医療情報システムの安全管理に関するガイドライン

第 6.1 版(案)

システム運用編

[Control]

目次

＜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~~方~~

【遵守事項】

① 法令上求められる医療情報システム~~に関するの~~要件等について、企画管理者の整理指示~~に基づいてそのもと~~、~~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、~~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、~~システム運用~~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~~技術的な~~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~~
  - ~~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

【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~~の利用者を~~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~~のにための必要な~~資料等を整備することが求められる。これらの資料は、常に最新化すること。~~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~~場合にと~~、脆弱性が残存する~~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~~については~~も~~明らかに明示~~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~~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、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~~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は、医療機関でのリスク評価に基づく要求仕様へとの適合性~~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~~を十分に確認し、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、~~の技術的な対応や対外的な説明に関~~して必要な~~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~~の責任分界についてには~~、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、~~を踏まえて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~~の運用等~~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できない~~することができないものも含まれている~~可能性がある。
- ~~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、事業者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~~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~~例えば~~、総務省・経済産業省の定める~~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」（以下「２省ガイドライン」）という）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~~ととされており、その基礎となる内容は同図る際に、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~~その基礎となる~~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。

- ~~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。~~
- 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~~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。~~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~~技術的な対応の~~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~~に関する取り決めを指す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、~~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~~が求められる~~。~~その際、~~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~~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~~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、~~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~~関する~~ついて、~~取り決め~~ることが求められる~~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~~事前に~~取り決めておくこと~~が重要であるが求められる~~。
- ~~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~~な面から、事業者~~にもわからない~~側でしか把握できない内容部分が存在すること~~があり~~えるため、~~。~~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

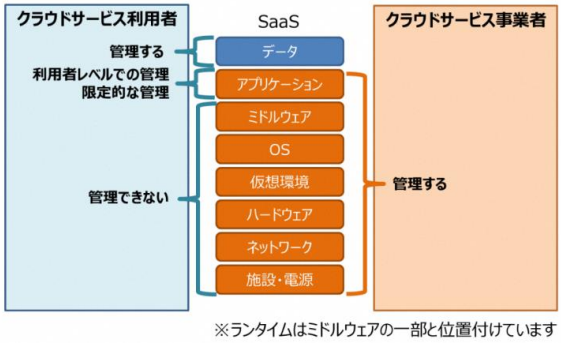
３．４．１　事業者が提供するサービスの類型による責任分界

- 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~~一般的に~~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~~するされることがある~~。
- 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~~が~~を~~サービスとして提供~~され~~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、~~委託により~~医療機関等が行うべき安全管理のうち、明確に~~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



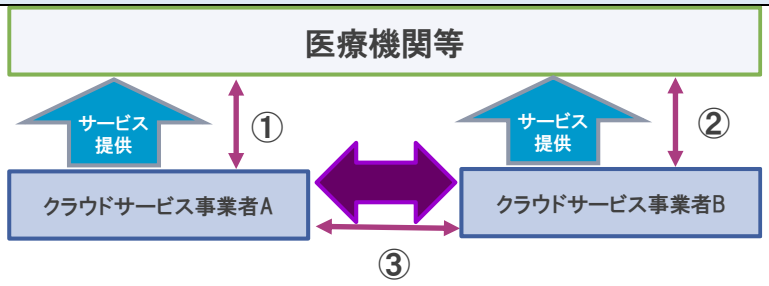
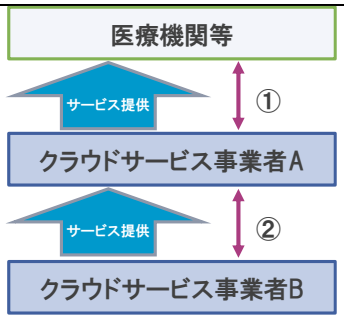
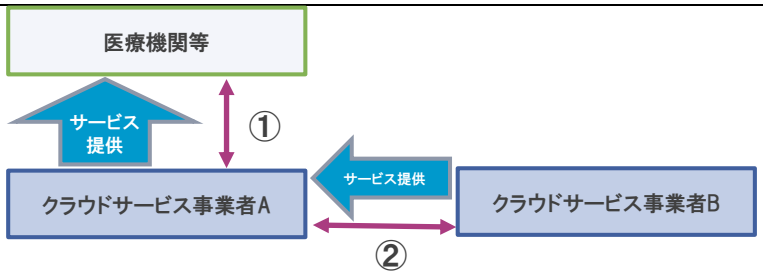
出所：「クラウドサービス提供における 情報セキュリティ対策ガイドライン（第３版）」（総務省、2021 年９月）より作成

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~~の~~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~~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~~対応なども含めて取り決めることが求められる~~役割分担も含まれる。

- 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が一般的である~~に~~なる。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~~に~~なることが多い。~~ので、~~これらの契約関係に留意して~~に従って~~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~~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、下記などが想定される。
  ・メール等による情報の送信
  ・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
  ~~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~~た~~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必要がある。例えば、メール~~による~~送信の場合~~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~~が考えられる。
- ~~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。

