参考資料１－６

医療情報システムの安全管理に関するガイドライン

第 6.0 版

システム運用編

[Control]

(案)

目次

【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。

＜医療機関等の特性に応じたガイドライン参照箇所＞

[医療機関等の特性についての考え方]

本ガイドラインは、すべての医療機関等における医療情報システムを対象とした安全管理に関して、各編で遵守事項や考え方等を示している。

医療機関等の組織体制や、稼働している医療情報システムの構成、採用しているサービス形態等の特性は様々であるため、それぞれの医療機関等の特性に応じたかたちで本ガイドラインを遵守していただく必要がある。そのため、以下のとおり、医療機関等の特性ごとに、医療機関等が必要な安全管理を確保するために本ガイドラインで最低限参照すべき箇所について明記する。

具体的には、医療機関等における専任のシステム運用担当者の有無と導入している医療情報システムの形態に応じた、４種の参照パターンを例示する。自施設の特性を分析した上で、最も近しい参照パターンに基づく対応を行っていただきたい。（なお、参照パターンに示した参照箇所以外の箇所についても、必要に応じてご参照いただきたい。）

医療機関等の特性に応じた本ガイドラインの参照パターン

	医療情報システムを 医療機関等に保有し運用 （いわゆるオンプレミス型）	医療情報システムを 医療機関等に保有しない運用 （いわゆるクラウドサービス型）
システム運用専任の 担当者がいる	Ⅰ	Ⅱ
システム運用専任の 担当者がいない	Ⅲ	Ⅳ

なお、医療機関等において、カルテ等の医療情報を紙媒体で扱い、情報システム上では医療情報を扱わない業務のみ行なっている場合でも、医療機関等内の端末上やシステムとの連携によって、医療機関等外の医療情報へのアクセスが発生する場合、参照パターンⅢやⅣに基づき本ガイドラインを参照する必要がある。

ただし、システム全体の構成等により、参照パターンが異なるので、必要に応じて、システムの提供元である医療情報システム・サービス事業者に参照パターンを確認すること。

［医療機関等の特性に応じたシステム運用編の参照箇所］

上記「医療機関等の特性に応じた本ガイドラインの参照パターン」によるシステム運用編の参照箇所の詳細を下表に示す。

パターン	システム運用編
Ⅰ 担当者あり	すべて参照
Ⅱ 担当者あり クラウド	以下項目は参照 １～４、６～８、１１、１２．３、１４，１８ ※ 他の項目は、医療情報システムの構成に応じて、当該情報システム・サービス事業者に確認し、事業者と締結する契約等に含まれている場合は、簡略化が可能。
Ⅲ 担当者なし	すべて参照 ※「担当者」という記載を「システム運用管理者」に置換し、参照
Ⅳ 担当者なし クラウド	以下項目は参照 １～４、6～８、１１、１２．３、１４，１８ ※ 「担当者」という記載を「システム運用管理者」に置換し、参照。 ※ 他の項目は、医療情報システムの構成に応じて、当該情報システム・サービス事業者に確認し、事業者と締結する契約等に含まれている場合は、簡略化が可能。

[システム運用編における参照パターンの付記]

システム運用編では、各章のタイトルの末尾に、以下のように、参照パターンを付記している。

１．情報セキュリティの基本的な考え方　［Ⅰ～Ⅳ］

↑

波線部の［　］内が参照パターンを示す。

１．情報セキュリティの基本的な考え方　　[Ⅰ～Ⅳ]

【遵守事項】

① 法令上求められる医療情報システムに関する要件等について、企画管理者の整理に基づいて、必要な技術的な対応を抽出し、各システムの整備において措置を行うほか、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、システム運用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技術的な対応を行う必要がある。

特に、

- 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。）~~個人情報保護法~~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 ~~e-文書法~~対応
- 電子署名、タイムスタンプ

等において必要な措置を行うことが求められる。

２．システム設計・運用に必要な規程類と文書体系　　[Ⅰ～Ⅳ]

【遵守事項】

① 医療情報システムにおいて採用するシステム、サービス、情報機器等の機能仕様や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 医療情報システムの利用者が適切に医療情報システムの利用ができるよう、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、技術的な対応に関する実際の運用に求められる手順や、医療情報システム等を構築するのに必要な資料等を整備することが求められる。これらの資料は、最新のものであることが不可欠である。古い手順や技術資料が混入する場合に、脆弱性が残ったり、正常な情報システムの稼働が損なわれたりするなどのリスクが生じる。

システム運用担当者は、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が求められる。非常時の場合には、特に体制面や情報照会・収集の対象などについても明らかにすることが重要である。

3．責任分界　［Ⅰ～Ⅳ］

【遵守事項】

① 医療情報システムに関する情報システム・サービスの委託において、技術的な対応の役割分担を検討するため、情報システム・サービス事業者（以下「事業者」という。）から必要な情報等の収集を行うとともに、提供された情報の内容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、要求仕様との適合性に関する確認を行い、医療機関等において実施する技術的な対応におけるリスク評価との間で齟齬が生じないことを確認し、齟齬がある場合には、必要な調整を行うこと。

③ 通常時の運用や、非常時の運用において発生する技術的な対応に関する役割分担を、委託先である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に、技術的な対応や対外的な説明に関して必要な役割について、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の責任分界について、企画管理者と協議の上で、医療機関等のリスク評価に従った範囲で、技術的な対応に関する責任分界の範囲を検討し、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

医療情報システムを委託する場合、提供される情報システム・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することができないものも含まれている。

従って、提供する情報システム・サービスの要求仕様に対する適合性に関しては、情報システム・サービス事業者（以下「事業者」という。）から資料の提供を受けるとともに、提供された情報が正確なものであることを確認する必要がある。

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が求められる。

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に際して、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、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」においては、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おり、その基礎となる内容はサービス仕様適合開示書等により示されている。

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し、必要があれば個別の調整を事業者と行うなどにより、技術的な対応に関するリスク分担などを行うことが求められる。

またクラウドサービスなどを利用する場合には、利用者側でも技術的な対応に関する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」（総務省　令和 4 年 10 月 31 日）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、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。

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

通常時の運用における責任分界は、技術的な対応という点で見ると主に、運用責任や管理責任などについて取り決めることになる。情報システム・サービスが提供される際の医療情報システムの運用が、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内容もあるため、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が求められる。その際、事業者が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、具体的なシステムの運用や管理などについては、事業者に役割を委ねることが求められる。

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責任分界は、技術的な対応という点で見ると主に、被害の拡大防止や原因究明などシステム対応に関する内容のほか、外部への説明責任に関する支援などについて、取り決めることが求められる。

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データ等の資料などを併せて検討することが求められるため、それぞれの役割の分担などを取り決めておくことが求められる。

特にサイバー攻撃による被害を受けた場合には、原因究明に際して専門的な知見が必要となり、この場合の責任分担などは非常に重要である。

外部への説明責任についても、事業者でしか、技術的にもわからない部分が存在することがあるため、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場合がある。

クラウドサービスの場合には、医療情報システムで利用する資源について SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）などの類型で提供することがある。

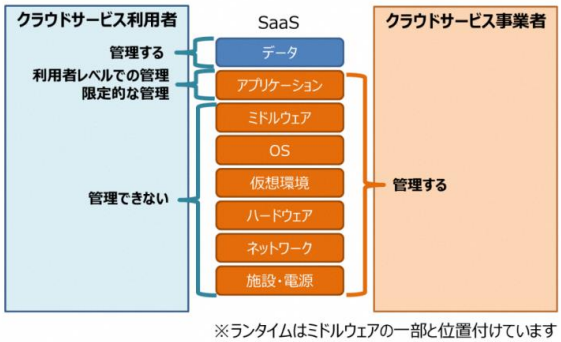
SaaS では、医療情報システムのアプリケーション部分、PaaS では、医療情報システムが利用するミドルウェアの部分、IaaS では医療情報システムが利用するインフラの部分をサービスとして提供することになる。

