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

システム運用編

目次

【はじめに】 - 1 -

1．情報セキュリティの基本的な考え方 - 2 -

1．1　安全管理に関する法制度等による要求事項 - 2 -

2．システム設計・運用に必要な規程類と文書体系 - 3 -

2．1　システム運用担当者において作成すべき文書類 - 3 -

3．責任分界 - 4 -

3．1　技術的な対応における責任分界決定の考慮事項 - 4 -

3．2　要求仕様適合性の確認を踏まえた調整 - 4 -

3．3　医療機関等が負う責任に関する責任分界 - 5 -

3．3．1　通常時の運用における責任分界 - 5 -

3．3．2　非常時の運用における責任分界 - 5 -

3．4　提供される情報システム・サービスに応じた責任分界 - 5 -

3．4．1　事業者が提供するサービスの類型による責任分界 - 5 -

3．4．2　複数の事業者に対する委託を含む場合の責任分界 - 6 -

3．5　第三者提供における責任分界 - 7 -

4．リスクアセスメントを踏まえた安全管理対策の設計 - 8 -

4．1　情報資産の種別に応じた安全管理の設計 - 8 -

4．2　リスクアセスメントを踏まえた安全管理対策の設計 - 8 -

5．システム設計の見直し（標準化対応、新規技術導入のための評価等） ..... - 9 -

5．1　医療情報システム等における情報の相互運用性と標準化の重要性 ..... - 9 -

5．2　標準化対応、データ形式・プロトコルの互換性の確保 ..... - 10 -

6．安全管理を実現するための技術的対策の体系 ..... - 11 -

6．1　安全管理対策に関するシステムアーキテクチャ（クライアント側、サーバ側、インフラ、セキュリティ）.. - 11 -

6．2　医療機関の規模や導入システム等の形態に応じた対応 ..... - 12 -

7．情報管理（管理・持出し・破棄等） ..... - 13 -

7．1　外部へ持ち出す医療情報の管理対策 ..... - 14 -

7．2　医療機関等外から医療情報システムに接続する利用の場合への対策 ..... - 14 -

7．2．1　医療機関等の職員による外部からのアクセス ..... - 14 -
7．2．2　患者等に診療情報等を提供する場合の外部からのアクセス ..... - 15 -
7．2．3　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 - 15 -

7．3　医療情報の破棄 ..... - 15 -

7．4　医療情報を格納する記録媒体、情報機器等の紛失、盗難等が生じた場合の対応 ..... - 16 -

8．利用機器・サービスに対する安全管理措置 ..... - 17 -

8．1　マルウェア対策 ..... - 17 -

8．2　情報機器等の脆弱性への対策 ..... - 18 -

8．3　端末やサーバの安全な利用の管理 ..... - 19 -

８．４　情報機器等の棚卸 ..... - 19 -

８．５　医療機関等が管理する以外の情報機器の利用に対する対策 ..... - 19 -

９．ソフトウェア・サービスに対する要求事項 ..... - 21 -

９．１　ソフトウェアの構成管理..... - 21 -

９．２　情報機器・ソフトウェアの導入や変更時における品質管理..... - 21 -

１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置 ..... - 22 -

１０．１　保守時の安全管理対策..... - 22 -

１０．２　リモートメンテナンスにおける安全管理対策 ..... - 23 -

１１．システム運用管理（通常時・非常時等）..... - 24 -

１１．１　通常時における運用対策 ..... - 24 -

１１．２　非常時における対応 ..... - 25 -

１２．物理的安全管理措置..... - 26 -

１２．１　サーバルーム等の物理的要件 ..... - 26 -

１２．２　バックアップの管理..... - 26 -

１２．３　その他 ..... - 27 -

１２．３．１　記録媒体等の経年変化の管理・委託事業者への配送等..... - 27 -

１２．３．２　端末・サーバ装置等の不適切な利用等に関する対策..... - 27 -

１３．ネットワークに関する安全管理措置..... - 28 -

１３．１　ネットワークに対する安全管理 ..... - 29 -
１３．１．１　セキュアなネットワークの構築 ..... - 30 -
１３．１．２　選択すべきネットワークのセキュリティ ..... - 30 -
１３．２　不正な通信の検知や遮断、監視 ..... - 32 -
１３．３　通信の暗号化・盗聴等の防止 ..... - 33 -
１３．３．１　ネットワーク回線の暗号化 ..... - 33 -
１３．３．２　情報に対する暗号化 ..... - 34 -
１３．３．３　盗聴防止等 ..... - 34 -
１３．４　無線 LAN の利用における対策 ..... - 34 -
１４．認証・認可に関する安全管理措置 ..... - 35 -
１４．１　利用者認証 ..... - 36 -
１４．１．１　利用者の識別・認証 ..... - 36 -
１４．１．２　外部のアプリケーションとの連携における認証・認可 ..... - 38 -
１４．２　アクセス権限の管理 ..... - 38 -
１４．３　電子カルテデータの確定 ..... - 38 -
１５．電子署名、タイムスタンプ ..... - 40 -
１５．１　電子署名、タイムスタンプが求められる場面での対策 ..... - 40 -
１６．紙媒体等で作成した医療情報の電子化 ..... - 41 -
１６．１　保存義務がある書面等に関する紙媒体等の電子化における技術的な対応 ..... - 41 -
１６．２　運用の利便性のためにスキャナ等で電子化を行う場合における技術的な対応 ..... - 41 -
１７．証跡のレビュー・システム監査 ..... - 42 -

１７．１　証跡のレビュー .....- 42 -

１７．２　監査の実施の支援.....- 42 -

１８．外部からの攻撃に対する安全管理措置..... - 44 -

１８．１　サイバーセキュリティ対応.....- 44 -

【はじめに】

＜システム運用編が想定する読者＞

システム運用編は、主に医療機関等において医療情報システムの実装・運用を担う担当者を対象にしており、医療機関等の経営層や企画管理者の指示に基づき、医療情報システムを構成する情報機器、ソフトウェア、インフラ等の各種資源の設計、実装、運用等の実務を担う担当者（以下「システム運用担当者」という。）として適切に対応すべき事項とその考え方を示している。

なお、医療情報システムの実装・運用において、医療機関等が事業者に委託し、その業務や責任を分担することも考えられる。そのため、委託事業者におかれても本編を参照のうえ、医療機関等と協働されたい。その際、業務や役割、責任の分担の在り方については、あらかじめ両者で取り決めておくことが望ましい。

１．情報セキュリティの基本的な考え方

【遵守事項】

① 法令上求められる医療情報システムの要件等について、企画管理者の指示のもと、各システムの措置や、必要な手順、資料の作成を行うこと。

１．１ 安全管理に関する法制度等による要求事項

- システム運用担当者は、本編に記載の技術的対策を講じる際、法制度により求められる対応を行う必要がある。
- 特に、下記に掲げる事項について適切に対応すること。
  - 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。）における安全管理措置
  - 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。）に関する対応
  - 電子署名、タイムスタンプ

２．システム設計・運用に必要な規程類と文書体系

【遵守事項】

① 採用するシステム、サービス、情報機器等の機能仕様及び利用方法に関する資料を整備し、常に最新の状態を維持すること。

② 医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者・関係者一覧（設置事業者、保守事業者等含む）を作成し、常に最新の状態を維持すること。

③ 医療情報システムの維持及び運用に必要な手順を整備し、常に最新の状態を維持すること。

④ 医療情報システムを適切に利用できるよう、マニュアル等の整備を行うこと。

⑤ 非常時や情報セキュリティインシデントが生じた場合の手順等を作成し、企画管理者の承認を得ること。

２．１　システム運用担当者において作成すべき文書類

- システム運用担当者は、企画管理者が策定した各種規程等を踏まえて、実際の運用に求められる手順や、システム等を構築するための資料等を整備することが求められる。これらの資料は、常に最新化すること。古い手順や技術資料が混入すると、脆弱性が残存する、正常な情報システムの稼働が損なわれる、などのリスクが生じる。
- 通常時だけではなく非常時や情報セキュリティインシデントが生じた場合の対応についても手順を整理するほか、即応できるための資料を整備すること。特に体制面や情報照会・収集の対象なども明示することが重要である。

3．責任分界

【遵守事項】

① 医療情報システムに関する委託において、役割分担を検討するため、事業者から必要な情報等の収集を行うとともに、提供された情報が正確であることを事業者に確認すること。

② 事業者と技術的な対応に関する責任分界を調整する際には、医療機関でのリスク評価に基づく要求仕様への適合性を十分に確認し、必要な調整を行うこと。

③ 技術的な対応に関する役割分担を、委託先事業者との間で調整し、企画管理者に対してその結果を報告すること。

④ サイバー攻撃等が生じた場合の技術的な対応や対外的な説明に関する役割について、事業者と調整し、その結果を企画管理者に報告すること。

⑤ 第三者提供を行う際には、企画管理者と協議の上、医療機関等のリスク評価を踏まえて技術的な対応に関する責任分界を検討し、企画管理者に報告すること。

3．1 技術的な対応における責任分界決定の考慮事項

- 医療情報システムの運用等を委託する場合、提供されるシステム・サービスの機能仕様が、法令、本ガイドラインや関連ガイドラインに適合していることを、医療機関等で直接確認できない可能性がある。
- システム運用担当者は、技術的な対応に関する情報システム・サービスの機能仕様に関する情報と、その内容が正確であることを示す資料を、事業者から提出を求め、その確認を行うこと。

3．2 要求仕様適合性の確認を踏まえた調整

- 技術的な対応に関する責任分界を設定する際は、提供される情報システム・サービスについて、事業者がどのようなリスク評価を踏まえて、対応を分担するのかに関する情報を収集することが求められる。
- 例えば、厚生労働省標準規格となっている「『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（略称：MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security）』ガイド」で示されているチェックリストの提供を受け、リスクコミュニケーションを図ることが想定される。
- その他、総務省・経済産業省の定める「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（以下「２省ガイドライン」という）において、医療機関等と事業者との間でリスクコミュニケーションを図る際には、合意形成に必要な情報を提供することとされている。具体的な内容は同ガイドライン別紙１「ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例」 により示されているため、参考とすること。
- システム運用担当者はこれらの資料を収集し、医療機関等におけるリスク評価との差異などを確認すること。また、必要に応じて事業者と個別の調整を行い、リスク分担などを行うこと。
- クラウドサービスなどを利用する場合には、利用者側でも設定等の役割を果たすことなどが求められる。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」（総務省令和４年10 月 31 日）などでも示されている。

３．３　医療機関等が負う責任に関する責任分界

３．３．１　通常時の運用における責任分界

- 通常時における技術的な対応の責任分界は、主に運用責任や管理責任に関する取り決めを指す。情報システム・サービスが提供される際の運用が、本ガイドライン等に従っていることは、事業者でしか把握できない場合もある。システム運用担当者は運用に関する実施報告などに関する情報の提出を事業者に求めて管理すること。事業者が業務の一部を再委託している場合には、再委託先における実施状況なども併せて報告を求めること。
- このように、システム運用担当者は、委託する情報システム・サービス全般の管理を担う中で、具体的な運用や管理については、事業者に役割を委ねることが想定される。

３．３．２　非常時の運用における責任分界

- 非常時の運用における技術的な対応の責任分界は、主に被害の拡大防止や原因究明などシステム対応のほか、外部への説明責任に関する支援などに関する取り決めを指す。
- 被害拡大防止や原因究明などに関しては、医療機関等側で把握できる運用に関する情報と、委託先である事業者が管理するシステム運用上の資料などを併せて検討することが求められる。それぞれの役割の分担などを事前に取り決めておくことが重要である。
- 外部への説明責任についても、技術的な面から、事業者側でしか把握できない内容がありえる。専門的な観点から適切な資料の準備と提供に関する内容も含めた、責任分担を行うことが求められる。

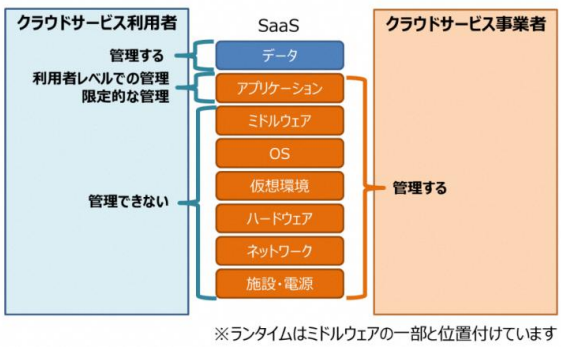
３．４　提供される情報システム・サービスに応じた責任分界

３．４．１　事業者が提供するサービスの類型による責任分界

- 事業者が提供するサービス類型により、医療機関等が直接責任を管理できる範囲が異なる。
- クラウドサービスの場合には、一般的に SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）などの類型で提供される。
- SaaS ではアプリケーション部分、PaaS ではミドルウェア部分、IaaS ではインフラ部分がサービスとして提供される。
- 例えばSaaS を利用する場合には、アプリケーション部分の管理や責任を事業者に委ねることになる。そこで本ガイドラインの遵守を確認するにあたっても、アプリケーション部分に関する安全管理対策項目などについて、事業者との責任分界を検討することになる。
- このように、利用するサービスの内容により、責任を分担する内容が異なるため、医療機関等が行うべき安全管理のうち、明確に責任分界を定め、具体的な管理内容について、事業者と取り決めること。

表３－１　SaaS の場合の技術的な対応における利用者と事業者の管理対象範囲

利用者側の管理対象範囲	事業者側の管理対象範囲
・ 利用者は、アプリケーションを利用するためのデータやアプリケーション上で生成したデータの管理（データに対する編集 ・削除等の行為）をする権限と責任を有する。 ・ アカウント管理などの限定的な管理権限をクラウドサービス事業者から付与され、外部からのアクセス権限を設定する場合がある。	・ クラウドサービス事業者は、契約 ・SLA（Service Level Agreement：サービス品質保証、サービスレベル合意書） に基づくサービスをクラウドサービス利用者に提供するために、アプリケーション層以下の実装、設定、更新及び運用を管理するとともに、クラウドサービス利用者に限定的な管理権限等を提供する場合がある