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~~に情報が保管されている患者数~~、のどのような~~情報~~の種別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の設定ルール、持ち出し状況など~~を整理すること~~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~~形式形~~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等をなども~~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、~~医療機関等で導入している医療情報システムの~~全体構成図（ネットワーク図、システム構成図等）、各~~医療情報~~システムを構築・導入する~~ためののに必要な~~資料~~やその等の~~管理状況（保管場所、作成時期等）、運用~~において必要な~~上の設定~~に関する~~情報やログ等~~のに関する~~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~~整理する際に、法令により保存などの要件が~~求め~~定められているもの~~について~~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。）~~など~~が求める~~内容に則しているか等が挙げられる~~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、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~~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~~をについて、~~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~~対策を講じる場合には、~~医療機関等ごとの~~組織~~のや~~規模等~~のの~~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~~対応できる~~負担（要員、費用等）

~~など~~を踏まえることも重要である~~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~~が必要だが、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）を有していない場合もある~~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~~よるリスクアセスメント結果を~~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~~想定される。なお、事業者に~~から~~は、~~「サービス仕様適合開示書」~~を提供させる~~の提示を受ける~~ことが想定される。
- 特に専任のシステム担当者~~情報システムの要員~~を要しがい~~ない医療機関等の~~場合には、事業者から安全な医療情報~~システム・サービス~~システムを~~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~~上記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）

【遵守事項】

① ~~①~~ システム更新の際の迅速な移行~~を迅速に行えるようにを可能とするため~~、診療録等のデータについて、原則として標準形式~~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が可能なシステムを選定すること。

② ~~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。~~たシステムを選定すること。

③ ~~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、~~が、その際にも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~~に対応可能な事業者を選定~~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~~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~~の情報~~電子化~~においてはは~~、~~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の業務を~~単に電子化するだけでなく~~効率化し、~~、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~~のを~~軽減等、~~し、~~業務の総量を減ずること~~も求められている~~にもつながる。また紙媒体等~~の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・誤読リスクも低減し~~の防止という観点から~~、医療安全にも資する~~ことにもなる~~。
- 電子化の過程では、~~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電子情報のやりとりを行う~~行う~~際~~のに必要となるのが、~~相互運用性の確保が必要となであ~~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、~~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~~などが挙げられる。
- ~~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~~確保が求められる。
- 医療情報の~~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）を利用することや、~~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~~のために向けて~~、システム~~・ベンダ及び~~サービス事業者に対して~~こういったこと~~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~~を導入しようとするときや~~の導入や~~、現に保有する医療情報システムの~~運用~~に当たって~~に当たっても~~、下記事項~~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

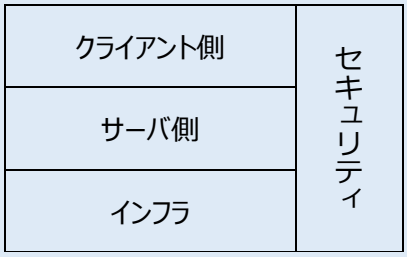
５．２　標準化対応、データ形式・プロトコルの互換性の確保

- 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~~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~~「保存すべき機関期間中において復元可能な状態で保存することができる措置を講じていること」が求められて~~いることから~~おり、~~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~~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~~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~~して把握すべき要素と~~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~~に~~は、~~今日、~~さまざまな形態のものがある。~~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~~を利用する場合~~（~~例えば~~アプリケーションのマクロ機能~~などを使ったりの利用や~~、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~~場合（~~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って~~り異なってくる~~変化~~する~~ことに留意する~~必要があること~~。
- 医療機関等~~の組織によっては、~~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~~とも~~場合もある~~ある~~。この~~場合にはとき~~、技術的な対応に関する内容の多くは、外部~~に~~委託~~するによる~~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、~~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）

【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、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、情報端末が情報漏洩漏えい、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~~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~~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~~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~~を~~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~~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 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。~~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、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~~記録媒体や~~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洩漏えいの可能性の発生含む）が生じた場合~~に、行うべき~~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、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こと。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関する手順も対象となる。
- 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、このパスワード等は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/ようにする旨させないことや、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などもことも有効である重要である。
- 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可能な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、その他のルールがに適合したサービスを利用させること、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、管理していないしたサービス以外の接続ができないようにしたりを遮断する等の技術的な対応を取るりながら、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で盛り込むなどの対応が想定される。
- 漏洩漏えい防止等の観点から、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、行為は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、持ち出しの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要すること等をの手順手続としてを定める必要があること。

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、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

- ~~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アクセスする~~ことを許可することもあり得る。この~~場合、安全管理のため、職員からの接続については、~~
  - 接続できる職員に対関する事前の許可
  - 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~~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。~~
- 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

  ~~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~~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 ~~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~~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~~てたうえで~~、十分なチャネル・セキュリティ~~を~~が確実に確保~~される措置を講じるする~~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~~により支給された端末を使うことが想定される。~~一方で、が、~~医療機関等によっては、「~~９~~９．ソフトウェア・サービスに対する要求事項~~．ソフトウェア・サービスに対する要求事項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）~~を~~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（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~~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~~内容~~が確実に実施されていること~~の実施状況を~~説確認明~~するためには、~~適切な~~運用の点検と監査が必要である~~が、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、~~極端な場合は~~不特定多数の人間~~大~~が使用する PC の場合~~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、~~の想定と異なる環境で使用~~していればされ、想定外の~~安全管理影響を受ける~~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、仮想デスクトップ等を利用する等の運用~~の~~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~~こと~~。~~その他これ以外には~~、ユーザ権限を厳格に管理した専用端末の貸与等~~も~~が考えられる。