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、委託により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、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、どの部分の責任を分担し、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が求められる。

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、クラウドサービス事業者が提供する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

医療機関等が事業者に委託を行う場合、この情報システム・サービスを利用するに際して複数の事業者が関与する場合がある。

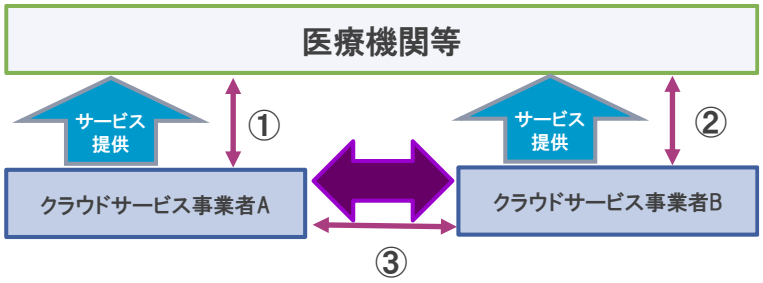
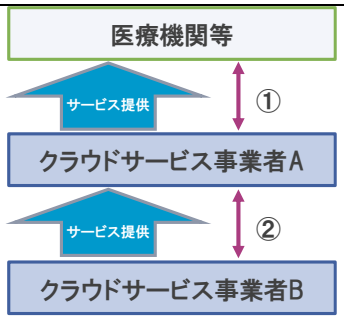
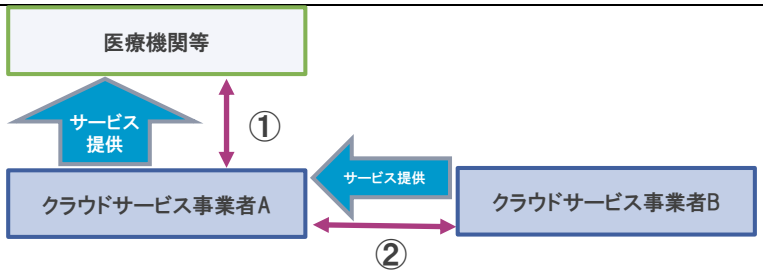
医療機関等が複数の情報システム・サービスのサービスを組み合わせて利用するような場合と、事業者が複数のサービスを組み合わせて、医療機関等に提供する場合などが想定される（表３－２参照）。

前者では、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が求められる。これは、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と、最終的に情報システム・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になる。この場合、事業者が利用する他の事業者のサービスとの関係では、再委託などの関係になることが多いので、これに従って取決めを行う。

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が求められる。

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、

・メール等による情報の送信

・提供者と利用者が利用する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

等が想定される。

この場合、提供方法により利用する技術的な対応に応じて、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を定める。例えば、メールによる送信であれば、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、提供先への到着まで責任を有する等を決定することになる。

システム運用担当者は、このような具体的な内容について、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。

4．リスクアセスメントを踏まえた安全管理対策の設計　［Ⅰ～Ⅳ］

【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、患者情報については、患者ごとに識別できるような措置を講じること。

② 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「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」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

医療機関等において、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医療機関等が保有する情報の棚卸を行うことになる。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、各システムにおいて、それぞれどのくらいの患者数のどのような情報が保管されているのか、それらの利用者の範囲や利用権限がどのように整理されているのか、などを整理するなどが挙げられる。併せて、バックアップなどについても、どのくらいの医療情報が、どこでどのような形で保管されているか、その他持出し対象となっている医療情報の状況なども把握することが求められる。

医療情報システムに関する情報は、医療機関等で導入している医療情報システムの全体図やネットワーク図、各医療情報システムを構築・導入するのに必要な資料等の管理状況（保管場所、作成時期等）、運用において必要な設定に関する情報やログ等に関する管理状況などを把握することなどが挙げられる。

情報種別を行う際に、法令により保存などの要件が求められているものについては、その状況も併せて確認する必要がある。「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。）~~施行通知~~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。）~~外部保存改正通知~~などが求める内容に則しているか等が挙げられる。

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、医療機関等が保有する医療情報等の情報種別や重要度を整理したうえで、リスクアセスメント（リスク分析、リスク評価）を企画管理者と行い、その結果を踏まえて、具体的な安全管理のための技術的な対応について、実装し、運用することになる。

医療情報システムの安全管理のための対策を、リスクアセスメント結果を踏まえて講じる場合には、医療機関等ごとの組織や規模等の実情や、医療情報システムの利用形態等のリスクに応じて、さまざま方法が挙げられる。また実装の検討に際しては、医療機関等における対応できる負担（要員、費用等）などを踏まえることも求められる。

そのため、安全管理対策の設計においては専門的な知見なども求められるが、医療機関等においては、必ずしもこのようなリスクアセスメントに基づく安全管理対策を行うのに十分な資源（要員、費用等）を有していないこともある。このような場合には、利用を想定する事業者において行うリスクアセスメントと、これを踏まえた技術的な対応における対策などを参考にすることなどが考えられる。なお事業者からは、「サービス仕様適合開示書」の提示を受けることが想定される。

特に専任の情報システムの要員がいない医療機関等の場合には、安全な医療情報システム・サービスを事業者から導入し、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、このような方法も含めて、リスクアセスメントを踏まえた技術的な対応における措置を整理し、企画管理者に報告することが求められる。

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）　［Ⅰ、Ⅲ］

【遵守事項】

① システム更新の際の移行を迅速に行えるように、診療録等のデータについて、標準形式が存在する項目は標準形式で、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、それぞれ出力及び入力できる機能を備えるようにすること。

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。その場合、外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持すること。

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すること。

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

医療機関等の情報化においては、情報利用についての従来の指示、報告、連絡等の意思の共有等の業務を単に電子化するだけでなく、その電子化された情報の再利用が可能であれば、幾度もの同一情報の入力作業を軽減し、業務の総量を減ずることも求められている。また紙等の情報を読解して再入力する際のミスの防止、指示の誤記・誤読の防止という観点から、医療安全に資することにもなる。

このような電子化された情報のやりとりを、段階的に導入されたシステム間や、異なるシステムベンダ及びサービス事業者から提供されたシステム間で行う際に必要となるのが、相互運用性の確保である。

一方、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、情報を利用する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、医療機関等で医療情報を長期間保存する際に、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も意味する。

さらに、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、相互運用性の考え方は重要である。

このような医療情報の相互運用性を確保するためには、誰もが参照可能かつ利用可能で将来にわたり保守（メンテナンス）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）を利用するか、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、これを推奨する等の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ところである。

医療機関等において、自らこれらの用語・コードの保守（メンテナンス）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に向けて、システムベンダ及びサービス事業者にこういったこと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、医療情報システムを導入しようとするときや、現に保有する医療情報システムの運用に当たっても、下記のこと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~~そ~~データ項目、データ形式等のほか、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、遵守事項に示す内容が求められていることから、対象となる文書の電子化においては、標準化に対する措置が求められる。

6．安全管理を実現するための技術的対策の体系　［Ⅰ～Ⅳ］

【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）

医療情報システムにおいては、医療従事者のほか職員などの利用に関する情報資産、利用者が利用する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、医療機関情報システムが利用するインフラに関する情報資産などから構成される。またそれらに共通して求められるセキュリティに関連する内容も共通する要素となる。

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対応としての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

医療機関等が利用する医療情報システムは、今日、さまざまな形態のものがある。例えば

- 医療機関等の内部で自ら開発するシステムやサービス（例えばアプリケーションのマクロ機能などを使ったり、簡易データベースソフトを用いて構築したりする場合等）
- 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もの（例えば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場合等）
- 事業者が提供するアプリケーションサービスを用いて、運用も含めて外部に委託する場合（クラウドサービスの利用等）