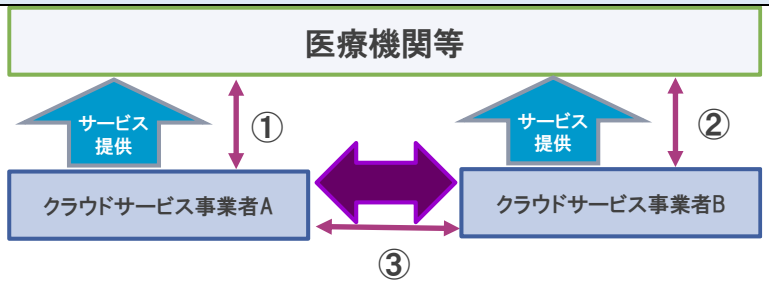


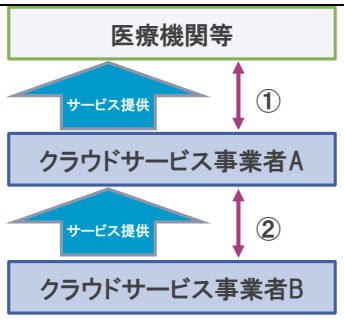
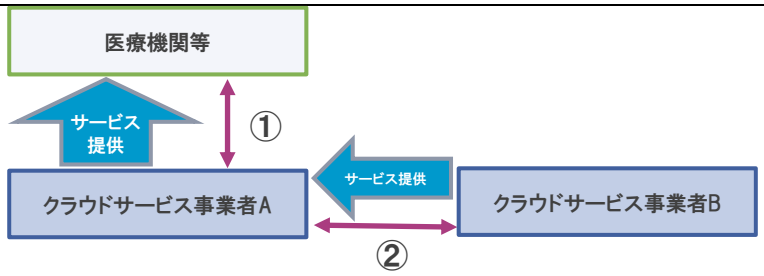
出所：「クラウドサービス提供における 情報セキュリティ対策ガイドライン（第 3 版）」
（総務省、2021 年 9 月）より作成

3．4．2　複数の事業者に対する委託を含む場合の責任分界

- 事業者に委託を行う場合、この情報システム・サービスの利用に際して複数の事業者が関与する場合がある。
- 医療機関等が複数の情報システム・サービスのサービスを組み合わせて利用するような場合と、事業者が複数のサービスを組み合わせて、医療機関等に提供する場合などが想定される（表 3 － 2 参照）。
- 前者では、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、複数の事業者のサービスを連携する部分についても併せて取決めを行うこと。これには、技術的な機能仕様等に関する取決めだけではなく、障害時などの対応などの事業者間での役割分担も含まれる。
- 後者の場合には、医療機関等と、情報システム・サービス等を取りまとめて提供する事業者との間で責任分界を定めることが一般的である。この場合、取りまとめ事業者が利用する他の事業者のサービスとの関係では、再委託などの関係となることが多い。これらの契約関係に留意して取決めを行うこと。
- 企画管理者はこれらのケースについて、各事業者に必要な対応を依頼できるよう、責任分界を設定し、契約や SLA（Service Level Agreement：サービス品質保証、サービスレベル合意書）などにおいて取り決めること。

表 3 － 2　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の部分を各①、②の契約内容を盛り込む必要がある。

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

3．5 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、医療機関等と提供先との間で責任分界を取り決めることになる。第三者提供を実施する方法としては、下記などが想定される。
  - ・メール等による情報の送信、及び受信
  - ・サーバやクラウドサービス等への提供
  - ・アプリケーションが連携する際のデータの提供
  - 提供方法に応じたデータの送受信に係る責任分界など技術的対策に関する内容を定める必要がある。例えば、メール送信の場合、医療機関等が利用するメールサーバまでは、医療機関等が責任を有する等が考えられる。
- システム運用担当者は、企画管理者が取り決めた第三者提供における責任分界と整合性をとれる責任範囲を設定し、企画管理者に報告すること。

４．リスクアセスメントを踏まえた安全管理対策の設計

【遵守事項】

① 企画管理者の指示に基づき、医療機関等で取り扱う情報を適切に管理するための手順等を作成し、運用すること。その際、情報種別による重要度を踏まえるほか、患者ごとに識別できるような措置を講じること。

③ 事業者から技術的対策等の情報を収集すること。例えば、総務省・経済産業省の定めた２省ガイドラインにおける「サービス仕様適合開示書」を利用することが考えられる。

４．１ 情報資産の種別に応じた安全管理の設計

- 情報資産の把握に基づくリスク分析は、安全管理の設計の起点となる。システム運用担当者は、企画管理者と協働して保有する情報の棚卸を行うこと。システム運用担当者は、医療情報システムが直接取り扱う医療情報や、医療情報システムに関する情報などについて、棚卸を行い、情報種別を整理する必要がある。
- 医療情報システムであれば、各システムに情報が保管されている患者数、情報の種別、それらの利用者の範囲、利用権限の設定ルール、持ち出し状況などを整理すること。バックアップについても、どのくらいの医療情報が、どこで、どのような形式で保管されているか、等を把握することが求められる。また情報のライフサイクルを踏まえ、必要な取扱制限（例：複製禁止、持出禁止、配布禁止）を実施する。
- 上述の「医療情報システムに関する情報」は、全体構成図（ネットワーク図、システム構成図等）、各システムを構築・導入するための資料やその管理状況（保管場所、作成時期等）、運用上の設定情報やログ等の管理状況などが挙げられる。
- 情報種別を整理する際に、法令により保存などの要件が定められているものは、その要件への適合状況も併せて確認する必要がある。具体的には「民間事業者等が行う書面の保存等における情報通信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。）や「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。）が求める要件などがある。

４．２ リスクアセスメントを踏まえた安全管理対策の設計

- システム運用担当者は、医療情報等の情報種別や重要度を整理したうえで、企画管理者とともにリスクアセスメント（リスク分析、リスク評価）を行い、技術的対応を実装、運用することになる。
- 対策を講じる場合には、組織の規模等の実情や、システムの利用形態等のリスクに応じて、さまざまな方法が考えられる。また実装の検討に際しては、医療機関等における負担（要員、費用等）を踏まえることも重要である。
- 安全管理対策の設計においては専門的な知見が必要だが、医療機関等においては、十分な資源（要員、費用等）を有していない場合もある。このような場合には、利用を想定する事業者によるリスクアセスメント結果を踏まえた対策を参考にすることなどが想定される。なお、事業者には「サービス仕様適合開示書」を提供させること。
- 特に専任のシステム担当者を要しない場合には、事業者から安全なシステムを導入し、構築と運用等は事業者に委ねるほうが、安全性や経済性で優れていることが多い。
- システム運用担当者は、上記を踏まえた技術的な対応を整理し、企画管理者に報告すること。

５．システム設計の見直し（標準化対応、新規技術導入のための評価等）

【遵守事項】

① システム更新の際の迅速な移行を可能とするため、診療録等のデータについて、原則として標準形式（標準形式が存在しない項目は変換が容易なデータ形式）で出力及び入力が可能なシステムを選定すること。

② マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えたシステムを選定すること。

③ データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと。保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられるが、その際にも以前のデータ形式や転送プロトコルに対応可能な事業者を選定すること。

④ 電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理すること。また、見読化手段である情報機器、ソフトウェア、関連情報等は常に整備された状態に保つこと。

５．１　医療情報システム等における情報の相互運用性と標準化の重要性

- 医療機関等における電子化は、従来の指示、報告、連絡等の意思の共有の業務を効率化し、入力作業の軽減等、業務の総量を減ずることにもつながる。また紙媒体の誤記・誤読リスクも低減し、医療安全にも資する。
- 電子化の過程では、段階的に導入されたシステム間や、異なる事業者から提供されたシステム間で電子情報のやりとりを行う際の相互運用性の確保が必要となる。
- 医療情報システムの安全な管理・運用における重要な観点として、情報セキュリティの重要な要素の一つである「可用性」が挙げられる。ここでいう可用性とは、必要なときに情報が利用可能であることを指し、任意の時点で可用性が確保されなければならない。例えば、システム更新を経ても旧システムで保存された医療情報を確実に利用できるようにしておくこと、すなわち相互運用性を確保することなどが挙げられる。
- なおプロトコルについては、危殆化したものを継続して使用するのではなく、最新のプロトコルに移行する等、安全性確保に配慮した対応が求められる。その際にも以前のデータ形式や転送プロトコルに対応可能な事業者を選定すること。
- 地域連携等における医療機関等間の情報の共有、蓄積、解析、再構築、返信、再伝達等といった場面においても、相互運用性の確保が求められる。
- 医療情報の相互運用性を確保するため、誰もが参照可能かつ利用可能で将来にわたり保守の継続が期待される標準規格（用語集やコードセット、保存形式、メッセージ交換手続等）を利用することや、それらに容易に変換できる状態で保管することが望ましい。
- 経済産業省・厚生労働省においても、種々の国際規格との整合を図り、これを推奨する取組みを進めてきた。特に、厚生労働省では、「厚生労働省標準規格」を示し、その実装を強く推奨しており、標準化の一層の推進が期待される。
- 医療機関等において、自らこれらの用語・コードの保守や標準規格の実装作業をすることは稀であろうが、標準規格に基づく相互運用性の確保の推進のため、システム・サービス事業者に対して標準規格の採用を要件として求めていくことが重要である。
- システム運用担当者は、医療情報システムの導入や運用に当たって、下記事項について事業者から説明を受ける等して、一定の理解を共有しておく必要がある。
  - 標準化に対する基本スタンス
  - 標準規格に対応していないならばその理由

・ 将来のシステム更新、他社システムとの接続における相互運用性に対する対応案

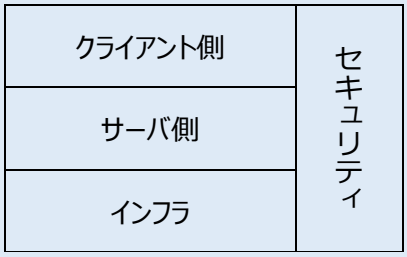
５．２　標準化対応、データ形式・プロトコルの互換性の確保

- システム運用担当者は、５．１の観点から、医療情報システムで用いるデータの構造や項目、形式等のほか、外部との連携に際して用いるプロトコル等について、標準的な規格や機能仕様を採用する必要がある。特に施行通知では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」が求められており、標準規格を採用するなどして対応すること。

6．安全管理を実現するための技術的対策の体系

【遵守事項】

① システム運用担当者は、医療情報システムの安全管理に関する技術的な対応を検討する際に、下記の体系に従った内容を参考として検討すること。



– クライアント側
・情報の持出し・管理・破棄等に関する安全管理措置
・利用機器・サービスに対する安全管理措置

– サーバ側
・ソフトウェア・サービスに対する要求事項
・事業者による保守対応等に対する安全管理措置
・事業者選定と管理
・システム運用管理（通常時・非常時等）

– インフラ
・物理的安全管理措置（サーバルーム等、バックアップ）
・ネットワークに関する安全管理措置
・インフラ運用管理（通常時・非常時等）

– セキュリティ
・認証・認可に関する安全管理措置
・電子署名、タイムスタンプ
・証跡のレビュー、システム監査
・外部からの攻撃に対する安全管理措置

6．1 安全管理対策に関するシステムアーキテクチャ（クライアント側、サーバ側、インフラ、セキュリティ）

- 医療情報システムは、
・職員などの利用に関する情報資産
・情報システムの提供元となるサービスに関する情報資産
・インフラに関する情報資産
などから構成される。またセキュリティに関連する内容も共通して把握すべき要素となる。
- 本ガイドラインでは、これらにつきクライアント側、サーバ側、インフラ、セキュリティとして区分し、それぞれに関する技術的な遵守事項を整理した。

６．２　医療機関の規模や導入システム等の形態に応じた対応

- 医療情報システムには、さまざまな形態のものがある。
  - 医療機関等の内部で自ら開発するシステムやサービスを利用する場合（アプリケーションのマクロ機能の利用や、簡易データベースソフトを用いて構築する場合等）
  - 情報システム・サービスベンダーが提供するアプリケーションを導入して、運用は医療機関等が行う場合（医療機関等がサーバを設置し、調達したアプリケーションを導入する等）
  - 事業者が提供するアプリケーションを用いて、運用も外部に委託する場合（クラウドサービスの利用等）
- システム運用担当者が直接対応するべき内容も、このようなシステムの形態によって変化することに留意すること。
- 医療機関等では、技術的な対応を行う専任のシステム運用担当者がいない場合もある。このとき、技術的な対応に関する内容の多くは、外部に委託することになる。
- システム運用担当者が行うべき技術的な対応を、事業者に委ねる場合には、本ガイドラインの該当部分について、事業者にその実施状況の確認を行うこと。

7．情報管理（管理･持出し･破棄等）

【遵守事項】

① 医療情報及び情報機器の持出しについて、運用管理規程に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。

② 保守業務を行う事業者に対して、原則として個人情報を含むデータの持出しを禁止すること。やむを得ず持ち出しを認める場合には、企画管理者の承認を得て許諾すること。

③ 医療情報及び情報機器等の持出しに際しての盗難、置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。

④ 持ち出した利用者が情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続する場合は、マルウェア対策ソフトやパーソナルファイアウォールの導入等により、情報端末が情報漏えい、改ざん等の対象にならないような対策を実施すること。

⑤ 持ち出した情報機器等について、公衆無線 LAN の利用がなされた場合には、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。

⑥ 持ち出した情報機器には、必要最小限のアプリケーションのみをインストールし、原則として情報機器に対する変更権限がないような設定を行うこと。業務に使用しないアプリケーションや機能については削除又は停止すること。

⑦ 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する手順を作成し、これに基づき持出し等の対応を行うこと。併せて定期的に棚卸を行う手順も作成すること。

⑧ セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置の IoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や連絡方法について、患者等に情報提供すること。

⑨ 破棄に関する規程を踏まえて、把握した情報種別ごとに具体的な破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。また情報の破棄については、企画管理者に報告すること。

⑩ 情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこと。また、破棄終了後に、残存し、読み出し可能な医療情報がないことを確認すること。