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~~む中み~~、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、~~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、医療情報の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~~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の対応~~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ことも選択肢となる~~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~~のに関する証明や~~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~~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~~って削除する~~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~~することで、その他の情報が利用不~~可~~能となるリスクがあることに~~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~~、システム運用担当者は、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~~の確認をすることで~~を~~確認して、~~破棄の状況を確認~~把握~~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~~手順等を作成する必要があること~~が求められる~~。紛失や盗難に関する報告を受けた場合には、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~~へ~~の接続防止等~~の対応~~が想定される~~~~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~~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~~~~した~~際に~~は~~、設定のミスなどによる~~り~~漏洩漏えいのリスク~~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

【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 ~~②~~ 常時マルウェアの混入を防ぐ適切な措置を実施し、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、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。

⑤ ~~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等の送受信の禁止、~~若しくは、又はその~~実行の停止~~の実施~~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 。

⑥ ~~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。~~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。~~

⑦~~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~~のファームウェア等~~に関する~~の脆弱性~~が発見されることがある。~~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、~~IoT 機器の~~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~~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。~~しないこと。

⑧~~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。

⑨~~⑧~~ BYOD の運用~~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。

⑩~~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　マルウェア対策

- 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~~入~~る可能性がある。マルウェアが侵入すると、~~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、情報の漏洩漏えいや改ざん、~~、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。~~またマルウェアの侵入は、何らかの問題が発生して初めて気付くことが多い。~~
- 対策としてはマル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、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~~が求められる~~。
- ~~これらの~~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、~~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~~必要があること~~。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、~~による医療情報システムへの影響を調査しておく等に関する情報を収集することも~~求められる~~必要である。
- また、マルウェア対策~~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、全てのマルウェアが検出できるわけではない。~~マル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~~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、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~~や~~「振る舞い検知」~~などの方策~~も有効な方策である。~~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~~に、網羅性に~~ついて、事前に十分~~な~~検討~~することが必要である~~。
- ~~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り、~~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

- システム運用担当者は、~~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~~ある。
- 近年の~~サイバー~~攻撃~~では、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 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、~~を~~攻撃~~して、外部から攻撃するなどがを受ける事案が~~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ランサムウェア攻撃~~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、定期的に脆弱性スキャンを行うほか、脆弱性に関する~~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~~に関する脆弱性情報は、OS やマルウェア対策ソフト~~ウェア~~を提供する事業者などが提供している~~ほか、~~。また、重大な脆弱性情報は~~重要なセキュリティ関する情報は、~~「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、~~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~~契約事業者に対応を確認するなどして、最新の情報~~を~~の入手~~を図ることが重要であるすること~~。
- ~~また~~利用するソフトウェアについて、~~（~~（Software Bill of Materials：ソフトウェア部品表）が~~医療情報システム等提供~~事業者から提供されることもある。~~医療機関等の~~システム運用担当者は~~これにより~~ SBOM を用いることで、~~システムの~~脆弱性を~~適切効果的~~に管理し、~~医療情報システム及びこれに接続されるシステムに対して識別された脆弱性の潜在的影響を理解し、医療情報システムの~~安全性及び~~性能~~可用性を~~維持するために対応することが可能となる脅かすリスクを低減できる~~。~~そこで~~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~~得ることを、~~医療情報システ

ム等提供事業者に求めることも重要である[1]。

- 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必要があるが、。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、代替策を講じる必要があること。
- 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。また医療機器が EOoS を迎えたとなった場合の対応等に関する管理者については、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なるため、と医療情報システム安全管理責任者等のシステム運用担当者は、医療機器安全管理責任者とが十分に連携を取りながら管理することを図ることが求められる。
- 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おり、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」（昭和 35 年 8 月 10 日法律第 145 号）[2]においてそ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をの稼働させは行わない、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り得え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）時間帯を含めそには医療情報システムのを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、システム運用担当者は、業務での必要性や利便性などをと勘案して、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の上して、適切な設定を行うことが求められる。

---

[1] 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。

[2] 昭和 35 年 8 月 10 日法律第 145 号

[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」

８．４　情報機器等の棚卸

- システム運用担当者は、~~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~~により~~で、~~医療情報を格納した~~情報機器の~~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、~~り、情報の~~紛失、漏洩漏えい等のリスク~~可能性~~を効率的に発見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~~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~~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 ~~においてはを~~許可する場合は、上記の要件を実現するため~~に~~、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 ~~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する。~~し、~~さらに個人でその設定を変更できないよう制御~~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~~する。
- ~~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~~マルウェアや不適切な設定~~がな~~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~~が発生することも想定されるため~~考えられるため~~、管理されていない端末での BYOD ~~は行わないは~~許可してはならない。また、BYOD の導入に際して、管理者~~はが 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