等がある。

医療機関等のシステム運用担当者が直接対応するべき内容も、このような医療情報システムの形態により異なってくることに留意する必要がある。

また医療機関等の組織によっては、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こともある。この場合には、技術的な対応に関する内容の多くは、外部委託によることになる。

このように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、システム運用担当者の職務を行う者は、事業者にその実施状況の確認を適切に行うことが求められる。

7．情報管理（管理・持出し・破棄等）　［Ⅰ～Ⅳ］

【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したりする場合は、不正ソフト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、情報端末が情報漏洩、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 持ち出した医療情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールするとともに、原則として情報機器対する変更権限がない設定を行うこと。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か、業務に対して影響がないことを確認すること。

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

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医療機関等への連絡方法について、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 保守作業等のどうしても必要な場合を除いてリモートログインを行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。

⑬ 利用者による外部からのアクセスを許可する場合は、~~PC~~ 利用する端末の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに、運用等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、医療情報を公開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記録媒体や情報機器の盗難や紛失（ネットワークサービスの利用等による漏洩の可能性の発生含む）が生じた場合に、行うべき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、医療機関等の外部への医療情報の持出しに関する具体的な手順を、企画管理者が策定する規程を踏まえて作成する。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。また手順における策定対象は、持出し前の手続から、外部からの持ち帰り等に至るまでを想定する。

記録媒体や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が求められる。例えば端末自体の起動パスワード等の設定は必須であり、認証等のルールに沿った内容であることが求められる。また記録媒体や端末内に患者等の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、アクセス先に存在する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求められる。

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ようにする旨や、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なども有効である。

持出しについて、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してもよい保存先やネットワーク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。クラウドサービスの中には、医療機関等が定める安全管理の基準を満たさないものや、プライバシーポリシー、その他のルールが、医療機関が定めるものと整合性が取れないこともある。

システム運用担当者は、例えば医療機関等が許可したり、管理していないサービス以外の接続ができないようにしたりする等の技術的な対応を取りながら、許可されていないサービスの利用禁止を規則等で盛り込むなどの対応が想定される。

保守等の目的で事業者が、医療機関等から医療情報を持ち出す場合、患者の個人情報を持ち出すことは、漏洩防止等の観点から、原則として禁止する必要がある。業務の必要上、やむを得ず持ち出す場合には、目的や持ち出す個人情報の件数とデータ項目、持出し後の対応や、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得て持ち出す等の手続を定める必要がある。

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、医療機関等の外部から医療情報システムに接続して利用する場合の、技術的対応への方策を講じることが求められる。利用場面としては、下記の場面が想定される。

- 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
- 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

７．２．１　医療機関等の職員による外部からのアクセス

医療機関等の職員がテレワークを含めて自宅等や訪問先などから医療情報システムへのアクセスすることを許可することもあり得る。この場合、職員からの接続については、

- 接続できる職員に関する事前の許可
- 外部から接続する際の技術的対応

等が挙げられる。事前の許可については、具体的な手続等について、システム運用担当者で手順等を定めて、外部から接続できる利用者と利用権限の範囲を設定するための手続を行い、その結果を企画管理者に報告するなどの対応が必要となる。

技術的な対応については、

- 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

等の措置を、システム運用担当者は講じる必要がある。

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を行う措置を講じることが求められる。認証等の要件は、「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」に示す。

外部から利用する場合のネットワークについては、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を経由することが想定される。この場合、「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」に示すオープンなネットワークを利用する場合の対策を講じたうえで、チャネル・セキュリティが確実に確保される措置を講じることが必要である。

外部から利用する端末等の要件については、医療機関等が管理する端末を使うことが想定されるが、医療機関等によっては、「９．利用機器・サービスに対する安全管理措置」に示す措置を講じて、個人の所有する、あるいは個人の管理下にある端末（ノートパソコン、スマートフォン、タブレット等）の業務利用（Bring Your Own Device：以下「BYOD」という。）など医療機関等が管理しない端末を使用することも想定される。端末等の要件に関しては、考慮すべき点が 3 つある。

- PC 等といっても、そ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、一般の職員にその知識と技能を要求することは難しい。
- 運用管理規程や手順等で定めたことが確実に実施されていることを説明するためには適切な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、監査することは通常は困難である。
- 医療機関等の管理が及ばない私物の PC や、極端な場合は不特定多数の人が使用する PC を使用する場合はもちろん、医療機関等が管理する情報機器を使用する場合であっても、異なる環境で使用していれば想定外の影響を受ける可能性がある。

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、利用する PC 等の端末の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術の導入を検討するなどの対応が求められる。

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む中、ネットワークを介して患者等に診療情報等を提供したり、患者等が医療機関等内の診療情報等を参照閲覧させたりす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、システム運用担当者は、ネットワークのセキュリティ対策、医療機関等内部の医療情報システム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。

ネットワーク対策等に関しては、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が求められる。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が求められる。

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、医療情報の破棄について企画管理者が作成した手順を踏まえて、情報種別ごとに破棄の具体的なルール等を作成することが求められる。

破棄の対象となるのは、

- 医療情報を格納した情報機器等（過去に格納して消去したものを含む）
- 医療情報システムのデータベース等に格納したデータ

等が想定される。

医療情報を格納した情報機器等については、単に OS 上のファイル管理システム上だけの削除では足りず、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により破棄することが求められる。なお、より確実なのは記録媒体などを物理的に破壊するなどが挙げられる。なお、リース等による情報機器等の返却についても、同様の措置が求められる。なお情報機器等の破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破棄に関する証明や証跡の提供などを求めて、確認することが求められる。

医療情報システムのデータベース等に格納したデータの削除については、通常利用するデータに関しては、システム管理機能が持つ削除等の機能によることになる。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したために、その他の情報が利用不可能になる場合もあるため、留意することが必要である。

外部保存などにより、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には、破棄の証明等が難しい場合も想定される。このような場合には、企画管理者と協働して、システム運用担当者は事業者のデータの破棄の手順などを確認して、破棄の状況を確認することが求められる。

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記録媒体、情報機器等の紛失、盗難が生じた場合の対応に関する手順等を作成することが求められる。紛失や盗難に関する報告を受けた場合に、対象となる記録媒体や情報機器等の特定、情報機器等の利用を目的として ID 等を発行している場合には、医療機関等におけるネットワークの接続防止等が挙げられる。また、事前に記録媒体の暗号化を図るほか、例えばモバイル~~デバイス~~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求められる。

なお、ネットワークを通じて外部サービスを利用した際に、設定のミスなどにより漏洩のリスクが生じた場合についても、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　［Ⅰ～Ⅳ］

【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不正なソフト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 常時不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。

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、不正ソフト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）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。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 情報機器に対して起動パスワード等を設定すること。設定に当たっては製品等の出荷時におけるパスワードから変更し、推定しやすいパスワード等の利用を避けるとともに、情報機器の利用方法等に応じて必要があれば、定期的なパスワードの変更等の対策を実施すること。

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。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。

(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 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器の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) 使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を実施すること。

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 の実施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 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　不正ソフトウェア対策

コンピュータウイルス、マルウェア、ワーム等様々な形態・呼称を持つ不正ソフトウェアは、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入る可能性がある。不正ソフトウェアの侵入に際して適切な保護対策が行われていなければ、セキュリティ機構の破壊、システムダウン、情報の漏洩や改ざん、情報の破壊、資源の不正使用等の重大な問題が引き起こされる。また不正ソフトウェアの侵入は、何らかの問題が発生して初めて気付くことが多い。

対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が効果的であると考えられ、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、不正ソフト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、このような不正ソフト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が求められる。

