医科・歯科共通

サイバーセキュリティ対策が義務化

医療情報システムの安全管理に関するガイドラインとチェックリストで対策を

2023 年 4 月に医療法施行規則が改定され、第 14 条第 2 項に「病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティを確保するために必要な措置を講じなければならない」との内容が追加され、サイバーセキュリティ対策が義務化されました。医療機関等は最新の「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）」を参照し、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行うこととされています。

ガイドラインの対象となるのは、医療機関等において、すべての医療情報システムの導入、運用、利用、保守及び廃棄に関わる者です。具体的な医療情報システムについては、ガイドラインに関するＱ＆Ａで「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だけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するようなコンピュータや携帯端末も範疇として想定している。また、医療情報が通信される院内・院外ネットワークも含まれる」と示されています。

厚労省は、ガイドラインに記載されている内容のうち、優先的に取り組むべき事項をまとめたチェックリストとチェックリストマニュアルを示しました。チェックリストは「医療機関確認用」と「事業者確認用」の 2 種類があり、少なくとも年 1 回は点検を行うことが求められています。

6 月に医療法第 25 条第 1 項の規定に基づく立入検査要綱が改正され、「サイバーセキュリティの確保」が追加されました。立入検査の際、チェックリストに必要な事項が記載されているかの確認が行われます。また、インシデント発生に備えた対応として、組織内と事業者等の外部関係機関への連絡体制図の現物が確認されますので、立入検査までに作成が必要です。

以下に立入検査での点検項目と、優先的に取り組むべき厚労省のチェックリスト（医療機関確認用）を掲載しています。チェックリストとマニュアルは当会ホームページからもダウンロードいただけます。また、保団連ホームページに「医療安全管理対策の基礎知識」の追補版として、「医療情報システムの安全管理」が掲載されていますので、そちらもご活用ください。

「医療安全管理対策の基礎知識」（追補から抜粋）

3. 立入検査での点検項目と、優先的に取り組むべき厚生労働省チェックリスト

（1）2023 年 6 月改定の「医療法第 25 条第 1 項の規定に基づく立入検査要綱」では、「2－19 サイバーセキュリティの確保」のチェック項目として下記が新たに追加された。

① 必要な措置は「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」参照
② ガイドライン第6.0版のうち、医療機関において優先的に取り組むべき事項として、「『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』及び『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～』について」（令和5年6月9日医政参発0609第1号）で示す、「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」に必要な事項が記入されていることを確認する。
※チェックリストは（2）を参照いただきたい。
③ チェックリストにおいて医療機関に求める項目のうち、インシデント発生時の連絡体制図については、連絡体制図の提示を求めることにより、その有無を確認する。体制図に記載する連絡先は、下記が想定される。
ア 外部委託業者
イ 厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室
ウ 個人情報保護委員会（個人情報保護法第26条に基づく場合）
エ 都道府県警のサイバー犯罪窓口
オ 独立行政法人情報処理推進機構（事後報告）

（2）医療機関用の「チェック項目」は下記の通りで、医療法第25条第1項に基づく立入検査において点検される。

【2023年度中に整備が必要な項目】

1．体制構築
（1）医療情報システム安全管理責任者を設置している。
2．医療情報システムの管理・運用
≪医療情報システム全般≫
（1）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）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。（事業者と契約していない場合は不要）
（3）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。（事業者と契約していない場合は不要）
≪サーバ≫
（4）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。
（5）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。
（6）アクセスログを管理している。

≪ネットワーク機器≫

(7) 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。

(8) 接続元制限を実施している。

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。

【2024 年度中に整備が必要な項目】

2. 医療情報システムの管理・運用

≪サーバ≫

(7) 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。

(9) 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。

≪端末 PC≫

(4) 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。

(5) 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。

(7) 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。

(9) 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。

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。

(3) サイバー攻撃を想定した事業継続計画（ＢＣＰ）を策定、又は令和 6 年度中に策定予定である。