【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 ~~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、~~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情報を速やかに検索表示、又は~~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~~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の直接管理する~~を直接行う~~ことが求められる。ソフトウェアの構成がを適切に~~行わないと~~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~~残存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、事業者に確認すること。~~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~~計画のが策定~~され~~、実施がなされていることを~~されていることを~~確認することが~~が求められる~~重要である。
- クラウドサービス~~など~~の場合は特に~~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困難であ~~。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

- ~~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~~は、想定した品質で稼働することのを確認が必要である~~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。安定的な医療の提供のため、このような~~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）。~~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~~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。~~なお移行時においては、機能面での品質管理のほか、~~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。~~できること、~~利用者権限をはじめ、各種設定が移行前~~のに~~設定~~したもの~~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が~~が求められる~~。

- 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、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~~が求められることもある。~~も必要となる。~~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．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~~おいては~~対しては、~~診療録等の~~個人情報の保護を厳格に~~行う~~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~~が必要である~~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~~を実施する~~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~~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、~~し、~~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~~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。

⑥ ~~㋅~~ リモートメンテナンスにおいて、事業者がやむを得ず~~事業者が、~~ファイルを医療機関等へ送信~~等を行う~~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 ~~㋆~~ ~~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、~~事業者がやむを得ず診療録等~~にアクセスを~~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における診療録等の個人情報と同様の~~と同等の秘密保持を行~~うと同時に~~うこと、~~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り、~~るが、特に~~障害対応~~において時~~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~~するすることがある~~。この~~際場合~~、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、下記が想定される。
  - 保守要員等からの医療情報の流出・漏洩漏えい
  - 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
- ~~影響確認~~
- 作業の監督
- ~~作業~~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~~関する手続き~~は、原則として事前申請・承認が必要だ~~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。

➢ 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~~の採用においては~~、業務効率~~を高めることが~~化が期待されるものの~~、物理的なアクセスをへないで、外部と内部ネットワークを接続するため~~、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~~脅威にさらされやすく~~の起点となり得る。~~、機密性・完全性・可用性を損なうリスクの顕在化が指摘される。~~

➢ 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~~については~~は、医療情報システム全体に共通する~~としても想定される~~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~~が求められる~~。

➢ ~~そのうえで~~また、リモートメンテナンス~~においては~~では、システムの管理者権限を要用する場合があり、~~いられることから~~高いリスク~~が認められるを~~伴うことから、下記の対策を行うこと~~が求められる~~。

表~~－~~１０~~－－－~~１　~~１~~リモートメンテナンスにおいて実施すべき事項

~~リモートメンテナンスで~~想定されるリスク	~~リモートメンテナンスにおいて~~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（なお「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 によ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[6]	・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）

[6] 医療機関等は、事業者がリモートメンテナンスをする場合には、適時、実施状況を確認することが求められる。事業者が行うリモートメンテナンスについては、「リモートサービスセキュリティガイドライン」が一般社団法人保健医療福祉情報システム工業会(JAHIS)より示されているので、上記の確認において参考となる。なお、同ガイドラインは適宜改定しているため、最新の版を参照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）

【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がないように管理するとともに、もし使用された場合に使用されたことがは検知できるよう、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／物理的に構成分割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 一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~~において行うべきを~~想定した技術的対応を、~~通常時から~~講じることが求められる。
- 非常時~~が発生すの~~る原因としては~~については~~、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~~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~~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、~~に整合~~性のある~~する内容~~のものを検討することが求められる~~とすること。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マルウェアの混入による影響が及んでいる可能性もが高く、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、場合によってはす、~~被害を拡大する等のことになりかねないリスクもある。~~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、~~総合的な観点からのリスク評価を踏まえてを行った~~技術的な検討を行い、結果を企画管理者に報告すること。~~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。~~い、~~~~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~~が~~ダウン~~したが生じた~~場合に、速やかに~~その状況が~~把握~~可能な状態と~~~~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~~。
- 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~~の~~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~~の作業を行う~~を実施することが求められる~~が、~~。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~~が求められる~~。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~~などの対応を行う~~ことが求められる。併せて~~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~~不可能~~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~~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~~アカウントの運用によりを用意し~~、~~患者の~~医療情報の利用を円滑化し、~~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~~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~~が求められる~~を行うこと。
- ~~非常時は、通常時とは異なる人の動き~~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~~がを考慮する等~~考えられ、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。一方で

[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が最小限となるよう、例えば影響の少ないセグメント~~にのみ~~から順にパッチを適用し、稼働を確認する等の対応が考えられる。

- 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、~~逆にリスクを増加~~させ~~が~~増え~~る懸念もあるため、~~~~運用管理は~~慎重に管理すること~~でなくてはならない~~。

１２．物理的安全管理措置

【遵守事項】

① ~~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~~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。

~~①~~ ~~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~~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は~~、持ち込まれる物品の確認・制限を実施すること。

~~④~~③ ~~④~~ 個人情報~~が保管されているの~~保管等、~~情報機器等の~~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 ~~⑤~~ 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~~に基づくと整合性がとれる~~措置~~を実施と~~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 ~~⑥~~ 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~~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、~~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~~への複写を実施する等、適切な保管措置を講じること。

