者が承認したもののみを利用できる措置を講じることが必要となる。その上で、ネットワークサービスを通じた医療情報の持ち出しに関する手順やルール等を定めること。
- ネットワークサービスの利用と管理に際して、担当者と協議し、必要に応じて接続制御などを行うことも想定される。

８．２．４　外部からのアクセスによる持ち出し

- 医療機関等が管理する医療情報システムに、医療機関等の外部からアクセスして、医療情報を参照・利用することが想定される。具体的には、
  ・ 医療機関等の職員が、訪問先やテレワークなどにより、医療機関等が管理する端末等を通じてアクセスする場合
  ・ 患者が、自宅等から自らの情報にアクセスする場合
  ・ 医療機関等が保有する医療情報システムに対して、事業者が外部からアクセスして保守等を行う場合
  等が想定される。
- 企画管理者は、このような外部からのアクセスによる医療情報の参照や利用を認めるかどうか、どのような場合に認めるか、認める際の条件や制限、技術的な対応による安全管理対策などについて整理し、規則や手順を策定する必要がある。また、技術的な対応による安全管理対策については、担当者に具体的な内容の検討を指示すること。

- 患者等が自らの情報にアクセスする場合には、必要な説明を行い、責任範囲等を明らかにすることも求められる。

８．２．５　持ち出した医療情報を格納する記録媒体等の紛失等への対応

- 持ち出した医療情報を格納する記録媒体等の紛失や盗難、あるいは利用するネットワークサービスに関する設定や誤操作により医療情報が漏えいした場合には、組織として速やかに必要な対応を行う必要がある。
- 漏えい時の初期対応などについて、企画管理者は情報管理規程や運用管理規程等の中で定めておくこと。例えば、紛失等が発覚した場合の連絡先や対応手順、対応方法などについてあらかじめ整理することが想定される。
- 漏えい又はその可能性がある場合には、医療情報の漏えいが生じた場合の対応（「３．１．２　非常時等の体制・CSIRT 等の整備」）や、非常時の対応（「１１．３　非常時の対応」）に基づいた対応が求められる。

８．２．６　持ち出し状況のレビュー

- 医療情報が外部へ持ち出される状況は限定されており、不正な持ち出し等が生じないように、定期的に持ち出し状況のレビューを行う必要がある。
- 不自然な持ち出し等がある場合には、その理由を確認する等、必要な管理を行うこと

８．３　医療情報の破棄

８．３．１　破棄の手順等の策定

- 医療情報の破棄に際しては、安全性を確保した上で適切に破棄するための手順の策定が必要となる。
  当該手順には、下記違いに応じた内容を示すこと。
  ・情報種別
  ・管理形態（紙媒体、システム管理等）
  ・破棄対象（情報だけか、記録媒体も対象か）
- 特にシステム上のデータの破棄や記録媒体・情報機器等の破棄については、漏えいや不正利用のリスクが生じることに留意が必要である。

８．３．２　外部保存をシステム関連事業者に委託している場合の対応

- 委託先事業者において医療情報を破棄する際、適切に破棄されたことを、医療機関等においても確認する必要がある。企画管理者は、破棄されたことを確認できる証跡の提供を、委託先事業者に求めること。
- クラウドサービス上での破棄など、その証明を行うことが困難な場合もある。その場合、破棄の手順や実際に行った処理に関する証跡の提供など、証明に代替する対応を委託先事業者に求めること。その上で、委託先事業者における破棄の手順や基準が、医療機関等における破棄の手順や基準に適合するよう、事前に協議した上で、委託契約等の内容にも含めること。

９．医療情報システムに用いる情報機器等の資産管理

【遵守事項】

① 医療情報システムにおいて用いる情報機器等の資産管理を行うのに必要な規程その他の資料を整備し、その管理を行うこと。（なお、情報機器等には、物理的な資産のほか、医療情報システムが利用するサービス、ライセンスなども含む。）

② 医療機関等が管理する情報機器等について、台帳管理等を行うこと。台帳管理等の対象は、医療機関等内部の購入部署や購入形態に関わらず、医療情報システムで利用する情報機器等全てとすること。

③ 台帳管理されている医療情報システムに用いる情報機器等の棚卸を定期的に行い、存在確認を行うこと。また担当者と協働して、滅失状況などについても適宜確認すること。

④ 医療情報システムにおけるサプライチェーンについて、医療情報システム等の情報資産に関係する事業者にシステムの管理体制や供給体制を確認し、サプライチェーンリスクの所在について整理すること。

⑤ 医療情報システムにおいて利用する情報機器等が、安全管理の観点から利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対して、情報機器等における状況（ソフトウェアやファームウェアのアップデートの状況、脆弱性に関する対応状況等）を確認するよう指示し、報告を受け、適宜必要な対応を行うこと。

⑥ 医療情報システムが利用するサービスに関して、安全管理の観点から、利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対してサービスにおける状況（サービスの機密性、クラウドサービス等における可用性、システム関連事業者が示す規約内容の変更状況等）が適切なものとなっていることを確認するよう指示し、報告を受けた上で、必要があれば契約変更等の対応を行うこと。

⑦ 医療機関等が管理しない情報機器で、医療情報システムに用いるもの（例えば BYOD（Bring Your Own Device：個人保有の情報機器）の利用による端末）について、利用を許諾する条件や、利用範囲、管理方法等に関する内容を規程等に含めること。また、これに基づいて利用される情報機器等について、利用の許諾状況も含めて、医療機関等が管理する情報機器同様に、台帳管理等を行うこと。

⑧ 医療情報システムで利用する情報機器等の資産管理状況を把握した上で、経営層に報告し、承認を得ること。

９．１ 情報機器等の台帳管理

- 医療情報システムで用いる情報機器等に関する安全性を確保するためには、利用を予定している情報機器等の所在、またそれらの情報機器等の使用可否等を、適切に管理する必要がある。
- 企画管理者は、医療情報システムで用いる情報機器等について、台帳管理を行い、情報機器等が利用に適した状況にあることを確認可能としておく必要がある。台帳で管理する内容としては、情報機器等の所在や利用者、使用するソフトウェアやサービスのバージョン、ライセンスの状況などが想定される。
- 昨今の医療情報システムでは、BYOD（Bring Your Own Device：個人保有の情報機器）などの利用も想定される。企画管理者は、こうした医療機関等が管理しない端末の利用についても、その利用条件や利用範囲、管理方法などについての規則を策定した上で、併せて台帳管理すること。加えて、BYOD での利用に関する具体的な条件等について担当者と協議し、必要に応じて技術的な対応を講じ、規則の内容に含めること。
- 整備した台帳を定期的に棚卸しして、適切な状況にあることを確認する必要がある。

