資料２

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

第25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

2025（令和7）年7月24日

医療情報システムの安全管理に関するガイドライン改定について

医政局医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

ガイドライン改定の背景・目的

改定の背景

○医療情報の安全管理に関するガイドライン（以下、本ガイドライン）については、令和5年5月に第6.0版を公表したところである。

○第6.0版は、医療機関等における医療情報の取扱いにおける安全管理の実効性向上を企図したものであり、外部サービスの利用に関する整理や非常時における対策、本人確認を要する場面での運用の検討等について新たに示した。

○一方で、ランサムウェアによる医療機関等に対する攻撃事案の発生が継続するほか、サイバー対処能力強化法の成立等、サイバーセキュリティへの社会的意識が一層高まっている。

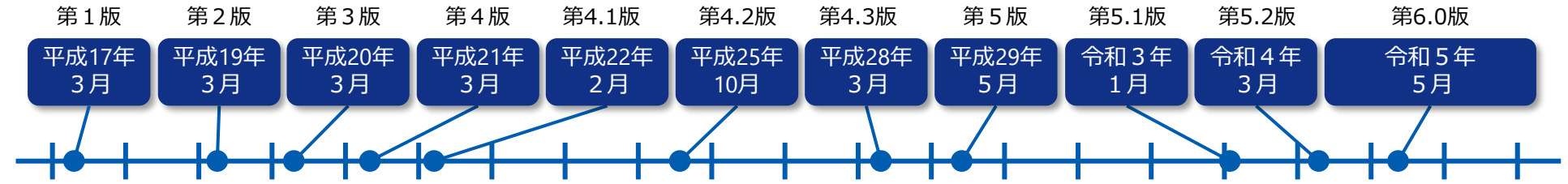
○また、生成AIをはじめとするAIサービス・クラウドサービスによる医療情報の取扱いの拡大、セキュリティ対策技術の進展や、それに伴う関係ガイドラインの改定も進み、これらに対応する必要がある。

目的

○医療情報の安全管理を強固なものとするため、セキュリティ対策技術の進展や、社会情勢の変化に対応した内容とすること。

医療情報システムの安全管理に関するガイドライン策定及び改定の経緯

- 医療情報システムの安全管理に関するガイドラインは、e-文書法、個人情報保護等への対応を行うための情報セキュリティ管理のガイドラインとして、平成17年3月に第１版を策定。
- 以降、各種制度の動向や情報システム技術の進展等に対応して改定し、**令和５年５月に第6.0版を策定。**



版	第１版、第２版、第３版	第４版（第4.1版、第4.2版、第4.3版）	第５版（第5.1版、第5.2版）	第6.0版
策定・改定概要	**第１版** • 医療情報システムのセキュリティ管理を目的とて策定 **第２版** • 重要インフラとしての医療情報システムという観点からの対応 **第３版** • 個人情報施策の議論およびモバイル端末普及への対応	**第4版** • 個人情報保護施策の議論およびモバイル端末普及への対応 **第4.1版** • 民間事業者のデータセンターにおける外部保存に関する対応 **第4.2版** • 調剤済み処方せん及び調剤録等の外部保存への対応 **第4.3版** • 「電子処方せんの運用ガイドライン」への対応	**第5版** • 医療機関等の範囲の明確化 • 改正個人情報保護法対応 • サイバー攻撃の動向への対応 **第5.1版** • クラウドサービスへの対応 • 認証・パスワードに関する対応 • サイバー攻撃等による対応 • 外部保存受託事業者の選定基準対応 **第5.2版** • ２省（総務省、経産省）GL等との整合性 • 改正個人情報保護法への対応 等 • 医療機関へのサイバー攻撃の多様化・巧妙化 • 「規制改革実施計画」等への対応 • 電子署名 • 外部ネットワーク　等	**第6.0版** 全体構成の見直し • 概説編、経営管理編、企画管理編、システム運用編の４編に再構成 • Q&Aの充実 等 技術的な動向 • 外部委託、外部サービスの利用に関する整理 • 情報セキュリティに関する考え方の整理 • 新技術、制度・規格の変更への対応 等