ただし、これらの不正ソフト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、医療機関等のシステムの環境等の状況を勘案して、可能な限り、常に最新のものに更新しておく必要がある。システム運用担当者は、パターンファイルの更新に先立ち、医療情報システムへの影響等に関する情報を収集することも求められる。

また、不正ソフトウェア対策のスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正ソフトウェアが検出できるわけではない。不正ソフトウェアの対策としては、スキャン用ソフトウェアを導入するだけでなく、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が重要である。そのために実施すべき対策として、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非活性化、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）や「振る舞い検知」などの方策も有効である。なお、いずれの対策を行う場合も、対策を実施した際の業務への影響や、対策処理の速度や可用性、網羅性について、十分な検討が必要である。

また、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ることから、これらの情報機器等についても、上記の対応を行うことが求められる。

８．２　情報機器等の脆弱性への対策

企画管理者は、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。

医療機関等において、医療情報システムが利用する情報機器等には、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、様々なものが挙げられる。

サイバー攻撃においては、近年は、情報機器等に内蔵されるファームウェアや、情報機器等に格納されるプログラム等の脆弱性、EOS（End of Sale, Support, Service：販売終了、サポート終了、サービス終了）の対象となった情報機器等を攻撃して、外部から攻撃するなどが多くみられている。特にランサムウェアなどのケースでは、必要な脆弱性対策が見逃されたことに起因するものも見られる。

システム運用担当者においては、医療機関等において利用している情報機器等に関して、どのような脆弱性があるか、最新の情報を収集することが求められる。PC 等の OS などに関する情報は、OS や不正ソフトウェア対策ソフトウェアを提供する事業者などが提供しているほか、重要なセキュリティ関する情報は、「内閣サイバーセキュリティセンター（NISC)」や「独立行政法人　情報処理推進機構」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、必要に応じて利用する情報機器等やソフトウェアを提供する事業者に対応を確認するなどして、最新の情報の入手を図ることが重要である。そのうえで、必要に応じて速やかに脆弱性対策を講じることが求められる。その際に、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ことから、事前に事業者に対応の可否を確認する必要がある。

なお、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。

本ガイドラインにおいては、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いるものであり、「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」[1]において定める医療機器のサイバーセキュリティの保全については、厚生労働省医薬・生活衛生局から発出されている「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」[2]、「医療機器のサイバーセキュリティの確保に関するガイダンス」[3]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も求められる。

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、医療情報システムで利用する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については、必ず製品出荷時のものから変更することが重要である。サーバで利用するソフトウェアの管理者権限を有する ID 等においても同様である。企画管理者はこのような情報機器の起動や初期設定に関する対応を図ることが求められる。

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の稼働は行わない、などの対応も必要である。例えば、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には、その情報機器等が攻撃対象となることも想定される。また医療機関等の業務によっては、明らかに利用する可能性がない（または低い）時間帯を含めて医療情報システムを稼働することにより、業務で利用されない時間帯に攻撃を受けることも想定される。従って、企画管理者は、業務での必要性や利便性などと勘案して、利用する情報機器等や医療情報システムの稼働時間等を整理して、適切な設定を行うことが求められる。

---

[1] 昭和 35 年 8 月 10 日法律第 145 号

[2] 平成 27 年 4 月 28 日付け薬食機参発 0428 第 1 号、薬食安発 0428 第 1 号

[3] 平成 30 年 7 月 24 日付け薬生機審発 0724 第 1 号、薬生安発 0724 第 1 号

８．４　情報機器等の棚卸

企画管理者は、医療情報システムで利用する情報機器等について、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棚卸をすることが求められる。棚卸を行うことにより、医療情報を格納した情報機器を含め、所在確認が明確になるほか、不明な情報機器等についてその所在状況を明確にすることにより、情報の漏洩等の可能性を速やかに発見することが期待される。また棚卸に際して、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、利用可能な情報機器であるのかを把握することができ、バージョンアップや買換え等、必要な方策を講じることが可能となる。なお情報機器等の滅失状況については、必要に応じて最新のソフトウェアへの対応の可否なども含めて、確認することも重要である。

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の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 においては、上記の要件を実現するために、管理者以外による端末の OS の設定の変更を技術的あるいは運用管理上で制御すること、あるいは、技術的対策として、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し、さらに個人でその設定を変更できないようにし、OS レベルで管理領域を分離すること、また、運用による対策として、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こと等、適切な対策を選択・採用し、十分な安全性が確保された上で行う必要がある。コンピュータウイルスや不適切な設定のされたソフトウェアにより、外部からの不正アクセスによって情報が漏洩することも考えられるため、管理されていない端末での BYOD は行わない。管理者が BYOD によるコスト・利便性とリスクを評価して検討することが求められる。

9．ソフトウェア・サービスに対する要求事項　［Ⅰ、Ⅲ］

【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し、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により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の管理を直接行うことが求められる。ソフトウェアの構成を適切に行わないと、医療情報システムの動作に支障をきたしたり、セキュリティ上の脆弱性が放置されたままになったりするなどのリスクが生じる。

ソフトウェアの構成については、ソフトウェアを開発・保守する事業者が行うことが多いが、適切な構成管理を行うための手順などにより行うことが想定される。

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（プログラム）のバージョンなどが適切に管理されているか等を、事業者に確認し、医療情報システムの導入や保守において、構成管理に関する手順に従った計画が策定され、実施されていることを確認することが求められる。

クラウドサービスなどの場合には、このような構成管理を直接、医療機関等が行うことは難しい。従ってクラウドサービスによる場合には、事業者において構成管理等の手順があり、それに基づいて実施していることの確認などを行うことなどが想定される。

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

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おいては、想定した品質で稼働することを確認することが求められる。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。このようなソフトウェアの品質が適切に確保されないと、結果として医療の提供に支障が生じるリスクがある（例えば迅速に診断ができないことにより、診断が滞るなど）。

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このような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などについて明示することで、事業者に品質確保を求めるなどが想定される。

なお、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。施行通知の基礎となるe-文書法の精神によれば、画面上での見読性が確保されていることが求められているが、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が求められることもある。品質を満たすかどうかについては、このような観点も考慮することが重要である。

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　［Ⅰ、Ⅲ］

【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おいては、診療録等の個人情報の保護を厳格に行う必要がある。受託する事業者の管理者であっても、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が必要である。

③ 保守を実施する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個人情報にアクセスした場合の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（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し、保守に関する作業計画書と照合するなどにより確認し、当該作業の終了後速やかに企画管理者に報告し、確認を求めること。

⑤ リモートメンテナンス（保守）において、やむを得ず事業者が、ファイルを医療機関等へ送信等を行う場合、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。

⑥ 診療録等を保管している設備に障害が発生した場合等で、やむを得ず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関等に許可を求めなければならない。

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（メンテナンス）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るが、特に障害対応においては、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とがある。この場合、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十分な対策が必要になる。

具体的には、

- 保守要員等からの医療情報の流出・漏洩
- 保守に伴う医療情報システムにおける医療情報の破壊・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

等が想定される。

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必要がある。

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
- 影響確認
- 作業の監督
- 作業報告・確認
- アクセス権限管理
- 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

保守に関する手続きは、原則として事前申請・承認であるが、障害時や緊急を要する脆弱性対応などにおいては、事後承認など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。

１１．システム運用管理（通常時・非常時等）　　[Ⅰ～Ⅳ]

【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。

－ 「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。

－ 非常時機能が通常時に不適切に利用されることがないようにするとともに、もし使用された場合に使用されたことが検知できるよう、適切に管理及び監査すること。

－ 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。

－ 医療情報システムに不正ソフト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。

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

－ 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、その一部は不正ソフト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、非常時において行うべき技術的対応を、通常時から講じることが求められる。