９．２　サプライチェーン管理

- サプライチェーンとは、一般的には原材料の調達から製造・物流・販売まで、製品やサービスが顧客に届くまでの一連のつながり（企業群）を指す。この連鎖のどこかでトラブルが起きると、自社への供給が止まる可能性があり、これをサプライチェーンリスクと呼ぶ。近年は自然災害などの物理的リスクだけでなく、取引先や委託先の IT の弱点を突く「サイバー起因のサプライチェーンリスク」が特に問題視されている。
- サプライチェーンリスクでは、不正機能等の埋め込み、サービスの供給途絶、外部サービスにおける情報の不適切な取扱い、海外拠点、グループ組織、取引先等を経由したサイバー攻撃などが挙げられる。
- 近年のサプライチェーンにおけるサイバー攻撃では、最終的な攻撃目標を生産している、セキュリティが堅牢な組織を狙うのではなく、そのサプライチェーン（供給の連鎖）工程上の、セキュリティレベルの低い組織（企業、委託先等）を狙って攻撃を仕掛け、最終的な攻撃目標に、マルウェアなどを仕込む手法がみられる。
- またサイバー攻撃以外でも、複数の事業者が提供するシステム・サービスを組み合わせて利用する際に、一部の事業者のシステム・サービスの提供終了や機能向上を図らないことによるリスクなども指摘されている。
- このような脅威に対するリスクを低減するため、医療情報システムに係る委託先や機器に関するサプライチェーン関係を整理し、リスクアセスメントや対策の整備を行うことが重要である。

９．３　情報機器等の安全性の確認

- 管理している情報機器等を医療情報システムとして利用するためには、情報機器等の安全性が確認されている必要がある。特にサイバー攻撃等への対応という観点からは、必要なファームウェアの更新や脆弱性対策の実施、EOS（End of Support：サポート終了）の対象となっていないことなどを確認すること。
- EOS を越えている場合、製造販売事業者等と連携し、補完的対策を講じること。
- 情報機器等の安全性の確認を行うためには、安全性に関する情報を的確に把握することが求められる。企画管理者は、担当者に安全に関する情報の収集（利用している情報機器等やシステム、プログラム等）と、それを踏まえた対応を指示し、その対応状況を確認すること。
- 安全性確認の対象は、情報機器だけではなく、利用するサービスも含まれる。サービスの場合、当該サービス提供事業者との委託契約等に、安全性の状況を定期的に確認する旨を含めることなどが想定される。
- クラウドサービスなどの場合は、サービス内容によっては、利用可能な情報システムの容量に上限があることが想定される。十分な容量を確保できないなどといった、可用性に関するリスクを低減するよう、システム関連事業者に対して、必要な事項を適宜確認すること。

９．４　情報機器等の資産管理状況の報告

- 情報機器の管理状況については、企画管理者が把握した上で、経営層に報告し、承認を得る必要がある。管理状況を把握する際は、担当者と協議の上、資料を整理すること。
- この際、情報機器やソフトウェアのアップデートの履行状況や、EOS の対象となった情報機器やソフトウェアの状況、委託契約の範囲（アップデート等に関する責任分界含む）を含めること。

１０．運用に対する点検･監査

【遵守事項】

① 医療機関等における医療情報システムの安全管理が適切に行われていることを把握するため、運用の点検を行うこと。技術的な対応に関しては、担当者に点検を命じ、その報告を受け、確認すること。点検に際しては、各規程、手順等による運用が適切に行われていることを、「５． 安全管理におけるエビデンス」で整備した証跡に基づいて確認し、必要があれば改善を行うこと。

② 医療情報システムの取扱いを委託している場合は、委託先事業者において医療情報システムの安全管理が適切になされていることを、委託先事業者からの報告に基づいて確認すること。医療情報システム･サービスの性格上、報告に基づく確認が難しい場合は、SLA に対する評価等の中で確認すること。

③ 医療情報システムの取扱いに関する点検結果を、経営層に報告し、承認を得ること。

④ 医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等内の企画管理者や担当者から独立した組織又は第三者による監査を実施すること。監査の実施に際しては、監査方針と監査計画を策定の上、経営層の承認を得ること。また、監査結果については、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。

１０．１ 運用に対する点検

- 医療情報システムの運用の安全管理を把握するために、企画管理者は、自ら通常時の運用状況を確認することが重要である。組織的な対応について、適切に運用できているか、改善点があるとすればどこか、定期的に点検することが求められる。併せて、担当者に対して、技術的な対応についての点検を指示し、改善すべき部分があればその旨の報告を求めることも必要となる。

１０．２ 運用に対する監査

- 安全管理が適切になされていることを担保するために、第三者による確認や監査を行うことは有効である。
- 監査については、企画管理者等から独立した組織等による内部監査と、外部の第三者による外部監査がある。医療機関等の組織形態や、医療情報システムの規模、利用形態に応じた確認であることが重要である。監査への対応の負担が過大となり、運用に多大な支障が出るような事態はさけるように留意すること。
- 企画管理者は、このような観点も踏まえて監査方針を策定し、経営層の承認を得て、必要な監査を実施すること。また、当該監査結果を経営層に報告し、監査における指摘事項等に対応するため、改善を図っていく必要がある。

１１．非常時（災害、サイバー攻撃、システム障害）対応と BCP 策定

【遵守事項】

① 医療情報システムの安全管理に関して、非常時における対応方針と対応手順・内容の整理を行い、BCP（Business Continuity Plan：事業継続計画）を策定すること。対応方針には、非常時の定義のほか、通常時への復旧に向けた計画を含め、経営層の承認を得ること。

② 医療機関等が定める非常時の定義や BCP との整合性を確認して対応方針を策定すること。

③ 非常時において、法令で求められる対応を事前に整理し、非常時に速やかに対応できる体制を講じること。

④ 各種規程等に非常時における対応手順・内容も含めること。

⑤ 非常時における安全管理対策について、担当者に対策の実装と対策を踏まえた文書の整備を指示し、確認すること。

⑥ 非常時における対応に関して、医療機関等の職員、外部の関係者等に対する教育を行うほか、定期的に訓練を実施すること。訓練等の結果や評価を、適宜、非常時の対応手順等に反映させること。

⑦ 非常時の対応状況を定期的に確認し、経営層に報告の上、承認を得ること。

⑧ 非常時には、安全管理の状況を適宜把握し、経営層に報告すること。また、関係者に対する説明責任等を果たすため、報告対応や広報対応を行うこと。

⑨ 非常時に対応した内容について、事後検証を行い、その内容を経営層に報告し、承認を得ること。その検証結果や評価を、適宜、非常時の対応手順等に反映させること。

１１．１ 非常時における対応方針の策定

- 医療サービスを継続して提供可能とするため、非常時における医療情報システムに関する対応は重要である。
- 災害やサイバー攻撃、システム障害が生じた場合に、経営層及び非常時における意思決定担当者は
  - 医療サービスの提供をどのように継続するか
  - どの医療情報システムをどのように利用するか