⑪ 外部保存を受託する事業者に破棄を委託した場合は、確実に医療情報が破棄されたことを、証憑または事業者の説明により確認すること。

⑫ リモートログインは、保守作業等の必要な場合に限定し、適切に管理されたものに限り実施できるよう制御すること。

⑬ 利用者による外部からのアクセスを許可する場合は、盗聴、なりすまし防止及びアクセス管理を実現した VPN 技術により安全性を確保した上で、仮想デスクトップ等を利用する運用の要件を設定すること。

⑭ 患者等に医療情報を閲覧させる場合、医療情報を開示しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、例えば、システムやアプリケーションを切り分け、ファイアウォール、アクセス監視、通信の TLS 暗号化、PKI（Public Key Infrastructure：公開鍵暗号基盤）認証等の対策を実施すること。

⑮ 医療情報を格納する情報機器等の盗難や紛失（ネットワークサービスの利用等による漏えいの可能性の発生含む）が生じた場合の対応手順を作成するとともに、可能な範囲で紛失や盗難に対応した措置を事前に講じること。

７．１　外部へ持ち出す医療情報の管理対策

- システム運用担当者は、企画管理者が策定する規程を踏まえて、外部への医療情報の持出しに関する具体的な手順を作成する。手順は、持ち出す医療情報や記録媒体、持出し方法の種類や特性に応じて策定すること。持出し前の手続から、外部からの持ち帰り等に関する手順も対象となる。
- 情報機器等を持ち出す場合には、盗難や紛失のリスクを想定した内容を含めること。例えば端末の起動パスワード等の設定は必須であり、このパスワード等は認証ルールに沿った内容であることが求められる。
- 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必要があるほか、患者等の医療情報を表示や編集できる場合は、その機能を持つアプリの起動にパスワードを設定するなどの措置も必要である。
- またタブレット PC 及びスマートフォンの持出しに際して、その目的から見て不要なプログラム等はインストールしない/させないことや、情報機器等に対する管理者権限等を原則付与しないなどの措置を講じることも重要である。
- ネットワークを通じて外部に保存する場合、システム運用担当者は利用可能な保存先やサービスを限定する必要がある。クラウドサービスは、容易に医療情報の外部保存ができるため、システム運用担当者が管理しないものが使われるリスクがある。医療機関等が定める安全管理の基準や、プライバシーポリシー、その他のルールに適合したサービスを利用させること。
- 例えば、医療機関等が許可したサービス以外の接続を遮断する等の技術的対応を取ることや、許可されていないサービスの利用禁止を規則等に盛り込むなどの対応が想定される。
- 漏えい防止等の観点から、保守等の目的で、事業者が医療情報を持ち出す行為は原則として禁止する必要がある。業務上、やむを得ず持ち出す場合には、持ち出しの目的や件数、項目、持出し先での保存環境等を事前に示したうえで、システム運用担当者の許可を要すること等を手順として定めること。

７．２　医療機関等外から医療情報システムに接続する利用の場合への対策

- システム運用担当者は、外部から医療情報システムに接続して利用する場合の、技術的対応を講じることが求められる。利用場面としては、下記が想定される。
  - ・ 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を通じてアクセスする場合
  - ・ 患者等が、自宅から自らの医療情報にアクセスする場合
  - ・ 事業者が外部から医療情報システムにアクセスして保守等を行う場合

７．２．１　医療機関等の職員による外部からのアクセス

- 職員が自宅等や訪問先などから医療情報システムへアクセスする場合、安全管理のため、
  - ・ 接続できる職員に対する事前の許可
  - ・ 外部から接続する際の技術的対応

  等の対応が考えられる。
- 事前の許可については、システム運用担当者が具体的手順等を定めて、接続可能な利用者と権限の範囲を設定すること。また、その結果を企画管理者に報告すること。
- 技術的な対応については、下記を含む措置を、システム運用担当者が講じる必要がある。
  - ・ 外部からのアクセスに関する認証・認可
  - ・ 外部から利用する際のネットワークの要件
  - ・ 外部から利用する端末等の要件

- 外部からの認証・認可については、外部の環境から医療機関等が管理するネットワークに接続するための認証等の措置を講じることが求められる。認証等の要件は、「１４．１利用者認証」に示す。
- 外部からネットワークを利用する場合、医療機関等が接続先を管理するネットワークに接続する前に、オープンなネットワーク（13.1 参照）を経由することが想定される。この場合、「１３．１　ネットワークに対する安全管理」に示す対策を講じて、十分なチャネル・セキュリティを確保すること。
- 外部から利用する端末等の要件については、医療機関等により支給された端末を使うことが想定される。一方で、医療機関等によっては、「９．ソフトウェア・サービスに対する要求事項」に示す措置を講じて、個人の所有する端末（ノートパソコン、スマートフォン、タブレット等）を業務利用すること（Bring Your Own Device：以下「BYOD」という。）も想定される。端末等の要件に関しては、考慮すべき点が 3 つある。
  - PC 等の安全管理対策を確認するためには一定の知識と技能が必要で、一般職員にその知識と技能を要求することは難しい。
  - 運用管理規程等で定めた内容の実施状況を確認するためには、運用の点検と監査が必要であるが、外部からのアクセスの状況を点検、監査することは負担が大きい。
  - 医療機関等の管理が及ばない私物の PC や、不特定多数の人間が使用する PC の場合、医療機関等の想定と異なる環境で使用され、安全管理上の支障が生じる可能性がある。したがって、職員による外部からのアクセスを行う場合は、盗聴、なりすまし防止及びアクセス管理を実現した VPN 技術等により安全性を確保した上で、仮想デスクトップを利用する等の運用要件を設定すること。ここでいう仮想デスクトップ等とは、利用する端末の作業環境内に、ユーザ認証を経た後で、医療機関等に設置した機器の画面を表示する仕組みである。その他、ユーザ権限を厳格に管理した専用端末の貸与等も考えられる。

７．２．２　患者等に診療情報等を提供する場合の外部からのアクセス

- 診療情報等の開示が進み、ネットワークを介して患者等に診療情報を提供したり、患者等が医療機関等内の診療情報を第三者に参照閲覧させることなどが想定される。
- 患者等に診療情報等を提供する場合には、ネットワークのセキュリティ対策、医療機関等内部のセキュリティ対策などに関する措置を講じるとともに、手順等を作成する必要がある。
- ネットワーク対策に関しては、基本的には「７．２．１　医療機関等の職員による外部からのアクセス」に示すものと同様の対策を講じること。なお、患者への情報提供は、一般的には参照のみとなること、患者等においては職員以上に単純な仕組みが求められることなどを考慮して、対応策を検討すること。

７．２．３　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

- こちらについては、「１０．システム・サービス事業者による保守対応等に対する安全管理措置」に示す。

７．３　医療情報の破棄

- システム運用担当者は、企画管理者が作成した手順を踏まえて、医療情報の種別ごとに破棄の具体的なルールを作成することが求められる。
- 破棄の対象となるのは、
  - 情報機器等に格納した医療情報（過去に格納して削除したものを含む）
  - クラウドサービス、外部委託先のシステム等に保存された医療情報

  等が想定される。

- 医療情報を格納した情報機器等に対しては、格納されている医療情報を確実に破棄するため、OS のファイル管理システムによる削除のみでは不十分であり、専用のソフトウェア等により復元不能な形で確実に情報を削除するなどの対応が求められる。なお、記録媒体などを物理的に破壊することも選択肢となる。リース等により情報機器等を返却する場合も、同様の措置が求められる。情報機器等の廃棄を外部の事業者に委託した場合には、委託先の事業者から廃棄の証跡の提供などを求めて、確認すること。
- 例えば、下記のような対応が考えられる。
  - 情報機器等の廃棄時に、医療機関担当者による立ち会いや、HDD（Hard Disk Drive）などの記録媒体を含む全ての機器等が廃棄された写真やソフトウェア消去に係るログの提出を求めること
  - 医療機関等が指定した第三者の廃棄事業者により、情報機器等の廃棄を実施すること
    その際、廃棄事業者から、廃棄対象、方法、実施日、実施者および結果を含む廃棄証明書その他の証跡を入手し、内容を確認すること
  - 委託契約時においても、契約条項として HDD などの記録媒体を含めた情報機器等の廃棄について明確に合意すること
- 医療情報システムのデータベース等に格納したデータは、システム管理機能により破棄することになる。なお、データベースのように情報が互いに関連して存在する場合は、一部の情報を不適切に破棄することで、その他の情報が利用不能となるリスクがあることに留意すること。
- 事業者が保有するシステムに医療情報を格納している場合、破棄の証明等が難しい場合も想定される。このような場合、システム運用担当者は、企画管理者と連携して、事業者のデータ破棄手順などの確認をすることで破棄の状況を把握すること。

７．４　医療情報を格納する記録媒体、情報機器等の紛失、盗難等が生じた場合の対応

- システム運用担当者は、医療情報を格納する情報機器等の紛失、盗難が生じた場合の対応手順等を作成する必要がある。紛失や盗難に関する報告を受けた場合には、対象となる情報機器等の特定、ネットワークへの接続防止等の対応が想定される。また、記録媒体の暗号化を図るほか、例えばモバイル端末については、MDM（Mobile Device Management）を導入して遠隔制御を行うなど、可能な対策を事前に講じることも必要である。
- ネットワークを通じて外部サービスを利用する際には、設定のミスなどによる漏えいのリスクについても、同様に対応の手順を作成することが求められる。

８．利用機器・サービスに対する安全管理措置

【遵守事項】

① システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウイルス等のマルウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。

② 常時マルウェアの混入を防ぐ適切な措置を実施し、その対策の有効性・安全性の確認・維持を行うこと。

③ 医療情報システムに接続するネットワークのトラフィックにおける脅威の拡散等を防止するために、マルウェア対策ソフトのパターンファイルや OS のセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用すること。

④ メールやファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるファイル等の送受信の禁止、実行の停止又は無害化処理等を行うこと。なお、保守等でやむを得ずファイル送信等を行う場合、送信側で無害化処理が行われていることを確認すること。

⑤ 情報機器に対するパスワードの設定に関しては、製品等の出荷時におけるパスワードから変更し、「１４．認証・認可に関する安全管理措置」に示すパスワードの要件を満たすこと。

⑥ IoT 機器を利用する場合、次に掲げる対策を実施すること。医療機器、及びそれらに付属するシステム・機器についても同様である。

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

(2) IoT 機器のファームウェア等の脆弱性リスクに対応するため、システムやサービスの特徴を踏まえてセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用すること。

(3) 不正な接続を防ぐため、使用を終了、又は停止した IoT 機器をネットワークに接続したまま放置しないこと。

⑦ 企画管理者と協働して、医療情報システムで用いる情報機器等やソフトウェアの棚卸を行うための手順を策定し、定期的に実施すること。棚卸の際には、情報機器等の滅失状況なども併せて確認すること。

⑧ BYOD の運用に関する規程に基づいて、具体的な手順と設定を行い、企画管理者に報告すること。

⑨ BYOD 端末であっても、医療機関等が管理する情報機器等と同等の対策が講じられるよう、手順を作成すること。

８．１　マルウェア対策

- コンピュータウイルス、ワーム等様々な形態・呼称を持つマルウェアは、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に侵入する可能性がある。マルウェアが侵入すると、セキュリティ機構の破壊、システムダウン、情報の漏えいや改ざん、破壊、資源の不正使用等、重大な問題が引き起こされる。
- 対策としてはマルウェア対策ソフトウェアの導入が効果的である。このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、マルウェアの検出と除去が期待できる。
- システム運用担当者は、企画管理者と協働して、このようなマルウェア対策についての措置を講じるほか、これに必要な規則等の策定を行うこと。
- マルウェアは常に変化しているため、検出するためのパターンファイル等を、可能な限り、常に最新のものに更新しておくこと。システム運用担当者は、パターンファイルの更新による医療情報システムへの影響を調査しておくことも必要である。
- また、マルウェア対策ソフトを導入したとしても、全てのマルウェアが検出できるわけではない。医療情報システム側の脆弱性を可能な限り小さくしておくことや被害拡大の防止策を講じておくことが重要である。対策としてはセキュリテ

ィ・ホール（脆弱性）が報告されているソフトウェアへのパッチ適用、利用していないサービスや通信ポートの閉鎖、ネットワークの構成分割やネットワーク間のアクセス制御、マクロ等の利用停止、メールやファイルの無害化がある。また、EDR（Endpoint Detection and Response）等による「振る舞い検知」も有効な方策である。いずれの対策を行う場合も、業務への影響や、処理の速度、可用性について、事前に十分検討すること。

- 医療機関等の外部で利用する端末や PC 等についても同様のリスクがあり、これらの情報機器等についても、上記の対応を行うこと。

8．2 情報機器等の脆弱性への対策

- システム運用担当者は、医療情報システムが利用する情報機器等の脆弱性に関する情報を常に収集し、脆弱性への対応を速やかに行う必要がある。
- 情報機器等には、利用者が直接利用する PC 等の端末のほか、医療情報システムで利用する機能等のサービスを提供するサーバや、ネットワークに関連する機器等、様々なものがある。
- 近年のサイバー攻撃では、情報機器等に内蔵されるファームウェアや、格納されるプログラム等の脆弱性、EOS（End of Support：サポート終了）の対象となった情報機器等が起点となり、攻撃を受ける事案が多くみられている。必要な脆弱性対策が見逃されたことに起因するランサムウェア攻撃も見られる。
- システム運用担当者は、情報機器等に関して、定期的に脆弱性スキャンを行うほか、脆弱性に関する最新の情報を収集することが求められる。PC の OS に関する脆弱性情報は、OS やマルウェア対策ソフトを提供する事業者などが提供している。また、重大な脆弱性情報は「国家サイバー統括室（NCO）」や「独立行政法人情報処理推進機構（IPA）」などが定期的に公表している。これらの情報を確認するほか、契約事業者に対応を確認するなどして、最新の情報を入手すること。
- 利用するソフトウェアについて、SBOM[1]（Software Bill of Materials：ソフトウェア部品表）が事業者から提供されることもある。システム運用担当者は SBOM を用いることで、脆弱性を適切に管理し、安全性及び可用性を脅かすリスクを低減できる。そのため、システム運用担当者は、医療情報システムの導入時、及び保守時などにおいて適宜、SBOM の提供、またはこれに基づく安全性の確認を医療情報システム等提供事業者に求めること[2]。
- 必要に応じて速やかに脆弱性対策を講じる必要があるが、他のソフトウェアの動作等に影響することも想定される。事前に事業者に脆弱性対策の実施の可否を確認し、対応が難しい場合には、当該リスクに対する対策や管理方法を協議の上、代替策を講じること。
- 検査装置等に付属するシステム・機器についても同様である。また医療機器が EOS を迎えた場合の対応等については、「医療機関における医療機器のサイバーセキュリティ確保のための手引書」を踏まえ、医療機器安全管理責任者等の医療機器を管理する部署の担当者と医療情報システム安全管理責任者等のシステム担当者が十分に連携を取りながら管理すること。

