医療機関における
サイバーセキュリティ対策
チェックリストの実践ガイド

公益社団法人 日本医師会

2024年9月発行

はじめに

医療機関の経営者の皆様へ

医療機関等に対するサイバー攻撃は年々増加傾向にあり、その脅威が急激に高まっています。
医療機関等がサイバー攻撃の被害を受けてしまうと、医療提供体制の継続が困難となるばかりでなく、原因や被害範囲の調査、情報漏えいの被害者対応等、その影響は計り知れないほど甚大なものとなります。
医療機関等の皆様が医療情報システムに対してサイバーセキュリティ対策を講じることによって、多発する**サイバー攻撃の被害の発生可能性を低減**させることができ、これら一連の**トラブルから自組織を守る**という大きなメリットがあります。
※医療機関等の定義はP5をご参照ください。

医療機関等の皆様がサイバーセキュリティ対策に取り組んでいただく際の参考資料として、厚生労働省が策定している**「医療情報システムの安全管理に関するガイドライン」**(以下「ガイドライン」という)と、ガイドラインから必要最低限の項目を抽出した**「医療機関におけるサイバーセキュリティ対策チェックリスト」**(以下「チェックリスト」という)があります。
ガイドライン及びチェックリストは、医療情報システムを安全に管理していくために必要な事項が記載されています。医療法に基づく立入検査の際には、本チェックリストを用いて、医療機関等の皆様の**サイバーセキュリティ対策状況の確認**が行われます。
※医療情報システムの定義はP5をご参照ください。医療情報システムはネットワークに接続されていないものであっても、ガイドライン及びチェックリストの対象となります。

ガイドライン及びチェックリストを用いてサイバーセキュリティ対策を講じていただくことは、医療提供体制の継続に大きく寄与するものですが、一方でこれらの内容を理解し実行していくことは、医療機関の皆様にとって大きな負担となるのも事実かと思います。
そのような医療機関等の皆様へのご支援策として、日本医師会では、医療機関等の皆様がチェックリストを用いた確認を効率的に実施いただくための解説資料を作成することにしました。本資料では、チェックリストで求められている項目を中心に、実践的に取り組んでいただけるよう具体的にわかりやすく記載するよう努めました。

厚生労働省が作成した「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル」もご参照の上、積極的にご活用ください。

目次

サイバーセキュリティ対策チェック!

すべての項目に ☑ は付きますか?

※立ち入り検査の際は、この目次ではなく、正規のチェックリストをご使用ください。チェックリストはP43のリンクから入手が可能です。

実践ガイドの読み方

チェックリストのチェック項目を記載しています。

チェック項目で具体的に何を実施すべきか等の実施内容を説明しています。

具体的な実施手順を説明しています。

2 医療情報システムの管理・運用

4 サーバ・端末PCについて、利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。

アクセスコントロールの実施

実施すること

ガイドライン企画管理編13④、13.1.3

- 医療情報へのアクセス権は、担当者の業務や役職に応じたものになるように**アクセス権管理**を行います。
- 各担当者に個別のアクセスを発行し、誰にどのアクセスを発行したのかを**台帳管理**します。
- ユーザアカウントの認証*1を導入し、**なりすましや不正侵入対策**を行います。

手順

STEP 1 医療情報システムについて、職種や業務内容に応じてどの担当者がどのシステムへアクセスする必要があるのかを**整理**します。

STEP 2 システムへアクセスする必要がある担当者にそれぞれ、個別に**アカウントを発行**します。
※どの担当者にどのシステムのアカウントを付与したのかは**利用者アカウント台帳等で管理**します。

STEP 3 ユーザアカウントの**認証は必須**とし、どの担当者がそのシステムを操作したのかを特定できるようにします。

※各システムのアカウント発行方法や認証機能の設定方法等は、システムを導入した事業者等に確認します。
※認証をIDとパスワード(PW)の組み合わせて行う場合は、**PWは必ず本人しか知りえないように保管**します。
※**多要素認証*2機能**を導入することも効果的です。
※人事異動等により役職や業務内容に変更が生じ得るため、利用者アカウント台帳は**定期的に点検・更新**します。

用語の定義

＊1 認証：ログイン等の操作を行っている人が、本当にその人物であることを確認すること。認証の方法には以下の3つの方法が存在する。
- 知 識 認 証：PW等、認証される人のみが知っている情報で認証を行うこと。
- 所有物認証：IDカード等、認証される人のみが有している所有物で認証を行うこと。
- 生 体 認 証：指紋や虹彩等の認証される人の身体的情報を用いて認証を行うこと。

＊2 多要素認証：3種類の認証方法の内、異なる認証パターンを複数組み合わせて認証を行う方法のこと。

4 サーバ・端末PCについて、利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。

? 対策が必要な理由

適切なアクセス権を設定することは、医療情報を保護するために必要な取り組みの一つです。担当者に対して、業務に関係ない情報へのアクセスを許可してしまうと、内部不正につながる可能性があります。このため、アクセス権は業務上の必要最低限のものに設定することが推奨されます。
また、アクセス権を適切に設定することは、サイバー攻撃の被害に遭った際にも、**被害の拡大防止に寄与**します。不正アクセス等のサイバー攻撃により、ある担当者のアカウント情報が窃取されてしまった際に、アクセス権管理が行われていた場合は、その被害はそのアカウントがアクセスできる範囲内の情報に留まります。しかし、アクセス権管理を怠っていた場合、被害範囲が拡大し、その被害範囲の特定にも時間を要する場合があります。
したがって、適切なアクセス権を設定することは、**内部不正やサイバー攻撃等の不正な行為による医療情報の侵害への対策として非常に有効**です。

なぜこのチェック項目を実施する必要があるのか、実施するメリットを説明しています。

ポイント

新規導入の医療情報システムには多要素認証の導入を!

ガイドラインでは、令和9年度に稼働していることが見込まれる医療情報システム（PWを用いた認証を行うもの）には多要素認証の導入が記載されています。今後、医療情報システムの新規導入・更改を検討されている方は、**多要素認証の導入を事業者等に相談**してください。

チェック項目を実施するうえでの重要ポイントを説明しています。

コラム

権限は最小限に!

セキュリティの世界では、利用者に業務上必要最低限の権限のみを付与すべきであるとする原則を「最小権限の原則」と呼びます。上述の通り、最小権限の原則は**内部不正の防止**につながるだけでなく、サイバー攻撃被害を受けた際の**影響拡大防止**にも役立ちます。
アカウントを発行するときは、その利便性から管理者アカウントを気軽に付与してしまいがちですが、医療情報のような重要データを扱う場合は、**管理者アカウントはシステム管理を行う限られた担当者に限定**し、通常の利用者にはより権限の低い一般ユーザアカウントのみ付与することを推奨します。

チェック項目には含まれていませんが、さらに先進的な取り組みであったり、参考となる情報を説明しています。

まずはここから！

- サーバ・端末PCを操作する利用者を特定し、アカウント台帳等で明確に管理しましょう。
- 台帳を定期的にアップデートし、無関係の人が利用することがないよう管理しましょう。
- 管理者アカウントと一般ユーザアカウントを分けて管理できるようシステム事業者等へ確認しましょう。

手順等を読んでも何から実施したらよいかわからない方向けに、まずは最低限取り組むべき事項を説明しています。

※P40に全チェック項目の「まずはここから」を一覧表で記載していますので、ご参照ください。

Check! 医療情報システムの有無

医療情報システムを導入、運用している。

医療情報システムを導入しているかを確認する

? 医療情報システムとは？

ガイドライン概説編2.3

医療情報*1システムとは、**医療に関する患者の個人情報（個人識別情報）を扱う情報システム**を指します。（医療情報を保存するシステムだけではなく、診療や医療事務を支援するシステム、医療情報を閲覧・取得するコンピュータや端末、それらをつなぐネットワーク機器等を含みます）

これらのシステムには、医療情報システム・サービス事業者により医療機器等へ提供されるシステムやサービス、医療機関等*2において自ら開発・構築されたシステムが含まれます。一般に、医療情報システムの範囲は以下のとおりです。

医療情報システムの範囲

対象の例

- 医療機関等のレセプト作成用コンピュータ（レセコン）、電子カルテ、オーダリングシステム等の医療事務や診療を支援するシステム
- 医療情報を保有するコンピュータ
- 遠隔で医療情報を閲覧・取得する端末（コンピュータ）
  ※端末には携帯端末も含む。
- 医療情報の閲覧や保存が行われる端末と接続する院内・院外ネットワーク機器

対象外

- 医療情報を含まない、費用請求に関する情報を取り扱う会計・経理システム
- 医療情報の閲覧や保存が行われる端末と接続をしない情報系ネットワーク機器
- 医療情報を含まない個人情報を取り扱うコンピュータやシステム（予約システム等）

※医療情報を含まない個人情報を取り扱うコンピュータ等はガイドラインの対象外となりますが、個人情報保護法に準拠した適切なセキュリティ対策が求められますのでご注意ください。

用語の定義

*1 医 療 情 報 ：医療に関する患者情報（個人識別情報）を含む情報と定義しており、病歴等の機微性の高い情報を含む情報を指す。
*2 医療機関等：医療機関等とは、病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等を指す。
*3 サ ー バ ：複数の端末にサービスや機能を提供するコンピュータを指す。

〈医療機関等における個人情報の例〉
診療録、処方せん、手術記録、助産録、看護記録、検査所見記録、エックス線写真、紹介状、退院した患者に係る入院期間中の診療経過の要約、調剤録　等

医療情報システムを導入、運用している。

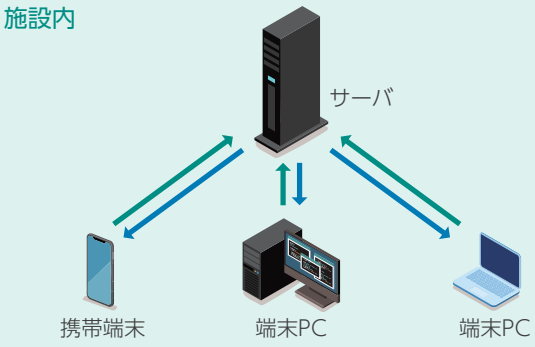
手順

STEP 1 医療情報システムの有無を**確認**します。医療情報システムがない場合、STEP 2 STEP 3 の確認は不要です。

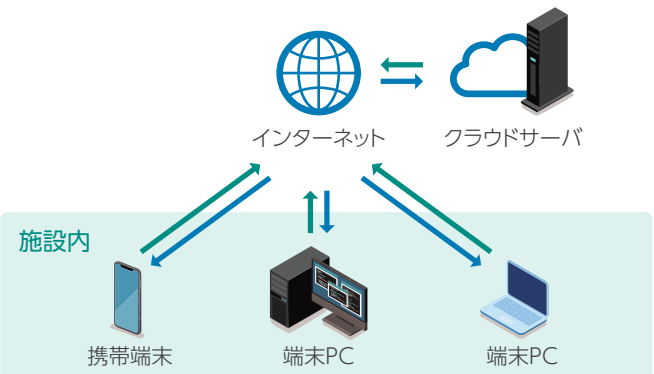
STEP 2 サーバ*3の有無を**確認**します。サーバがない場合、STEP 3 の確認は不要です。

STEP 3 医療情報システムが、自組織で保有・運用しているオンプレミス型か、外部事業者が提供するサービスをインターネット経由で利用するクラウドサービス型か**判別**します。クラウドサービス型の場合、一部の項目の対応が不要です。(下記コラムをご参照ください)

オンプレミス型



クラウドサービス型



コラム

本項目に該当する医療情報システムは、ガイドラインを満たす必要があり、後述の**サイバーセキュリティ対策の各チェック項目について対応を実施**する必要があります。

医療情報システムがオンプレミス型かクラウドサービス型かでガイドラインでの対応が一部異なります。クラウドサービス型でかつ、契約にて当該システム事業者等が以下項目の責務を負う場合、医療機関は以下対応の簡略化が可能です。

