

改定概要

【第2版】

本ガイドライン初版公開（平成17年3月）後の平成18年1月、高度情報通信技術戦略本部（IT戦略本部）から、「IT新改革戦略」が発表された。IT新改革戦略では、「e-Japan戦略」に比べて医療情報の活用が重視されている。様々な医療情報による連携がメリットをもたらすものと謳い、連携の手法、またその要素技術について種々の提言がなされており、そのひとつに「安全なネットワーク基盤の確立」が掲げられている。

他方、平成17年9月に情報セキュリティ政策会議により決定された「重要インフラの情報セキュリティ対策に係る基本的考え方」において、医療をIT基盤の重大な障害によりサービスの低下、停止を招いた場合、国民の生活に深刻な影響を及ぼす「重要インフラ」と位置付け、医療におけるIT基盤の災害、サイバー攻撃等への対応を体系づけ、明確化することが求められた。

これらの状況を踏まえ、医療情報ネットワーク基盤検討会では、「(1) 医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義」、「(2) 自然災害・サイバー攻撃によるIT障害対策等」の検討を行い、本ガイドラインの改定を実施した。

「(1) 医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義」では、想定される用途、ネットワーク上に存在する脅威、その脅威への対抗策、普及方策とその課題等、様々な観点から医療に関わる諸機関間を結ぶ際に適したネットワークの要件を定義し、「6.10 外部と個人情報を含む医療情報を交換する場合の安全管理」として取りまとめている。さらには、関連個所として「8 診療録及び診療諸記録を外部に保存する際の基準」の中のネットワーク関連の要件について6.10を参照すること、医療機関等における当該ネットワークの運用の指針となる「10 運用管理について」の一部改定を実施している。

また、「(2) 自然災害・サイバー攻撃によるIT障害対策等」では、医療のITへの依存度等も適切に評価しながら、医療における災害、サイバー攻撃対策に対する指針として「6.9 災害等の非常時の対応」を新設して取りまとめ、情報セキュリティを実践的に運用して行くための考え方として「6.2 医療機関における情報セキュリティマネジメント（ISMS）の実践」の概念を取り入れ、「10 運用管理について」も該当個所の一部追記を行った。

なお、本ガイドライン公開後に発出、改正等がなされた省令・通知等についても制度上の要求事項として置き換えを実施している。基本的要件について変更はないが、制度上要求される法令等が変更されている点に注意されたい。