  等を総合的に判断する必要がある。
- 企画管理者は、経営層等の判断を見据えて、非常時における対応方針や手順などを策定する必要がある。その内容は、医療機関等で策定される BCP との整合性を踏まえた内容とすること。併せて「非常時」の定義も明らかにすることが求められる。策定した方針や手順等については、経営層に対して報告の上、承認を得ること。
- 非常時の発生原因としては、主に災害、サイバー攻撃、システム障害などが挙げられ、それぞれの原因に対して、具体的な対応が異なる。対応方針や手順等を策定する際も、具体的な事象発生原因や被害の規模等を勘案して、それぞれに対応した内容とすること。

表１１－１　非常時の事象発生原因に応じた必要な対応例

原因	概要	必要な対応
災害	・災害による医療情報システムの停止、あるいは損傷・破壊 ・災害による医療情報システムの運用管理に必要な資源（要員、機材、電源等）の不足等に伴う運用等への支障　など	・災害発生時のフェールセーフ ・復旧、復帰に向けた対応 ・資源配分、運用規模の変更　など
サイバー攻撃	・外部からの攻撃による医療情報システムの停止、あるいは損傷・破壊 ・医療情報の改ざんや漏えい　など	・被害状況の把握 ・証拠・証跡の保全 ・被害拡大の防止 ・原因の究明 ・復旧計画の策定　など
システム障害（ネットワーク障害含む。）	・医療情報システム（サービス）の停止・パフォーマンス低下　など	・障害状況の把握 ・障害の原因究明 ・復旧、改修の計画策定　など

- 企画管理者は、非常時に法令で求められる対応についても、適切かつ迅速に対応できるよう体制を整備しておく必要がある。また、サイバー攻撃に際しては、「１２．サイバーセキュリティ」に示すように、所管官庁等への迅速な連絡が求められる。

１１．２　非常時に備えた通常時からの対応

- 非常時に適切に対応するためには、通常時からの準備等が重要である。通常時から対応する内容としては、非常時の具体的な手順や連絡体制等の構築のほか、医療情報システムにおける被害極小化や迅速な復旧のための対策、冗長化等が挙げられる。
- 具体的な対応は、発生原因によって異なる。例えばバックアップの設計・確保も、災害の場合は大規模災害を視野に入れた内容となるが、サイバー攻撃においては、耐攻撃性や業務継続性という観点から対応が必要となる。また、システム障害においては、システム復旧や原因究明の迅速性などが優先されることもある。
- 企画管理者は、このような非常時の発生原因による違いを考慮して、通常時に実施できる対応を整理し、経営層の承認を得ること。

表１１－２　非常時の事象発生原因に応じた通常時からの対策例

原因	必要な対応	求められる対策例
災害（主に地震、水害、火災等、医療情報システムのみに限らず、医療機関等全体への被災が想定されるもの）	災害発生時のフェールセーフ	・情報システムの冗長化（電源、ネットワーク、サーバ等） ・情報システム・サービスの安全な停止のための手順の整備 ・非常時のリスクを踏まえたセキュリティ対策の準備（認証方法等） ・遠隔制御等による対応方法に関する手順等の整備 ・利用者等の関係者の教育・訓練　など
	復旧、復帰に向けた対応	・BCP に基づく情報システムにおける運用手順の整備 ・発災直後の運用から、通常時の運用への復帰手順の整備 ・最新の医療情報システムの状態に復旧・復帰するための手順整備 ・バックアップ整備（大規模災害等を想定した遠隔保管を含む。） ・臨時措置(仮復旧など)として必要な情報システム資源（情報機器等）の確保方法の準備　など
	資源配分、運用規模の変更	・資源不足の程度に応じた対応の確認　など
サイバー攻撃	攻撃による被害発生のリスク回避や低減	・緊急時対応体制（CSIRT）の整備 ・利用者等の関係者の教育・訓練 ・脆弱性対策等 ・情報共有体制の構築（外部有識者、事業者） ・攻撃を受けた際の代替運用や手段の確保　など
	被害拡大の防止	・BCP を踏まえた情報システムに関する手順整備 ・ネットワークやバックアップ等に関する安全性の確保（論理的／物理的ネットワークの構成分割、追記不能型のバックアップなど）　など
	復旧計画の策定	・医療情報システムに関する各種ドキュメント（構成、設定、手順など）の整備 ・臨時措置（仮復旧など）に必要な情報システム資源（情報機器等）の確保方法の準備　など
システム障害（ネットワーク障害含む）	障害発生時のリスク回避やリスク低減	・組織内外の周知、障害対応体制の整備 ・冗長化対策（ホットスタンバイ／コールドスタンバイ、ネットワーク等の二重化など） ・長期間にわたる障害の場合の方針や手順の整備 ・データやシステムのバックアップの確保　など

１１．３　非常時の対応

- 非常時の対応には、主に状況把握・拡大防止・原因究明等と、通常時への復旧・復帰に向けた対応などがある。
- 非常時には、あらかじめ準備した手順等に基づいて対応する必要がある。一方で、事前に想定していない事象の発生もありうることから、想定外の状況に対する方針などもあらかじめ定めておく必要がある。
- 企画管理者は、想定される非常時の原因に応じた具体的な対応や措置を整理する必要がある。

表１１－３　非常時の原因に応じた対応例

非常時の原因	必要な対応	求められる対応や措置例
災害 （主に地震、水害、火災等、医療情報システムのみに限らず、医療機関等全体への被災が想定されるもの）	災害発生時のフェールセーフ	・要員・情報システムの安全性の確保 ・冗長化した情報システム等の切り替え ・情報システム・サービスの安全な停止 ・リスクを踏まえた臨時措置（認証方法の変更など）の実施　など
	復旧、復帰に向けた対応	・発災直後の非常時の運用から、通常時の運用への復旧、復帰 ・医療情報システムの復旧、最新化　など
	資源配分、運用規模の変更	・要員（臨時要員含む）確保　など
サイバー攻撃	攻撃による被害発生のリスク回避やリスク低減	・被害状況、業務影響の把握 ・不正アクセスやマルウェアに対する検知・遮断・隔離 ・代替運用や手段への切り替え　など
	被害拡大の防止	・発生原因の特定と被害拡大防止策の検討（サービスの遮断等） ・組織内の連絡・情報共有体制の整備 ・システム関連事業者を含む対策を実施するための協働体制の整備 ・外部有識者、システム関連事業者からの情報収集・支援 ・所管官庁・関係者への報告や広報（状況説明等）など
	復旧、復帰に向けた対応	・証拠、証跡の分析検証、原因の特定 ・医療情報システムの復旧、最新化 ・安全性の確認（被害原因の封じ込め・解消等） ・所管官庁・関係者への報告、広報（復旧予定等）など
システム障害 （ネットワーク障害含む。）	障害発生時のリスク回避やリスク低減	・障害状況、業務影響の把握 ・代替運用や手段への切り替え　など
	復旧、復帰に向けた対応	・障害原因の特定 ・改修予定や再発防止措置の策定　など

