資料５

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

第32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

2026（令和８）年５月29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

厚生労働省　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

○　令和５年５月の前回改定においては、ガイドライン全体構成の見直しを行うとともに、医療情報システムの外部委託に関する整理等に対応したところ。

○　前回の改定以降、医療機関等を対象としたサイバー攻撃事案の発生が継続しているほか、サイバー対処能力強化法の成立等を背景として、サイバーセキュリティに対する社会的関心及び重要性が一層高まっている。安全管理ガイドライン第6.0版の改定以降の、制度的、技術的、社会的な動向は以下のとおり。

安全管理ガイドライン　6.0版

新たな課題の発生

制度的な動向

○　国家サイバー統括室（NCO）が策定する「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」の改定（令和５年７月）

○　経産省・総務省の策定する「2省ガイドライン」の改定（令和７年３月）

○　厚生労働省として、クラウドネイティブ型の電子カルテを普及する方針

技術的・社会的な動向

○　単純なパスワードやその使い回しによる、サイバー攻撃被害の発生

○　医療情報システムの利用・運用にあたり、クラウドサービスを導入する医療機関の増加

ガイドラインに対するご意見

○　二要素認証が令和9年度から遵守事項となるにあたり、二要素認証を実装すべき対象を明確にする必要がある

○　医療機関等におけるセキュリティ人材の不足により、安全管理ガイドラインの読解・対応が困難

新たな課題への対応

安全管理ガイドライン　7.0版

安全基準等策定指針：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。各分野におけるサイバーセキュリティガイドラインに含むべき項目を示している。
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

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 • 石川 左門　日本薬剤師会　HPKI認証局 • 太田 聡司　保健医療福祉情報システム工業会　電子カルテ委員会 • 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
オブザーバー	• 山本 隆一　医療情報システム開発センター　理事長 • デジタル庁　国民向けサービスグループ • 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 • 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NTTデータ経営研究所

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てきたところ。

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

第7.0版

全体構成の見直し
- 保守委託機関編の追加

制度的な動向等
- 安全基準等策定指針等への対応
- クラウドネイティブ型電子カルテの推進
- パスワード要件の変更
- 二要素認証の対象明確化

等

医療情報システムの安全管理に関するガイドラインの改定
～ 制度的な動向を受けての改定内容 ～

前回改定からの制度的変化	改定内容
NCOの策定する「安全基準等策定指針」の改定	■ NCO（旧NISC）の策定する「安全基準等策定指針」の本ガイドラインへの影響を確認し、対応すべき項目を追記。 （追記内容例） ・関連する法令として、サイバーセキュリティ基本法を追加 ・サプライチェーンリスクの追記　等
経産省・総務省の策定する「2省ガイドライン」の改定	■2省ガイドラインによる影響を確認し、下記を含む追記と整合性の確認を実施。 （追記内容例） ・医療機関等と事業者との役割分担 ・医療機関とのリスクコミュニケーションについて　等
厚生労働省によるクラウドネイティブ型電子カルテの導入の推進	■ システム導入や運用におけるセキュリティ対応には、高い専門性が求められる。この実施を可能な限り事業者に委託するため、クラウドサービスの積極的な活用を推進する旨を追記。

NCO：国家サイバー統括室（National Cybersecurity Office）

医療情報システムの安全管理に関するガイドラインの改定
～ 技術的・社会的な動向を受けての内容 ～

前回改定からの技術的・社会的動向	改定内容
単純なパスワードやその使い回しによるサイバー攻撃被害の発生	■ パスワードルールに関して、使い回しの禁止、アカウントロックの導入について追記。 ■ 一方で、セキュリティ面の強化につながらないとされる「定期的な変更」の要件を削除。

ガイドラインに対するご意見	改定内容
二要素認証対象が明示されていない	■ 二要素認証の導入について、医療情報システムのうち、クライアント端末およびサーバについて対応することを明確化。 ■ これまで対象が明確化されていなかった点も踏まえ、令和9年4月1日時点での対応が困難な医療機関等においては、次期システム改修での対応を許容する旨の緩和措置を設定。
医療機関におけるセキュリティ人材の不足によりガイドラインの読解・対応が困難	■ 専門人材の不足している小規模医療機関を想定した医療機関等保守委託機関編を策定。すべてのサーバ（※） におけるセキュリティアップデートを委託（クラウドサービスの利用を含む）している医療機関等においては、保守委託機関編を遵守することで、その他の編の項目も遵守できているものとみなす旨を追記。 （※）例えばCD-Rで電子カルテのアプリケーションをインストールして運用するなど、サーバ機能を果たすPC等の端末も含む。