- 医療情報システム・サービスのマニュアル等の整備
- 医療情報システムの仕様書、設計書、プログラム開発資料、構成図、担当責任者等の資料の整備
- 医療情報システムの操作履歴、システムログの収集、レビュー、管理

1 体制構築

医療情報システム安全管理責任者を設置している。

医療情報システム安全管理責任者を設置する

実施すること

ガイドライン経営管理編3.1.2②、3.2

医療情報システムの**安全管理責任者を任命**します。
ガイドラインでは、経営層が医療情報システムの安全管理責任者に就くことが望ましいとされていますが、医療機関の規模や組織等の事情により、経営層からの任命が難しい場合は、企画管理者（企画管理・システム運用の実務者）が兼務することも認められています。ガイドラインで定義されている医療情報システムの安全管理責任者の職務は以下となります。

医療情報システムの安全管理責任者の職務〈ガイドラインによる定義〉

1. リスク評価及びリスク管理方針を踏まえて、**情報セキュリティ方針を整備**すること。
2. 情報セキュリティ方針に基づき、自組織の実態を踏まえて、実施可能な内容で実効性のある適切な**情報セキュリティ対策を整備**すること。（チェックリスト記載のセキュリティ対策等）
3. 職員等に対して定期的に情報セキュリティに係る**研修**を行うこと。
4. 上記を推進していくために、経営層に対してセキュリティリスクや自組織の対策の現状について**報告**すること。

実施にあたって

医療情報システムの安全管理責任者には、**自組織に関する知識とマネジメント能力**[*1]**が第一に求められます**。したがって、理想的には経営層から任命することが望ましいです。しかし、前述の通り企画管理者から任命することも容認されます。
一方、マネジメント能力が問われるため、マネジメント能力が十分ではない若手職員等を医療情報システムの安全管理責任者に任命することは避けた方がよいでしょう。

*1 システムやセキュリティに関する技術的な知見は、システム運用担当者*2や外部の専門家の力等を借りながら対応することで補うことが可能です。
*2 システム運用担当者：医療機関において医療情報システムの実装・運用を行う担当者のこと。

医療情報システム安全管理責任者を設置している。

? 対策が必要な理由

医療情報システムの安全管理責任者を設置することは、平時のセキュリティ対策と有事のインシデント対応のそれぞれにおいてメリットがあります。
平時のセキュリティ対策の観点では、医療情報システムの安全管理責任者を設置することによって、**セキュリティ対策に実効性を持たせることが可能**となります。ガイドラインでは、医療情報システムの安全管理責任者は経営層または企画管理者から任命することが推奨されているため、経営的観点からセキュリティ対策の方針を策定したり、セキュリティ対策の予算や必要な人員の確保等を行うことが期待されています。
有事のインシデント対応の観点では、医療情報システムの安全管理責任者を設置することによって、**インシデントの早期収束へ寄与**します。インシデント対応では、経営層の適切な意思決定と、それに基づく現場の迅速な対応が求められます。医療情報システムの安全管理責任者が経営層と現場のシステム運用担当者との橋渡し役を担うことで、両者の円滑なコミュニケーションを実現し、**迅速かつ正確な状況把握、リソースの確保等が可能**になります。

コラム

セキュリティ教育って何から始めればよいの?

医療情報システムの安全管理責任者に求められる職務の一つに、**職員に対するセキュリティ教育の実施**が挙げられます。とはいえ、医療機関自らセキュリティ教育を一から企画し、教育計画や教材を作成していくのは難易度が高く感じられるかもしれません。実は、セキュリティ教育のお手本となるような教材はインターネット上等で無料公開されているものがあるので、医療機関の皆様の負荷軽減のためにも、これらを活用することもご検討ください。
例えば、独立行政法人情報処理推進機構(IPA)は、新入社員向け等の対象者別やテレワーク等の状況別に多数の教育コンテンツを無償で公開しています。詳細はP44記載の「ここからセキュリティ!情報セキュリティ・ポータルサイト(教育・学習)」をご参照ください。
これらの既存資料の内、自組織の状況等から必要なものを取捨選択し、職員の方に受講いただくことを第一のステップとして設定するのも有効です。是非ご検討ください。
また、前述のIPAは公式のYouTubeチャンネルを開設しており、セキュリティの普及啓発に向けた動画も無償で公開されています。P44にチャンネルのリンクを記載しています。こちらも是非ご参照いただき、自組織のセキュリティ教育のご参考としてご利用ください。

✓ まずはここから!

医療情報システムの安全管理責任者を任命しましょう。
※小規模医療機関の場合は、院長が医療情報システムの安全管理責任者を兼務することが現実的な対策になります。

2 医療情報システムの管理・運用

1 医療情報システム全般について、サーバ、端末PC、ネットワーク機器の台帳管理を行っている。

医療情報システム全般について台帳管理を行う

実施すること

ガイドライン経営管理編1.2.1②／企画管理編9.1

医療情報システムで用いるサーバや端末PC、ネットワーク機器等の情報機器等（医療情報システム全般*1）の所在や状態を適切に把握し管理するために、**定期的に棚卸を行います**。

手 順

企画管理者とシステム運用担当者は、サーバや端末PC、ネットワーク機器等の情報機器等の管理を行うために、医療情報システムで利用する情報機器等について**台帳管理***2を行います。
台帳で管理するための情報には、次のような項目が想定されます。

- 機器の名称
- 型番
- 製造事業者名
- 製造番号（シリアル番号）
- 購入年月日
- サポート期限
- 機器の所在場所
- ネットワーク情報（IPアドレスやホスト名）
- 利用者や機器の管理者
- 使用しているOSやソフトウェア、ファームウェア等のバージョン
- 関連するシステム名
- 主な用途
- 保存されているデータの概要
- ライセンスの情報

1 医療情報システム全般について、サーバ、端末PC、ネットワーク機器の台帳管理を行っている。

? 対策が必要な理由

情報機器等の棚卸を行うことにより、以下のように対象機器のメンテナンス等の管理や障害時の復旧の際にも役立ちます。

- 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。
- 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、**情報の漏えい等の可能性を速やかに発見**することができる。
- 情報機器等の滅失状況等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。
- 必要に応じて最新のソフトウェアへの対応の可否等も含めて**確認**することも重要である。

用語の定義

＊1 医療情報システム全般：サーバ、端末PC、ネットワーク機器を指す。
＊2 台帳管理：情報機器等（医療情報システムにおいて利用する物理的な資産、サービス、ライセンス等）や ID・パスワード（PW）、医療情報そのものといった、医療機関等において管理する情報資産を洗い出した上で、保存先や利用者範囲、保存期限等を台帳に記録して管理する方法のこと。

まずはここから！

- 付録資料（P46）のひな型を参考に、情報資産台帳を作成しましょう。
- 台帳管理するための各項目（P9の手順に記載）について、システム事業者等に情報提供を依頼しましょう。
- システム事業者等からの情報を保管し、情報資産台帳として運用しましょう。

※情報に更新がある場合についても、都度システム事業者等に同様の依頼をしましょう。

2 医療情報システムの管理・運用

2 医療情報システム全般について、リモートメンテナンス(保守)を利用している機器の有無を事業者等に確認した。

リモートメンテナンスの有無を事業者等へ確認する

実施すること

ガイドライン企画管理編9.1／システム運用編10.1

システム事業者等により、遠隔地からネットワーク経由で**システムのメンテナンス作業が実施されているか**システム運用担当者が**確認**します。

手順

STEP 1 2-1 P9で作成した情報資産台帳を基に、医療情報システム機器がどのシステム事業者等でメンテナンス(保守)されているか**確認**します。

STEP 2 メンテナンスがリモートで行われているか、システム事業者等から**回答をもらいます**。

対策が必要な理由

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)が必要です。ネットワーク経由でメンテナンスを実施する場合、医療システムが閉域網でなくなり、**外部から侵入されるリスクが高くなります**。あらかじめシステム事業者等に医療情報システムについてリモートメンテナンスの有無を確認することで、リモートメンテナンス時に**外部から侵入されるリスクを事前に把握**できます。

システム事業者等にメンテナンス作業内容を確認し、外部からのネットワークの侵入経路を特定する必要があります。リモートメンテナンスを実施する場合、**外部からの攻撃を防ぐための予防策が必要**になります。

2 医療情報システム全般について、リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。

コラム

メンテナンス実施時にシステム運用担当者が対応すべき事項

メンテナンス実施時には、システム事業者等に対して以下の項目について何らかの対応や報告を求めることで、しっかり管理を行うことが重要です。

- メンテナンス計画の策定・確認
- メンテナンス作業の影響確認
- メンテナンス作業報告・確認
- メンテナンス作業時のアクセス権限管理
- メンテナンス作業時のログ取得

まずはここから！

各システム事業者等へリモートメンテナンスの有無を確認しましょう。

3 医療情報システム全般について、事業者から製造業者/サービス事業者によるMDS/SDSを提出してもらう。

事業者からMDS/SDSを提出してもらう

実施すること

ガイドライン概説編4.5

医療機関等は、医療情報システム全般について、システム事業者等から**「MDS*1/SDS*2」を要求し、入手**します。

実施にあたって

自組織のリスクの把握や評価のために、システム事業者等から**MDS/SDSの提出を求めましょう。**
厚生労働省から医療情報システム事業者団体に対して、医療機関からMDS/SDSの提出を依頼された際は、それに応じるよう要請されています。

対策が必要な理由

医療機関は、ガイドラインに記載されているセキュリティ対策を講じ、安全に医療情報システムを管理していくことが求められますが、これにはシステム事業者等からのサポートが必要不可欠となります。
MDS/SDSをシステム事業者等から入手することにより、自組織が保有する医療機器やサービスのセキュリティ上の課題を理解することが容易となり、必要なセキュリティ対策を理解することの助けとなります。MDS/SDSを入手することは、**自組織の現状を把握し、その後の対策の立案に寄与**します。

用語の定義

*1 MDS：「Manufacturer Provider Disclosure Statement for Medical Information Security」の略。
「製造業者による医療情報セキュリティ開示書」のこと。医療機器等の製造業者により作成された文書で、医療機関等が必要なセキュリティ対策を実施する上で、必要な情報が含まれている。
*2 SDS：「Service Provider Disclosure Statement for Medical Information Security」の略。
「サービス事業者による医療情報セキュリティ開示書」のこと。MDSが医療機器の製造業者向けであるのに対し、SDSはサービス提供業者及び提供するサービスが対象となる。

3 医療情報システム全般について、事業者から製造業者/サービス事業者によるMDS/SDSを提出してもらう。

コラム

現状把握の重要性

厚生労働省のチェックリストによる確認や、MDS/SDSをシステム事業者等から入手することは、**医療機関が自組織のセキュリティ対策の現状を把握するための非常に有用な取り組み**です。
セキュリティ対策を講じていく上で、**現状把握は第一に取り組むべき事項**です。医師による診察なしに闇雲に薬ばかり飲んでも効果的な治療にならないのと同様に、セキュリティにおいても効果のないセキュリティ機器やサービスを導入しても費用や投資に見合った効果は得られないばかりか、使いにくいシステムとなってしまいます。現在の医療情報システムの状況や課題を把握し、特にリスクが高い事項に対して優先的にリソースを投入することが、効果的なセキュリティ対策を講じていく上で重要となります。これは、予算や人員等のリソースが限定される診療所等の小規模医療機関にこそ当てはまります。

現状把握を行う方法には複数のものがあります。以下に例をあげます。

	チェックシート方式や専門家が問診を行う方法 (本チェックリストやMDS/SDS等を効果的に利用した方法)	**専門家や専門ツールによる技術的な診断方法** (脆弱性診断やペネトレーションテスト(疑似的な攻撃))
メリット	技術的な課題だけでなく、ガバナンスや人的課題等も含めて診断することができるため、網羅的に課題を抽出することに優れています。	診断対象者が無自覚だった課題の抽出が可能です。
デメリット	セルフチェック方式であったり、問診等を診断の根拠とするため、抽出できる課題は回答者が自覚しているものに限定されます。	サーバの設定不備等の技術的な側面のみの診断となります。