１２．サイバーセキュリティ

【遵守事項】

① サイバーセキュリティに関する組織的対策、職員や委託先事業者への対策を検討し、整理すること。技術的な対応・措置については、担当者にリスク評価を踏まえた対策の検討を指示し、状況を確認すること。

② 整理したサイバーセキュリティ対策を踏まえ、サイバーセキュリティ対応計画を策定し、当該計画の内容について経営層に報告し、承認を得ること。

③ サイバーセキュリティ対応計画を踏まえ、その内容を医療機関等で定める各規程や手順等に反映すること。

④ サイバーセキュリティ対応計画を踏まえ、各対策の実施状況を確認すること。技術的な対応・措置については、担当者に対応計画を踏まえた文書の整備を指示し、対応状況を確認すること。

⑤ サイバーセキュリティ対応計画を踏まえた訓練を定期的に実施し、その結果を経営層に報告し、承認を得ること。また、訓練結果を踏まえ、対応計画の検証・見直しを実施し、必要に応じて対応計画等の改善を行うこと。

⑥ サイバーセキュリティインシデントが発生した際に、情報交換等を行う関係者の情報をあらかじめ整理し、必要に応じて契約等を行うこと。（ここでいう関係者には、利用する医療情報システム・サービスのシステム関連事業者をはじめ、報告対象となる行政機関等、その他必要に応じて助言等の支援を求める外部有識者等が含まれる。）

⑦ サイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏えいや医療サービスの提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（平成 30 年 10 月 29 日付け医政総発 1029 第 1 号・医政地発 1029 第 3 号・医政研発 1029 第 1 号厚生労働省医政局関係課長連名通知）に基づき、所管官庁への連絡等の必要な対応を行うほか、そのために必要な体制を整備すること。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。

⑧ サイバーセキュリティインシデントが発生した際には、その状況について、定期的に経営層に報告すること。また、当該事象を踏まえ、サイバーセキュリティ対応計画の検証・見直しを実施し、必要に応じて改善を行うこと。

⑨ サイバーセキュリティ事象による非常時としての対応が生じた場合には、「１１．非常時（災害、サイバー攻撃、システム障害）対応と BCP 策定」に示す内容を実施すること。

１２．１ サイバーセキュリティ対応計画の策定

- 非常時の原因の一つであるサイバー攻撃は、攻撃者が悪意を以て行う犯罪行為であり、その方法も様々である。情報システムの高度化に合わせて変化することや、システム利用者側の過失や知識の不足などを利用した攻撃も存在することから、システム側のみの対応では防御が不十分となることもあり、対策を困難にしている。
- 企画管理者は、具体的に、医療機関等や企業、行政機関等でどのような被害が生じているのか等を含めたサイバーセキュリティ事案の実情を把握することが重要である。
- その上で、組織的な対応と技術的な対応の両面から担当者と協議し、対策を整理する必要がある。
- 攻撃を受ける前の通常時における対応、攻撃を受けた場合の非常時としての対応、被害からの復旧・復帰などのフェーズの対応策をサイバーセキュリティ対応計画等の形で整理し、経営層の承認を得ること。
- 対応計画の具体的な内容の検討に際しては、経済産業省及び独立行政法人情報処理推進機構において策定している「サイバーセキュリティ経営ガイドライン」などが参考となる。

１２．２　サイバーセキュリティ対応計画の実践

- サイバーセキュリティ対応計画には、通常時と攻撃を受けた際の非常時における対策のいずれをも含んだものとする必要がある。通常時に適切な対策を実施することで、攻撃に備えるとともに、非常時の対応計画に盛り込んだ対策が想定通りに機能するかどうかをあらかじめ確認・検証することが重要である。企画管理者は、担当者と協働して、定期的に非常時を想定した訓練や機能テストなどを行うこと。また、訓練の結果得られた課題等については、サイバーセキュリティ対応計画等に反映することが求められる。
- 情報機器等の脆弱性や利用者の過失等が起点となって被害が生じている事象もみられている。通常時における情報収集や点検、未然防止策を検討するためのシステム関連事業者も含めた協働体制づくりが重要である。
- サイバー攻撃は日々巧妙化、多様化、高度化することから、サイバーセキュリティ対応計画等については、少なくとも年１回以上の頻度で見直しを図ること。

１２．３　サイバー攻撃被害時の対応

- サイバー攻撃を受けた際には、医療機関等独自の対応では対処しきれない事案も想定される。所管官庁への迅速な連絡や情報共有を行うことができるよう、通常時から連絡先や連絡手順、連絡体制を整備しておくこと。
- 非常時は、医療機関等内の職員や契約事業者だけでなく、一時的に医療情報システムに接続する関係者に対しても、速やかに情報共有が可能な体制を講じることも重要である。

１３．医療情報システムの利用者に関する認証等及び権限

【遵守事項】

① リスク評価に基づいて、医療情報システムにおける利用者の認証及びアクセス権限等に関する規程を整備し、管理すること。

② 医療情報システムで利用する認証方法が安全なものとなるよう、担当者に対して、リスク評価に基づいて適切な方法を採用することを指示し、その報告を受けること。

③ 医療機関等の内部における利用者については、医療機関等に所属することが前提となるよう管理すること。所属に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、人事等の情報と整合性をとって利用者の ID 等を付与する等の必要な手順を作成するよう指示すること。

④ 医療情報システムの利用権限は、医療従事者の資格や医療機関内の権限規程に応じて管理すること。資格や権限に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、利用者が所属する部署等からの申請を踏まえて権限を付与し、その結果について申請部署の管理者から確認を得る等の必要な手順を作成するよう指示すること。

⑤ 医療機関等の外部の利用者について、医療情報システムの利用におけるアクセス権限とアクセス状況を管理すること。利用用途とアクセス範囲、アクセス権限等をリスク評価に基づいて整理した上で、その内容に応じて ID やアクセス権限を付与すること。この際、管理者権限の付与については細心の注意を払って、最小限の対象者にのみ付与すること（OS の管理者権限がなければ稼働しないシステムを利用している場合は、次期システム改修時に必ず管理者権限がなくとも稼働するシステムを選定すること）。その具体的な手順については、担当者に作成を指示すること。

⑥ 医療情報システム等の管理権限や ID の安全管理を行うこと。管理権限の種類とその ID、利用が認められている者等を管理して一覧化し、必要に応じて認証に関する情報の変更等を指示すること。