---

[1] ソフトウェアの構成部品や依存関係等を網羅したリストであり、脆弱性管理などの安全対策における基礎情報となるもの

[2] SBOM の取扱いについては、「医療機器のサイバーセキュリティ導入に関する手引書」の「附属書 A. ソフトウェア部品表（SBOM）の扱い」が参考になる。

- 本ガイドラインは、医療情報の適切な保全を目的として IoT 機器の適切な取扱いに関する要件を定めており、「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」（昭和 35 年 8 月 10 日法律第 145 号）の定める医療機器のサイバーセキュリティの対策については、「医療機器におけるサイバーセキュリティの確保について」[3]、「医療機器のサイバーセキュリティ導入に関する手引書」[4]、「医療機関における医療機器のサイバーセキュリティ確保のための手引書」[5]等を踏まえて、医療機器の製造販売業者と必要な連携を図ること。

8．3　端末やサーバの安全な利用の管理

- システム運用担当者は、端末やサーバ等の情報機器が安全に利用されていることを確認する必要がある。
- 安全な利用については、8．1、8．2に示す対策のほか、例えば情報機器の起動にパスワード等の設定を行うなど、必要な措置を講じることが求められる。また製品出荷時にパスワード等が設定されているものは、必ず製品出荷時から変更すること。サーバで利用するソフトウェアの管理者権限を有するアカウントのパスワードにおいても同様である。
- 外部からの攻撃等のリスクを下げる方法の一つとして、不要な情報機器等を使用しない、不要な医療情報システムを稼働させない、などの対応も必要である。利用されていないにもかかわらず、外部と接続可能な情報機器がある場合、攻撃対象となり得る。また業務によっては、明らかに利用する可能性がない（または低い）時間帯にはシステムの稼働を停止することにより、業務時間外の攻撃リスクを低減できる。システム運用担当者は、業務での必要性や利便性などを勘案して、システムの稼働時間等を整理の上、適切な設定を行うこと。

8．4　情報機器等の棚卸

- システム運用担当者は、企画管理者が行う台帳管理を踏まえて、企画管理者と協働して情報機器等の棚卸をすることが求められる。棚卸を行うことで、情報機器の所在が明確になり、紛失、漏えい等のリスクを効率的に発見することが期待される。また情報機器等の滅失状況なども併せて確認することにより、利用の可否も確認でき、バージョンアップや買換え等、必要な対応が可能となる。

8．5　医療機関等が管理する以外の情報機器の利用に対する対策

- システム運用担当者は、医療機関等が管理する以外の情報機器を、医療情報システムにおいて利用するために必要な措置を講じ、そのための手順等を策定したうえで、企画管理者に報告することが求められる。
- BYOD を許可する場合は、上記の要件を実現するため、下記に掲げるような対策を選択・採用し、十分な安全性を確保する必要がある。

  ・管理者以外による端末の OS 設定の変更を技術的あるいは運用管理上で制御する

  ・他のアプリケーション等からの影響を遮断しつつ、端末内で医療情報を取り扱うことを制限する。さらに個人でその設定を変更できないよう制御し、OS レベルで管理領域を分離する。

  ・運用管理規程によって利用者による OS の設定変更を禁止し、かつ安全性の確認できないアプリケーションがモ

[3] 平成 27 年 4 月 28 日薬食機参発 0428 第 1 号、薬食安発 0428 第 1 号「医療機器におけるサイバーセキュリティの確保について」

[4] 令和 5 年 3 月 31 日薬生機審発 0331、第 11 号薬生安発 0331 第 4 号「医療機器のサイバーセキュリティ導入に関する手引書の改訂について」

[5] 令和 5 年 3 月 31 日医政参発 0331 第 1 号、薬生機審発 0331 第 16 号、薬生安発 0331 第 8 号「医療機関における医療機器のサイバーセキュリティ確保のための手引書について」

バイル端末にインストールされていないことを管理者が定期的に確認する。

- マルウェアや不適切な設定がなされたソフトウェアにより、外部からの不正アクセスが発生することも想定されるため、管理されていない端末での BYOD は許可してはならない。また、BYOD の導入に際して、管理者はコスト・利便性とリスクを評価して検討すること。

9．ソフトウェア・サービスに対する要求事項

【遵守事項】

① システムがどのような情報機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにするとともに、システムの機能仕様を明確に定義すること。

② 情報機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを規定すること。

③ 医療情報システムで利用するシステム、サービス、情報機器等の品質を定期的に管理するための手順を作成すること。また、これに従い必要な措置を講じ、企画管理者に報告すること。

④ 医療情報システムの目的に応じて情報を速やかに検索表示、又は書面に表示できるよう措置を講じること。

9．1 ソフトウェアの構成管理

- システム運用担当者は、医療情報システムで利用するソフトウェアが、適切な構成となっていることを確認する必要がある。特に医療情報システムをオンプレミスで構築している場合には、医療情報システムを構成するソフトウェアのバージョンや組み合わせ等を適切に管理することが求められる。ソフトウェアの構成が適切に管理されない場合、医療情報システムの動作に支障をきたす、セキュリティ上の脆弱性が残存するなどのリスクが生じる。
- システム運用担当者は、このような構成管理について、手順（あるいはこれに相当するバッチ処理のための仕組み等）が整備されているか、本来構成すべきソフトウェアのバージョンが適切に管理されているか等を、事業者に確認すること。構成管理に関する計画の策定、実施がなされていることを確認することが重要である。
- クラウドサービスの場合は特に、このような構成管理を直接、医療機関等が行うことは困難であり、同様に手順や計画の整備状況、実施状況の確認を行うこと。

9．2 情報機器・ソフトウェアの導入や変更時における品質管理

- 医療情報システムの導入や変更時は、想定した品質で稼働することの確認が必要である。施行通知では、「目的に応じて速やかに検索表示又は書面に表示できる」ことを求めている。安定的な医療の提供のため、このようなソフトウェアの品質を適切に管理すること。
- システム運用担当者は、医療情報システムの導入や変更時に直接品質を確認するほか、要求仕様書等において特に重視する品質について明示することで、事業者に品質確保を求めることが想定される。
- システムの移行時についても同様である。移行時の特殊性として、移行前のデータが正しく移行後のシステムに反映され、利用可能であることが求められる。利用者権限をはじめ、各種設定が移行前の設定が、適切に移行後にも設定されていること等を確認すること。
- 求められる品質は、医療情報システムの特性や目的に応じて異なる。e-文書法によれば、画面上での見読性が求められているが、業務の要求によっては対象の情報の内容を直ちに書面等に表示できることも必要となる。

１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置

【遵守事項】

① 動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、保守終了後に確実にデータを消去することを求め、その結果の報告を求めること。

② 診療録等の外部保存を受託する事業者に対しては、個人情報の保護を厳格に監督する必要がある。受託する事業者であっても、保存を受託した個人情報に、正当な理由なくアクセスできない仕組みを設けること。（ただし、事業者が個人情報を保存するのみで、取り扱わない契約となっている場合、医療機関等には個人情報保護法第 27 条第 5 項第 1 号に基づく監督義務は生じない。この時、適切に事業者に対してアクセス制御がされている必要がある。）

③ 保守作業のためにサーバに事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びにアクセスした対象個人情報及び作業内容を記録すること。なお、これは利用者を模して操作確認を行う際の識別・認証についても同様である。

④ リモートメンテナンスを行う場合には、外部からの攻撃等のリスクを低減するために、外部接続等への対策等、必要な措置を講じること。

⑤ リモートメンテナンス（保守）によるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集すること。作業終了時には、保守に関する作業計画書と照合することなどにより確認を実施し、終了後速やかに企画管理者に報告し、確認を求めること。

⑥ リモートメンテナンスにおいて、事業者がやむを得ずファイルを医療機関等へ送信する場合、送信側で無害化処理が行われていることを確認すること。

⑦ 事業者がやむを得ず診療録等を参照する必要がある場合も、医療機関等に許可を受けたうえでアクセスし、医療機関等で求められる水準と同等の秘密保持を行うこと。

１０．１　保守時の安全管理対策

- 医療情報システムの適切な稼働を維持するためには、定期的な保守（メンテナンス）が必要である。保守作業には主に障害対応や予防保守、ソフトウェア改訂等があり、障害対応時は、原因特定や解析等のために障害発生時のデータを利用する。この際、保守要員が管理者権限で直接医療情報に触れる可能性があるため、想定される脅威に対する対策が必要になる。具体的には、下記が想定される。
  - 保守要員等からの医療情報の流出・漏えい
  - 保守に伴う医療情報の破壊・破棄
  - 保守に伴う医療情報システムの破壊、障害の発生
  - 保守作業または保守環境に対するサイバー攻撃
- システム運用担当者は、このようなリスクに対応するために必要な措置を講じるほか、手順等を作成し、企画管理者に報告すること。
- システム運用担当者は、保守に当たって以下の内容について、確認することが求められる。
  - 保守計画等の策定・確認
  - 作業の監督・報告・確認
  - アクセス権限管理（不要な管理者権限を付与しない）
  - ログ取得
  - 動作確認時のテストデータに個人情報が含まれる際の対策

・　リモートメンテナンス（保守）時の対策

- 保守には、原則として事前申請・承認が必要だが、障害時や緊急を要する脆弱性対応などにおいては、事後承認によることも想定される。
- オンプレミスの場合には、保守に関しては個別の申請や承認により行うことが可能であるが、パブリッククラウドによるサービスにおいては、個々の利用者に対する保守の申請や承認によることが難しい場合がある。システム運用担当者は、クラウドサービスにおける保守の場合には、保守の対象時間について事業者に確認したうえで、医療機関等内部で利用している情報システムへの影響範囲、必要があれば代替措置等について確認し、企画管理者に報告の上、医療機関等内部及び関係者に周知することが求められる。
- また保守を行う際には、サーバ上の OS や DBMS などで製品出荷時に設定されている管理者 ID（例えば Administrator）などは使わず、各保守担当者の ID を設けて、管理者権限を付与する等、保守した者が特定できるようにすることも求められる。

１０．２ リモートメンテナンスにおける安全管理対策

- リモートメンテナンスの採用は、業務効率化が期待されるものの、攻撃者にとって「正規のルートを装って侵入できる絶好の裏口」となり、サイバー攻撃の起点となり得る。
- リモートメンテナンスにおけるリスクとしては、認証・アクセス管理に関するリスク、通信経路・接続方式に起因するリスク、システム・ツール関連のリスク、人的・運用関連のリスク等が指摘される。これらのリスクは、医療情報システム全体に共通するものであるため、本ガイドラインで示す対策を適切に講じること。
- また、リモートメンテナンスでは、システムの管理者権限を要する場合があり、高いリスクを伴うことから、下記の対策を行うこと。

表１０―１　リモートメンテナンスにおいて実施すべき事項

想定されるリスク	実施すべき事項（各リスクに示される実施すべき事項は、選択して対応すること）
認証・アクセス管理に関するリスク	・OS の二要素認証の採用（「１４．１．１　利用者の識別・認証」参照） ・特権 ID 権限の厳格管理（管理者共通アカウントの禁止等） ・アクセス経路の制限（端末・IP アドレスを限定等） ・セッション・タイム・アウト機能の導入
通信経路・接続方式に起因するリスク	・暗号化（SSH、VPN 等、「１３．ネットワークに関する安全管理措置」に記載されている安全なプロトコルの採用、RDP・VNC などを直接インターネットに開放しない利用等） ・リモートアクセス用ゲートウェイの利用
システム・ツール関連のリスク	・管理端末のセキュリティ強化（マルウェア対策、USB 端末規制等）
人的・運用関連のリスク	・ログの定期的レビュー ・管理監督強化 ・外部委託管理強化 （外部委託者用アカウントの管理、契約上の責任管理等）

１１．システム運用管理（通常時･非常時等）

【遵守事項】

① 非常時の医療情報システムの運用について、次に掲げる対策を実施すること。

(1) 「非常時のユーザアカウントや非常時用機能」の手順を整備すること。

(2) 非常時機能が通常時に不適切に利用されることのないように管理するとともに、もし使用された場合には検知できるよう、適切に管理及び監査すること。

(3) 非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更すること。

(4) 医療情報システムにマルウェアが混入した場合に備えて、関係先への連絡手段や紙での運用等の代替手段を準備すること。

(5) サイバー攻撃による被害拡大の防止の観点から、論理的／物理的に構成分離されたネットワークを整備すること。

(6) 重要なファイルは数世代バックアップを複数の方式で確保し、その一部はマルウェアの混入による影響が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。

② 医療情報システムの稼働状況などを把握するため、パフォーマンス管理、死活監視などを行うこと。

１１．１　通常時における運用対策

- システム運用担当者は、通常時から非常時を想定した技術的対応を、講じることが求められる。
- 非常時の原因としては、下記が想定される。
  - 災害
  - サイバー攻撃
  - システム障害（ネットワーク障害含む）
- 上記対策として共通することは、非常時の医療情報システムの利用に関する手順等について、通常時から整理をすることや、非常時を想定した訓練を行うことなどが挙げられる。
- 通常時における対策例については、企画管理編「11．２　非常時に備えた通常時からの対応」の「非常時の事象発生原因に応じた通常時からの対策例」に示しているが、技術的な対応としては、
  - ネットワーク（論理的／物理的な構成分割など）
  - バックアップ（冗長化、データバックアップなど）
  - 非常時用の情報システム、情報機器