非常時が発生する原因については、

・ 災害
・ サイバー攻撃
・ システム障害（ネットワーク障害含む）

等が想定される。

それぞれの原因により、講じるべき対策が異なるところがあるが、共通することは、システム運用担当者は非常時が生じた際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、非常時を想定した措置について、通常時に訓練を行うなどが挙げられる。

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）
- 非常時用の臨時措置としての情報システム、情報機器

等に対する技術的な対応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を踏まえて、整合性のある内容のものを検討すること求められる。特にサイバー攻撃などの場合、医療情報や、医療情報システムのソフトウェアのバックアップデータには既に不正ソフトウェアが混入による影響が及んでいる可能性が高く、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繰り返し、場合によっては被害を拡大することになりかねない。加えて、ハードウェアについても原因検証のために利用できないなどのリスクもあることから、バックアップの設計や整備に関しては、総合的な観点からリスク評価を行った技術的な対応が求められる。

検討結果については、企画管理者に報告する必要がある。

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 ・追記不能型のデータバックアップの記録媒体の整備 ・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	・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
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

システム運用担当者は、医療情報システムの稼働状況が正常であることを把握するため、医療情報システムのパフォーマンス管理や、死活管理を行うことが必要である。医療情報システムのパフォーマンスが低下した場合やシステムダウンが生じた場合に、速やかにその状況が把握できるようにする必要がある。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も求められる。

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などの対応を行うことが求められる。併せて非常時に講じた措置から、通常時の運用への復旧・復帰の手順なども整備する必要がある。

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不可能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に備え、非常時用ユーザアカウント運用が講じられることがある。非常時用ユーザアカウントを用意し、患者の医療情報へのアクセス制限が医療サービス低下を招かないように配慮するなどのほか、通常時への復旧・復帰後に非常時ユーザアカウントを更新するなどの措置が求められる。

非常時は、通常時とは異なる人の動きが想定される。例えば、災害時は、受付での患者登録を経ないような運用を考慮する等、必要に応じて非常時の運用に対応した機能を実装する必要がある。

非常時への対応機能の用意は、関係者に周知され非常時に適切に用いられる必要があるが、逆にリスクが増える懸念もあるため、運用管理は慎重でなくてはならない。

１２．物理的安全管理措置　［Ⅰ、Ⅲ　なお遵守事項⑤・⑥及び１２．３は、Ⅱ、Ⅳも参照］

【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について、リスク評価を踏まえて、その場所の選定を企画管理者と協働して検討し、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を設置されていることを確認すること。

③ 個人情報が保管されている情報機器等の重要な情報機器には盗難防止を講じること。

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と整合性がとれる措置とし、確保したバックアップは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不能又は不完全な読み取りを防止するため、記録媒体が劣化する前に、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に複写等の情報の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）について、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。特に医療情報を保護するという観点から、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･構造にあるよう考慮するほか、医療情報システムの運用の確保の観点から結露や高温による情報機器等の暴走などが生じないような措置が講じられている環境を選定するなどが求められる。

サーバルームやマシンルームなどのうち、医療情報や医療情報システムが格納されているセキュリティ区域については、サーバルーム等の職員を含め、入退管理がなされており、カメラ等による監視などがなされていることなども考慮に入れる必要がある。

さらに、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については、施錠管理されていることが求められる。

１２．２　バックアップの管理

システム運用担当者は、バックアップについては、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、適切に確保し、非常時に利用できるよう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、方法等を明らかにすることとされているが、非常時に利用できることを想定し、「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、非常時の事象発生原因に応じて行うことが求められる。またサイバー攻撃への対応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」参照。

外部保存で委託を行っている場合には、委託先の事業者に対して、バックアップの対象、バックアップ頻度、復旧できる世代、バックアップ方法、保存場所等について確認し、SLA 等において明らかにすることが求められる。

またシステム運用担当者は、バックアップを含む記録媒体について、記録媒体や、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止するための措置を講じることが求められる。記録媒体の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、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に複写する等の情報の保管措置を講じることが求められる。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行える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、記録媒体の保管場所の特徴等に応じて、定期的に可読に関するチェックを行うことが求められる。併せてシステム運用担当者は、この手順を作成することが求められる。

なお、患者の個人情報の保護等に関する事項は、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、個人情報が存在する限り配慮する必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。

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

記録媒体による外部保存を、可搬媒体を用いて行う場合、委託する医療機関等と受託する事業者はネットワークで結ばれないため、ネットワーク上の脅威に基づくなりすましや盗聴、改ざん等による情報の大量漏洩や大幅な書換え等の危険性は少なくなる可能性がある。

可搬媒体による保存の安全性は、紙やフィルムによる保存の安全性と比べて概ね優れているといえる。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可搬媒体等のパスワードによるアクセス制限が可能な記録媒体を用いればさらに機密性は増す。

しかしながら、可搬媒体の耐久性の経年変化については、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、記録媒体を遺失した際に紛失、漏洩する情報量も多くなるため、より慎重な取扱いが必要である。

そこで、システム運用担当者は、診療録等を可搬媒体に記録して搬送する場合は、可搬媒体の遺失や他の搬送物との混同を防止するために、以下の点に注意する必要がある。

－　診療録等を記録した可搬媒体の遺失防止

運搬用車両を施錠する等、搬送用ケースを封印する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、他の搬送物と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保存を受託する事業者、搬送業者に対して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。

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・参照のおそれがある場合には、クリアスクリーン等の対策を実施することが求められる。

１３．ネットワークに関する安全管理措置　［Ⅰ、Ⅲ］

【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、オープンではない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、採用する通信方式や、採用する認証手段を決めること。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。

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データやソフトウェア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。

⑥ オープンなネットワークにおいて、IPsec による VPN 接続等を利用せず HTTPS を利用する場合、TLS のプロトコルバージョンを TLS1.3 以上に限定した上で、クライアント証明書を利用した TLS クライアント認証を実施すること。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。その際、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 3.0.1 版」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。なお、SSL-VPN は利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと。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。

⑦ 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。

⑧ 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。またネットワークの転送途中で診療録等が改ざんされていないことを保証できるようにすること。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。

⑨ ネットワーク経路でのメッセージ挿入、不正ソフト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。

⑩ 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴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、通信の相手先が正当であることを認識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が、互いに通信目的とする正当な相手かどうかを認識するための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。

－　適切な利用者以外に無線 LAN を利用されないようにすること。例えば、ANY 接続拒否等の対策を実施すること。

－　不正アクセス対策を実施すること。例えば MAC アドレスによるアクセス制限を実施すること。ただし、MAC アドレスは詐称可能であることや、最近のモバイル端末においては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。

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

－　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、医療情報システムにおいて利用するネットワークについて、リスク評価を踏まえて、その選定を企画管理者と協働して検討することが求められる。

医療情報システムで利用するネットワークという場合、その語は多義的であるため、本ガイドラインでは、下図のように整理を行った。ネットワークの安全性を検討する場合には、実際には、ネットワークにおける各レイヤで、対策が講じられることになり、その結果、アクセス先が限定されたり、アクセス先がオープンになったりする。