⑦ 医療情報システムで利用する ID 等についての棚卸を定期的に行い、不要なものは削除すること。棚卸については、担当者に具体的な手順の策定を指示すること。また、棚卸結果を経営層に報告し、承認を得ること。

⑧ 電子カルテにおける記録の確定に関して、以下の事項を規程等に含めること。

- 入力者及び確定者の識別・認証
- 記録の確定手順、識別情報の記録の保存
- 更新履歴の保存
- 代行入力を実施する場合、代行入力を認める業務、代行が許可される依頼者と実施者

１３．１　医療情報システムに共通する利用者に関する認証等及び権限

１３．１．１　医療情報システムの利用者

- 利用者認証に関するルールを策定する際は、企画管理者はまず想定される利用者について整理する必要がある。
- 利用者としては、医療情報システムを業務等で利用する医療機関等の内部の職員や、自身の情報を参照する患者等の医療機関等の外部関係者が想定される。
- そのほか、利用者に付与される ID としては、医療情報システムの管理権限を有する ID や、ソフトウェア、システムに接続する情報機器等において便宜的に利用する ID なども想定される。
- 企画管理者は、担当者と協議して、利用者の種類などを整理し、その利用目的に応じて ID の運用規則等を定めること。

１３．１．２　医療情報システムの利用者の登録と認証

- 適切な情報セキュリティを確保するため、医療情報システムの利用に必要な ID を登録する必要がある。医療情報システムでは機微な情報を取り扱うため、利用者の登録や認証をする際の本人確認の方法については、厳格な信頼性が要求される。
- 利用者登録の際には、高い強度の身元確認を行うことが必要であり、対面又はこれに準じた形で確認することが求められる[10]。医療機関等では、例えば人事名簿において職員登録をするなどのプロセスを経ることから、職員登録の内容と整合性が取れる形で利用者登録を行う必要がある。職員が退職する場合なども、削除状況に応じて、医療情報システムの利用者登録からも削除すること。
- 登録された ID を利用する際の当人認証についても、厳格な認証方法が求められており、多要素認証やこれに準じた方法によること等を要する。
- 企画管理者は、身元確認と当人認証の方法を、アクセス管理に関する規程に含めるとともに、担当者に対して、これに対応した措置を講じることを指示する必要がある。

１３．１．３　医療情報システムの利用者の権限設定

- 医療情報システムでは、利用者に応じてアクセスできる情報の範囲や、作業の内容（参照のみ、作成権限あり、更新権限あり等）に関する権限が付与される。医療機関等の人事で定めた権限規程や、医療従事者の資格などに応じて適切な権限を設定すること。
- システム上は利用権限が付与されていても、医療機関等内部のルール等により、利用範囲が制限されることがある。このような場合には、システムの利用ルールについて規程等として文書化し、権限の範囲を明確にすること。

１３．２　電子カルテにおける記録の確定

- 施行通知では、電子カルテ記録に関して、記録の確定、更新履歴、代行入力などに関する利用者の識別や権限等の機能を備えることを求めている。
- 企画管理者は、運用管理規程等にこれらの内容を含めるほか、担当者に対して、規程等に定めた内容に対応する措置をシステムに反映するよう指示し、管理すること。

---

[10]「Digital Identity Guidelines」（NIST SP800-63-4)では、身元確認は IAL（Identity Assurance Level）の強度として整理され、個人の安全への影響に鑑みると、IAL：Level 3 が望ましいとされるが、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る。レベル区分については「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」（令和 7 年 9 月 30 日デジタル社会推進会議幹事会決定）のレベル区分を参照。

表１３－１　当人認証の保証レベルと考え方

当人認証保証レベル	保証レベルの位置づけ
Level 1	当人認証に関するリスクの影響度が「高位」となる対象手続が 該当する保証レベル。 多要素認証を必須とし、さらにフィッシング耐性をもつ認証手法を全ての利用者が利用することを必須とすることで、厳格な 耐性を確保する。
Level 2	当人認証に関するリスクの影響度が「中位」となる対象手続が 該当する保証レベル。 多要素認証を必須とし、さらにフィッシング耐性をもつ認証手法を希望する利用者が選択的に利用できるようにすることで、 標準的な耐性を確保する。
Level 3	当人認証に関するリスクの影響度が「低位」となる対象手続が該当する保証レベル。 単要素認証により、簡易的な耐性を確保する。

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】

① 法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行うこと。

1. 以下の電子証明書を用いて電子署名を施すこと

(1)「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条第１項に規定する電子署名を施すこと。なお、これはローカル署名のほか、リモート署名、立会人型電子署名の場合も同様である。

(2) 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、国家資格の確認が電子的に検証可能な電子証明書を用いた電子署名等を用いること。

(a) 厚生労働省「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」において策定された準拠性監査基準を満たす HPKI（Healthcare Public Key Infrastructure）認証局の発行する電子証明書を用いて電子署名を施すこと。

HPKI 認証局が発行する電子証明書内には、医師等の保健医療福祉に係る資格情報が含まれている。したがって、HPKI 認証局の発行する電子証明書を使用して電子署名をすると、電子的な本人確認に加え、医師等の国家資格を電子的に確認することが可能である。

ただし、当該電子署名を施された文書を受け取る者が、国家資格を含めた電子署名を正確に検証できる必要がある。

(b) 認定認証事業者（電子署名法第２条第３項に定める特定認証業務を行う者として主務大臣の認定を受けた者をいう。以下同じ。）又は認証事業者（電子署名法第２条第２項の認証業務を行う者（認定認証事業者を除く。）をいう。）の発行する電子証明書を用いて電子署名を施すこと。その場合、当該電子署名を施された文書を受け取る者が、国家資格の確認を電子的に検証でき、電子署名を正確に検証できる必要がある。事業者（認証局あるいは立会人型電子署名の場合は電子署名サービス提供事業者をいう。以下「14．法令で定められた記名・押印のための電子署名」において同じ。）を選定する際には、事業者が次に掲げる事項を適切に実施していることについて確認すること（ローカル署名のほか、リモート署名、立会人型電子署名の場合も同様）。

・ 事業者による利用者の実在性、本人性及び利用者個人の申請意思の確認に当たっては、 オンラインの場合、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）第 3 条第 1 項に規定する署名用電子証明書に係る電子署名により確認を行うこと。マイナンバーカードによる確認が行えない場合は、身分証明書と住民票等の公的証明書をスキャンしたデータ（いずれも本項と同等の電子署名（資格確認を除く）を施すこと）により確認を行うこと。郵送の場合は、身分証明書のコピー（署名又は押印（実印が捺印され、印鑑登録証明書が添えてあること ））、住民票等の公的証明書により確認を行うこと。対面の場合は、身分証明書と住民票等の公的証明書により確認を行うこと。なお、新たな技術により、医療分野の特性を踏まえた現行の本人確認に必要な保証レベルと同等のレベルが担保される方法を用いることが可能となった場合には、これを活用することも可能であるため、本ガイドライン及び関連資料を参照の上、選択・採用すること。