  等を検討することが求められる。技術的な検討は、経営層が行うリスク判断や企画管理者によるリスク評価に整合する内容とすること。特にサイバー攻撃の場合、バックアップデータには既にマルウェアの混入による影響が及んでいる可能性も高く、不用意にバックアップデータから復旧することで被害を拡大する等のリスクもある。総合的な観点からのリスク評価を踏まえて技術的な検討を行い、結果を企画管理者に報告すること。

表１１－１　通常時に対応すべき技術的対応例

対応目的	バックアップ	非常時用の臨時システム
災害	・広域災害対策（遠隔地バックアップ等）　など	・代替するバックアップサイトの構築 ・臨時の認証方法の採用　など
サイバー攻撃	・論理的／物理的なネットワークの構成分割	・サイバー攻撃時においても利用可能な情報システム資源の確保　など

	・追記不能型のデータバックアップの記録媒体の整備（一定期間追記不能型の WORM[6]ストレージを含む） ・システム再構築のための情報機器等のインフラバックアップ など	
システム障害 （ネットワーク障害も含む）	・即時切換え可能なシステムバックアップ など	・冗長化と切換え対応 など

- 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、医療情報システムの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。医療情報システムの運用に専任の担当者を設けることができない場合には、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。
- また非常時に備えた対策として、OS のセキュリティ・パッチ適用後やマルウェア対策ソフトのパターンファイル最新化後の稼働確認、あるいはバックアップファイルの復旧テストなどを実施することが求められる。この際に、これらの作業は、実際の運用環境とは分離して行うこと。テスト環境などを用意して上記の作業を行い、実際に稼働している運用環境に影響が生じないようにすることが必要である[7]。

１１．２ 非常時における対応

- システム運用担当者は、非常時において、あらかじめ作成した手順に従い必要な措置を行うことが求められる。併せて通常時の運用への復旧手順も整備すること。
- 非常時における対応の一つとして、非常時用ユーザアカウントの運用が挙げられる。災害等により通常時のユーザ認証が困難な場合や正規のアクセス権限者による操作が望めない場合、非常時用アカウントの運用により、医療情報の利用を円滑化し、医療サービス低下を最小限とすることが想定される。通常時への復旧・復帰後には非常時ユーザアカウントを更新するなどの措置を行うこと。
- 非常時は、通常時とは異なる運用が想定される。例えば、災害時は、受付での患者登録を経ないような運用が考えられ、必要に応じて運用に対応した機能を実装する必要がある。一方で非常時への対応機能の用意は、逆にリスクを増加させる懸念もあるため、慎重に管理すること。
- 非常時の運用に関する事前の準備や周知不足は医療情報システムや医療機器の円滑な利用を阻害するリスクがある。システム運用担当者を含む関係者間で十分な準備を実施し、情報を共有しておくこと。

[6] WORM：WORM=Write Once Read Many。データを一度書き込んだ後は、内容の変更や削除をできないようにする仕組みで、保存後のデータ不変性を仕組みとして担保し、改ざんや意図しない消失を防ぐことを目的とする。

[7] 予算や運用上の制約でテスト環境の用意が難しい場合は、運用環境全体への影響を最小限とするため、まず影響の少ないセグメントから段階的にパッチを適用し、稼働状況に問題がないことを確認しながら、順次適用範囲を拡大していく対応等が考えられる。

１２．物理的安全管理措置

【遵守事項】

① 医療情報及び医療情報システムを保管する場所を選定する際には、リスク評価を踏まえ、企画管理者と協働して検討、決定すること。検討に際しては、医療情報を格納する情報機器や記録媒体を物理的に保管するための施設が、災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置することなどを考慮すること。

② 医療情報を保護する施設について、医療情報を格納する情報機器や記録媒体の設置場所等のセキュリティ境界への入退管理が、個人認証システム等による制御に基づいて行われていることを確認すること。また建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等が設置されていることを確認すること。

③ サーバルーム等の十分なセキュリティ確保が求められる領域においては、持ち込まれる物品の確認・制限を実施すること。 個人情報の保管等、重要な用途に利用される情報機器には盗難防止策を講じること。

④ 医療情報及び医療情報システムのバックアップは、企画管理者が定める運用管理規程等に基づく措置を実施し、非常時に利用できるよう、適切に管理すること。

⑤ 記録媒体、ネットワーク回線、設備の劣化による情報の読み取りが不能となる等のリスクを防止するため、記録媒体が劣化する前に、新たな記録媒体への複写を実施する等、適切な保管措置を講じること。

⑥ 利用者が医療情報を入力・参照する端末から長時間離席する際など、正当な利用者以外の者による入力・参照が生じないよう対策を実施すること。

１２．１ サーバルーム等の物理的要件

- システム運用担当者は、医療情報及び医療情報システムを保管する場所（サーバルーム、マシンルーム等）を、リスク分析の結果を踏まえて、企画管理者と協議の上、選定することが求められる。災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能・構造であるよう考慮するほか、結露や高温による情報機器の暴走するリスク等にも留意すること。
- サーバルーム等の医療情報システムが格納されているセキュリティ区域は、職員を含め、入退管理がなされており、カメラによる監視などがなされていることも必要である。
- 医療情報の記録媒体や医療情報システムが格納されるキャビネットやシステムラックなどは、施錠管理すること。
- サーバルーム等のセキュリティ境界へ持ち込む物品を確認・制限すること。例えば可搬型記録媒体の持ち込みは、大量のデータ漏えいにつながるリスクがある。

１２．２ バックアップの管理

- システム運用担当者は、企画管理者が運用管理規程等に定めたルールに基づいて、適切にバックアップを確保し、非常時に利用可能な状態で管理することが求められる。運用管理規程では、バックアップ頻度、方法等を明らかにし、原因に応じて、「１１．１ 通常時における運用対策」に示すバックアップ対応を行うこと。またサイバー攻撃を想定したバックアップの確保については、「１８．外部からの攻撃に対する安全管理措置」を参照すること。
- バックアップの外部保存を委託している場合は、委託先事業者に対して、バックアップの対象、頻度、復旧できる世代、バックアップ方法、保存場所等を確認し、SLA 等において明らかにすること。
- バックアップを含む記録媒体について、媒体そのものや設備等の劣化によって情報の読み取りが不能となることを防止するための措置を講じること。保管環境に留意するほか（高温多湿を避ける、直射日光等を避ける等）、記録媒体が劣化する前に、保管されている情報を新たな記録媒体に複写する等の措置を講じること。また記録媒

体及び情報機器ごとに劣化が起こらずに正常に保管が可能な期間を明確にするとともに、使用開始日、使用終了予定日を管理して、定期的に可読性に関するチェックを行うこと。また、この手順を作成すること。

- 診療録等の法的な保存期間が終了した場合や、外部保存を受託する事業者との契約期間が終了した場合でも、個人情報の保護には十分に配慮する必要がある。また、バックアップにおける個人情報の取扱いについても、オリジナルデータと同様の水準が求められる。
- 具体的には、システム運用担当者は以下についての対応が求められる。
  （1） 診療録等の記録された可搬媒体が搬送される際の個人情報保護
  （2） 診療録等の外部保存を受託する事業者内における個人情報保護

１２．３ その他

１２．３．１ 記録媒体等の経年変化の管理・委託事業者への配送等

- ネットワークに接続されない可搬媒体を用いて外部保存を行う場合、ネットワーク上の脅威に基づくなりすましや盗聴による情報の大量漏えい等のリスクは低減される。
- 可搬媒体を目視しても内容が見えるわけではないので、搬送時の機密性は比較的確保しやすい。暗号化機能を有する媒体では、パスワードによるアクセス制限により、さらに機密性は増す。一方で、可搬媒体には耐久性の低い製品も存在し、経年変化等に対して慎重に対応する必要がある。また、一記録媒体あたりに保存される情報量が極めて多いことから、紛失リスクに対してより慎重な対応が必要である。
- 診療録等を可搬媒体に記録して搬送する場合は、混同や紛失を防止するため、以下の点に注意すること。
  － 診療録等を記録した可搬媒体の紛失防止
  運搬用車両や搬送用ケースの施錠等の処置を施すこと
  － 診療録等を記録した可搬媒体と他の搬送物との混同の防止
  他の搬送物との混同が予測される場合には、別のケースや系統に分け、同時に搬送しないこと
  － 搬送業者との守秘義務に関する契約
- 外部保存を委託する医療機関等は、受託事業者に個人情報を取り扱わせる場合、個人情報保護法を遵守させる管理義務を負う。したがって両者の間での責任分担を明確化し、守秘義務に関する事項等を契約上明記すること。
- なお、受託事業者に個人情報を取り扱わせない契約としている場合には、医療機関等は、自医療機関等の安全管理措置の一環として、個人情報保護法を遵守しつつ、安全管理に関する措置をとることが求められる（個人情報保護法に関するガイドライン Ｑ７－５４参照）。

１２．３．２ 端末・サーバ装置等の不適切な利用等に関する対策

- システム運用担当者は、利用者が医療情報を入力・参照する端末から長時間離席する際に、正当な利用者以外の者による入力・参照を防止するため、自動での画面ロックアウト等の対策を実施すること。

１３．ネットワークに関する安全管理措置

【遵守事項】

① ネットワーク利用に関連する具体的な責任分界、責任の所在の範囲を明らかにし、企画管理者に対して報告すること。

② セッション乗っ取り、IP アドレス詐称等のなりすましを防止するため、原則として医療機関等が経路等を管理する、セキュアなネットワークを利用すること。

③ オープンなネットワークからオープンではないネットワークへの接続までの間にチャネル・セキュリティの確保を期待してネットワークを構成する場合には、選択するサービスのチャネル・セキュリティの確保の範囲を電気通信事業者に確認すること。

④ オープンではないネットワークを利用する場合には、必要に応じてデータ送信元と送信先での、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じて、必要な単位で、互いに確認し、通信方式や、認証手段を採用すること。採用する認証手段は、PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、容易に解読されない方法が望ましい。また、暗号を用いる場合は、電子政府推奨暗号の暗号方式を採用すること。

⑤ 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し、不正な機器の接続や不正なソフトウェア等の混入が生じないよう、セキュリティ対策を実施すること。特に VPN 接続による場合は、施設内のルータを経由して異なる施設間を結ぶ通信経路の間で送受信ができないように経路を設定すること。また、機器の管理インターフェイスやログインページ、管理ポートに対して接続を許可されていない機器が、外部からアクセスできないよう設定すること。

⑥ オープンなネットワークにおいて、IPsec による VPN 等を利用せずプロトコルを限定した TLS 接続をする場合（HTTPS、FTPS 等）、TLS のプロトコルバージョンを TLS1.3 以上に限定した上で、クライアント証明書を利用した TLS クライアント認証（mutual-TLS）、または、これと同等以上の安全性を有する、端末の識別・認証による接続端末制限の措置をすること。ただしシステム・サービス等の対応が困難な場合には TLS1.2 の設定によることも可能とする。TLS の設定はサーバ/クライアントともに「TLS 暗号設定ガイドライン[8]」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。

⑦ 医療機関等が管理する医療情報システムと接続する際に用いる通信経路の暗号化を図る場合には、原則として専用線、IP-VPN、又は IPsec＋IKEv2(PSK 認証を除く)によること。SSL-VPN は、偽サーバへの対策リスクや長時間の接続におけるリスク等が含まれるため、使用する場合には⑥に示す対策を行ったうえで、「クライアント型」を選択すること。クライアント型では専用のクライアントソフトがインストールされた端末との間でのみアクセスが可能となる。

また、ソフトウェア型の IPsec 又は TLS1.2 以上により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃への適切な対策を実施すること。

⑧ 利用するネットワークの安全性を勘案して、送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。

⑨ 医療機関等で用いる通信において、ネットワーク上で「改ざん」されていないことを保証すること。なお、可逆的な情報の圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにはあたらない。

⑩ ネットワーク経路でのメッセージ挿入、マルウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。

⑪ 医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざ

[8] IPA より公表。なお、随時改定されるため、最新のものを参照すること。

ん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。

⑫ 医療機関等がネットワークを通じて通信を行う際には、正当な通信の相手であることを確認するための相互認証を行うこと。また診療録等のオンライン外部保存を受託する事業者と委託する医療機関等との間でも同様に相互認証機能を設けること。

⑬ 医療情報システムにおいて無線 LAN を利用する場合、次に掲げる対策を実施すること。

(1) 適切な利用者のみに無線 LAN の利用を制限すること。例えば、ANY 接続拒否等の対策を実施することが考えられる。

(2) 不正アクセス対策を実施すること。例えば電子証明書、IP アドレス、MAC アドレス等によるアクセス制限を実施すること。ただし、例えば MAC アドレスによるアクセス制限の場合、モバイル端末においてプライバシー保護の観点から MAC アドレスランダム化が標準搭載されていることや、詐称可能であることから、MAC アドレスによるアクセス制限の効果が限定的であることに留意する必要がある。

(3) 不正な情報の取得を防止するため、WPA2-EAP、WPA3 等により通信を暗号化すること。

(4) 利用する無線 LAN の電波特性を勘案して、通信を阻害しないものを利用すること。

１３．１ ネットワークに対する安全管理

- システム運用担当者は、リスク評価を踏まえ、企画管理者と協働して利用するネットワークを選定すること。
- 本ガイドラインでは、下図のようにネットワークに関する用語の整理を行った。ネットワークの安全性を検討する際には、ネットワークにおける各レイヤで、対策が講じられると想定される。