⑥ ~~⑦~~ 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~~にて~~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~~するリスク等にも留意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~~などが求められること~~。
- サーバルーム~~やマシンルームなどのうち、医療情報や~~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~~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~~こともことなども考慮に入れる~~必要~~で~~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~~は、施錠管理~~することされていることが求められる~~。
- ~~また~~サーバルーム~~等のセキュリティ境界へやマシンルームへ~~持ち込む~~物品を確認・ものを適宜~~制限~~し、確認~~すること必要がある~~。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~~ためである~~。
-

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

切にバックアップを確保し、非常時に利用できるよう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、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」を参照すること。

- バックアップの外部保存をで委託を行っている場合にはしている場合は、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、保存場所等をについて確認し、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、媒体そのものや記録媒体や、設備等の劣化によってる情報の読み取りが不能又は不完全な読み取りとなることを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可能な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、定期的に可読性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、また、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、バックアップ情報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運用体制水準が求められる。
- 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漏えいや大幅な書換え等のリスク危険性は少なくなる可能性がある低減される。
- 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媒体では、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により、さらに機密性は増す。しかしながら、一方で、可搬媒体にはの耐久性の低い製品も存在し、の経年変化等に対してについては、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、記録媒体を遺失遺失した際に紛失、漏洩する情報量も多くなるため、リスクに対してより慎重な対応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や遺失を防止するために、以下の点に注意する必要があること。
  － 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、や搬送用ケースの施錠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、受託事業者（搬送事業者等を含む）に個人情報を取り扱わせる場合、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。

➢ 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・参照のおそれがある場合にはを防止するため、自動での画面ロックアウト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

【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、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。

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 を利用接続する場合、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、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。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[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。

⑦⑦ 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 IP-VPN か IPsec＋IKE によること。やむを得ず SSL-VPN は利用する場合、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、適切な手法の選択及び必要な対策を行う「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。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。

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 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。

⑫ 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] 独立行政法人情報処理推進機構より公表。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。

⑬ 医療機関等がネットワークを通じて通信を行う際には、~~通信の相手先が~~正当な通信の相手であることを認識~~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~~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と~~の間でも同様に相互認証機能を設けること。

⑭ 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~~以外に~~無線 LAN ~~を利用されないようにする~~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 ~~MAC アドレスや~~ IP 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 アドレスについては、~~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、WPA~~3~~3 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、~~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利用するネットワークを選定すること。~~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~~場合際~~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~~ると想定される。

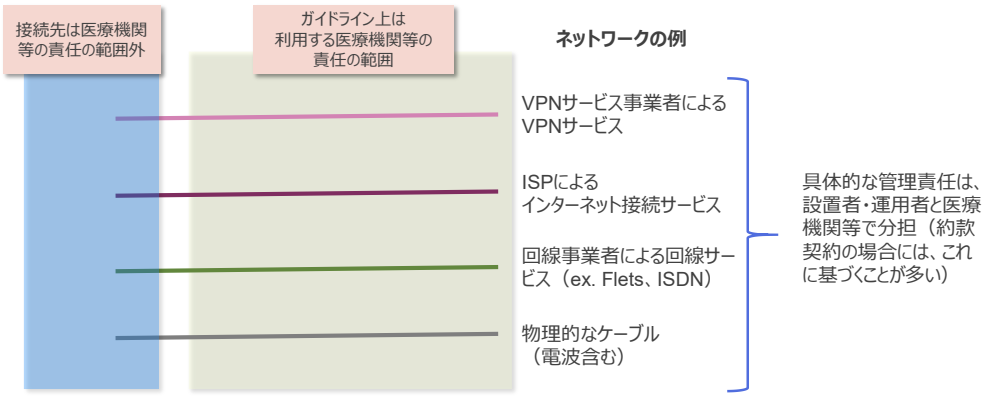


図１２－１ ネットワークの管理に対する考え方

- ~~このように~~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~~た場合~~る。このとき、~~、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、~~は、「~~その~~接続先が限定されているか~~されている~~」、~~と「あるいは~~経路が等が管理されているか~~されているか否かで~~」、~~を~~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。リスクの違いはあるものの、~~が、いずれの場合にも、~~回線の暗号化~~など~~を講じることで、いずれの場合にも、~~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い場合には、いわゆる「オープンなネットワーク」としてに位置付けられ、境界防御的な対応は難しいる。但しこの場合でも、インターネット VPN 等のサービスを利用することでなどにより、境界防御に近い対応が可能である。的な対応を行うことが期待できる。