※ 身分証明書の確認は、公的な写真付きの身分証明書であればマイナンバーカード、運転免許証、パスポート等のいずれか１種類により、又はその他の身分証明書であれば２種類以上により行うこ

と。

・ 事業者による利用者の国家資格保有の確認は、

(イ) 利用者が HPKI 認証局の発行する署名用証明書を用いた電子署名を事業者へ提供することによりオンラインで行う方法

(ロ) 利用者が官公庁の発行した国家資格を証明する書類（以下「国家資格免許証等」という。）の原本又はコピー等（紙媒体の場合は、国家資格免許証等のコピーに署名又は押印（実印が捺印され、印鑑登録証明書が添えてあること）があること。電子媒体の場合は、本項と同等の電子署名（資格確認を除く）をスキャンしたデータに施すこと。）を事業者へ持参、郵送又は送信する方法

(ハ) 利用者が電子署名による確認方法以外の電子的に国家資格等情報と連携して提示できる仕組みを用いて事業者へ提示する方法

(ニ) 利用者の所属又は運営する医療機関等が利用者の国家資格保有の事実の立証を事業者へ行う方法

のいずれかによって利用者の登録時において確認すること（電子署名を行う都度、事業者による医師等の国家資格保有の確認を求めるものではない）。

なお、(イ)～(ハ)の場合、事業者は、資格確認に用いた国家資格免許証等のコピーや証明書等について、保存年限を定めて保存しておくこと。(ニ)の場合、次に掲げる事項が適切に行われていることについて事業者が確認を行うこと。

– 医療機関等の管理者が、自組織の実在性を事業者に対して立証すること。

– 医療機関等の管理者が国家資格保有の確認を行った者の「氏名、生年月日、性別、住所」（以下「基本４情報」という。）を事業者へ提出すること（これによって、利用者が実在性、本人性及び利用者個人の申請意思を立証した際に、国家資格保有の立証もなされたものとみなすこととする。）。

– 医療機関等による国家資格保有の立証に当たって、医療機関等が責任の主体としての説明責任を果たすため、資格確認を行った実施記録の作成を行うこと。また、資格確認を実施した国家資格免許証等のコピーや利用者の基本４情報を提出した書類のコピー等について保存年限を定めて保存し、医療機関等の内部の独立した監査部門による定期的な監査を行うこと。

・ 事業者が、上記の事項について、適切な外部からの評価を受けていること。

※ (イ)～(ニ)のいずれかによって資格確認を行った後、利用可能となった当該電子署名を利用者が他の事業者に提供した場合、提供を受けた事業者が別途資格の確認を行う必要はない。なお、この場合であっても以下の事項を行うこと。

- 適切な外部からの評価を受けること。
- 資格確認に用いた証明書等について、保存年限を定めて保存しておくこと。

(c) 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、その署名用電子証明書に係る電子署名に紐づく国家資格が検証時に電子的に確認できること、当該電子署名を施された文書を受け取る者が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. 法定保存期間等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて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、第三者による検証を可能にするため、時刻認証業務の認定に関する規程（令和 3 年総務省告示第 146 号）に基づき認定された事業者（認定事業者）が提供するものを使用すること。

(2) 法定保存期間中、タイムスタンプの有効性を維持するための対策を実施すること。
(3) タイムスタンプの利用や長期保存に関しては、今後も、関係府省庁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実施すること。
(4) 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。

② 電子署名に用いる秘密鍵の管理が、認証局が定める「証明書ポリシー」（CP）等で定める鍵の管理の要件を満たして行われるよう、利用者に指示し、管理すること。

１４．１　法令で定められた記名・押印のための電子署名の要件

- 平成 12 年 5 月に電子署名法が成立した。また、e-文書法省令において指定された医療関係文書においては、電子署名法第 2 条第 1 項に規定する電子署名によって、記名・押印に代わり電子署名を施すことで、作成・保存が可能となった。
- 近年、ローカル署名に加え、リモート署名や、クラウド技術を活用した立会人型電子署名を用いたサービスが登場している。電子署名法第 2 条第 1 項の要件を満たすものは、電子署名法における電子署名に該当する。
- 利用者と認証局あるいは電子署名サービス提供事業者の間で行われる本人確認（利用者の実在性、本人性、利用者個人の申請意思の確認及び当人認証）等のレベルや電子署名サービス提供事業者内部で行われるプロセスのセキュリティレベルは様々である。各サービスの利用に当たっては、当該各サービスを利用して締結する契約等の性質や、利用者間で必要とする本人確認レベルに応じて、適切なサービスを選択すること。
- 立会人型電子署名の選択に当たっては、総務省・法務省・経済産業省から令和 2 年 7 月 17 日に示されている「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A（電子署名法 2 条 1 項に関する Q&A）」も参照すること。

表１４－１　電子署名の種類

署名方式	概要
ローカル署名	IC カードやパソコン等の記録媒体に格納された、本人が管理する鍵で署名するもの
リモート署名	クラウド上のサーバに利用者※自身の署名鍵を格納し、利用者が当該サーバにリモートでログインした上で行う電子署名 ※電子署名法第 2 条第 2 項における自らが行う電子署名についてその業務を利用する者
立会人型電子署名	利用者の指示に基づき電子署名サービス提供事業者※自身の署名鍵による暗号化等を行う電子署名 ※電子署名法に規定する電子署名に関するサービスを提供する者のうち、立会人型電子署名に関するサービスを行う者