このように、現状把握はセキュリティ対策を講じていく上で非常に重要で、第一に取り組むべき事項です。また、その方法は様々な方法があり、それぞれメリット/デメリットがあります。これらのメリット/デメリットを踏まえたうえで、**自組織にとって最適なものを選択したり、組み合わせながら、現状把握に取り組んでください**。

まずはここから！

各システム事業者等へMDS/SDSの提出を依頼しましょう。
※仮に提出に応じないシステム事業者等がいましたら、P45記載の日本医師会セキュリティガイドライン相談窓口へご連絡ください。

2 医療情報システムの管理・運用

4 サーバ・端末PCについて、利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。

アクセスコントロールの実施

実施すること

ガイドライン企画管理編13④、13.1.3

- 医療情報へのアクセス権は、担当者の業務や役職に応じたものになるように**アクセス権管理**を行います。
- 各担当者に個別のアカウントを発行し、誰にどのアカウントを発行したのかを**台帳管理**します。
- ユーザアカウントの認証*1を導入し、**なりすましや不正侵入対策**を行います。

手 順

STEP 1 医療情報システムについて、職種や業務内容に応じてどの担当者がどのシステムへアクセスする必要があるのかを**整理**します。

STEP 2 システムへアクセスする必要がある担当者にそれぞれ、個別に**アカウントを発行**します。
※どの担当者にどのシステムのアカウントを付与したのかは**利用者アカウント台帳等で管理**します。

STEP 3 ユーザアカウントの**認証は必須**とし、どの担当者がそのシステムを操作したのかを特定できるようにします。

※各システムのアカウント発行方法や認証機能の設定方法等は、システムを導入した事業者等に確認します。
※認証をIDとPWの組み合わせて行う場合は、**PWは必ず本人しか知りえないように保管**します。
※**多要素認証*2機能**を導入することも効果的です。
※人事異動等により役職や業務内容に変更が生じ得るため、利用者アカウント台帳は**定期的に点検・更新**します。

用語の定義

＊1 認証：ログイン等の操作を行っている人が、本当にその人物であることを確認すること。認証の方法には以下の3つの方法が存在する。
- 知 識 認 証：PW等認証される人のみが知っている情報で認証を行うこと。
- 所有物認証：IDカード等、認証される人のみが有している所有物で認証を行うこと。
- 生 体 認 証：指紋や虹彩等の認証される人の身体的情報を用いて認証を行うこと。

＊2 多要素認証：3種類の認証方法の内、異なる認証パターンを複数組み合わせて認証を行う方法のこと。

4 サーバ・端末PCについて、利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。

? 対策が必要な理由

適切なアクセス権を設定することは、医療情報を保護するために必要な取り組みの一つです。担当者に対して、業務に関係ない情報へのアクセスを許可してしまうと、内部不正につながる可能性があります。このため、アクセス権は業務上の必要最低限のものに設定することが推奨されます。
また、アクセス権を適切に設定することは、サイバー攻撃の被害に遭った際にも、**被害の拡大防止に寄与**します。不正アクセス等のサイバー攻撃により、ある担当者のアカウント情報が窃取されてしまった際に、アクセス権管理が行われていた場合は、その被害はそのアカウントがアクセスできる範囲内の情報に留まります。しかし、アクセス権管理を怠っていた場合、被害範囲が拡大し、その被害範囲の特定にも時間を要する場合があります。
したがって、適切なアクセス権を設定することは、**内部不正やサイバー攻撃等の不正な行為による医療情報の侵害への対策として非常に有効**です。

ポイント

新規導入の医療情報システムには多要素認証の導入を!

ガイドラインでは、令和9年度に稼働していることが見込まれる医療情報システム（PWを用いた認証を行うもの）には多要素認証を導入することが要求されています。今後、医療情報システムの新規導入・更改を検討されている方は、**多要素認証の導入を事業者等に相談**してください。

コラム

権限は最小限に!

セキュリティの世界では、利用者に業務上必要最低限の権限のみを付与すべきであるとする原則を「最小権限の原則」と呼びます。上述の通り、最小権限の原則は**内部不正の防止**につながるだけでなく、サイバー攻撃被害を受けた際の**影響拡大防止**にも役立ちます。
アカウントを発行するときは、その利便性から管理者アカウントを気軽に付与してしまいがちですが、医療情報のような重要データを扱う場合は、**管理者アカウントはシステム管理を行う限られた担当者に限定**し、通常の利用者にはより権限の低い一般ユーザアカウントのみ付与することを推奨します。

まずはここから！

- サーバ・端末PCを操作する利用者を特定し、アカウント台帳等で明確に管理しましょう。
- 台帳を定期的にアップデートし、無関係の人が利用することがないよう管理しましょう。
- 管理者アカウントと一般ユーザアカウントを分けて管理できるようシステム事業者等へ確認しましょう。

2 医療情報システムの管理・運用

5 サーバ・端末PCについて、退職者や使用していないアカウント等、不要なアカウントを削除している。

不要アカウントの削除

実施すること

ガイドライン企画管理編13⑦

退職や異動により**不要となった職員等のアカウントを削除（無効化）**します。
またその**ルールを整備**します。

手 順

STEP 1 2-1 P9で作成した情報資産台帳や 2-4 P15で作成したアカウント台帳を参照し、退職者等の**不要なアカウントを速やかに削除（無効化）**します。

STEP 2 人事異動や入退社の都度、アカウントの追加、削除を行い、定期的に棚卸を行う等、**アカウント管理のルールを定め、手順を確立**し、定期的に**実施状況を確認**します。

対策が必要な理由

医療情報システムにおいては、機微な情報を扱うという観点から、**システムの担当者の管理に厳格な信頼性が求められます**。
退職者や異動者のアカウントが放置されると、そのアカウントが不正に利用されることで、意図しないシステムの停止や、患者の個人情報や機密情報の漏えいや改ざん、不正な削除等のリスクが増大するため、**医療機関の信頼を大きく損なうリスク**があります。
そのようなリスクを回避するためにも、医療情報システムで利用するアカウント等の定期的な見直し等、適切な管理を励行するようにしましょう。

5 サーバ・端末PCについて、退職者や使用していないアカウント等、不要なアカウントを削除している。

コラム

アカウントの削除と無効化の違いは？ どちらがよい?

一般的に、アカウントを使用不可能にするためには、**「アカウントを無効化する場合」**と、**「削除する場合」**の2つの方法があります。

無効化の場合	削除の場合
無効化の場合は、アカウントそのものの情報はシステム上に残っているため、一定期間後に再度、そのアカウントを利用する場合に**復活しやすい**等の利点があります。	削除の場合は、アカウントそのものが削除されることになります。この場合に、**アカウントに紐づいたシステム内の各情報が削除される場合がある**等注意が必要です。

例えば、MicrosoftのWindowsでは、アカウントが削除されると、そのアカウントが所有者となっていたファイルの所有者がユーザ名で表示できなくなる(SIDと呼ばれる内部形式で表示され所有者の判断が困難になる)等の影響があります。また、アカウントを無効化しても、システム上はアカウントが存在したままとなりソフトウェアやサービスのライセンスが必要となる場合等もあるため、**どちらの方法を使用するかは、システムの運用方法等や影響を考慮し、検討**する必要があります。

まずはここから！

作成した情報資産台帳やアカウント台帳をしっかり管理しましょう。
また実態にあわせて更新していきましょう。

2 医療情報システムの管理・運用

6 サーバについて、アクセスログを管理している。

アクセスログの管理

実施すること

ガイドライン経営管理編4.2／企画管理編5.3／システム運用編17①②

医療情報システムの**アクセスログ（通信記録）を取得**し、システムの**利用者の操作を記録**し、確認します。

※アクセスログには、少なくとも利用者のログイン時刻、アクセス時間及び医療情報への操作内容が特定できるように記録します。

取得したアクセスログは、**定期的にレビューを行い、不正な利用等がないことを確認**します。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併せて講じます。

医療情報システムにアクセスログの記録機能がない場合は、代替手段として業務日誌等により、利用者、操作内容等を記録するようにします。

手順

STEP 1 チェック対象であるサーバが存在するか、2 1 P9で作成した情報資産台帳で**確認**します。サーバがない場合は、本項目の対応は不要です。

STEP 2 医療機関で取り扱う医療情報システムにアクセスログを収集する機能が備わっているかをシステム事業者等に**確認**します。

※業務日誌での記録等、手作業によるアクセスログの記録は運用上負荷が高いため、医療情報システムに記録機能が備わっていない場合には、システム事業者等にログ機能の実装を依頼するのが望ましいでしょう。

アクセスログの例

ユーザID	氏名	時刻	カテゴリ	操作情報
abc@def	abcdef	2023/5/16　8:30:00	管理メニュー	ログイン
abc@def	abcdef	2023/5/16　8:30:20	管理メニュー	起動
abc@def	abcdef	2023/5/16　8:31:00	入力メニュ	起動
abc@def	abcdef	2023/5/16　8:32:00	入力メニュー	カルテ入力
abc@def	abcdef	2023/5/17　12:30:00	管理メニュー	ログオフ
ghi@jkl	ghijkl	2023/5/17　8:40:00	管理メニュー	ログイン
ghi@jkl	ghijkl	2023/5/17　8:40:30	管理メニュー	起動
ghi@jkl	ghijkl	2023/5/17　8:45:00	管理メニュー	ログオフ

※収集したログは、少なくとも**1年程度保持**することが望ましいです。

用語の定義

*デジタルフォレンジック（Digital Forensics）：サイバー攻撃等を受けた際に、デジタル機器に記録された情報の回収と分析等を行うことを指す。その主な目的は、原因究明、事件捜査、訴訟の証拠保全及び分析、不正行為防止等がある。

6 サーバについて、アクセスログを管理している。

? 対策が必要な理由

外部からの不正アクセスやウイルス感染、組織内部からの情報漏えい等のインシデントが発生した場合、事態にいち早く気づき、被害状況や影響範囲の把握等の事後対応を効果的に行うためには、アクセスログ等の取得と保管状況が重要となります。
アクセスログ等が取得されていれば、医療情報システム内でどのような通信や操作が行われていたか、何が起こっていたか**等速やかな被害範囲の特定や影響調査等が可能**となり、**事後の抜本的な対策**にもつながります。
アクセスログ等が十分に取得されていない、または必要な期間分のアクセスログが保存されていないと、事象の把握が困難となり、初動対応が遅れ、結果として事態の収束や事業の再開が大幅に遅延する事態になりかねません。
上述のように、ログの取得は非常に重要な取り組みであり、可能であれば**医療情報システム全般に対してログの取得を実施**しましょう。チェックリストで対象となっているサーバについては、最低限の取り組みとしてログの取得を必ず行うようにしてください。

コラム

ログ管理システムの導入は有効?