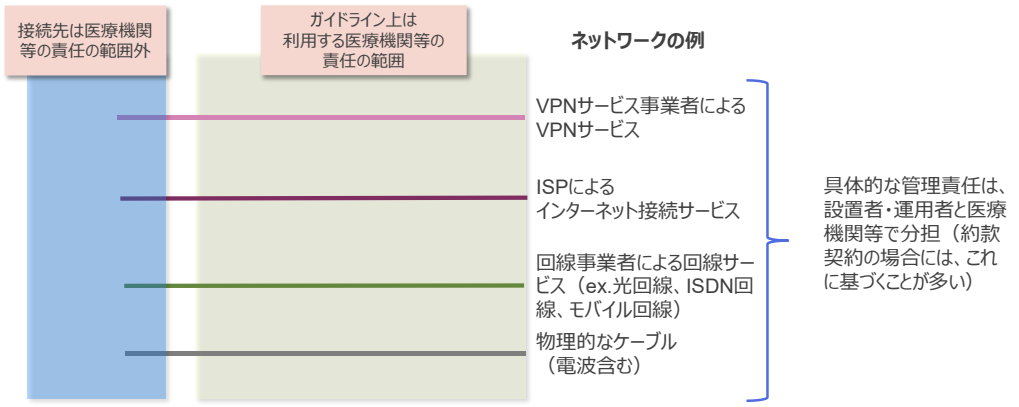


図１３－１ ネットワークの管理に対する考え方

- 本ガイドラインでは回線のレイヤと接続先が限定されているか否かは別の概念であると考える。このとき、ネットワークの安全性は、「接続先が限定されているか」と「経路が管理されているか」を考慮するのが妥当である。
- 図１３－２のように、ネットワークの接続先の限定は、さまざまな形で実現できる。リスクの違いはあるものの、回線の暗号化を講じることで、いずれの場合にも、従来の境界防御として整理することができる。
- 一方、接続先が限定されていなかったり、経路が管理されていない場合には、「オープンなネットワーク」に位置付けられる。この場合も、インターネット VPN 等のサービスを利用することで、境界防御に近い対応が可能である。

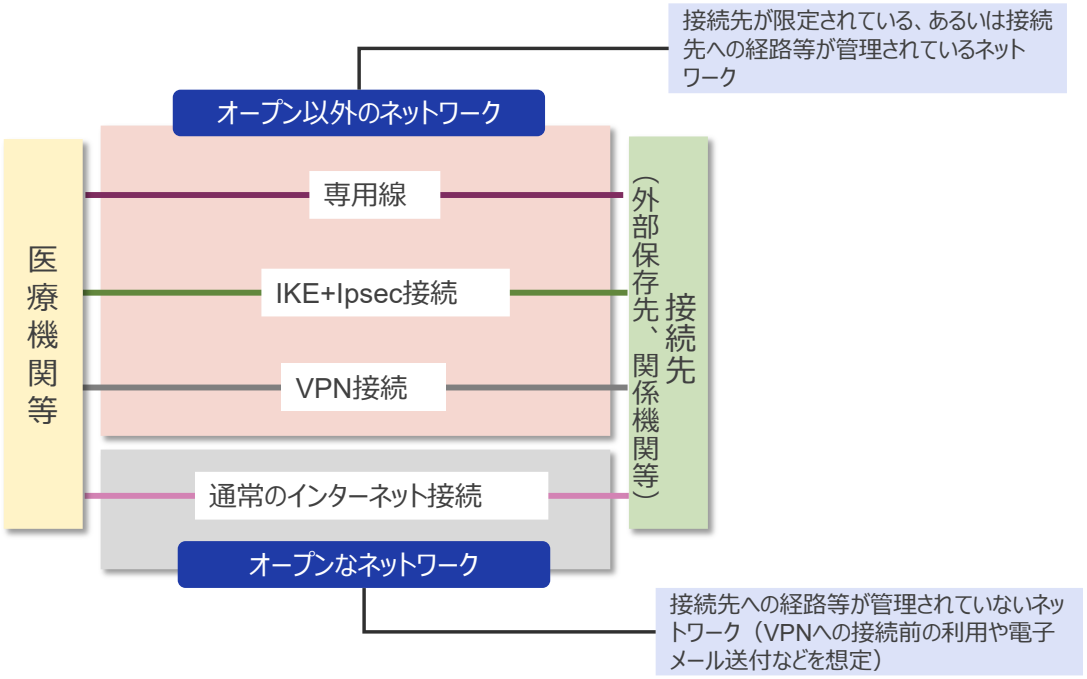


図１３－２　本ガイドラインにおけるネットワークの整理

- 本ガイドラインでは、接続先等の管理がなされていないネットワークを「オープンなネットワーク」とし、接続先が限定されている、あるいは接続先までの経路等が管理されているオープンではないネットワークを「セキュアなネットワーク」と称する。医療情報システムの利用は、原則として「セキュアなネットワーク」を用いること。但し「セキュアなネットワーク」と同様の安全性を確保する途中経過として「オープンなネットワーク」を用いたり、電子メールの送信時において、データを暗号化して送信する際に用いることなどが想定されるため、併せて利用のための遵守事項を整理する。

１３．１．１　セキュアなネットワークの構築

- システム運用担当者には、医療情報システムへの不正な機器の接続、不正ソフトウェア等の混入、異常データ通信を防止するため、セキュアなネットワークを構築し、接続する機器の構成を適切に管理することが求められる。
- セキュアなネットワークを構築するために、ネットワークの論理的または物理的な構成分割、接続機器の制御、通信するデータの制御等のセキュリティ対策を実施すること。
- ネットワーク構築にあたり、使用する IP アドレスの割当の規格として IPv6（Internet Protocol Version 6）の採用が進んでいる。IPv6 は透明性、完全性、可用性、管理性などの観点から、有効なセキュリティ対策として期待される。

  一方で、IPv6 の採用に伴い、新しい機能に関連する脆弱性（拡張ヘッダーの複雑な設定に伴う攻撃パケットの透過、一時 IPv6 アドレスを採用する場合に生じるリスクや、管理上の煩雑性の増加、IPv6 との併用に伴うトンネリング技術に内在するリスク等）が指摘されている。IPv6 を採用する場合にも、ネットワーク構成を踏まえたリスクの精査を行ったうえで、適切な対応を行うこと。

１３．１．２　選択すべきネットワークのセキュリティ

- システム運用担当者は、医療情報の安全管理が確保できるネットワークを選定することが求められる。
- ネットワークに関しては、専用線を用いることが最も安全であると言われてきた。専用線は、2 拠点間を物理的に接続し、利用者が独占的に使用する回線であることから、外部からの侵入や盗聴のリスクが小さいとされる。一方で専用線による場合には、高コストであることや、多目的な利用にはなじみにくいというデメリットもある。

- 専用線以外の仕組みを利用する際には、VPN（Virtual Private Network）と呼ばれる専用線同様のサービスを仮想的に実現する仕組みがある。VPN にはいくつかの実装方法がある。
- IP-VPN は、通信事業者が管理する閉域ネットワークを利用するため、通信事業者以外の侵入のリスクは小さい。但し専用線ほどではないものの、利用コストは高いものとなる。
- オープンなネットワークであるインターネットを用いるサービスとしては、IPsec＋IKE で実現する VPN と SSL-VPN がある。IPsec は、ネットワーク層レベルでの暗号化を図る方法で、インターネット VPN の中でも安全性が高いとされる。SSL-VPN は SSL 技術を利用した VPN でセッション層における暗号化を図るものである。端末側でのアプリケーションが不要など、導入が容易である反面、偽サーバへの対策リスクや長時間の接続におけるリスク等があるとされる。
- IKE が使われている機器については、すでに寿命を迎えた暗号技術（DES, 3DES, MD5, SHA-1 など）がデフォルト設定になっている機器が多いことに伴うリスクが内在する。従って、新規に購入する場合には、IKEv2 に対応したものを購入すること。また IKE が使われている機器については、「電子政府における調達のために参照すべき暗号のリスト」[9]に準拠していることを確認し、アグレッシブモードを使用している場合は、速やかに IKEv2 に移行すること。基本的には IPsec など安全性が高いネットワークを利用することが望ましいが、医療機関等のシステム化計画なども踏まえて、適切なものを選択すること。

表１３－１　通信経路・接続方式の適合性

<table>
<tr><th colspan="4">通信経路・接続方式</th><th>適合性[10]</th></tr>
<tr><td colspan="4">専用線</td><td rowspan="3">適合</td></tr>
<tr><td colspan="4">IP-VPN</td></tr>
<tr><td rowspan="4">インターネット</td><td rowspan="3">インターネット VPN</td><td colspan="2">IPsec ＋ IKE、IKEv2</td></tr>
<tr><td rowspan="2">SSL-VPN</td><td>クライアント型</td></tr>
<tr><td>その他</td><td>―</td></tr>
<tr><td rowspan="2">オープンなネットワーク</td><td colspan="2">TLS1.3 (高セキュリティ型)+クライアント証明書</td><td rowspan="2">適合</td></tr>
<tr><td colspan="2">TLS1.2 (高セキュリティ型)＋クライアント証明書</td></tr>
</table>

- オープンなネットワークを通じて接続先が限定されているセキュアなネットワークへ接続する場合、セキュアなネットワークに到達するまでのオープンなネットワーク（インターネット）経由において、事業者によるチャネル・セキュリティが確保されないリスクがある。チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、事前に事業者との契約を確認し、確実にチャネル・セキュリティを確保すること。
- 最新の VPN 技術を利用する場合であっても、それが盗聴防止、なりすまし防止、アクセス管理、適切な認証手段の確保といったガイドラインが要求するセキュリティレベルを確実に満たし、特に外部アクセスにおいて求められる厳格な安全対策（例：二要素認証に相当する措置）を組み合わせて実現できるのであれば、利用可能と解釈できる。ただし、実際に新しい VPN 技術を採用する際には、事前のリスク評価に基づいて、そのプロトコルが要求される安全水準を満たしていることを確認すること。また、システム関連事業者からサービス仕様適合開示書な

[9] 「電子政府における調達のために参照すべき暗号のリスト」(CRYPTREC 暗号リスト)。デジタル庁、総務省及び経済産業省が、CRYPTREC の活動を通して安全性・実装性能等を評価したうえで公表するリスト。電子政府推奨暗号リスト、推奨候補暗号リスト及び運用監視暗号リストで構成される。

[10] ここで言う適合性はあくまで表１３－１における適合性であり、「１３．ネットワークにおける安全管理措置」の遵守事項をすべて満たして初めて本ガイドラインに適合しているとみなすことができる。

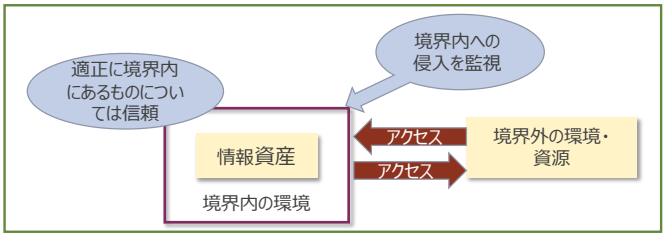
どの必要な情報提供を受けて、責任分界を含めた具体的な運用を取り決めること。

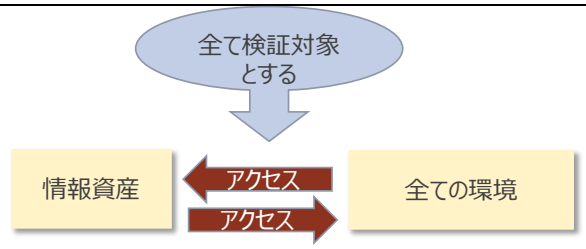
- なお、VPN 機器への脆弱性対策として、クラウド型 VPN の採用や、自動アップデートに対応した製品を選定することが望ましい。ルータ等のネットワーク機器は管理インターフェイスやログイン画面が露出していることが侵害される原因になっているので、これらを露出させない必要がある。そのため、機器の管理インターフェイスやログインページ、管理ポートに対して接続を許可されていない機器が、外部からアクセスできないようにすること。
- 医療機関等がクラウドサービスを利用する場合、事業者との間の通信経路が暗号化されていれば、当該経路の盗聴のリスクは小さい。TLS の設定を適切に行い、TLS クライアント証明書による認証を受けることにより通信経路のセキュリティは確保されるが、クラウドサービス事業者内部での通信について、十分な安全性は保証されない。医療機関等は、クラウドサービス事業者内部で用いる通信について、暗号化等十分な安全性を講じることを求めること。
- 医療機関等が管理する医療情報システムに対して、外部から接続する場合（リモートメンテナンス、テレワーク等）には、内部のネットワークにおける盗聴のリスクも考慮し VPN 等を用いたセキュアなネットワークによる接続を要する。このとき、併せて「７．２　医療機関等外から医療情報システムに接続する利用の場合への対策」、「１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置」に示す対策を講じること。
- なお、システム運用担当者はネットワークを選定した際に、その管理や非常時の対応など、具体的な技術的な対応について、ネットワークを提供する電気通信事業者や、情報システム・サービスを提供する事業者との間での責任分界の範囲を明らかにしたうえで、企画管理者に報告すること。

１３．２　不正な通信の検知や遮断、監視

- 医療分野では、セキュアなネットワークを選択し、境界防御を想定した対応が一般的である。一方で、クラウドサービスの普及や、テレワークによる業務システム環境の変化等、情報資産を取り巻く脅威は変化しており、このような新たな環境における脅威に対して境界防御のみによる十分なセキュリティ対策は困難になりつつある。例えばVPN 装置による境界での対策を過信しており、内部に侵入された際の横断的侵害（水平展開）への対策が不足していたことで、サイバー攻撃の被害が拡大した例も複数存在する。
- 近年は、境界防御の思考による安全性に限らず、全てのトラフィックについての安全性を検証するという「ゼロトラスト」の概念が普及しつつある。ゼロトラスト思考は、利用者の行動も含めて全て検証し、異常とみられる事象が発生したタイミングで、利用者の正当性などを確認する仕組み等で構成される。

表１３－２　境界防御型思考とゼロトラスト思考の比較

境界防御型思考 	・　オープンな環境（管理者により管理されていない環境）とオープンではない環境（管理者により管理されている環境）を想定したうえで、オープンではない環境については、その境界部分への侵入を防ぐため、監視を行う。 ・　オープンではない環境では、医療情報等、特に重要な情報の管理を行う。
ゼロトラスト思考	・　オープンではない環境とオープンな環境のいずれにおいても、情報資産へのアクセスについては、不正なものが含まれうることを