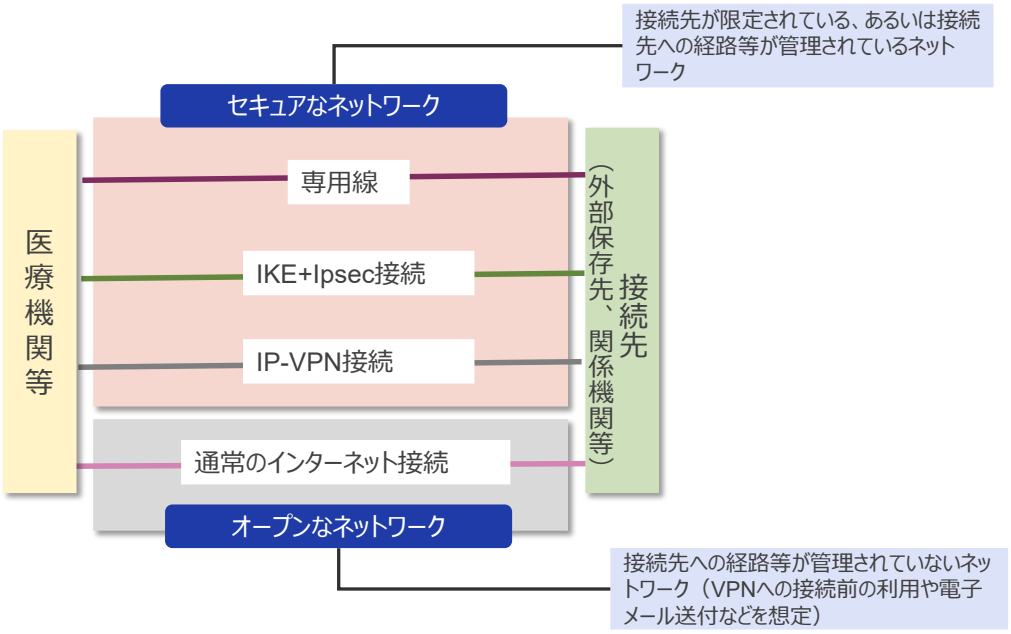


図１２－２　本ガイドラインにおけるネットワークの整理

- 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「オープンなネットワーク」を用いたり、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、不正な機器の接続、が接続したり、不正なデータやソフトウェア等のが混入したり、異常なデータ通信が発生したりしないようを防止するため、、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こと。
- ネットワーク構築にあたり、ネットワークで使用する IP アドレスの割当の規格として IPvV6（Internet Protocol Version 6）の採用が進んでいる。IPvV6 6 の採用は以下透明性、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も有効な期待方策とされる。、
  - 透明性：NAT による隠蔽がなくなり、通信ログから直接端末を特定可能
  - 完全性：プロトコルレベルで認証・暗号化（IPsec）の仕組みを組み込み
  - 可用性：広大なアドレスにより、アドレス競合の防止
  - 管理性：自動設定機能により、ネットワーク管理の負担と設定ミスの減少

一方で、IPv~~v~~6 の採用に伴い、新しい機能に関連する脆弱性（~~例えば~~拡張ヘッダーの複雑な設定に伴う攻撃パケットの透過、~~や~~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、IPv~~v~~6~~4~~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~~ある~~。~~ため、そのため、~~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~~が求められる~~。

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ネットワーク~~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~~というデメリットもある。
- ~~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、~~る。VPN にはいくつかの ~~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。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。~~なお、VPN 機器への脆弱性対策として、クラウド型の VPN の採用や、自動アップデートを行うことが望ましい。~~
- ~~システム運用担当者は、~~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~~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~~。

表１３－１　ネットワークの安全性

ネットワーク				安全性
専用線				高
IP-VPN				高
インターネット	インターネット VPN	IPsec ＋ IKE		高
		SSL-VPN	クライアント型	高
			その他	低
	オープンなネットワーク	TLS1.3 ＋ クライアント証明書		高
		TLS1.2 (高セキュリティ型)＋クライアント証明書		高

- ~~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~~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~~をが確実に~~確保~~されるようにしておく必要がある~~すること。
- ~~なお~~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~~であると~~と解釈~~することが可能である~~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、医療機関等は、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~~、事前のリスク評価に基づ~~

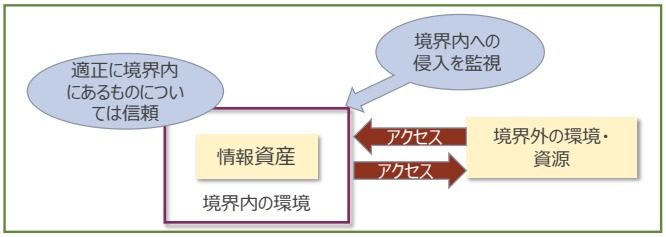
いて確認すること。また、し、システム関連事業者からサービス仕様適合開示書などの必要な情報提供を受けて、責任分界を含めた具体的な運用を取り決めることが求められる。

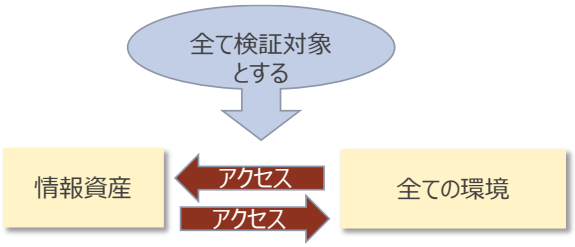
- なお、VPN 機器への脆弱性対策として、クラウド型 VPN の採用や、自動アップデートに対応した製品を選定することが望ましい。
- 医療機関等がクラウドサービスを利用する場合、事業者との間の通信経路が暗号化されていれば、当該経路の盗聴のリスクは小さい。TLS の設定を適切に行い、TLS クライアント証明書による認証を受けることにより通信経路のセキュリティは確保されるが、クラウドサービス事業者内部での通信について、十分な安全性は保証されない。医療機関等は、クラウドサービス事業者内部で用いるの通信について、暗号化等十分な安全性を講じているることを求めること。
- 医療機関等が管理する医療情報システムに対して、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、医療機関等の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、そ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にしたうえで、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