アクセスログ等のログ管理システムを導入することで、アクセスログの取得と保存、監視等を一元管理することが可能となります。一元管理を行うことで、**サイバー攻撃等の検出がより容易**になることもあります。
サイバー攻撃の際には、攻撃者は、大量の証跡を発生させることでログを上書し、結果として証跡を削除したり、管理者権限へ昇格した際には、実際にログ本体の消去を試みます。ログ管理システムを導入し、ログを集中管理することで、これらの**リスクを低減することが可能**となります。
また、サイバーリスク保険に加入している医療機関等においては、保険の適用の判定の際に、攻撃の証跡が必要となります。ログ管理システムを導入することで、デジタルフォレンジック*等の高度な調査を行わなくても、**有効な証跡を提示できる可能性が高くなります**。このためログ管理システムは費用対効果の観点からも、**最適**な方法だと言えるでしょう。

✓ まずはここから！

サーバにアクセスログ機能があるのか、システム事業者等に確認しましょう。ない場合は、実装についてシステム事業者等に依頼しましょう。

2 医療情報システムの管理・運用

7 ネットワーク機器・サーバ・端末PCについて、セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。

最新のセキュリティパッチの適用

実施すること

ガイドラインシステム運用編8③8.1、8.2、13.2

システムの安全性を確保するために、セキュリティパッチと呼ばれる**OSやアプリケーションの脆弱性を解消するための修正プログラムを適用**します。

手 順

STEP 1

医療機関等で管理している医療情報システムを構成している機器やソフトウェア（ネットワーク機器*1、サーバ、端末PC等）のシステムに脆弱性がないか、セキュリティパッチがリリースされていないかをシステム事業者等に**確認**します。

※未適用のセキュリティパッチがある場合は、速やかに適用します。

STEP 2

最新のセキュリティパッチを適用する場合には、パッチを適用しても問題がないかシステム事業者等に**確認**を行うか、あらかじめ影響のない環境等で**テストを実施**することが望ましいです。

※システム事業者等への確認やテストを行わずに本番環境に適用すると、**動作に不具合がでる可能性もあるため注意が必要**です。

※新たな脆弱性は、継続的に発見されることが多いため、セキュリティパッチの適用は1回で終わりではなく、定期的に確認し、**常に最新の状態に管理をする体制の構築が必要**です。

用語の定義

*1 ネットワーク機器：端末PC等のデバイスをインターネットに接続する際に使用するWi-Fi機器*2、ルータ*3、ファイアウォール、VPN接続装置といった機器のことを指す。
*2 Wi-Fi機器：無線を利用して、ネットワークを利用できる機器。広範囲に電波を飛ばせるため、適切に設定しないと、セキュリティ上脆弱となる。
*3 ルータ：異なるネットワークを接続する役割を持つ機器。インターネットと組織内のネットワーク等、複数のネットワーク間を接続する際に利用される。

7 ネットワーク機器・サーバ・端末PCについて、セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。

? 対策が必要な理由

セキュリティパッチの適用は、既知の脆弱性や脅威に対して修正を行うためのアップデートであり、**システムの安全性を確保するために不可欠**です。
OSやアプリケーションでは、製品が販売された後に新たな脆弱性やセキュリティホール（プログラムの不具合や設計上のミス）が発見されることがあります。このような脆弱性の発生を抑えることは実質不可能であり、速やかにセキュリティパッチを適用することが、**サイバー攻撃等のリスクを低減**する対策の一つです。セキュリティパッチを適用せず放置することで、ランサムウェア等の悪質なマルウェアに感染するリスクが増加してしまいます。

実際に、医療機関等においても、ソフトウェアの既知の脆弱性を突かれた情報漏えいやシステム停止等の重大なサイバーインシデントが多数発生していますので、注意しましょう!

ポイント

セキュリティパッチの適用可否を事前にシステム事業者等に確認すること!

医療情報システムによっては、OS等が特定のバージョンでないと正常に動作しないものが存在します。そのため、Windows Update等に代表されるようなセキュリティパッチを適用する際は、事前に適用の可否をシステム事業者等に確認し、医療情報システムの動作に影響を及ぼすことがないことを確認してから、パッチの適用を実施するようにしましょう。

まずはここから！

脆弱性情報を自組織で収集するのは困難なため、保守契約の範囲内でシステム事業者等へ対応を依頼しましょう。

2 医療情報システムの管理・運用

8 ネットワーク機器について、接続元制限を実施している。

接続元制限の実施

実施すること

ガイドラインシステム運用編13⑪

医療情報システムをインターネット等の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特に気を付け、ネットワーク、機器、サービス等を**適切に設定し、監視**を行う必要があります。

手 順

STEP 1

2 1 P9で作成した情報資産台帳を基に、自組織が保有するネットワーク機器を**確認**します。

STEP 2

外部から自組織のネットワークへ不正な接続が行われないように、それぞれのネットワーク機器を管理するシステム事業者等へ**接続元制限を依頼**しましょう。
具体的には、接続元や接続先のIPアドレス・プロトコル・ポート番号の制限を行い、接続先と接続元を限定します。なお、通信を許可する際には、許可リスト方式*で設定します。

※テレワーク等の都合上、接続元の制限が難しい場合には、多要素認証や端末認証を導入する等、**高度な認証方法を利用**してください。特に、各装置の管理インターフェースについては、外部ネットワークからの直接の接続は許可せず、**必ず、内部ネットワーク経由のみを許可**してください。

※外部ネットワークとの通信においては、通信の暗号化や接続先の認証を行い、盗聴や改ざん、なりすまし、中間者攻撃を踏まえた対策を実施してください。また、アクセスログを取得し、**定期的な確認、サイバー攻撃の監視**を行いましょう。

用語の定義

*許可リスト方式：事前に登録した機器のみ通信を許可し、その他通信の一切を遮断する方式。

8 ネットワーク機器について、接続元制限を実施している。

? 対策が必要な理由

IPアドレス等によるアクセス制限を実施することで、許可されていない端末からの通信を拒否することができます。これにより、第三者の侵入が困難になります。**ネットワークに不正なソフトウェアが混入したり、重要な情報が漏えいするリスクを低減**することができます。
あわせて、ネットワークの通信状況を適切にモニタリングすることで、接続制限の有効性を確認できるほか、不審な兆候を早期に発見することが可能となり、**安全性をさらに高める**ことができます。

ネットワークを安全に利用するために、セキュリティ対策として接続元制限を設定し、通信状況を監視をすることは重要です。

✓ まずはここから！

P9記載の情報資産台帳を基に、自組織で所有するネットワーク機器を確認し、外部から不正な接続をされないよう、機器を管理するシステム事業者等へ接続元制限を依頼しましょう。

2 医療情報システムの管理・運用

9 サーバ・端末PCについて、バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。

不要なソフトウェア及びサービスを停止する

実施すること

ガイドラインシステム運用編8.1

医療情報システムにおいては、その機能を提供されるために必要なソフトウェアやサービスのみが、サーバ及び端末PCで動作することが求められます。
どのようなソフトウェアやサービスが不要なものであるかは、医療情報システムの構築事業者等へ確認の上、**バックグラウンドで動作している不要なソフトウェア及びサービスがあれば**、そのソフトウェアやサービス等を**停止**させます。

手 順

サーバ及び端末PCにおいて、必要のないソフトウェアやサービス等が動作していないか、**確認**を行い、不要なものがある場合には、そのソフトウェアやサービス等をシステムから**削除または停止**させます。

- 一般的に、「どのようなソフトウェアやサービスが医療情報システムの動作に必要か、または不要か」を医療機関等の担当者が判断するのは困難なため、医療情報システムの各機器やソフトウェアの製造者やシステムの構築事業者等に確認を行い、構築事業者等に必要な設定等の**対策を依頼**することになります。特に、医療システムの導入時システムの機能追加、機器の変更や追加等の構成が変更される際には、**必ず不要なソフトウェア及びサービスを動作させないように依頼**することが重要となります。
  また、医療情報システムの設計書や設定書等の文書に、必要なソフトウェアやサービス等についての**情報を記載**するようにすることも必要となります。
- インターネット上には悪意のあるソフトウェアも存在しているため、インターネットから不用意にソフトウェアをダウンロード／インストールするのは危険です。ダウンロード／インストールが必要な場合はシステム事業者等に当該ソフトウェアの安全性を相談する等対策を講じるようにしましょう。医療情報システムをインターネットに接続している場合は、特に注意が必要です。

9 サーバ・端末PCについて、バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。

? 対策が必要な理由

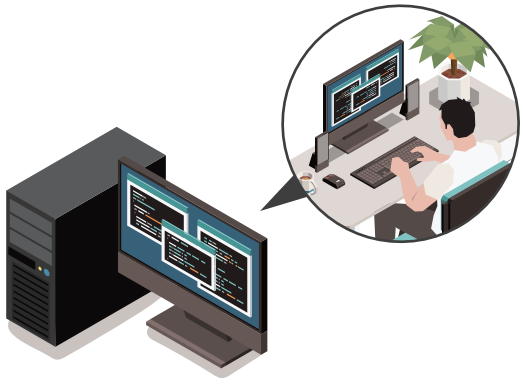
医療情報システムに限らず、ソフトウェアやサービスには、常に何らかの脆弱性が潜んでいる可能性があります。これらの脆弱性は、ソフトウェアの瑕疵や設定上の誤り等様々なものが想定されます。このため、医療情報システムの動作に不要なソフトウェアやサービスが医療情報システムで動作していると、それらに潜む脆弱性が利用され、**サイバー攻撃等のインシデントにつながる可能性が高くなります**。

このため、可能な限り、不要なソフトウェアやサービスを停止することが重要となります。不要なソフトウェアやサービスが停止されていれば、これらに脆弱性が発見された場合でも、ソフトウェアやサービスが停止されているため、**脆弱性への対策が不要**になります。

コラム

リモートからの操作を受けるソフトウェアやサービスの対策

特に、リモートデスクトップサービス等、サーバ及び端末PCに対して、リモートからの操作を受けるソフトウェアやサービスについては、その必要性等を確認し、サービスの無効化等の対策を検討することが重要です。サービスを有効化する場合には、適切な認証やアクセス制限、接続の履歴の保存等の**対策が必須**になります。



まずはここから！

- システム事業者等に不要なソフトウェアが存在していないか確認しましょう。
- インターネット上から不用意にソフトウェアをダウンロード／インストールするのは控えましょう。

3 インシデント発生に備えた対応

1 インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。

連絡体制図を作成する

実施すること

ガイドライン経営管理編3.4.2①、3.4.3①／企画管理編12.3

サイバーインシデント発生時に速やかに情報共有ができるよう、緊急連絡網を明示した**連絡体制図を作成**します。

手順

STEP 1

組織内にCSIRT*1を設置できる一定規模以上の医療機関では、最高情報セキュリティ責任者（CISO*2）を**任命**します。

※診療所等小規模な医療機関では、各責任者を「院長」が兼ねることとなります。

STEP 2

有事に連絡をとる必要がある外部関係機関を**洗い出します**。主な外部関係機関は以下のとおりです。

- 医療情報システム事業者（レセコン・電子カルテ事業者等）
- 情報セキュリティ事業者
- 外部有識者（顧問弁護士等）
- 都道府県警察の担当部署
- 厚生労働省
- 各都道府県衛生主管部（局）
- 保険会社（サイバーリスク保険に加入している場合）
- 日本医師会サイバーセキュリティ対応相談窓口（緊急相談窓口）（P45記載）

STEP 3

STEP 2 を次頁のような**連絡体制図に落とし込みます**。

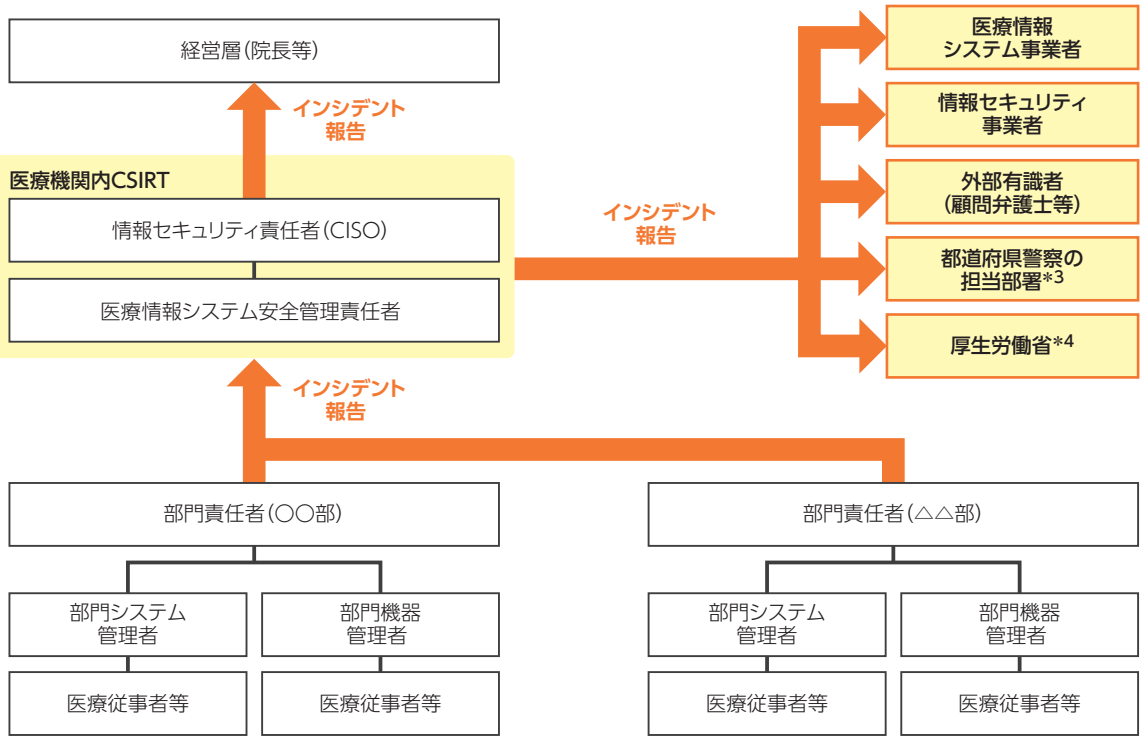
用語の定義

*1 CSIRT：「Computer Security Incident Response Team」の略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定等の活動をする。