	前提（ゼロトラスト）に、全てを検証対象とする。 ・ 検証は、情報資産に対するアクセスにおいて、不正なトラフィックやアクセス等の異常行動などを起点として捉える。

- 例えば振る舞い検知機能により、利用者のアクセスを監視し、通常の運用と異なるアクセスが生じた際に、必要な制御を行うことができる。一方で、これを実装するためには、現時点では費用や管理に対する負担が大きいとされており、医療機関等においても小規模の医療機関等で導入することは必ずしも容易ではない。導入に当たってはリスク分析の結果を踏まえて判断することが望ましい。
- 医療機関で境界防御を採用する場合でも、トラフィックの監視等、多層防御による対策が必要である。
- 例えば、クラッカーやマルウェアによる攻撃から情報を保護するための一つの手段として、ファイアウォールの導入があるが、これに加えて、不正な攻撃を検知するシステム（IDS：Intrusion Detection System）、不正な攻撃を遮断するシステム（IPS：Intrusion Prevention System）などを採用することが考えられる。またシステムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断や脆弱性スキャン）を定期的に実施し、パッチ適用等の対策を講じておくことも重要である。これは、「８．２　情報機器等の脆弱性への対策」と併せて実施すること。
- 内部脅威監視や EDR などの措置を講じることも、有効な対策として挙げられる（「８．１　マルウェア対策」参照）。モニタリングについては、費用対効果を鑑みて、リスクの高い箇所に対し重点的に実施することも想定される。

１３．３　通信の暗号化・盗聴等の防止

- システム運用担当者は、医療情報システムが利用するネットワークの安全性を確保するために、利用するネットワークの回線、または送信する医療情報に対して暗号化措置を講じることが求められる。
- また送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威に対して適切な対策を講じること。

１３．３．１　ネットワーク回線の暗号化

- 特にオープンなネットワークでは、盗聴のリスク等があることから、医療機関等の外部と医療情報のやり取りする場合には、TLS の設定を適切に行って、暗号化することが求められる。またオープンなネットワークを経由して SSL-VPN を利用する場合には、クライアント型を採用すること。
- 医療機関等がクラウドサービスを利用する場合、クラウドサービス事業者との間の通信経路の暗号化が保証されていれば、当該経路の盗聴のリスクは小さい。TLS の設定を適切に行い、TLS クライアント証明書（2026 年以降のパブリック認証局による制限に留意し、公的認証局から発行されたクライアント証明書、又はプライベート認証局の利用を検討すること）[11]等による認証を受けることにより、必要な暗号化がなされる。但しこの場合、クラウドサービス事業者内部での通信は暗号化されないため、医療機関等は、クラウドサービス事業者内部で用いる通

[11] 公的認証局から発行されたサーバ証明書をクライアント証明書に利用してはならない。サーバ証明書をクライアント証明書にも利用するとセキュリティ上のリスクを有することから、大手ブラウザ事業者において、2026 年 6 月 15 日以降、「正当な端末」と認識されなくなるとされる。

信についても十分な安全性対策を求めること[12]。

- 医療情報システムに対して、医療機関等の外部から接続する場合（例えばリモートメンテナンスによる場合や、テレワーク、訪問看護など）、医療機関等の内部のネットワークにおける盗聴リスクがあることから、セキュアなネットワークによる接続が必要となる。これに対応するため、VPN 等を用いた経路の暗号化措置を施すこと。このとき、併せて「７．２　医療機関等外から医療情報システムに接続する利用の場合への対策」、「１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置」に示す対策を講じること。

１３．３．２ 情報に対する暗号化

- 医療機関等の内部のネットワークを通じて外部に医療情報を送信する場合、必要に応じて、送信する医療情報自体に暗号化を施すことが求められる。特にオープンなネットワークの場合には、医療情報が相手先までに到達する経路が保証されないリスクに留意すること。

１３．３．３ 盗聴防止等

- ネットワークを利用して医療情報を外部と交換する場合、送信先に確実に情報を送り届ける必要がある。システム運用担当者は下記脅威に対して適切な措置を講じることが求められる。
  - 盗聴
  - 改ざん
  - なりすまし
  - マルウェアの混入等や中間者攻撃

  措置としては、ネットワークや機器、サービス等の監視、通信の相手先との相互認証などが想定される。

１３．４ 無線 LAN の利用における対策

- システム運用担当者は、医療情報システムにおいて無線 LAN を利用する際に、不正利用や盗聴などのほか、可用性にも配慮した対策を講じることが求められる。
- 無線を用いたネットワークであることから、本来利用が許されない第三者の利用に利用される、侵入者による攻撃を受ける等のリスクがある。また適切な暗号化を講じないと、盗聴やマルウェアの混入などのリスクも生じる。さらに無線 LAN で使用される電波は、その特性や、医療機関等の構造により接続がしにくくなるケースが生じることから、可用性に留意した対応が求められる。

  無線 LAN 通信の暗号化に際しては、通信内容の漏えいリスクを低減するため、安全な方法による暗号鍵の管理が求められる。WPA2-PSK など事前入手方式は、利用者が同一の暗号鍵を共有することで、鍵が漏えいするリスクが高いため、利用を避けること。

[12] クラウドサービス事業者において、外部からの不正なアクセスを防止する観点から、併せて WAF（Web Application Firewall）を用いることも効果的であることから、このような対策を講じている事業者を選択することで、より安全性が向上すると考えられる。

１４．認証・認可に関する安全管理措置

【遵守事項】

① 医療情報システムへアクセスする際には、利用者の識別・認証を行うこと。また、利用者認証方法に関する手順等は、規則、マニュアル等で文書化すること。

② 利用者の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施すること。

③ 利用者の識別・認証にセキュリティ・デバイス（例：IC カード）等を用いる場合、セキュリティ・デバイス等の破損等を想定し、緊急時の代替手段によるバイパス等、一時的なアクセスルールを用意すること。

④ 規程に基づいてアクセス権限を付与する場合、利用者が所属する部署等からの申請など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の確認を得る等の手順を作成すること。

⑤ 令和９年度（令和 9 年 4 月 1 日時点）時点で稼働していることが想定される医療情報システムを、今後、新規導入又は機器の入替等を伴うシステム更改をするに際しては、二要素認証を採用、又はこれに相当する対応を行うこと。なお技術的な理由等により令和９年度までの対応が困難な場合には、令和９年度以降、直近の次期の医療情報システムの更新までを期限とする。

- クライアント端末とサーバのいずれも二要素認証の実装を要する。
- クライアント端末では電子カルテ等のアプリケーションのログイン時に二要素認証を実装すること。
- サーバについては OS での二要素認証を実装すること。

⑥ パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。

(1) 類推されやすいパスワードを使用させないよう、設定可能なパスワードに制限を設けること。

(2) 異なる医療情報システムにおいて用いるパスワードの使い回しは行わないこと。

(3) 医療情報システム内のパスワードファイルは、パスワードのハッシュ値を保存するなどして平文パスワードを復元できない状態にした上で、適切な手法で管理・運用すること。

(4) 利用者のパスワードの失念や、パスワード漏えいのおそれなどにより、医療情報システムのシステム運用担当者がパスワードを変更する場合には、利用者の本人確認を行うとともに、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）すること。また、変更したパスワードは、利用者本人以外が知り得ない方法で通知すること。なお、パスワード漏えいのおそれがある場合には、速やかにパスワードの変更を含む適切な処置を講じること。

(5) システム運用担当者であっても、利用者のパスワードを推定できないようにすること（設定ファイルにパスワードが平文で記載される等があってはならない）。

(6) 一定回数、認証に失敗した場合には、以降一定時間ログイン試行が不能となる仕組みを講じること。

⑧ 医療情報システムにおいて用いる ID について、台帳管理等を行うほか、定期的に棚卸しを行い、不要なものは適宜削除すること。また、これを実施するうえでの手順を作成すること。

⑨ 電子カルテシステムにおける識別情報の記録について、以下の機能があることを確認すること。または、記録の確定手順等を確立すること。

(1) 電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合

(a) 診療録等の作成・保存を行おうとする場合、確定された情報を登録できる。その際、登録する情報に、入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時を含む。

(b) 「記録の確定」を行うに当たり、内容を十分に確認できる。

(c) 「記録の確定」を、確定を実施できる権限を持った利用者に限定する。

(d) 確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策と、原

状回復のための手順を検討すること。

(e)　一定時間経過後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを運用管理規程に定めること。

(f)　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。

(2) 臨床検査システム、医用画像ファイリングシステム等の装置又はシステムにより記録が作成される場合

(a)　運用管理規程等に当該装置により作成された記録の確定ルールを定義すること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時を記録に含めること。

(b)　確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。

(3) 一旦確定した診療録等を更新する場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合わせることができる。

(4) 同じ診療録等に対して複数回更新が行われた場合でも、更新の順序性が識別できる。

(5) 代行入力が行われた場合には、誰の代行がいつ誰によって行われたかの管理情報を、代行入力の都度記録すること。

(6) 代行入力により記録された診療録等は、できるだけ速やかに確定者による「確定操作（承認）」が行われるようにすること。この際、内容の確認を行わずに確定操作を行ってはならない。

１４．１　利用者認証

１４．１．１　利用者の識別・認証

- アクセスを正当な利用者のみに限定するため、医療情報システムは利用者の識別・認証を行う機能を備えなければならない。システム運用担当者は、リスク分析の結果を踏まえ、企画管理者と協働して、適切な利用者認証のための措置を講じるほか、その運用の具体的な手順の作成を行うこと。
- これは、小規模な医療機関等で医療情報システムの利用者が限定される場合においても、同様である。
- 認証をするためには、医療情報システムへアクセスする全ての職員及び関係者に対し ID・パスワードや IC カード、電子証明書、生体認証等、本人の識別・認証に用いる手段を用意し、医療機関等の内部で統一的に管理する必要がある。また更新が発生する都度速やかに更新作業を行うこと。
- このような利用者の識別・認証に用いられる情報は、本人しか知り得ない、又は持ち得ない状態を保つ必要がある。利用者認証を ID とパスワードにより行う際には、システム運用担当者は、推定困難なパスワードが設定されるよう、安全性を考慮した機能仕様とすること。また、システム運用担当者も利用者のパスワードが把握不能となるような措置を講じることが求められる。
- 本ガイドラインでは令和３年度より二要素認証技術の実装を促してきた。令和９年度時点（令和９年４月１日時点）で稼働していることが想定される医療情報システムを、今後、導入又は更新する場合、原則として二要素認証を採用すること。
- ここでいう、医療情報システムとは、医療情報を作成、更新、閲覧、削除等を行うアプリケーションまたはサービスのほか、医療情報を格納するサーバも含まれる。アプリケーションまたはサービスについては、これらを提供する事業者が技術的な対応を行っていないことで、二要素認証が実装不能なケースも想定される。令和 9 年度時点までに

システム更新を行う場合には、二要素認証対応をしているアプリケーションまたはサービスを選定することが求められる。令和 9 年度時点の対応が間に合わない場合には、令和９年度以降、直近のシステムの更改、新規導入までの間を経過措置とする。

- また、医療情報を格納するサーバの OS についても、原則として二要素認証の実装を目指すこと。サーバでは例えばアプリケーションを介さずにデータベースにアクセス可能であることから、OS のログイン時に二要素認証を実施することが合理的である。ただし、運用対応等の技術的な理由で対応が間に合わない場合には、令和９年度以降、直近のシステムの更改、新規導入までの間を経過措置とする。
-

表１４－１　医療情報システムにおける二要素認証の要否

	アプリケーション	ミドルウェア	OS
クライアント端末	要※	―	―
サーバ	―	―	要

※認証した情報をアプリケーションの資格情報等と連携し、適切な権限付与が可能な場合は OS やミドルウェアでの二要素認証を許容する。ただし、OS で一要素、アプリケーションで一要素のような認証は許容されない。

- クライアント端末のアプリケーションログイン時の二要素認証の実装は普及しつつあるが、サーバ OS ログイン時の二要素認証については、導入のために大規模な院内のネットワークやシステムの再構築が必要となる場合がある。
- このため、サーバ OS については以下①②いずれか、またはそれと同等以上の措置が施されていれば[13]、二要素認証を実装できているものとみなす。

① 以下 2 つを満たすもの

・医療情報システムのサーバ群（以下、サーバ群と呼ぶ）へのアクセスを別ドメインに設置された踏み台端末からの RDP や SSH 等による接続のみに限定する。

・踏み台端末の OS ログイン時に二要素認証を実装する。

② 以下 3 つを満たすもの

・サーバ群へのアクセスを、別ドメインに設置された踏み台端末からの RDP、SSH 等による接続に限定する。

・踏み台端末には EDR 機能を具備し、運用上想定されない
振る舞いを検知可能とする。
（必ずしも EDR 製品を要せず、例えば Windows 標準機能等によって振る舞い検知が可能であればよい。）

・医療機関等の外部からの接続は VPN を経由し、踏み台端末への RDP、SSH 等による接続に限定する。

上記措置を講じる際には、以下 3 つが適用されていることが前提となる。これらが満たされない場合、十分な措置とは見なされない。

・外部から踏み台端末にログインするユーザに管理者権限を与えない

・十分な OS のセキュリティアップデート

・医療情報システムサーバ群と踏み台端末で共通のパスワードを利用しない

- 認証により実現される対策の強度は、単に認証方法だけで判断されるものではない。二要素認証等の認証強化と併せて他の対策（ネットワーク接続管理や端末管理等）を講じることが必要である。二要素認証を採用してい

[13] 同等以上の措置とは、例えば医療法に基づく立入検査の際に同等性を検査職員に対して説明できること、などが想定される。

ることを前提とした場合、パスワードの桁数は 8 桁（PIN であれば 4 桁）以上が求められる。この際、英数字の混在（大文字小文字は問わない）を求める。ただし、二要素認証を採用していない場合には 13 桁以上とすること。システムの仕様上、13 桁以上の設定ができない場合には、設定可能な最大桁数を設定し、直近のシステムの更改、新規導入時に必ず対応すること。

- いずれの場合においても、パスワードの定期的な変更は不要とする。
- PIN の定義としては、「特定のデバイスにおける電子証明書等の使用のための 4-8 桁の暗証番号」とする。
- また、VPN 装置においてもパスワードの使い回しや、単純なパスワードの利用によりサイバー攻撃被害が多発している。VPN 装置においても記憶認証のみに依存するのではなく、二要素認証等を導入することが望ましい。