- また、施行通知に示される電磁的記録の保存等が可能な文書は、正当な権限で作成された記録であり、虚偽入力、書換え、消去及び混同が防止され、かつ、第三者から見て作成の責任の所在が明確であることが求められる。電子署名法第 3 条では、電子文書（デジタル情報）について、本人すなわち当該電子文書の作成名義人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われていると認められる場合には、当該作成名義人が当該電子文書を作成したことが推定されることとしている。
- 医療分野において電子署名に係る争訟が生じた場合に備え、立証責任を軽減する観点から、下記のような特徴を備えた措置の利用を検討すること。
  - 十分な暗号強度を有し、他人が容易に同一の鍵を作成できないものであること
  - 電子署名が本人の意思に基づき行われたことを確認できること
- 立会人型電子署名の選択に当たっては、総務省・法務省・経済産業省から令和２年９月４日に示されている「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A（電子署名法 3 条に関する Q&A）」も参照すること。
- 処方箋のように、医師等の有資格者に作成が求められる文書が医師法等の法令で定められている場合がある。これらの多くには記名・押印が求められており、記名・押印は本人の証明だけでなく、有資格者としての当該行為に対する責務も示す。当該資格者による行為であることの証明を電子的に担保する考え方を「Nonrepudiation（否認防止）」と呼び、医師等の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名等により担保可能となる。
- また、特に医療に係る文書では一定期間、信頼性を持って署名を検証可能である必要がある。電子署名は紙媒体への署名や記名・押印と異なり、電子署名法第２条第１項の要件該当性は厳密に検証することが可能である反面、電子証明書等の有効期限が過ぎたり、失効させた場合は検証不能となるという特徴がある。さらに、電子署名の技術的な基礎となっている暗号技術は、解読法やコンピュータの演算速度の進歩につれて次第に脆弱化が進み、中長期的にはより強固な暗号アルゴリズムへ移行することも求められる。
- このような点を踏まえ、電子証明書を利用する場合には、有効期間や失効の有無、暗号アルゴリズムの脆弱化の影響を受けることなく、法定保存期間等の一定期間にわたり電子署名の検証を継続できることが求められる。また、対象文書は行政による監査等の対象となるため、付与された電子署名は行政機関等においても検証可能でなければならない。
- なお、デジタルタイムスタンプ技術を用いた長期署名方式の標準化が進んでおり、長期的な署名検証の継続を可能とする方式が ISO 規格として制定されている[11]。
- 医療情報の保存期間は、生物由来製剤に係る文書として 20 年以上の長期にわたるものも存在する。システム更新や検証システムの互換性等の観点からも、例えば、前述の標準技術を用い、必要な期間、電子署名の検証を継続して検証可能とすることが想定される。

[11] ISO14533-1：2022CMS 利用電子署名(CAdES)の長期署名プロファイル、ISO14533-2:2021XML 署名利用電子署名(XAdES)の長期署名プロファイル、ISO14533-3:2017PDF 長期署名プロファイル(PAdES)、ISO14533-4:2019proofofexistenceobjects

１４．２　電子署名を含む文書全体に付与するタイムスタンプの要件

- タイムスタンプは、タイムスタンプに刻印されている時刻以前にその文書が存在し（存在証明）、その時刻以降文書が改ざんされていないことを証明する（非改ざん証明）。
- 法令で保存が義務付けられた文書の場合においては、第三者による電子署名の検証を可能とするため、「時刻認証業務の認定に関する規程」に基づき認定された事業者が提供するタイムスタンプを使用すること。また、法定保存期間中、タイムスタンプの有効性を継続できるようにするために必要な対策を実施すること。
- なお、法令保存期間等がない文書については、「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 – 」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することも可能である。
- タイムスタンプの利用や長期保存に関しては、今後も、関係府省庁の通知や指針、標準技術、関係ガイドラインに留意しながら適切な対策を実施すること。
- 電子証明書は、タイムスタンプを付与する時点で有効なものを用いて電子署名を行わなければならない。本来法定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。具体的には、電子証明書が有効な期間内に、電子署名の検証に必要な情報（関連する電子証明書や失効情報等）を収集し、署名対象文書及び署名値と併せてタイムスタンプを付与する等の対策が求められる。

１５．技術的な安全管理対策の管理

【遵守事項】

① 物理的安全管理対策のうち医療情報及び医療情報システムを保管する場所の選定について、リスク評価を踏まえて、担当者と検討すること。またその結果を経営層に報告の上、承認を得ること。医療情報システムに関する整備計画等を策定している場合には、これと整合性をとって選定すること。

② 個人情報の保存場所及び入力・参照可能な端末等が設置されている区画等への入退室管理（施錠、識別、記録）を行うよう、管理内容を含む規程等を策定すること。

③ 記録媒体及び記録機器の保管及び取扱いについて、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関係者に周知徹底するとともに、教育を実施すること。また、保管及び取扱いに関する作業履歴を残すこと。

④ 医療情報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、バックアップの頻度や方法等を明確にすること。これらを運用管理規程に定め、その運用を関係者全員に周知徹底すること。

⑤ 記録媒体の劣化への対応を図るための一連の運用の流れを運用管理規程に定めるとともに、関係者に周知徹底すること。

⑥ システム運用に関する安全管理対策として必要な項目を担当者と協働して検討すること。特に医療情報システムの脆弱性（マルウェア対策ソフトウェアやサイバー攻撃含む）への対策に関する項目については、定期的に見直しを図ること。

⑦ 医療機関等において利用するネットワークは、リスク評価を実施したうえで選定し、経営層の承認を得ること。なお、医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。また、ネットワークの安全性確保を目的とした実装と運用設計を企画管理者等が実施した場合には、その内容を確認の上、経営層に報告し、承認を得ること。

⑧ 保守に関する安全管理対策として必要な項目を担当者と協働して検討すること。また、必要に応じて、保守を行うシステム関連事業者と契約や SLA 等により管理項目（OS やソフトウェアのアップデート、パッチ適用に関する役割分担含む）について取決めを行うこと。

⑨ 医療情報システムの動作確認や保守においては、原則として個人情報を含む医療情報を用いないことを運用管理規程等に含めること。また、やむを得ず医療情報を用いる場合には、漏えい等が生じないために必要な対策を講じる旨を示し、その具体的な手順の策定を担当者に指示すること。

⑩ 医療情報システムで用いるシステム、サービス、情報機器等の品質を適切に管理し、必要に応じて、改善措置を講じること。品質の管理方法については、担当者と協働して検討すること。

⑪ 情報機器、ソフトウェアの品質管理に関する対応を運用管理規程で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。

⑫ 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。

⑬ 医療情報システムが法令等で求められている要件を満たすよう適切に管理すること。特に施行通知、外部保存通知などで求める要件を満たしていることを確認し、調達においては当該要件を満たすシステムを選定すること。具体的な確認項目や、医療情報システムにおける実装内容等については、担当者に確認の上、必要な検討を行うよう指示すること。

⑭ ①～⑬において、担当者が整備した対策について、関連規程等に反映すること。また、システム運用の実施状況については、定期的に担当者から報告を受け、経営層に報告して承認を得ること。

１５．１　技術的な対応の管理

- 企画管理者は、通常時から経営層に代わって医療情報システムの様々な運用管理を担う。
- 一方で、医療情報システムにおける技術的対応については、専門的な知見が必要であり、これを有する担当者に委ねることが想定される。この場合、技術的な対応のうち、基本的なルールを規程や規則などで定め、具体的な運用管理は担当者に権限移譲することとなる。また、運用管理は事業者に委託することも想定される。特に、アップデートについては可能な限り、事業者の保守範囲に含めることが望ましい。保守範囲とならない場合は、医療機関等の責任でアップデートが必要となる。
- この場合、企画管理者は、技術的な対応のうち特に重要な部分について指示するほか、通常時における運用、事業者からの情報収集等の実施を担当者に指示すること。また、実施状況の報告を受けて状況を把握すること。また、医療情報システム全般の運用状況について、経営層に報告し、承認を得ながら管理すること。