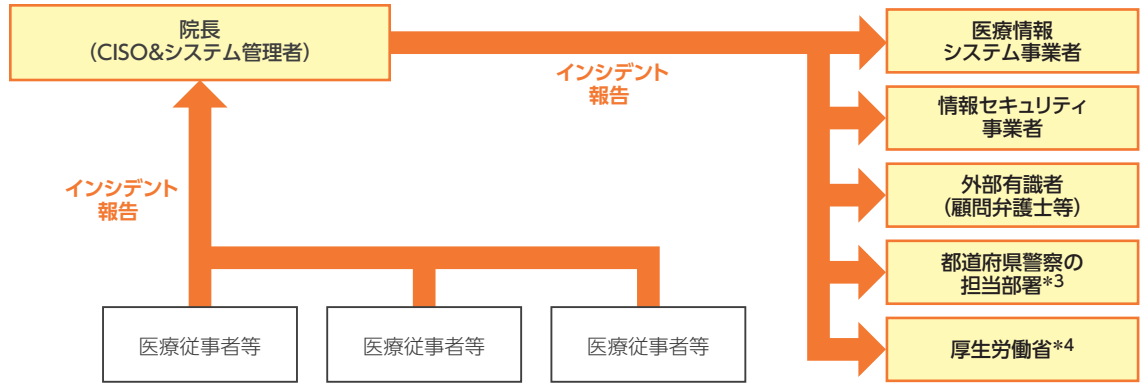
*2 CISO：「Chief Information Security Officer」の略。最高情報セキュリティ責任者。施設や組織における情報セキュリティを統括する責任者を指す。

1 インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。

連絡体制図の例（大規模医療機関の一例）



連絡体制図の例（小規模医療機関の一例）



*3 各都道府県警の問い合わせ先はP45を参照ください。
*4 厚生労働省の連絡先はP45を参照ください。
※上記記載の体制・名称はあくまで一般的な参考例を示したものであり、必ず自組織の実態に即した体制・名称等に置き換えてください。

1 インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。

ポイント

連絡体制図のポイント

- 診療所や小規模な医療機関等、「院長」が各責任者を兼ねる場合は、連絡体制図はP28のような簡略な体制図となります。
- 外部連絡先には、日本医師会の相談窓口や、サイバー保険窓口（契約している場合）を記載するのも有効です。

? 対策が必要な理由

サイバー攻撃等によるインシデント（疑い含む）が発生した際は、発生した事象を**正確に把握・分析し、原因調査、被害拡大防止、復旧、再発防止等を迅速かつ的確に行う**必要があります。また、発生したインシデントの内容によっては、法律やガイドライン等で報告が求められている場合もあります。このようにインシデント発生時に必要となる関係者は多岐に亘るため、あらかじめ院内および外部関係機関との連絡フロー等を可視化した体制図を作成しておくことが重要です。

なお、**医療法に基づく立入検査でも連絡体制図の確認が必要とされるため、確実に準備し、その内容を定期的に確認し見直しましょう。**

まずはここから！

付録資料（P47・P48）のひな型に必要事項を記入し、連絡体制図を完成させましょう。

1 インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。

コラム

いざインシデントが起こってしまったら!

万全のセキュリティ対策を実施している組織でも、いつサイバー攻撃の被害が顕在化するかはわかりません。つまり、どの医療機関でも、セキュリティの専門部署の有無にかかわらず、インシデントが発生すれば、その対応を余儀なくされることになります。また、**インシデント対応も迅速な対応が求められると同時に、初動対応が極めて重要**になってきます。
ここではその初動対応手順について、以下に実施する概要を整理します。

インシデント初動対応手順

STEP 1 発見・報告

インシデントの兆候となる事象や、具体的な被害の事実を確認したら、**速やかに経営者や責任者に報告**することが必要です。報告が終了したら情報セキュリティ責任者が中心になり、インシデント対応体制を構築しましょう。インシデント対応体制については、P35記載のBCPを参照してください。情報セキュリティ責任者がいない場合は、インシデント対応を行う責任者をすぐにアサインします。

STEP 2 被害拡大防止・二次被害抑止

インシデント対応体制構築と並行して、応急処置等を行い、**被害の拡大や二次被害を防ぎます**。端末PC等の機器がマルウェアに感染した疑いがあれば、Wi-Fiや有線LAN等のネットワークから切り離してください。類似の現象が他の部署にも発生していないか確認し、複数の部署にて発生している場合は組織内のネットワークを停止してください。

STEP 3 調査・情報整理

適切な対応をするために「5W1H（いつ、どこで、誰が、何を、なぜ、どうしたのか）」の観点で**被害の事実を調査し、情報を整理**します。不正アクセス等の可能性がある場合は、侵入ルート等の原因調査を行う必要があるため、システム上の証跡を消さないようにします。（安易なPCの初期化やウイルスソフトによるスキャン等は控えるようにします）

STEP 4 通知・連絡・公表等

発生した事象について、**関係各所にその事実を通知**する必要があります。医療システム事業者、取引先、警察等への連絡や、個人情報の漏えいやそのおそれがある場合には、個人情報保護委員会への報告も義務化されています。監督官庁である厚生労働省への報告も必須です。また、インシデントの規模によってはホームページ（HP）やマスコミへの公表を検討する必要があります。

いずれの段階においても、「どのような対応をしたらよいかがわからない場合」は、躊躇せず速やかに外部のセキュリティ専門事業者に連絡を入れ、本格対応に関する支援を要請してください。サイバー保険に加入している場合は、保険会社で専門的なアドバイスを得られるかどうかも確認することをお勧めします。

3 インシデント発生に備えた対応

2 インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。

データ・システムをバックアップする

実施すること

ガイドライン経営管理編3.4.1／企画管理編11.2／システム運用編11.1、12.2、18.1

十分な対策を実施していても、サイバー攻撃や意図しない操作ミスや故障、自然災害等により医療情報システムが停止し、医療機関等の業務に影響を与える可能性があります。
このような場合に備えて、診療を継続するために何が必要か検討し、準備を行う必要があります。
医療情報システムについては、復旧のための手順を整備し、医療情報やシステムの**適切なバックアップを実施**することが求められます。

推奨策

医療情報システムは一般的に複雑で、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す。したがって、一様に手順等指針を示すことは困難となりますが、推奨策として例を示します。

必要なデータの洗い出し・整理

医療情報システムが停止した際に、システムを使用しなくとも診療を継続するために必要なデータ・情報を**洗い出します**。

バックアップの実施

- データのバックアップは**複数世代（3世代以上が推奨）取得**するようにしましょう。例えば、日次でバックアップを行う場合、3世代とは**「3日前時点のデータ」、「2日前時点のデータ」、「前日時点のデータ」**の3つのバックアップを保有することを指します。
- 取得した3世代のバックアップの一部（最も古いデータ等）は、ネットワークから切り離した**オフライン環境に移動し、編集ができない様式で保存**するようにしましょう。これを行うことによって、3世代バックアップの場合は、少なくとも「3日前時点のデータ」まで復旧することが可能になります。バックアップデータをネットワークにつないだ状態で保管していると、ランサムウェア等の被害がバックアップデータにまで及ぶ可能性があります。
- **バックアップを異なるメディアに保存**することにより、保存する機器の故障等に対するリスクヘッジにもつながります。

2 インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。

バックアップデータの復旧

1 バックアップの状況（使用するバックアップ機器やメディア等）を踏まえ、データ復旧について、誰が、何を、どのように行うかを整備し、必ず**復旧の手順書やチェックリストを作成**して医療機関内の関連する担当者で共有します。

※実際に医療システムが停止したことを想定し、策定手順が適切に機能することを**訓練等によって確認**しておくことも重要です。

2 バックアップデータを復旧する際には、再度サイバー攻撃被害に遭わないように、事前に以下の対策を講じるようにしましょう。

- 攻撃者によって無効にされたセキュリティ機能を復旧する
- 同じ脆弱性や他の脆弱性を突かれて侵入されないよう、脆弱性の特定と是正措置を行う
- 不正に作成されたり、盗まれたりしたID・PW等を使われないようにする　等

専門的な知見に関して、情報処理推進機構（IPA）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「情報セキュリティ安心相談窓口（P45を参照）」を開設しているため、活用を推奨します。

2 インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。

? 対策が必要な理由

どのようなデータをバックアップするか、すなわち、診療を継続するために必要なデータ・情報がどのようなものかを洗い出し、整理し、必要なデータのみをバックアップすることで**実効性を高める**ことに繋がります。
また、復旧手順についてもあらかじめ整備・確認を行い、関連する担当者に周知しておくことで、いざというときに**早期のデータ復旧が可能**となり、**診療の継続（もしくは復旧）をスムーズに行うことができます**。

コラム

適切なバックアップとは?

ガイドラインにおいても、適切な方法でのバックアップの実施が求められており、医療機関等は、システムやアプリケーション等の特性にあわせた最適な方法でバックアップを実施する必要があります。適切なバックアップの実施のための一例として、**「3-2-1 バックアップ*」**と呼ばれる考え方があります。「3-2-1 バックアップ」では、以下のルールに従いバックアップを実施します。

3-2-1 バックアップ

3 つ以上のデータを確保
オリジナルの元データとは別に、常に2つ以上のバックアップを用意し、合計で3つ以上のデータを保持。

2 種類以上の記録デバイスを使用
ディスクとテープ等、特性や耐久性の異なる2種類以上のデバイスを利用してバックアップを作成。

1 つのバックアップは、物理的に離れた場所に保管
火災や水害、地震等の大規模な災害等で、同時に複数のバックアップが失われる場合に備え、バックアップのうちの1つは、外部でデータを保持。

*[3-2-1 バックアップ]についての詳細は、米国US-CERT の「Securing Your Computer」の「Data Backup Options 」で紹介されています。
(https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf)

2 インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。

まずはここから！

- 診療の継続に必要となるデータを特定し、システム事業者等と相談しながらバックアップを実施してみましょう。
- バックアップの取得だけでなく、バックアップからの復旧手順も整備しましょう。
- 複数世代バックアップについては、バックアップデータが使用できない場合の影響や費用対効果等を勘案し検討しましょう。

3 インシデント発生に備えた対応

3 サイバー攻撃を想定した事業継続計画(BCP)を策定している

事業継続計画の策定

実施すること

ガイドライン経営管理編3.4.1／企画管理編11.1

サイバー攻撃を想定した事業継続計画(BCP*1)を策定します。
「サイバー攻撃は完全に排除できない」を大前提とし、診療業務の中断が発生しないよう(または、短期間で再開できるよう)に、インシデント発生時の医療情報システムの復旧の手順等を事前に整え、**事業を継続できる体制を整えます**。

手順

STEP 1

自然災害を想定したBCP(既に策定済の場合)と整合をとりながら、重要情報の漏えいや身代金を目的とした脅迫行為等、サイバー攻撃特有の発生事象を想定した**非常時の対応方針・手順を定めます**。

非常時の体制面の整備

組織における非常時の定義、役割、責任、意思決定者等の明確化、報告フロー等を計画に盛り込みます。

非常時の具体的な対応方針

1 発生した事象への対応、**2 業務復旧対応**の観点で対応手順を計画に盛り込みます。

1 発生した事象への対応 (被害を最小限に留めるための対応)		2 業務復旧対応 (早期に通常業務に戻るための対応)
● 被害範囲の把握	● 代替手段の策定	● システム復旧対応
● 証拠の保全	● 監督官庁等への連絡	● データ復旧対応
● 原因調査	● 広報対応	● バックアップ取得対応 等
● ネットワークの遮断	● 法令対応 等	

STEP 2

策定したBCPが、非常時に有効に機能するかどうか、自組織業務に即した内容になっているか等をチェックするために、**定期的に訓練を実施**し、結果を計画に反映させます。

STEP 3

復旧手順とともに、代替手段による重要業務の迅速な復旧策についても、検討を行います。

3 サイバー攻撃を想定した事業継続計画(BCP)を策定している

対策が必要な理由

セキュリティ対策を講じたとしても、もはや完全に排除できないサイバー攻撃。「もし起こったら」ではなく「いつ起こるのか」という意識で、**非常時の際に診療への影響を最低限に抑えるための対応**をあらかじめ策定しておくことが極めて重要です。
実際にサイバー攻撃に直面し、長期にわたる診療の停止という事態が現実的に発生しています。紙カルテによる代替運用等、医療情報システムが停止した際の対応手順として自然災害用BCPを参照することも有用ですが、自然災害用BCPではサイバーインシデントへの対応は想定されていないため、サイバーインシデントに特徴的な対応についてはカバーしきれません。サイバーインシデントに直面したとしても、診療の継続もしくは短期間での業務復旧を実現できるよう、**サイバー攻撃を想定したBCPの策定および平時からの訓練も実施**しておくことをお勧めします。
BCPは策定して終わりではなく、生きたBCPとするためにも、経営者を含む医療機関全体で策定に取り組みましょう!

