「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」の骨子（案）について（概要）

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

１．趣旨

○　「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。）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・厚生労働省医薬食品局長・厚生労働省保険局長連名通知）の別添として、医療情報システムの安全管理や、個人情報の保護に関する法律（平成 15 年法律第 57 号）、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）等の法令等への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したものである。

○　ガイドラインは平成 17 年３月の策定以降、技術の進展や制度改定等に対応する観点から、数度の改定を行っている。直近では、令和４年３月に、最新の制度的な動向や、医療情報システムに対するサイバー攻撃の巧妙化等の技術的な動向等を踏まえ、第 5.2 版に改定した。

○　ガイドライン第 5.2 版の策定以降の医療情報システムに関する動向として、「経済財政運営と改革の基本方針 2022」（令和４年６月７日閣議決定）を踏まえ、保険医療機関・薬局においては令和５年４月からオンライン資格確認の導入が原則義務化されることとなった。今後はガイドラインに記載されているネットワーク関連のセキュリティ対策がより多くの医療機関等に共通して求められることとなるため、これまで以上に医療機関等にガイドラインの内容の理解を促し、医療情報システムの安全管理の実効性を高めていくことが必要となる。

○　加えて、第 5.2 版の策定に向けた議論を行った「第８回健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ」（令和３年 12 月 17 日）において、引き続き十分な検討が必要であり、中長期的な論点として検討を継続することとされていたもの（※）について、必要な見直しを行う必要がある。

（※）クラウドサービス利用における課題や必要な対策、ゼロトラスト思考を踏まえたネットワーク上の対策、新技術並びに制度及び規格の変更への対応等。

○　以上を踏まえ、医療機関等におけるガイドラインの内容の更なる理解の促進を図るため、全体構成の見直しを行うとともに、第 5.2 版策定時において中長期的に検討を継続することとされた論点を中心に、最新の技術的な動向、巧妙化する医療機関へのサイバー攻撃の状況等を踏まえた内容面の必要な見直しを行うため、ガイドライン第 5.2 版を改定し、新たにガイドライン第 6.0 版を策定する。

２．第6.0版の骨子（案）

○　ガイドライン第5.2版の本編と別冊について、内容面の必要な見直しを行った上で、対象とする読者類型ごとに分冊化を行い、①各編に共通する前提内容を整理した概説編（Overview）、②医療機関等において組織の経営方針を策定し意思決定を担う経営層を対象とした経営管理編（Governance）、③医療情報システムの安全管理（企画管理、システム運営）の実務を担う担当者を対象とした企画管理編（Management）、④医療情報システムの実装・運用の実務を担う担当者を対象としたシステム運用編（Control）の４編構成とする。

○　４編については、それぞれ以下の内容を記載するものとする。

① 概説編（Overview）

各編を理解する上で前提となる考え方や各編の概要等を示すものとする。主な内容は以下のとおり。

- ガイドラインの目的
- ガイドラインの対象
  （医療機関等の範囲、医療情報・文書の範囲、医療情報システムの範囲）
- ガイドラインの構成、読み方
- ガイドラインの各編を読むに当たって前提となる考え方
  （医療情報システムの安全管理の目的、安全管理に必要な要素、関連する法令等）

等

② 経営管理編（Governance）

主に以下の内容について、経営層として遵守・判断すべき事項、企画管理やシステム運営の担当部署及び担当者に対して指示、管理すべき事項とその考え方を示すものとする。

- 医療情報システムの安全管理に関する責任・責務
- リスク評価を踏まえた管理
  （情報セキュリティマネジメントシステム（ISMS）の実践等）
- 医療情報システムの安全管理全般
  （経営層による内部統制、情報セキュリティ対策の設計及び管理、事業継続計画（BCP）の整備を含む情報セキュリティインシデントへの対策等）
- 医療情報システム・サービス事業者との協働
  （当該事業者の選定、管理、当該事業者との責任分界等）

等

③ 企画管理編（Management）

主に以下の内容について、医療機関等において組織体制や情報セキュリティ対策に係る規程の整備等の統制等の安全管理の実務を担う担当者として遵守すべき事項、医療情報システムの実装・運用に関してシステム運用担当者に対する指示・管理を行うに当たって遵守すべき事項とその考え方を示すものとする。

・　医療情報システムの安全管理全般
（関連する法制度、安全管理方針の策定、責任分界、管理・監査体制、必要な規程・文書類の整備、職員及び委託先の医療情報システム・サービス事業者の人的管理等）
・　リスクアセスメント（リスク分析・評価）とリスクマネジメント（リスク管理）
・　情報管理（情報の持ち出し、破棄等）
・　医療情報システムに用いる情報機器等の管理
・　非常時（災害、サイバー攻撃、システム障害）の対応と非常時に備えた通常時からの対策
・　サイバーセキュリティ対策
（通常時、サイバー攻撃に起因する非常時及び復旧対応時における対応を整理した計画の整備等）
・　医療情報システムの利用者に関する認証等及び権限管理
・　法令で定められた記名・押印のための電子署名

等

④　システム運用編（Control）

主に以下の内容について、医療機関等の経営層や企画管理者の指示に基づき、医療情報システムを構成する情報機器、ソフトウェア、インフラ等の各種資源の設計、実装、運用等の実務を担う担当者として適切に対応すべき事項とその考え方を示すものとする。

・　医療情報システムの安全管理における技術的対策
（端末等の情報機器、ソフトウェア、ネットワークに対する安全管理措置等）
・　システム設計・運用に必要な規程類と文書体系
・　技術的な対応における責任分界
・　リスクアセスメントを踏まえた安全管理対策
・　非常時（災害、サイバー攻撃、システム障害）の対応と非常時に備えた通常時からの対策
・　サイバーセキュリティ対策
（情報機器等の脆弱性対策、バックアップの実施・管理等）
・　医療情報システムの利用者や連携するアプリケーションの認証等及び権限管理
・　電子署名に関する技術的対応

等

○　各医療機関等が、それぞれの特性に応じたかたちでガイドラインを遵守し、必要な安全管理を確保できるよう、医療機関等の組織体制（専任のシステム運用担当者の有無）や稼働している医療情報システムの構成（オンプレミス型／クラウドサービス型）、採用しているサービス形態（医療情報システム・サービス事業者による提供サービスの範囲）等に応じたガイドラインの参照パターンを例示するとともに、当該パターンに応じた参照項目を示すこととする。

○　４編に加え、Ｑ＆Ａや用語集、小規模医療機関（病院、診療所、薬局等）向けの特集、サイバーセキュリティ対策に関する特集等により、４編の内容面の補足を行うものとする。