１４．１．２　外部のアプリケーションとの連携における認証・認可

- クラウドサービスの普及から、医療機関でも外部のアプリケーションを連携して用いる場面が増えている。この時、アプリケーション間でデータが引き渡されることが想定される。昨今、システム間連携のインターフェイスとして、Web 技術のうち、REST API（Representational State Transfer Application Programming Interface）が活用されている。REST API は Web の技術を用いてサーバにアクセスして情報をやりとりする手順であるが、インターネット上で公開されることにより、IoT 機器やアプリケーションサーバ等も含め、広くシステム間での情報連携の促進が期待できる。一方で、このような API がサイバー攻撃の起点となる可能性を踏まえ、セキュリティ上の対応策が求められる。
- システム運用担当者は、API 連携のセキュリティ確保のため、外部からの攻撃や意図せぬアクセスを防止する措置を講じること。ネットワークセキュリティの確保や、API 連携により利用するユーザ・アプリケーションやデバイスの範囲の限定、責任分界とアクセスポリシーやログ管理を明確にした上での認証・認可の実装などが想定される。

１４．２　アクセス権限の管理

- 医療情報システムの利用に際しては、情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループ（業務単位等）ごとに利用権限を規定する必要がある。また付与する権限は必要最小限とすることが重要である。医療情報システムに、参照、更新、実行、追加等のようにきめ細かな権限の設定が可能なシステムを採用し、適切に活用すれば、さらにリスクを低減できる。
- アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜更新する必要がある。システム運用担当者は、組織の規程等と照合して、アクセス権限の設定を行う必要がある。
- 医療情報システムによっては、利用者がアプリケーション等を利用する際に、端末の OS の管理者権限を要するものがある。利用者に対する過度の権限付与を避けるため、このようなアプリケーション等の選定は避けること。
- クラウドサービスを利用する場合、利用するサービスによっては、医療機関等の規程に基づいて定めたシステム上の設定（ポリシー）が、デフォルトの設定となる等、自動的に意図しない内容に変更されてしまうことがある。これにより、アクセス権限等が変更され、医療情報が意図しない相手先に送信されるなどのリスクが想定される。
- このような状況を防ぐため、システム運用担当者は、意図せぬ設定の変更を検知できるよう措置を講じること。特に自動的に検知し、運用に反映できることが重要である。
- 利用するクラウドサービスの事業者から必要な情報を収集し、これらに対応できる措置を講じること。

１４．３　電子カルテデータの確定

- 法的に保存義務のある文書等を電子的に保存するためには、日常の診療や監査等において、電子化した文書

を利用可能であることの担保に加え、その内容の正確さについても訴訟等において証拠能力を有するレベルを担保することが要求される。誤った診療情報は、患者の生命に関わる可能性もあり、電子化した情報の正確さの確保には最大限の努力が必要である。また、診療に係る文書等の保存期間が各種の法令に規定されているため、所定の期間において安全に保管されなければならない。

- 法律上、保存義務のある文書等の電子保存の要件として、施行通知では真正性などを要件としている。真正性とは、正当な権限で作成された記録に対し、虚偽入力、書換え、消去及び混同が防止されており、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を指す。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。
- ネットワークを通じて外部に保存を行う場合、委託元の医療機関等から委託先の外部保存施設への転送途中で、診療録等に改ざんや混同が発生しないよう、措置を講じる必要がある。故意又は過失、使用する情報機器・ソフトウェアなどそれぞれの原因に対して、運用も考慮したうえで対応すること。
- 作成責任の所在を明確にすることも求められる。入力者及び確定者について、識別、認証を適切に行うとともに、記録の確定、識別情報の付与及び更新履歴の保存のための措置を講じること。なお、代行入力を行う場合には、入力者と確定者の責任関係が明確となるよう、識別及び認証の方法に留意すること。

１５．電子署名、タイムスタンプ

【遵守事項】

① 法令で定められた記名・押印のための電子署名について、企画管理編「１４．法令で定められた記名・押印のための電子署名」に示す要件を満たすサービスを選択し、医療情報システムにおいて、利用できるように措置を講じること。

１５．１ 電子署名、タイムスタンプが求められる場面での対策

- システム運用担当者は、法令で定められた記名・押印のための電子署名については、企画管理編「14. 法令で定められた記名・押印のための電子署名」で示す要件を満たしたものを選択し、措置を講じることが求められる。
- 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の場合は、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）第 2 条第 1 項を満たす電子署名であることに加えて、署名者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を用いることなどが求められる。システム運用担当者は、必要に応じて、求められる要件を満たす電子署名を付すことができるよう、技術的対応を行うこと。
- 医療情報について、作成時刻又は変更時刻を証明する必要がある場合には、適切なタイムスタンプを付与し、保存義務のある期間中にその時刻及び真正性を検証できるよう、必要な技術的措置を講じること。
- システム運用担当者は、タイムスタンプの付与対象、付与のタイミング、検証手順及び保存期間中の検証可能性の維持方法を定め、必要な情報及び検証手段を保全すること。
- なお共通鍵、秘密鍵を格納する機器、媒体については、FIPS 140-3 レベル 1 [14]相当以上の対応を図ること。

[14]FIPS 140-3 では、製品に求めるセキュリティ要件として、Level 1 から Level 4 の 4 段階のレベルのものを定めている。このうち最も低い Level 1 では、「少なくとも 1 つの承認されたセキュリティ機能または機微なセキュリティパラメータ（SSP）を含み、かつ最低限の物理的セキュリティ要件を満たすこと」などが求められる。（"FIPS PUB 140-3: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES"（NIST、2019.3.22））

１６．紙媒体等で作成した医療情報の電子化

【遵守事項】

① 紙媒体等で作成した医療情報を電子化する際には保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。また、スキャン等を行う前に対象書類に他の書類が重なって貼り付いている等、電子化可能な範囲外に情報が存在しないか確認すること。

② スキャナ等で電子化を行うが、紙等の媒体もそのまま保管を行う場合、必要時に閲覧できるよう、紙媒体等の検索性にも留意して保管すること。

１６．１ 保存義務がある書面等に関する紙媒体等の電子化における技術的な対応

- システム運用担当者は、紙媒体等を電子化する際は、スキャン後も保存義務を満たす文書として必要な情報量を確保するための措置を講じることが求められる。
- なお、スキャナ等で電子化した場合、どのように精密な技術を用いても、元の紙等の媒体の記録と同等にはならない。また、スキャニングにより、保存できない有用な情報も存在し得るため、電子化は慎重に行う必要がある。電子化後に、元の紙媒体も保存することは真正性・保存性確保の観点から極めて有効であり、可能であれば外部への保存も含めて検討すること。

１６．２ 運用の利便性のためにスキャナ等で電子化を行う場合における技術的な対応

- スキャナ等による電子化後も、紙等の媒体の保存を継続する場合、電子化した情報はあくまでも参照情報であり、保存義務等の要件は課せられない。一方で、個人情報保護上の配慮は同等に行う必要がある。また業務等に差し支えない精度の確保も必要である。

１７．証跡のレビュー・システム監査

【遵守事項】

① 利用者のアクセスについて、アクセスログ等を記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日誌等により操作者、操作内容等を記録すること。

② ログへのアクセス制限を行い、ログの不当な削除／改ざん／追加等を防止する対策を実施すること。

③ ログの記録に用いる時刻には、信頼できる情報を利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を保つ必要がある。

④ 監査等を行うに際し、技術的な対応に関する監査実施計画の作成や証跡の整理等を行い、企画管理者に報告すること。

１７．１ 証跡のレビュー

- システム運用担当者は、医療情報システムが適切に運用されていることを確認するため、システム上のログを収集し、レビューすることが求められる。特に個人情報を含む資源については、全てのアクセスログを収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。この確認は、全てのログを目視確認することを指すのではなく、システムでの監視や、実際の運用に基づく適切な閾値を用いたスクリーニング後のログを確認することを想定する。
- アクセスログは、それ自体に個人情報が含まれている可能性があること、情報セキュリティインシデントが発生した際の調査に非常に有用な情報であることから、その保護は必須である。システム運用担当者は、ログへのアクセス制限や不当な削除／改ざん／追加等を防止する対策を講じること。
- なお、例えば外部ネットワークとの接続点の集約に際しては、外部に接続されているサービス毎にログ管理等を分散させるのではなく、接続先制御・監査ログ集約・責任分界整理を一元管理することが負担軽減のために有効である。
- ログの正確性を保つため、記録する時刻の精度も重要である。精度の高いものを使用し、管理対象の全てのシステムで同期を取ること。
- アクセスログを分析し、緊急時にアラートを発する仕組みを講じることも求められる。
- 医療情報システムの管理を委託している場合には、事業者との間でログの管理方法や提供等に関して、明確に取り決めを行うこと。
- なお、医療情報システムにアクセスログを収集する機能がない場合には、システム操作に係る業務日誌等を作成し、操作の記録（操作者及び操作内容等）を管理するなどの代替策を講じることが必要となる。

１７．２ 監査の実施の支援

- システム運用担当者は、企画管理者が監査実施計画を作成する際に、技術的な対応に該当する内容を作成し、企画管理者に報告することが求められる。また監査に必要な証跡（手順等の実施証跡や、システムログ及びレビューの結果等）を整理したうえで、企画管理者に報告すること。監査で指摘された事項については、企画管理者と協議し、改善に向けた対応を行うこと。
- 日々のセキュリティ対策の発展に対応するためには、システムセキュリティ監査（内部・外部）を継続的に実施す

ることが重要である。例えば、毎年テーマを決めて部分的に監査を実施することで、各回の負荷が軽減され、継続的に実施することが可能となる。医療機関全体での安全管理に関する認知度を向上させ、医療従事者全員に意識づけを行うことにも資する。

１８．外部からの攻撃に対する安全管理措置

【遵守事項】

① 医療情報システムに対するマルウェアの混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。

- 攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時切断
- 他の情報機器への混入拡大の防止や情報漏えいの抑止のための当該混入機器の隔離
- 他の情報機器への波及の調査等、被害の確認のための業務システムの停止
- バックアップからの重要なファイルの復元（数世代バックアップを複数の方式で確保すること）。

１８．１ サイバーセキュリティ対応

- システム運用担当者は、サイバーセキュリティ対応の必要が生じた際に、技術的な対応を行う。またサイバー攻撃等に備え、関係先への連絡手段や紙での運用等の代替手段を準備しておく必要がある。
- PC や VPN 機器等の脆弱性対策については、「８． ２ 情報機器等の脆弱性への対策」を参照するほか、NCO から示されている最新の「政府機関等のサイバーセキュリティ対策のための統一基準群」（令和７年７月１日サイバーセキュリティ戦略本部決定）[15]、令和３年４月30日の「ランサムウェアによるサイバー攻撃に関する注意喚起について」も参照すること。
- JPCERT/CC と IPA が提供する MyJVN を利用することで、登録した情報資産に関する Japan Vulnerability Notes のアラートが配信され脆弱性情報の検知が可能となる製品もある。資産管理台帳と組み合わせて有効活用するとよい。

  十分な情報収集やシステム担当者自身による VPN 機器等のアップデートが困難と想定される場合には、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を選定、活用することが望ましい。
- 非常時に備えたバックアップの実施と管理については、「１１．システム運用管理（通常時・非常時等）」、「１２． ２ バックアップの管理」も参照すること。
- なお、医療情報システムは一般に複雑で、医療機関の規模等によって運用やバックアップの方法も様々である。一様に指針を示すことは困難であるが、医療機関においては、重大な障害により医療提供体制に支障が生じた場合であっても、診療の継続や早期復旧が求められる。全ての情報をバックアップから復元するのではなく、診療のために直ちに必要な情報をあらかじめ十分に検討し、確実に運用できるバックアップを確保しておくこと。
- 特に、一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、バックアップデータまでランサムウェア等の被害が拡大することのないよう、バックアップデータの記録媒体を端末及びサーバ装置やネットワークから切り離して保管することが強く求められる。また、世代管理を行うことも重要である。日次でバックアップを行う場合、数世代（少なくとも３世代）を保持し、少なくとも３世代目以降の古い世代はネットワーク的あるいは論理的に書き込み不可の状態にする等の対策が必要となる。
- また、複数の方式でバックアップを確保することにより、単一の障害で全てのバックアップが利用不能となるリスクを低減できる。例えば下記から２つ以上を選択することが想定される。
- ・外部ストレージ/内蔵ストレージ（HDD：Hard Disk Drive、SSD：Solid State Drive 等）

[15] 統一基準群は https://www.cyber.go.jp/policy/group/general/kijun.html を参照。統一基準群を構成する文書は、適宜改訂されることがあるため、最新のものを参照すること。

- ・リムーバブルメディア（RDX：Removable Disk Exchange system、磁気テープ、DVD 等）
  ・NAS（Network Attached Storage）
  ・クラウドサービス
- サイバー攻撃による情報セキュリティインシデントが発生した際、数世代前までのバックアップデータは既にマルウェアの影響が及んでいる可能性があり、不用意にバックアップデータから復旧すると被害を繰り返すことになる。復旧するための手順をあらかじめ検討し、BCP として定めておくこと（電子カルテシステムが長期間にわたり停止した場合に、医師法（昭和 23 年法律第 201 号）第 24 条に定める診療録の作成への対応を整理する等）。また、BCP が機能することを訓練等により確認することも重要である。
- なお、復旧するにあたっては、侵入継続と被害拡大を防ぐ観点から、
  - バックドアを残さない
  - 無効にされたセキュリティ機能を復旧する
  - 利用された脆弱性に対処する
  - 他にリスクとなる既知の脆弱性がないか十分に検証、対応する
  - 不正に作成されたり、侵害された可能性のある機器に保存されていた ID・パスワード等を無効化する

  などの方策をとり、同様の被害を繰り返したり、盗まれた情報による被害を拡大させないよう対処すること。なお専門的な知見に関して、IPA が、マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口[16]を開設している。

[16] サイバーセキュリティ 相談・届出窓口 （IPA）