コラム

平時からのBCP対策の重要性

BCPは非常時におけるサイバー攻撃からの「復旧」が主眼となりがちですが、実は平時における**サイバー攻撃を発生させないための「予防」**や、**目に見えない攻撃を可視化する等の「検知」**も重要な概念であり、これらも絡めたBCP策定が推奨されます。

「予防」の重要性	「検知」の重要性
繰り返しになりますが、セキュリティパッチの適用等の脆弱性対策の実施によりシステムやソフトウェアのセキュリティレベルを高い状態に維持することで、**非常時のリスクを低減**させることができます。	災害時とは異なり、サイバー攻撃は攻撃を受けていること自体に気が付かない場合があります。インシデントを早期に検知するために、EDR*2等のセキュリティ監視ツールを導入し、ネットワークの状況を**リアルタイムで把握し発見の遅れをなくす取り組み**も重要です。

用語の定義

*1 BCP:「Business Continuity Plan」の略で、事業継続計画を指す。自然災害やサイバー攻撃、システム障害が発生した際に、事業の継続または早期の復旧を可能とするための計画のこと。
*2 EDR:「Endpoint Detection and Response」の略で、ユーザが利用するPCやサーバ(エンドポイント)における不審な挙動を検知し、迅速な対応を支援するセキュリティツールのこと。

まずはここから!

付録資料(P49〜P54)のひな型を参照し、BCPを策定しましょう。

4 FAQ

Q1 自組織は規模も小さくサイバー攻撃の標的になる可能性は低いと思われますが、それでもセキュリティ対策を実施することは必須でしょうか?

セキュリティ対策は必須です。
近年のサイバー攻撃は、特定の組織を標的とした攻撃よりも、広範囲に無差別に仕掛ける攻撃が主流となっており、セキュリティ対策が不十分な医療機関が、その攻撃に巻き込まれる事例が多発しています。

Q2 ガイドラインを見ましたが、正直内容が理解できず、何から手を付けたらよいかわかりません。どうすればよいですか?

まずチェックリスト項目にしたがって対応をお願いします。
このチェックリストは、ガイドラインの記載内容のうち、医療機関の皆様が優先的に取り組むべき事項を抽出したものです。チェックリスト項目内でも、優先順位により対応時期が定められていますので、まずはそこから着手されることを推奨いたします。

Q3 チェックリスト項目をクリアすれば、これ以上のセキュリティ対策は不要と考えてよいですか?

継続的なセキュリティ対策が必要です。
チェックリスト項目はあくまで、取り組むべきセキュリティ対策のうち、診療を停止しないように最低限実施すべき事項を選定したものにすぎません。チェックリスト項目は早期にクリアし、更なるセキュリティ対策に取り組むことを推奨いたします。

Q4 「医療機関におけるサイバーセキュリティ対策に係る立入検査」では、どのようなことを求められますか?

立入検査時には、サイバーセキュリティ確保のために必要な措置が行われているかを確認されることになっています。具体的には、以下の対応への準備をお願いします。

① チェックリスト項目すべてに、確認結果(日付と「はい」または「いいえ」のチェック)の記入
② 「いいえ」にマルが付いた場合は、目標日の記入
③ 連絡体制図の現物確認

Q5 立入検査で対応に不備が認められた場合、ペナルティ等が課されることはあるのでしょうか?

現状罰則はございませんが、立入検査で指摘があった内容について改善がみられない場合等において、医療法第24条第2項における改善命令が出されます。

Q6 現状のセキュリティ対策に自信がないのですが、誰に相談すればよいかわかりません。どうすればよいですか?

P45記載の日本医師会セキュリティガイドライン相談窓口にご相談ください。
医療機関の皆様のお悩み事項をヒアリングさせていただき、ご希望に応じて具体的なセキュリティ対策をご支援できるセキュリティ事業者のご紹介をさせていただきます。

Q7 チェック項目2-③については、必ずMDS/SDSの標準様式で提出してもらわないといけないのでしょうか?

必ずしもJAHIS(一般社団法人保健医療福祉情報システム工業会)が定めたMDS/SDSである必要はありませんが、医療機関が事業者から提供されているサービスのセキュリティについてMDS/SDS等の標準様式で記載されているものと同様の内容を確認するようにしてください。

Q8 現在取引のあるシステム事業者等が、セキュリティ対策を実施していれば、自組織で別途セキュリティ対策を実施する必要はないと考えてもよいですか?

まず現在のお取引のあるシステム事業者等との契約内容やサービス利用規約等をご確認いただき、セキュリティ対策に関する事項が盛り込まれているかをご確認ください。セキュリティ対策に関する事項が盛り込まれていない場合は、自組織の責任で対応しなければならないことが想定されます。

Q9 サイバー攻撃の被害について、委託しているシステム事業者等に責任を問うことはできますか?

システム事業者等との契約内容やサービス利用規約等に、業務や役割、責任の分担に関する記載があるかを確認してください。記載が確認できない場合は、あらかじめシステム事業者等とこれらの取り決めについて合意を取り付けておくことが望ましいです。

Q10 サイバー攻撃の被害が発生した場合の対応手順を教えてください。

医療機関でサイバー攻撃が発生した場合、①被害拡大防止、②事業継続・復旧、の両面で迅速な対応が求められます。また、発生した事象を関係者へ適切に共有することも重要です。対応手順の詳細については、P30に記載がありますのでご参照ください。

Q11 サイバー攻撃の被害が発生した場合、法令上の報告義務等はありますか?

2022年4月1日に施行された改正個人情報保護法では、個人データの漏えい等が発生し、個人の権利利益を害するおそれがあるときは、①個人情報保護委員会への報告、②本人への通知、が義務化されました。サイバー攻撃は、「不正の目的をもって行われた漏えい等」に該当する可能性があります。
個人情報保護委員会への報告は、速やかに(概ね3〜5日以内)に実施する必要がありますので注意してください。詳細は以下をご参照ください。あわせて、法令上の義務ではありませんが、厚生労働省への報告も必ず実施してください。なお、日本医師会にてサイバー攻撃被害に対する支援金制度を用意しておりますので、P45記載の日本医師会サイバーセキュリティ対応一時支援金窓口へもお気軽にご相談ください。

〈個人情報保護委員会HPより〉
https://www.ppc.go.jp/news/kaiseihou_feature/roueitouhoukoku_gimuka/

Q12 実際にサイバーインシデントが発生した場合、自組織のみでの対応には限界があります。どうすればよいですか?

まず事前に作成した連絡体制図に定められた担当者から関係者へ報告を実施しましょう。インシデント対応の具体的な進め方や手順については、サイバーインシデントに精通した専門家のアドバイスを求めることが大切です。お困りの際は、P45記載の日本医師会セキュリティガイドライン相談窓口にご相談ください。
サイバーリスク保険にご加入の場合は、保険会社でインシデント対応の支援サービスが提供されておりますので、保険会社にもご確認ください。

Q13 ランサムウェア被害に遭った時に、暗号化されたデータは復旧できるものですか?

ランサムウェアの種類によっては、暗号化されたファイルが復号できる可能性はありますが、多くのケースではデータが復元できることは期待できません。大事なデータや情報を失わないためにも、バックアップの取得が大切です。また、バックアップの取得に加え、バックアップからの復旧手順を整備することも非常に重要になりますので、あわせて実施しましょう。
また、身代金を要求されても決して対応しないことが大切です。身代金を支払ってもデータが戻る保証はありませんし、犯罪者の攻撃を更に助長させるおそれがあります。

5 実施する対応 一覧

まずはここから始めましょう! 実施する対応 一覧

大項目	No.	チェック項目	実施する対応
1 体制構築	—	医療情報システム安全管理責任者を設置している。	医療情報システムの安全管理責任者を任命しましょう。 ※小規模医療機関の場合は、院長が医療情報システムの安全管理責任者を兼務することが現実的な対策になります。
2 医療情報システムの管理・運用	1	医療情報システム全般について、サーバ、端末PC、ネットワーク機器の台帳管理を行っている。	●付録資料(P46)のひな型を参考に、情報資産台帳を作成しましょう。 ●台帳管理するための各項目(P9の手順に記載)について、システム事業者等に情報提供を依頼しましょう。 ●システム事業者等からの情報を保管し、情報資産台帳として運用しましょう。 ※情報に更新がある場合についても、都度システム事業者等に同様の依頼をしましょう。
	2	医療情報システム全般について、リモートメンテナンス(保守)を利用している機器の有無を事業者等に確認した。	各システム事業者等へリモートメンテナンスの有無を確認しましょう。
	3	医療情報システム全般について、事業者から製造業者/サービス事業者によるMDS/SDSを提出してもらう。	各システム事業者等へMDS/SDSの提出を依頼しましょう。 ※仮に提出に応じないシステム事業者等がいましたら、P45記載の日本医師会セキュリティガイドライン相談窓口へご連絡ください。
	4	サーバ・端末PCについて、利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	●サーバ・端末PCを操作する利用者を特定し、アカウント台帳等で明確に管理しましょう。 ●台帳を定期的にアップデートし、無関係の人が利用することがないよう管理しましょう。 ●管理者アカウントと一般ユーザアカウントを分けて管理できるようシステム事業者等へ確認しましょう。
	5	サーバ・端末PCについて、退職者や使用していないアカウント等、不要なアカウントを削除している。	作成した情報資産台帳やアカウント台帳をしっかり管理しましょう。 また実態にあわせて更新していきましょう。
	6	サーバについて、アクセスログを管理している。	サーバにアクセスログ機能があるのか、システム事業者等に確認しましょう。ない場合は、実装についてシステム事業者等に依頼しましょう。
	7	ネットワーク機器・サーバ・端末PCについて、セキュリティパッチ(最新ファームウェアや更新プログラム)を適用している。	脆弱性情報を自組織で収集するのは困難なため、保守契約の範囲内でシステム事業者等へ対応を依頼しましょう。
	8	ネットワーク機器について、接続元制限を実施している。	P9記載の情報資産台帳を基に、自組織で所有するネットワーク機器を確認し、外部から不正な接続をされないよう、機器を管理するシステム事業者等へ接続元制限を依頼しましょう。
	9	サーバ・端末PCについて、バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	●システム事業者等に不要なソフトウェアが存在していないか確認しましょう。 ●インターネット上から不用意にソフトウェアをダウンロード／インストールするのは控えましょう。
3 インシデント発生に備えた対応	1	インシデント発生時における組織内と外部関係機関(事業者、厚生労働省、警察等)への連絡体制図がある。	付録資料(P47・P48)のひな型に必要事項を記入し、連絡体制図を完成させましょう。
	2	インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。	●診療の継続に必要となるデータを特定し、システム事業者等と相談しながらバックアップを実施してみましょう。 ●バックアップの取得だけでなく、バックアップからの復旧手順も整備しましょう。 ●複数世代バックアップについては、バックアップデータが使用できない場合の影響や費用対効果等を勘案し検討しましょう。
	3	サイバー攻撃を想定した事業継続計画(BCP)を策定している	付録資料(P49～P54)のひな型を参照し、BCPを策定しましょう。