改定内容の検討

想定される改定論点

カテゴリ	論点
認証に関する論点	■ 医療情報システム等の制約や、業務上の制約等により、二要素認証の導入が難しい場合、システム運用編において、二要素認証に相当する認証対策が講じられている場合について示している。今後もこのようなケースを認めていくことの可否、認められる場合の具体的な要件等についての精緻化が求められる。 ■ NISTの”Digital Identity Guidelines”は現在第4版改定作業が進められている。この中でパスワードルールとして推奨する内容に変更が生じており、本ガイドラインへの適用の必要性等について検討する。
AI利用時の情報管理について	■ AIの開発、利用においては、モデルの学習のために医療情報の提供とその解析などのプロセスが存在する。本ガイドラインにおける第三者提供や事業者による解析について必要な対応を検討する。
クラウドサービス	■ 医療機関等が利用する医療情報システムにおいて、複数のクラウドサービスの連携により行われるケースが拡大していることが想定される。現行のガイドラインにおいては、認証・認可の関係やAPI等の連携について示しているところであるが、よりサプライチェーンリスクを想定した内容の追記を検討する。
関連ガイドライン等との整合性の確保	■ NCO（旧NISC）の策定する「重要インフラのサイバーセキュリティに係る安全基準等策定指針」や、2省ガイドライン等の改定が行われており、それによる本ガイドラインへの影響を確認し、必要があれば整合性の調整等をおこなう。

NIST：米国立標準技術研究所（National Institute of Standards and Technology）
NCO：国家サイバー統括室（National Cybersecurity Office）
NISC：内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity）
API：Application Programming Interface
2省ガイドライン：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

改定内容の検討

想定される改定論点

カテゴリ	論点
テレワーク等への対応	■ 医療機関等における従業者において、テレワーク等の導入が進められている。本ガイドラインでは、デバイスの持ち出しやBYOD、公衆LAN等に関する内容について定めているものの、医療従事者が医療機関等の外部から利用する際の内容は必ずしも明確にしていない。
サイバーセキュリティ対策	■ サイバーセキュリティ対策として、第6.0版からは多層境界防御による対策だけではなく、ゼロトラストの導入の有効性を示している。サイバー攻撃の巧妙化等は、第6.0版公表後も進んでいることから、ゼロトラスト対応や振る舞い検知などの有効な対策について、より具体的に示すことが想定される。
利用者（医療機関等）における理解	■ 第6.0版では、本ガイドラインにおいては、小規模医療機関等向けの特集を示すなどにより、小規模医療機関等における理解を促している。 ■ 本改定においても、より広く本ガイドラインの遵守を促すための対策を検討する。
外部委託	■ 本ガイドラインでは、外部保存を実施する場合に委託事業者に対して求める遵守事項や選定基準を示している。一方で、外部保存を伴わない形で医療機関等が機器やシステムの運用等を委託するケースも存在する。このため、必要に応じて外部委託全般に対する選定基準等についても検討する。 ■ また、クラウドサービス等の利用時には約款や利用規約への同意のみにより外部委託がなされる実態がある。その際のガイドラインへの適合性への課題、対応策等を必要に応じて検討する。

BYOD：Bring Your Own Device
LAN：Local Area Network

改定作業班構成員等

役職	氏名・所属等
座長・構成員 (五十音順・敬称略)	【座長】 ・田中 勝弥　国立がん研究センター 情報統括センター センター長 【構成員】 ・秋山 祐治　川崎医科大学 副学長・教授 ・石川 左門　日本薬剤師会 HPKI認証局 ・太田 聡司　一般社団法人 保健医療福祉情報システム工業会 電子カルテ委員会 副委員長 ・門林 雄基　奈良先端科学技術大学院大学情報科学領域 教授 ・菊池 浩明　明治大学大学院 先端数理科学研究科 専任教授 ・高倉 弘喜　国立情報学研究所 教授 ・武田 理宏　日本病院会、大阪大学医学部附属病院医療情報部 教授 ・玉川 裕夫　日本歯科医師会 情報管理担当 ・矢野 一博　日本医師会 総合政策研究機構 主任研究員 ・山田 哲史　京都大学 法学系 教授 大学院法学研究科附属法政策共同研究センター
オブザーバー	• 山本 隆一　医療情報システム開発センター • 総務省　情報流通行政局 地域通信振興課 デジタル経済推進室 • 経済産業省　商務・サービスグループ　ヘルスケア産業課 • デジタル庁　国民向けサービスグループ • 厚生労働省　医政局 医療情報担当参事官室
事務局	• 株式会社エヌ・ティ・ティ・データ経営研究所