１６．紙媒体等で作成した医療情報の電子化

【遵守事項】

① 医療情報を含む文書等の紙媒体をスキャナ等で読み取り、電子化する場合には、これに必要な情報機器等の条件や手順等を運用管理規程等に定めること。

② スキャナにより読み取った電子情報と元の文書等から得られる情報が同等であることを担保する情報作成管理者を配置すること。

③ 医療情報を含む文書等をスキャナにより電子化する場合、スキャナによる読み取りに係る責任を明確にするため、作業責任者（実施者又は情報作成管理者）が電子署名法に適合した電子署名を遅滞なく行う旨を、運用管理規程等に定めること。なお、電子署名については「14．法令で定められた記名・押印のための電子署名」を参照すること。

④ 情報作成管理者に対して、スキャナによる読み取り作業が運用管理規程に基づき適正な手続で確実に実施されるために必要な措置を講じるよう指示し、その結果の報告を求めること。

⑤ 診療等の都度スキャナ等で電子化して保存する場合、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を運用管理規程等に定めること。

⑥ 過去に蓄積された紙媒体等をスキャナ等で電子化して保存する場合、以下の措置を講じること。

・ 対象となる患者等に、スキャナ等で電子化して保存することを事前に院内掲示等で周知し、異議の申立てがあった場合、その患者等の情報は電子化を行わないこと。

・ 必ず実施前に実施計画書を作成すること。実施計画書には次に掲げる事項を含めること。

– 運用管理規程の作成と妥当性の評価方法（評価は、大規模医療機関等にあっては、外部の有識者を含む公正性を確保した委員会等で行うこと（倫理委員会を用いることも可））

– 作業責任者

– 患者等への周知の手段と異議の申立てに対する対応方法

– 相互監視を含む実施体制

– 実施記録の作成と記録項目（次項の監査に耐え得る記録を作成すること）

– 事後の監査人と監査項目

– スキャン等で電子化を行ってから紙やフィルムの破棄までの期間及び破棄方法

・ 事後の監査は、システム監査技術者や Certified Information Systems Auditor（ISACA 認定）等の適切な能力を持つ外部監査人によって実施すること。

⑦ 企画管理者は、紙の調剤済み処方箋をスキャナ等で電子化して保存する場合、以下の措置を講じること。

・ 紙の調剤済み処方箋の電子化のタイミングに応じて、⑤又は⑥の措置を講じること。

・ 「電子化した紙の調剤済み処方箋」を修正する場合、「『元の』電子化した紙の調剤済み処方箋」を電子的に修正し、「『修正後の』電子化した紙の調剤済み処方箋」に対して薬剤師の電子署名が必須となる。電子的に修正する際には、「『元の』電子化した紙の調剤済み処方箋」の電子署名の検証が正しく行われる形で修正すること。

⑧ スキャナ等で電子化を行った後も、紙等の媒体をそのまま保存する場合、元の紙媒体やフィルムの安全管理を行うこと。

１６．１ 診療録等をスキャナ等により電子化して保存する場合の共通要件

➢ 「診療録等をスキャナ等により電子化して保存する場合」とは、診療録等の「施行通知」に示される電磁的記録による保存等が可能な文書を、スキャナ等により電子化して保存する場合を指す。具体的には、

・ 電子カルテ等により、診療に用いる文書の大部分が電子化されている一方、他院から紙やフィルムでの診療情報提供書等の受け入れが必要な場合
・ 電子カルテ等の運用を開始し、電子保存を施行したが、施行前の診療録等が紙やフィルムで残り、一貫した運用ができない場合
・ 電子化の対象が、オーダエントリシステムや医事システムのみの運用であって、紙等の保管に窮している場合

が挙げられる。

- 企画管理者は、このような場合の手順等や情報機器等の条件について、業務に支障が生じることのないよう整理し、運用管理規程等に定めることが求められる。

１６．２　診療等の都度スキャナ等により電子化して保存する場合

- 診療に用いる文書の大部分が電子化されている一方、他院から紙やフィルムでの診療情報提供書等の受け入れが必要な場合、診療等の都度スキャナ等による電子化が実施されることも想定される。
- 企画管理者は、スキャナ等により電子化して保存する場合の共通要件や、改ざん動機が生じないと考えられる時間内に適切に電子化を行うことなどを、運用管理規程等に定めること。

１６．３　過去に蓄積された紙媒体等をスキャナ等により電子化して保存する場合

- 電子カルテ等の運用を開始した後も、過去の診療録等が紙又はフィルム媒体で残存し、一貫した記録管理ができない状況が生じ得る。この場合は、診療の都度電子化して保存する場合と異なり、既存の原本を後日電子化することになるため、記録の真正性に疑義が生じ得る。説明責任を担保する観点から相応の対策が必要となり、スキャナ等により電子化して保存する場合の共通要件に加え、厳格な監査の実施が求められる。
- 企画管理者は、このような説明責任への対応の観点から、本項の遵守事項①～④に加えて、遵守事項⑥に記載する措置を講じること。

１６．４　紙の調剤済み処方箋をスキャナ等により電子化して保存する場合

- 紙の調剤済み処方箋の電子化とは、記名押印又は署名を行い調剤済みとした処方箋を電子化することをいう。
- 紙の処方箋を薬局で受け取った場合、調剤済みとなるまでは電子化したものを原本としてはならない（誤った運用例：薬局で紙の処方箋を受け付けた時点で電子化し、それを原本として調剤を行い、薬剤師の電子署名をもって調剤済みとする等）。
- 調剤終了時までは特段の問題なく経過した処方箋であっても、その後内容の修正が発生することがある（例：記載事項を確認したものの修正を忘れた場合等）。
- 企画管理者は、診療録等をスキャナ等により電子化して保存する場合の共通要件に加えて、一旦電子化した紙の調剤済み処方箋の修正等、実際の運用を踏まえて、遵守事項⑦に記載のとおり、対応を行うこと。

１６．５　運用の利便性のためにスキャナ等により電子化を行うが、紙等の媒体もそのまま保存を行う場合

- スキャナ等で電子化した後も、紙等の媒体の保存は継続して行う場合、電子化した情報には、保存義務等の要件は課せられない。しかし、個人情報保護上の配慮は同等に行う必要がある。
- またスキャナ等による電子化の際に医療に関する業務等に差し支えない精度の確保も必要である。
- 企画管理者は、このような観点から、遵守事項⑧に記載する措置を講じること。