チェックリストとの対応表

厚生労働省の「医療機関におけるサイバーセキュリティ対策チェックリスト」と本実践ガイドとの対応表です。
該当のページを参照の上ご活用ください。

令和6年度版
医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）	

Check! P5・P6へ

*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果（日付） 1回目	目標日	2回目	備考	R5年度項目	
1 体制構築	医療情報システム安全管理責任者を設置している。(1-(1))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※	1 P7・P8へ
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**						
	サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-(1))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※	2 1 P9・P10へ
	リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-(2)) ※事業者と契約していない場合には、記入不要	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※	2 2 P11・P12へ
	事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。(2-(3)) ※事業者と契約していない場合には、記入不要	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※	2 3 P13・P14へ
	サーバについて、以下を実施している。						
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※	2 4 P15・P16へ
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※	2 5 P17・P18へ
	アクセスログを管理している。(2-(6))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※	2 6 P19・P20へ
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）			2 7 P21・P22へ
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）			2 9 P25・P26へ
	端末PCについて、以下を実施している。						
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）			2 4 P15・P16へ
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）			2 5 P17・P18へ
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）			2 7 P21・P22へ
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）			2 9 P25・P26へ
	ネットワーク機器について、以下を実施している。						
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※	2 7 P21・P22へ
	接続元制限を実施している。(2-(8))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※	2 8 P23・P24へ
3 インシデント発生に備えた対応	インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。(3-(1))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※	3 1 P27〜P30へ
	インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-(2))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）			3 2 P31〜P34へ
	サイバー攻撃を想定した事業継続計画（BCP）を策定している。(3-(3))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）			3 3 P35・P36へ

- 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。
- R5年度項目欄（※）：「医療機関におけるサイバーセキュリティ対策チェックリスト（令和５年６月版）」において令和５年度中に対応することを目標として掲げた項目

参考情報

医療機関のセキュリティに関する参考情報

資料名		発行元	URL
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(令和5年5月)	概説編	厚生労働省	https://www.mhlw.go.jp/content/10808000/001102570.pdf
	経営管理編	厚生労働省	https://www.mhlw.go.jp/content/10808000/001102573.pdf
	企画管理編	厚生労働省	https://www.mhlw.go.jp/content/10808000/001102575.pdf
	システム運用編	厚生労働省	https://www.mhlw.go.jp/content/10808000/001112044.pdf
	Q&A	厚生労働省	https://www.mhlw.go.jp/content/10808000/001145860.pdf
医療機関におけるサイバーセキュリティ対策チェックリスト(令和5年6月)	チェックリスト	厚生労働省	https://www.mhlw.go.jp/content/10808000/001253950.pdf
	チェックリストマニュアル	厚生労働省	https://www.mhlw.go.jp/content/10808000/001253953.pdf

医療機関のセキュリティに関する参考情報

項目	発行元	URL
医療分野のサイバーセキュリティ対策について	厚生労働省	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html
医療機関向け セキュリティ教育支援ポータルサイト	厚生労働省委託事業	https://mhlw-training.saj.or.jp/
日本医師会 サイバーセキュリティ支援制度	日本医師会	https://www.med.or.jp/doctor/sys/cybersecurity/001566.html
日本医師会 公式YouTubeチャンネル	日本医師会	https://www.youtube.com/@JMAyoutube
サイバーセキュリティ政策	経済産業省	https://www.meti.go.jp/policy/netsecurity/index.html
みんなで使おう サイバーセキュリティ・ポータルサイト	内閣サイバーセキュリティセンター(NISC)	https://security-portal.nisc.go.jp/
ここからセキュリティ! 情報セキュリティ・ポータルサイト	情報処理推進機構(IPA)	https://www.ipa.go.jp/security/kokokara/
ここからセキュリティ! 情報セキュリティ・ポータルサイト(教育・学習)	情報処理推進機構(IPA)	https://www.ipa.go.jp/security/kokokara/study/company.html
IPA Channel (情報処理推進機構公式YouTubeチャンネル)	情報処理推進機構(IPA)	https://youtube.com/@ipajp?si=osjJiu5UXw_yGp2v

各種相談窓口・連絡先

日本医師会 各種相談窓口・連絡先

連絡先	運営時間	電話番号・メールアドレス・URL
日本医師会サイバー攻撃一時支援金・ 個人情報漏えい一時支援金制度事務局	平日9時～18時 （土日、祝日、年末年始は休業）	TEL：0120-411-250 MAIL：jma-cyber@qag.jp https://www.med.or.jp/japanese/members/info/cyber_shien.html
日本医師会サイバーセキュリティ 対応相談窓口（緊急相談窓口）	年中無休 6時～21時	TEL：0120-179-066 https://www.med.or.jp/doctor/sys/cybersecurity/001566.html
日本医師会セキュリティガイドライン相談窓口	平日9時～18時 （土日、祝日、年末年始は休業）	TEL：0120-339-199

その他の相談窓口・連絡先

相談窓口	連絡先	電話番号・メールアドレス・URL
医療機関等がサイバー攻撃を受けた際の 厚生労働省連絡先	医政局特定医薬品開発支援・ 医療情報担当参事官室	TEL：03-6812-7837 MAIL：igishitsu@mhlw.go.jp
医療機関向け セキュリティ教育支援ポータルサイト （インシデントかも?）	厚生労働省委託事業	https://mhlw-training.saj.or.jp/incident/
サイバー事案に関する相談窓口	都道府県警察	https://www.npa.go.jp/bureau/cyber/soudan.html
情報セキュリティ安心相談窓口	情報処理推進機構	https://www.ipa.go.jp/security/anshin/about.html
漏えい等の対応とお役立ち資料	個人情報保護委員会	https://www.ppc.go.jp/personalinfo/legal/leakAction/#leak_report

6 付録

資料1

情報資産台帳ひな型

以下のひな型を参考に、情報資産台帳を作成しましょう。

※ひな型はあくまで一般的な参考例を示したものであり、必ず自組織の実態に即した情報資産台帳に修正することを推奨します。

情報資産台帳

No.

① 管理番号	② 設置場所	③ 管理部門/使用者	④ 機器名称	⑤ 種別	⑥ 製造事業者名	⑦ 型番	⑧ OS	⑨ IPアドレス
H25-001	1F受付	総務部門	受付用PC	ハードウェア	A社	*******	Windows11	192.xxx.xxx.xxx
H25-002	2F事務室	総務部門	ファイルサーバ	ハードウェア	B社	*******	Windows Server2022	192.xxx.xxx.〇〇〇
H25-003	2F事務室	総務部門	オンライン資格確認用ルータ	ハードウェア	C社	*******	—	192.xxx.xxx.△△△
H25-004	クラウド	総務部門	電子カルテシステム	クラウド	D社	—	—	—
H25-005	診療室	総務部門	電子カルテシステムアクセス用PC	ハードウェア	A社	—	Windows10	自動割り当て(DHCP)

⑩ 購入年月日	⑪ サポート期限	⑫ システム事業者/購入先				⑬ セキュリティ対策	備考
		事業者名称	担当者名	TEL	e-mail		
2023/4/1	—	〇〇商会	佐藤氏	000-0000-000	***@***.**.**	E社アンチウイルスソフト	
2023/4/1	—	〇〇商会	佐藤氏	000-0000-000	***@***.**.**	—	
2023/4/1	—	〇〇商会	佐藤氏	000-0000-000	***@***.**.**	—	
2023/4/1	2028/4/1	〇〇ソフトウェア	山田氏	000-0000-000	***@***.**.**	—	
2023/4/1	—	〇〇商会	佐藤氏	000-0000-000	***@***.**.**	E社アンチウイルスソフト	

① 各機器を識別するための項目です。番号体系は、自組織で管理しやすいようなものに設定してください。

② 管理する機器の数が多い場合や、複数の拠点がある場合に、設定してください。

③ 機器の責任の所在を示す項目です。部門が特にない場合は、「使用者」を記載しましょう。

④ 機器の名称を記載する項目です。名称は一意になるように設定し、名称をテプラ等で実機に貼り付けておくと管理が容易になります。

⑤ 情報資産の種別を管理する項目です。種別としては、ハードウェア、クラウド、仮想マシン等を設定します。

⑥ 機器の管理や保守に必要な項目です。保証期間や修理に必要な部品の調達等にも役立ちます。

⑦ 機器を特定するために設定する項目です。モデル名等も合わせて記載しておくと現物を特定するのに便利です。

⑧ OSのバージョンを管理するための項目です。バージョンが古いものを特定するために設定しましょう。

⑨ ネットワーク上で機器を特定するのに必要な項目です。不正なアクセスがあった場合、IPアドレスからどの機器が攻撃を受けたのかを特定することができます。特定方法がわからない場合は、システム事業者等に確認しましょう。

⑩ 各機器の取得日を記載することで、保証期間や耐用年数等を把握することができ、更新や買い替え等にも役立ちますので記載するようにしましょう。

⑪ 機器の保守(メンテナンス)情報を管理する項目です。保守契約を締結している場合は必ず設定しましょう。契約内容、期限等が不明の場合はシステム事業者等に確認しましょう。

⑫ 各機器の購入先やメンテナンスを委託している事業者の連絡先を管理する項目です。トラブル発生時に迅速に連絡を取るために設定しましょう。

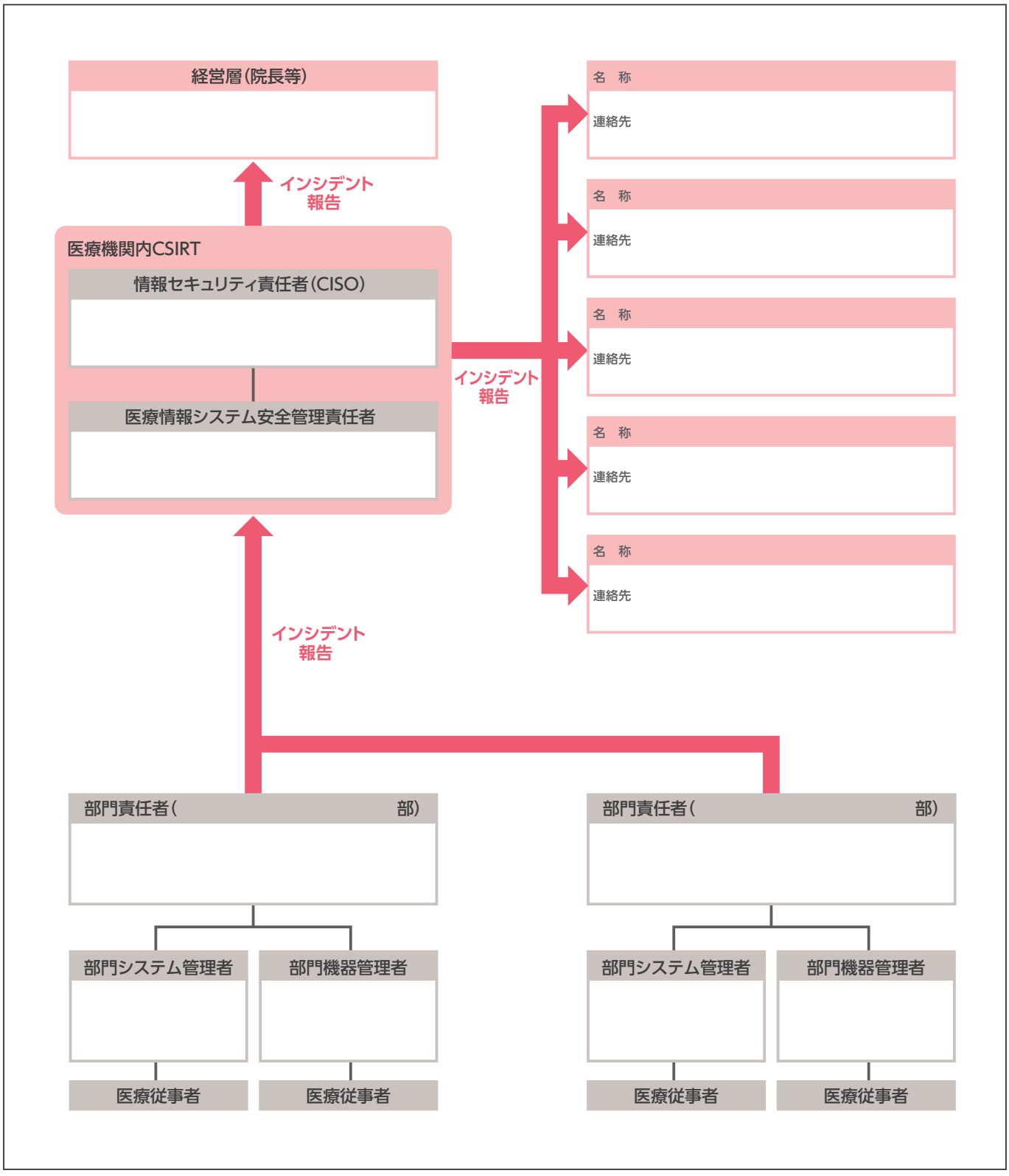
⑬ セキュリティ対策状況を管理する項目です。管理しておくと対策の抜け漏れや新たな計画策定にも役立ちます。