- 医療分野ではネットワークの選択においては、セキュアなネットワークを選択し、境界防御を想定した的な対応が一般的である。一方で、を原則とするが、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により、組織内の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だけでは十分なセキュリティ対策の実施は困難になりつつある。例えば VPN 装置による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や、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るこも指摘されているていたことで、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のみに限らず、すべて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などの仕組み等で構成される。

表１３２－２１　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~~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。

- ~~ゼロトラスト思考は、ゼロトラスト思考の有効性は、下記の観点から有効性が確認されている。~~
  - ~~・多様な業務環境への適用~~
  - ~~・複数の情報を用いたアクセス制御~~
  - ~~・アクセス制御に関する観測情報の拡大~~
  - ~~・連携する外部システムの拡大~~
  - ~~・アクセス制御機能における評価と施行を分離~~
- 例えば振る舞い検知機能~~など~~により、利用者のアクセス~~に関する行動~~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~~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、多層防御による対策が必要である~~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~~。
- 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~~の~~採用~~もシステム運用担当者は、検討することが考えられる必要がある~~。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、マル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（「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~~ところについて~~重点的に実施することも想定される~~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、~~に対して適切な対策を講じること~~が求められる~~。

１３．３．１　ネットワーク回線の暗号化

- 特に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、通信するための措置を講じ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、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には、医療機関等と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、クラウドサービスを用いる際に医療情報を取扱う場合でも、当該経路の盗聴のリスクは小さい。よって、TLS の設定を適切に行い、TLS クライアント証明書等（クライアント証明書を用いる場合は、2026 年以降のパブリック認証局による制限に留意し、プライベート認証局（プライベート PKI）の利用を検討すること）[9]に等による認証を受けることにより医療機関等とクラウドサービス事業者の間で、必要な暗号化がなされるものと考えられる。但しこの場合でも、クラウドサービス事業者内部での通信は暗号化については、十分な安全性が確保されてされないないため、医療機関等は、クラウドサービス事業者内部で用いる通信についても十分な安全性対策を講じていることを求めること[10]。
- 医療機関等が管理する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、訪問看護などの必要により接続する場合）には、医療機関等の内部のネットワークにおける盗聴の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。そのため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が求められる。このとき、なおこのような場合には、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必要があること。

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、リスクに特に留意すること必要がある。

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るあり、。「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。
  - 盗聴されないこと
  - 改ざんされないこと
  - なりすまし
  - メッセージ挿入やマル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

  措置としては、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

---

[9] 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も利用する場合には、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。

[10] 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。

~~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~~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~~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~~に利用されるが生じるほか~~、侵入者による攻撃~~を受ける等など招く~~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~~漏洩~~漏えい~~解読~~リスクを~~避ける~~低減するため、安全な方法による~~り~~暗号~~化キー~~鍵の~~が~~管理提供されること~~が求められる。WPA2-PSK など事前入手方式~~の場合に~~は、利用者が同一の~~同じ~~暗号鍵~~化キー~~を~~利用することになり~~共有することで、鍵が~~漏洩~~漏えいする~~解読~~リスクが~~あることから、高いため、利用を避ける~~避ける~~こと~~が求められる~~。
- ~~―~~

１４．認証・認可に関する安全管理措置

【遵守事項】

① ~~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~~アクセスする際には、利用者の識別・認証を行~~う~~こと。また、~~い、~~利用者認証方法に関する手順等~~に関しては~~、規則、マニュアル等で文書化すること。

② ~~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~~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（例：IC カード）等を用いる場合、セキュリティ・デバイス等 ~~IC カード~~の破損等~~、セキュリティ・デバイス等が利用できないとき~~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 ~~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（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~~所定の~~医療情報システムを、今後、新規導入又は更新するに際しては、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。なお技術的な理由等により令和９年度までの~~、これによれない~~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~~し、~~パスワード等一要素のみの利用者認証を用いることができ~~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 のログイン時に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。

(4) 利用者のパスワードの失念や、パスワード漏洩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、パスワード漏洩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) ~~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~~できなくなる~~不能となる仕組みを講じること。

⑦ ~~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等を含む~~手順を作成すること。

⑧ ~~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。~~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~~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ようにすること。

(c) 「記録の確定」をは、確定を実施できる権限を持った確定利用者者に実施させること限定する。

(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を実施するとともにと、原状回復のための手順を検討することしておくこと。

(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、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。

(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ようにすること。

(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ようにすること。

(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

- 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そ、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、その運用に必要なの具体的な手順の作成を行う必要があること。
- 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、一般的にこの機能は必須である同様である。
- 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が行われなければならないこと。
- 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。なお利用者認証を 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、パスワードが第三者に推定され

~~にくいものとするよう~~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~~必要があるほか、シ~~こと。~~ステム側でのパスワードの管理については、~~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~~でも~~わからないようにする~~ような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。~~