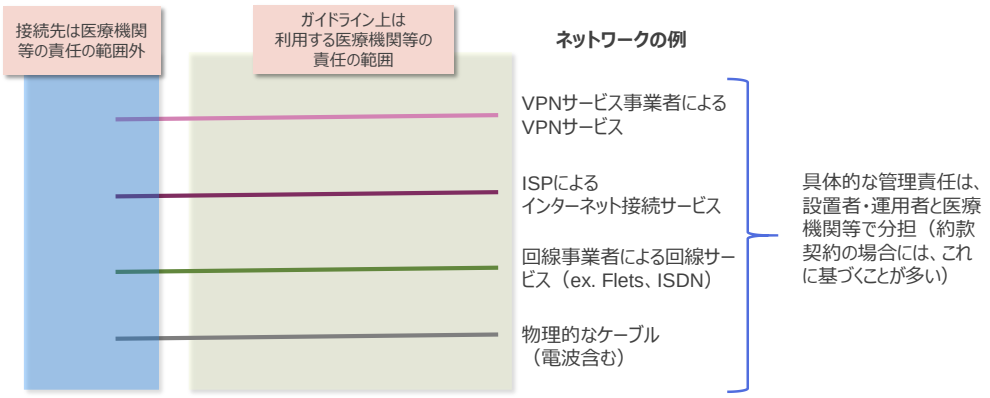


図１２－１　ネットワークの管理に対する考え方

このように回線のレイヤと接続先が限定されているか否かは別であると考えた場合、医療機関等が利用するネットワークの安全性については、その接続先が限定されている、あるいは経路等が管理されているか否かで、考慮するのが妥当であると考える。

図１２－２のように、ネットワークの接続先の限定等は、さまざまな形で実現できるが、いずれの

場合にも、回線の暗号化などを講じることで、リスクの違いはあるものの、従来の境界防御としてのネットワーク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かったりする場合には、いわゆるオープンなネットワークとして位置付けられ、境界防御的な対応は難しい。但しこの場合でも、インターネット VPN のサービスを利用するなどにより、境界防御的な対応を行うことが期待できる。

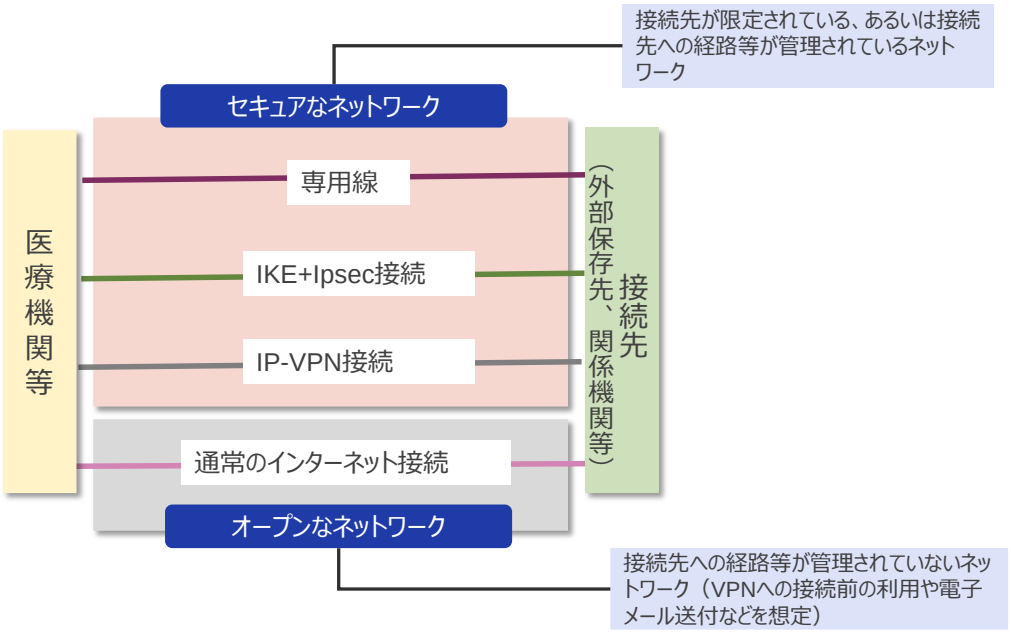


図１２－２　本ガイドラインにおけるネットワークの整理

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」と称することとし、医療情報システムでの利用は、原則として「セキュアなネットワーク」を用いることと整理する。但しオープンなネットワークも、「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用いたり、あるいは電子メールの送信時において、送信するデータ自体を暗号化して送信したりするなどで用いることが想定されるため、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は、医療情報システムの構成に応じて、安全性が確認できるネットワーク機器を利用し、不正な機器が接続したり、不正なデータやソフトウェアが混入したり、異常なデータ通信が発生したりしないよう、セキュアなネットワークを構築し、ネットワークに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の分割、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必要がある。

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、ネットワークの選定に際しては、医療情報の安全管理が確保できるもの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、独占的な回線利用となるため高コストであることや、多目的な利用にはなじみにくいなどがある。

これに対して、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り、いくつかの VPN の実装方法がある。

IP-VPN は、インターネットを用いず、通信事業者が提供するものである。このサービスの場合にも、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。IP-sec 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等があるとされる。

システム運用担当者は、基本的には IP-sec 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等の方針なども踏まえて、適切なものを選択することが求められる。

なお、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オープンではない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こともあり得る。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、チャネル・セキュリティが確実に確保されるようにしておく必要がある。

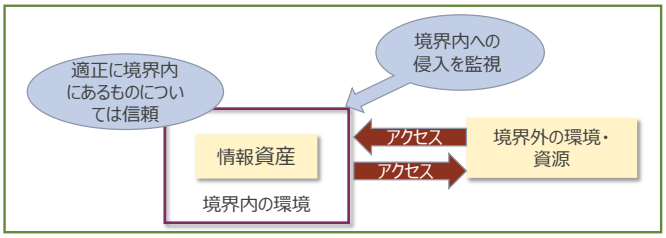
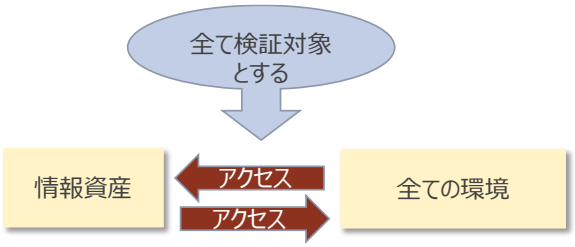
なお、システム運用担当者は医療情報システムが利用するネットワークを選定した際に、ネットワークの管理や非常時の対応など、具体的な技術的な対応に関する内容について、ネットワークを提供する電気通信事業者や、情報システム・サービスを提供する事業者との間での責任分界の範囲を明らかしたうえで、企画管理者に報告することが求められる。

１３．２　不正な通信の検知や遮断、監視

ネットワークの選択においては、オープンではないセキュアなネットワークを選択し、境界防御的な対応を原則とするが、巧妙化するサイバー攻撃に対しては、境界防御的な対応だけでは十分ではない。例えば VPN 装置の脆弱性を攻撃することにより、ランサムウェアによる被害なども見られることから、境界防御だけでサイバー攻撃への対応を図ることは困難と言える。

近年は、境界防御の思考による安全性のみ限らず、すべ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」の概念による考え方も出てきている。ゼロトラスト思考では、利用者の行動も含めてすべて検証し、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などの仕組みで構成される。

表１２－１　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、すべ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。

ゼロトラスト思考の有効性は、認められるものの、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。また医療機関等の場合、接続先が多方面にわたっていない医療機関等が多いことから、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。

但し、境界防御ではサイバー攻撃への対応としては十分ではないことから、境界防御を採用する場合でも、トラフィックの監視等、多層防御の考え方を導入することが、医療機関等においては求められる。

クラッカーや不正ソフト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）などの採用もシステム運用担当者は、検討する必要がある。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）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、「９．２　情報機器等の脆弱性への対策」と併せて実施することが求められる。

さらに、外部からのサイバー攻撃の高度化・多様化に鑑みると、境界防御の対策を行っていたとしても、不正ソフトウェア等の攻撃や侵入があることから、このような場合を想定して、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（「~~9~~8．１　不正ソフトウェア対策」参照）。モニタリングについては、費用対効果を鑑みて、リスクの高いところについて重点的に行うなども考えられる。

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」等の脅威から守られるよう、対策を講じることが求められる。