資料2

医療情報システム障害発生時 連絡体制図ひな型（大規模医療機関用）

P28を参考に、このひな型を修正し、連絡体制図を完成させましょう。

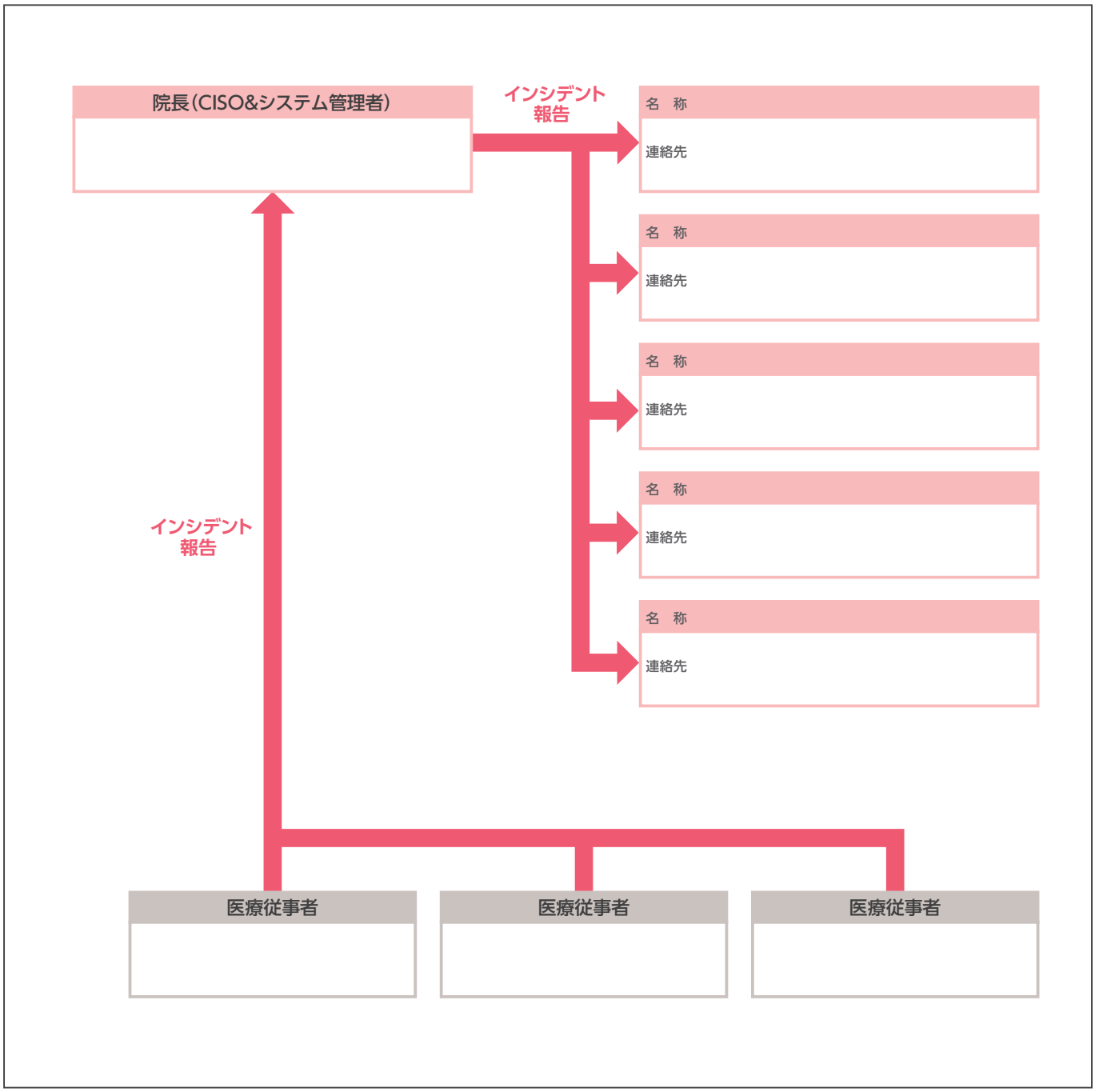
※ひな型はあくまで一般的な参考例を示したものであり、必ず自組織の実態に即した連絡体制図に修正することを推奨します。



医療情報システム障害発生時 連絡体制図ひな型（小規模医療機関用）

P28を参考に、このひな型を修正し、連絡体制図を完成させましょう。

※ひな型はあくまで一般的な参考例を示したものであり、必ず自組織の実態に即した連絡体制図に修正することを推奨します。



資料3

事業継続計画（BCP）ひな型

以下のひな型を参考に、BCPを策定しましょう。

※ひな型はあくまで一般的な参考例を示したものであり、必ず自組織の実態に即した計画に修正することを推奨します。

事業継続計画（ＢＣＰ）

―サイバー攻撃―

〇〇年〇〇月〇〇日

〇〇病院

第１章　総則

1.1　目　的

本事業継続計画（以下、「本ＢＣＰ」という。）は、〇〇病院（以下、「当院」という。）がサイバー攻撃を受けた場合の組織的対応の基本方針および職員の取るべき行動の基本原則を示すことによって、サイバー攻撃に対する体制の速やかな構築と、組織としての適切な対応の実施に資することを目的とする。

1.2　基本方針

当院は、医療サービスを提供する立場から、上記 1.1 目的に照らし、サイバー攻撃を受けた場合においても、業務を継続し、または可能な限り速やかに復旧させることが社会的使命と考え、次の方針に基づいて業務継続性の確保を図る。

（１）　サイバー攻撃による被害を極小化し、速やかな現状復帰を目指す。
（２）　お客様の信頼と業務継続性の確保のため、各担当部門における即応体制を整備し、実際の被害状況に応じて柔軟な対応を行う。

1.3　本ＢＣＰの適用範囲

本ＢＣＰは、当院内全部門に適用する。

1.4　文書の管理および周知

本ＢＣＰは、〇〇部門が原本の最新版管理を行い、当院内全部門の職員に開示し周知する。

第２章　想定する事象

2.1　対象とする医療情報システム

本ＢＣＰで、対象とする医療情報システムは以下のとおり。

（１）外来受付システム「〇〇」
（２）医療会計システム「〇〇」
（３）電子カルテ・オーダリングシステム「〇〇」
（４）医療情報を取扱う全職員端末

2.2　想定する事象

本ＢＣＰで想定する事象とは、以下のサイバー攻撃による医療情報システムの利用停止、または医療情報の漏えいまたはそのおそれとする。

（１）標的型メール攻撃
（２）不正アクセス等
（３）マルウェア感染（ランサムウェアを含む）
（４）上記の予兆と思われる事象

第３章　サイバー攻撃発生時の対応

3.1　初動対応

（１）発生事象の発見・報告

事象の発見者は、速やかに以下の内容を情報セキュリティ責任者（以下、「ＣＩＳＯ」という。）へ報告する。

① 発見日時・経緯
② 発生状況
③ 処置内容

（２）被害拡大防止・二次被害抑止

ＣＩＳＯは、被害拡大防止や二次被害抑止の観点で、以下の対応または指示を速やかに実施する。

① 事象が発生した該当端末等を院内ＬＡＮやインターネット等のネットワークから切り離す。
② 類似事象が他部門で発生していないかを確認し、発生している場合はネットワークを停止する。

（３）証拠保全・原因調査

ＣＩＳＯは、サイバー攻撃の原因や被害範囲の特定のために、以下の対応を行う。

① 発生した事実関係を時系列で整理し、情報を管理する。
② 端末初期化等を控えるよう指示し、外部調査に必要なシステム上の証拠を保全する。
③ 外部関係先と連携し、原因や被害範囲の特定のために必要な調査を実施する。
④ 調査の結果を踏まえ、関連法令に則り適切に情報を開示し、監督官庁への報告などを実施する。

（４）外部関係先への連絡

ＣＩＳＯは、以下に記載の外部関係先に、速やかに状況を連絡する。

外部関係先	組織名	担当者	連絡先
医療情報システム事業者	○○	○○	○○
顧問弁護士	○○	○○	○○
都道府県警	○○	○○	○○
厚生労働省	○○	○○	○○

3.2　業務継続対応

（１）業務継続対応

ＣＩＳＯは医療情報システムの継続利用の可否を判断し、縮退運用やシステムの利用中止を判断する。また、縮退運用やシステムの利用中止を判断した場合は、紙カルテによる代替措置など、自然災害を想定した事業継続計画（もしくはシステムダウン時マニュアル等）に則り運用する。

（２）業務復旧対応

早期に通常業務に戻るために、以下の対応を行う。

①　システム復旧について、システム事業者と連携し、その可否を判断する。

②　データ復旧について、バックアップデータの復旧手順に従い、データ復旧可否を判断する。

（３）診療可否の判断と診療形態の決定

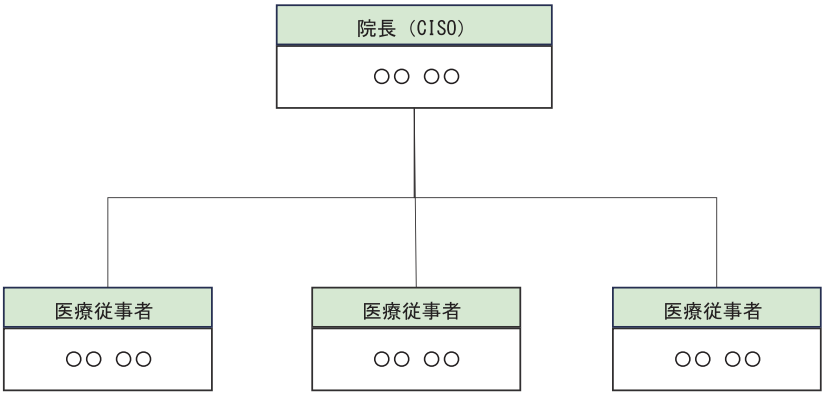
診療継続と判断した場合、提供可能な診療形態を速やかに決定する。

第４章　体制

4.1　医療情報システム安全管理責任者

院長を、当院のＣＩＳＯとする。

4.2　組織体制図



附　則

本ＢＣＰは、令和○○年○○月○○日から施行する。

公益社団法人 日本医師会