➢ 本ガイドラインでは令和３年度より二要素認証技術の~~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(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~~が求められる~~。

➢ 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~~を対象とする~~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~~ため~~ことで、~~医療機関等のシステムにおいて~~二要素認証が実装~~されていない可能性~~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~~する~~場合には、~~可能な限り、~~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。~~が、システム導入計画等の関係で~~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	不要	不要
サーバ	不要	不要	要

➢ 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、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（Endpoint Detection and Response）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ふるま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

➢

➢ また、医療情報を格納するサーバについても、すでにネットワーク接続管理や端末管理等による安全性確保対策を実施していると考えられるが、巧妙化する不正接続対策の観点から、原則として二要素認証を求める。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。

- 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。二要素認証が技術的に採用できない場合には、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）と併せて対策を講じることが必要である。「二要素認証を採用してい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、英数字のが混在する形で（大文字小文字は問わない）を要する求める。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、新規導入までの間を経過措置期間とする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。

➢ 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、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等が多くなってきて増えている。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、この時、アプリケーション間でデータがの引き渡されることが想定される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 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~~できるようにする措置を講じること。、必要に応じて~~ネットワークセキュリティ~~の~~を確保~~やし~~、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~~の~~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~~で、~~それに沿ったの~~認証・認可~~に関する仕組みを設ける必要があるの~~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~~利用~~権限は必要最小限~~と~~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、~~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~~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。
- 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。~~このような場合には、~~利用者に~~端末に~~対する過度の権限~~を与えることになることから~~付与を避けるため、このような~~設計の~~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~~危険性~~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情報が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~~に関しそ~~を検知できる~~よう~~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~~重要である。
- ~~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、電子化した文書を利用可能であることの~~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~~いて証拠能力を有する~~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~~に関わる可能性もあり、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~~についてそ~~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~~なければそれなくては~~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~~が書換えや消去されないように、また他の情報との~~に改ざんや混同が発生しないよう、~~注意する~~措置を講じる必要がある。~~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~~考慮したうえで対応すること~~が求められる~~。

- 作成~~の~~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~~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。（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。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

【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）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~~。
- なお共通鍵、秘密鍵を格納する機器、媒体については、FIPS140-3~~2~~レベル 1 相当以上の対応を図ること~~が求められる~~。

１６．紙媒体等で作成した医療情報の電子化

【遵守事項】

① ~~①~~ 紙媒体等で作成した医療情報を電子化する際には~~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~~いている等、~~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 ~~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、~~一緊急に閲覧が~~必要~~になったときに迅速に~~時に閲覧~~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~~にも留意して保管維持~~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は~~、スキャン~~による情報量の低下を防ぎ、後も~~保存義務を満たす文書情報として必要な情報量を確保する~~ため等~~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~~も存在し得~~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ため、~~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~~後に、元の紙~~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~~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

- ~~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~~スキャナ等による電子化~~後も~~するが、紙等の媒体の保存~~をは~~継続~~して行う~~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。~~しかしながら、一方で、~~個人情報保護上の配慮は同等に行う必要があ~~り、~~る。また~~スキャナ等による電子化の際に医療に関する~~業務等に差し支えない精度の確保も必要である。
- ~~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

【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 ~~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 ~~③~~ ~~アクセス~~ログの記録に用いる時刻に情報は、信頼できる~~もの~~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~~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用~~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~~ログの正確性を保つ~~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~~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~~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~~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、改善に向けた対応を行う~~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

【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洩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（~~（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）~~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しておく~~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、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３年度版）~~」（令和７年７月１日サイバーセキュリティ戦略本部決定）[11]、~~2021~~ 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~~が求められる~~。
- JPCERT/CC と IPA が提供する MyJVN[12]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することが望ましい。
- ~~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、診療の継続や早期復旧~~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

[11] 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。

[12] https://jvndb.jvn.jp/apis/myjvn/

データ~~を保存したの~~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~~等を考慮して対策を講じること~~が強く求められる。また、~~例えば、~~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~~確保持保~~し、少なくとも~~遅くとも~~ 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~~すべて~~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
  - ・HDD（Hard Disk Drive）
  - ・RDX（Removable Disk Exchange system）
  - ・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が混入によるの影響が及んでいる可能性が高くあり、不用意にバックアップデータから復旧することでと被害を繰り返し、場合によっては被害を拡大するすことになりかねないる。マル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 として定めておくこと（システム的な観点で見ると、電子カルテシステムが長期間にわたり停止した場合に、医療法（昭和 23 年法律第 205 号）第 24 条に定める診療録の作成をどうするのかへの対応を整理する等）とともに。また、サイバー攻撃を想定した対処手順が適切にBCP が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
  - 利用された脆弱性に対処する同じ脆弱性を突かれて侵入されない
  - 他にリスクとなるの脆弱性を突かれないがないか十分に検証、対応する
  - 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たりしないようにする必要がある対処すること。なお専門的な知見に関して、情報処理推進機構 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[13]を開設している。

[13] サイバーセキュリティ 相談・届出窓口 （IPA）

【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 6.1 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

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。

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 6.1 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 6.1 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 6.1 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 6.1 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 6.1 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~~
~~(2) 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~~