１３．３．１　ネットワーク回線の暗号化

ネットワーク回線の暗号化については、特にオープンなネットワークを利用する際に求められる。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、システム運用担当者は、医療情報を医療機関等の外部とやり取りする場合には、TLS の設定を適切に行って、通信するための措置を講じ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、偽サーバの接続リスクなども鑑みて、適切な手段を選択することが求められる。

１３．３．２　情報に対する暗号化

システム運用担当者は、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こともあるため、特に留意する必要がある。

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、送信元から送信先に確実に情報を送り届ける必要があり、「送信すべき相手に」、「正しい内容を」、「内容を盗み見されない方法で」送信しなければならない。そのため、システム運用担当者は送信する情報が

- 盗聴されないこと
- 改ざんされないこと
- メッセージ挿入や不正ソフトウェアの混入等や中間者攻撃を受けないこと
- なりすまされた相手先に送信しないこと

等のための措置を講じることが求められる。そのために、ネットワークや機器、サービス等の監視などを行うほか、通信の相手先との相互認証を行うなどの措置を必要に応じて行うなどが求められる。

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、可用性などにも配慮した対策を講じることが求められる。

無線 LAN は無線を用いたネットワークであることから、適切な措置を講じないと本来利用が許されない第三者の利用が生じるほか、侵入者による攻撃などを招くリスクがある。また適切な暗号化を講じないと、盗聴や不正ソフト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。

１４．認証・認可に関する安全管理措置　［Ⅰ～Ⅳ］

【遵守事項】

① 医療機関等で用いる医療情報システムへのアクセスにおいて、利用者の識別・認証を行い、利用者認証方法に関する手順等に関して、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 IC カード等のセキュリティ・デバイスを用いる場合、IC カードの破損等、セキュリティ・デバイスが利用できないときを想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。

④ アクセス管理に関する規程に基づいてアクセス権限を付与する場合、権限の実態が反映できるよう、システム運用担当者に対して、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よう指示すること。

⑤ 利用者認証にパスワードを用いる場合には、令和 9 年度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、新規導入又は更新に際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこと。

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。

－ 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。

－ 医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換によること）した状態で、適切な手法で管理・運用すること。

－ 利用者のパスワードの失念や、パスワード漏洩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、パスワード漏洩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。

－ 医療情報システムの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記載される等があってはならない）。

⑦ 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、定期的に棚卸を行い、不要なものは適宜削除すること等を含む手順を作成すること。

⑧ 電子カルテシステムにおける記録の確定手順の確立と、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。

－ 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仕組みをシステムに備えること。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めること。

b 「記録の確定」を行うに当たり、内容を十分に確認できるようにすること。

c 「記録の確定」は、確定を実施できる権限を持った確定者に実施させること。

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。

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。

－　臨床検査システム、医用画像ファイリングシステム等、特定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。

－　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ようにすること。

－　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ようにすること。

－　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。

－　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

医療情報システムへのアクセスを正当な利用者のみに限定するために、医療情報システムは利用者の識別・認証を行う機能を持たなければならない。システム運用担当者は、リスク分析の結果を踏まえて、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、その運用に必要な具体的な手順の作成を行う必要がある。

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、一般的にこの機能は必須である。

認証を実施するためには、医療情報システムへのアクセスを行う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が行われなければならない。

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。なお利用者認証を ID とパスワードによりには、システム運用担当者は、パスワードが第三者に推定されにくいものとするよう、安全性を考慮した機能仕様とする必要があるほか、システム側でのパスワードの管理については、システム運用担当者でもわからないようにする措置を講じることが求められる。

認証強度の考え方として、現状において、医療情報システムにアクセスする端末ごとに二要素認証を追加実装することは、医療機関等の負担が増加すると考えられる。このような技術は、本来システムにあらかじめ実装されているべきであり、今後、認証に係る技術の端末への実装状況等を考慮し、できるだけ早期に対応することが求められる（※）。

※　二要素認証技術の端末等への実装を促してきたが、さらに強く推し進めるため、令和９年度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が求められる。

また医療情報システムに二要素認証が実装されていないとしても、例えば放射線管理区域や薬局の調剤室など、指定された者以外の者の入室が法令等により制限されるような区画の中に端末が設置されている医療情報システムであって、当該区画への入場に当たって利用者の識別・認証が適切に実施されており、入場時と端末利用時を含め二要素以上（記憶・生体計測・物理媒体のいずれか２つ以上）の認証がなされている場合には、二要素認証に相当すると考えてよい。

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

クラウドサービスなどの普及から、外部のアプリケーションを連携して用いる場面等が多くなってきている。院内のシステムと外部アプリケーションを連携して用いる場合や、複数のクラウドサービスを連携して用いる場合には、アプリケーション間でデータの引き渡しなどを行う必要が生じる。昨今、システム間連携のインタフェースとして、Web 技術のうち、連携のしやすさから、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 ASP 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できるように、必要に応じてネットワークセキュリティを確保し、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を限定し、その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、それに沿った認証・認可に関する仕組みを設ける必要がある

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。また付与する利用権限は必要最小限にすることが重要である。

知る必要のない情報は知らせず、必要のない権限は付与しないことでリスクを低減できる。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を行う機能があれば、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行う必要があるため、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。

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危険性がある。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、意図せぬ設定の変更に関して検知できる措置を講じることが求められる。特に自動的に検知し、運用に反映できることが必要となる。

システム運用担当者は、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が求められる。

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、電子化した文書を支障なく取り扱えることが当然担保されなければならないことに加え、その内容の正確さについても訴訟等における証拠能力を有する程度のレベルを担保することが要求される。誤った診療情報は、患者の生命や身体に関わることであるので、電子化した診療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について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ていなくてはならない。

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である。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、診療録等が書換えや消去されないように、また他の情報との混同が発生しないよう、注意する必要がある。

したがって、システム運用担当者はネットワークを通じて医療機関等の外部に保存する場合は、医療機関等に保管する場合の真正性の確保に加えて、ネットワーク特有のリスクにも留意しなくてはならない。例えば虚偽入力、書換え、消去及び混同を防止するためには、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、運用も含めて対応することが求められる。

また作成の責任の所在を明確にすることも求められる。具体的には入力者及び確定者の識別・認証、記録の確定、識別情報の記録、更新履歴の保管において、対策を講じる必要がある（代行入力を行う場合には、確定者の識別・認証において留意が必要である）。

１５．電子署名、タイムスタンプ　［電子署名を利用するシステムがあれば、Ⅰ～Ⅳ］

【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、これが利用できるよう、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）~~電子署名法~~第 2 条第 1 項を満たす電子署名であることに加えて、署名者の医師等の国家資格の確認が電子的に検証できる電子署名等を用いることなどが求められる。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ることができるよう、技術的な対応を行うことが求められる。

１６．紙媒体等で作成した医療情報の電子化　[紙媒体等で作成した医療情報の電子化をしている場合には、Ⅰ～Ⅳ]

【遵守事項】

① 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、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、スキャンによる電子化で情報が欠落することがないよう、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けられていたり、スキャナ等が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 運用の利便性のために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、以下の措置を講じること。

- 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぐため、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。
- 緊急に閲覧が必要になったときに迅速に対応できるよう、保管している紙媒体等の検索性も必要に応じて維持すること。

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に、医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保する等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などがある場合もある。したがって、一旦紙等の媒体で運用された情報をスキャナ等で電子化することは慎重に行う必要がある。電子情報と紙等の情報が混在することで、運用上著しく障害がある場合等に限定すべきである。その一方で、電子化した上で、元の媒体も保存することは真正性・保存性の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されるべきである。

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

紙等の媒体で扱うことが著しく利便性を欠くためにスキャナ等で電子化するが、紙等の媒体の保存は継続して行う場合、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。しかしながら、個人情報保護上の配慮は同等に行う必要があり、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。

システム運用担当者は、このような観点から、運用の利便性のために電子化をスキャナ等で行う場合に、スキャナや電子化されたファイルに対して、技術的な対応を行うことが求められる。

１７．証跡のレビュー・システム監査　［Ⅰ、Ⅲ］

【遵守事項】

① 利用者のアクセスについて、アクセスログ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 アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を実施すること。

③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。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に、技術的な対応として、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。

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、さらには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効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、アクセスログへのアクセス制限や改ざん防止措置等を行い、アクセスログへの不当な削除／改ざん／追加等を防止する対策を講じることが求められる。

アクセスログの正確性のため、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らなければならない。

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、明確にする必要がある。

なお、医療機関等において取り扱っている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、技術的な対応における部分の内容を作成し、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が求められる。監査結果で指摘された事項については、企画管理者と協議し、改善することも求められる。

１８．外部からの攻撃に対する安全管理措置　［Ⅰ～Ⅳ］

【遵守事項】

① 医療情報システムに対する不正ソフトウェア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洩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（重要なファイルは数世代バックアップを複数の方式（追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等）で確保することが重要である）

１８．１　サイバーセキュリティ対応

システム運用担当者は、サイバー攻撃を受けた等、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必要が生じる場合がある。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する必要がある。

サイバー攻撃への対策については、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、NISC から示されている「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３年度版）」、2021 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」も参照することが求められる。

また、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」も参照することが求められる。

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、診療の継続や早期に業務を再開することが求められる。バックアップに関しては、全ての情報をバックアップから復元するのではなく、ある程度のリスクを許容することで運用が容易になり、確実に対応することが可能になることも多い。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が必要である。

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、ランサムウェア等のようにデータ自体を利用不能にするようなものについてバックアップデータまで被害が拡大することのないよう、バックアップを保存する電磁的記録媒体等の種類、バックアップの周期、世代管理の方法、バックアップデータを保存した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等を考慮して対策を講じることが強く求められる。例えば、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）確保し、遅くとも３世代目以降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、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不正ソフトウェアが混入による影響が及んでいる可能性が高く、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繰り返し、場合によっては被害を拡大することになりかねない。不正ソフトウェア対策を講じつつ復旧するための手順をあらかじめ検討し、BCP として定めておくとともに、サイバー攻撃を想定した対処手順が適切に機能することを訓練等により確認することなども重要である。

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
- 同じ脆弱性を突かれて侵入されない
- 他の脆弱性を突かれない
- 不正に作成されたり、盗まれたりした ID・パスワード等を使われないようにする

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たりしないようにする必要がある。なお専門的な知見に関して、情報処理推進機構が、不正ソフト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を開設している。

【別添】

e-文書法対応に求められる技術的対策（見読性、真正性、保存性）

「医療情報システムの安全管理に関するガイドライン」第 5.2 版第 7 章では、施行通知に基づいて求められる安全管理対策について示している。示されている内容の中には、施行通知で対象となる文書の電子化だけではなく、医療情報システムで取り扱う医療情報全般においても求められると考えられるものを含むことから、本ガイドライン第 6.0 版においては、これらの安全管理対策については分けて記載せず、共通できる内容として記載した。

「医療情報システムの安全管理に関するガイドライン」第 5.2 版第 7 章における安全管理対策につき、本ガイドライン第 6.0 版での記載箇所との対応関係を以下に示す。

1.「見読性」確保のための対策

「医療情報システムの安全管理に関するガイドライン」第 5.2 版では、見読性の確保の安全管理対策について、

- ネットワークを通じて医療機関等の外部に保存する場合
- 医療機関等に保存する場合
- ネットワークを通じて外部に保存する場合

の 3 つのケースについて、それぞれ対応策を整理している。

また、どちらの場合にも対応すべき対策として

- 情報の所在管理
- 見読化手段の管理
- 見読目的に応じた応答時間

等の対策が示されている。

具体的な対策として規定されている内容を以下に示す。

「医療情報システムの安全管理に関するガイドライン」 第 5.2 版の項目 7.2　　C.最低限のガイドライン	本ガイドライン 第 6.0 版での記述箇所
（1）情報の所在管理	4.1
（2）見読化手段の管理	5.1
（3）見読目的に応じた応答時間	9.2
（4）システム障害対策としての冗長性の確保	11.2

２.「真正性」確保のための対策

「医療情報システムの安全管理に関するガイドライン」第 5.2 版では、真正性の確保にかかる安全管理対策について、

- 医療機関等に保存する場合
- ネットワークを通じて医療機関等の外部に保存する場合

の２つのケースについて、それぞれ対応策を整理している。

医療機関等に保存する場合では、さらに、

- 入力者及び確定者の識別及び認証
- 記録の確定手順の確立と、作成責任者の識別情報の記録
- 更新履歴の保管
- 代行操作の承認機能
- 情報機器･ソフトウェアの品質管理

等の対策が示されている。

また、ネットワークを通じて医療機関等の外部に保存する場合については、

- 通信の相手先が正当であることを認識するための相互認証を行うこと
- 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
- リモートログイン機能を制限すること

の 3 点について対策が示されている。

本版との対象関係について、以下に示す。

【医療機関等に保存する場合】

「医療情報システムの安全管理に関するガイドライン」 第 5.2 版の項目 7.1　　C.最低限のガイドライン	本ガイドライン 第 6.0 版での記述箇所
（１）入力者及び確定者識別及び認証	14.3
（２）記録の確定手順の確立と、識別情報の記録	14.3
（３）更新履歴の保管	14.3
（４）代行入力の承認機能	14.3
（５）情報機器･ソフトウェアの品質管理	8.1、8.2、8.4、10.1

【ネットワークを通じて医療機関等の外部に保存する場合】

「医療情報システムの安全管理に関するガイドライン」 第 5.2 版の項目 7.1　　C.最低限のガイドライン	本ガイドライン 第 6.0 版での記述箇所
（１）通信の相手先が正当であることを認識するための 相互認証をおこなうこと	13.2
（２）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	13.3
（３）リモートログイン機能を制限すること	9.2

3.「保存性」確保のための対策

「医療情報システムの安全管理に関するガイドライン」第 5.2 版では、保存性の確保の安全管理対策について、

- 医療機関等に保存する場合
- ネットワークを通じて医療機関等の外部に保存する場合

の 2 つのケースについて、それぞれ対応策を整理している。

医療機関等に保存する場合では、さらに、

- ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止
- 不適切な保管･取扱いによる情報の滅失、破壊の防止
- 記録媒体、設備の劣化による読み取り不能又は不完全な読み取りの防止
- 記録媒体･情報機器･ソフトウェアの整合性不備による復元不能の防止

等の対策が示されている。

具体的な対策として規定されている内容を以下に示す。

【医療機関等に保存する場合】

「医療情報システムの安全管理に関するガイドライン」 第 5.2 版の項目 7.3　　C.最低限のガイドライン	本ガイドライン 第 6.0 版での記述箇所
(1) ウイルスや不適切なソフトウェア等による 情報の破壊及び混同等の防止	8.3
(2) 不適切な保管･取扱いによる情報の滅失、破壊の防止	12.2、18.1
(3) 記録媒体、設備の劣化による読み取り不能 または不完全な読み取りの防止	12.2
(4) 記録媒体･情報機器･ソフトウェアの整合性不備による 復元不能の防止	5.2

【ネットワークを通じて医療機関等の外部に保存する場合】

「医療情報システムの安全管理に関するガイドライン」 第 5.2 版の項目 7.3　　C.最低限のガイドライン	本ガイドライン 第 6.0 版での記述箇所
(1) 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おこなうこと	5.2
(1) ネットワークや外部保存を受託する機関の 設備の劣化対策をおこなうこと	12.2