医療情報システムの安全管理に関するガイドラインの改定
～ パブリックコメントの状況（R7.3.27-4/17） ～

○　3週間のパブリックコメント募集を実施し、294件のご意見を賜り、適宜いただいたご意見を本文に反映した。
○　いただいたパブリックコメントのうち、引き続きの検討が必要と考えられるものにつき順次対応を行う。

対象(編)	件数	備考
概説編	25	ガイドライン全体の方向性・用語・記述の正確性に関する意見
経営管理編	24	中小規模医療機関への配慮、経営層の責務、グループ管理
企画管理編	42	責任分界、外部委託、人的管理、認証、診療録等電子化
システム運用編	134	二要素認証、VPN、医療機器、技術的対策、フィッシング対策
保守委託機関編	50	対象範囲、認証取得、責任分界、タイトル変更、契約ひな型
全体	15	用語整理、文書品質、章構成等の総論
その他	3	AI、データ主権等のガイドライン本体外の論点
QA	1	医療機器と薬機法等との関係整理(Q&A化要望)
合計	**294**	

医療情報システムの安全管理に関するガイドラインの改定
～ パブリックコメントを受けての積み残し課題 ～

○　以下2点の積み残し課題について、7.0版改定後も継続して検討し、可及的速やかに7.1版への改定を目指す。
○　一方で、その他の事項については7.1版への改定では原則検討しないものとする。

課題①：医療機器の二要素認証

○　医療機器については、現在、世界的な動向としても二要素認証が必須化されていないこともあり、今回の改定では改変を見送る。

○　二要素認証を求める対象等について、引き続き検討する。

課題②：国内法の執行に関する規制

○　「情報機器等が、国内法の適用及び執行の及ぶ範囲にあること」としたが、実際にはがんパネル検査のように日本でのサービス供給量が十分でなく、当然海外に保存されているような医療情報も存在する。現状の記載がこのような実態に則さない規制となっている可能性がある。

○　このため、まずは現状の把握に努めるとともに、それを踏まえた対応案について引続き検討する。

Ministry of Health, Labour and Welfare of Japan

参考資料

ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

（参考）電子処方箋・電子カルテの目標設定等の概要①

第７回「医療DX令和ビジョン2030」
厚生労働省推進チーム
（令和７年７月１日）　資料２

１．電子処方箋の新目標

- 電子処方箋については、「概ね全国の医療機関・薬局に対し、2025年３月までに普及させる」※1こととしていた。
  2025年６月時点で運用開始済の薬局は８割を超えており、薬局については今夏には概ね全ての薬局での導入が見込まれる。
  一方、医療機関への導入は１割程度に留まる。
- 医療機関において電子処方箋の導入を進めるにあたっては、電子カルテが導入されていることが重要であるため、**電子処方箋の新たな目標では、電子カルテ／共有サービスと一体的な導入を進めることとし、「患者の医療情報を共有するための電子カルテを整備するすべての医療機関への導入を目指す」**。

  歯科医療機関については、現場に求められる電子カルテ・電子処方箋の機能に関し、本年度から検討を行い2026年度中に具体的な対応方針を決定する。

※１ 医療 DX の推進に関する工程表 2023.6.2 医療ＤＸ推進本部

２．電子カルテ／共有サービスの普及策

- 電子カルテについては、「遅くとも2030年には概ねすべての医療機関において必要な患者の医療情報を共有するための電子カルテの導入を目指す」※1こととしている。この目標達成に向け、オンプレ型で、かつ、カスタマイズしている現行の電子カルテから、いわゆるクラウドネイティブを基本とする廉価なものへと移行することを図りつつ、
  ① 電子カルテ導入済の医療機関※2には、次回更改時に、共有サービス／電子処方箋に対応するシステム改修等の実施、
  ② 電子カルテ未導入の医療機関※2には、**共有サービス／電子処方箋に対応できる標準化された電子カルテの導入**を進める。

※２ 医科診療所／病院が対象。歯科医療機関については、現場に求められる電子カルテ・電子処方箋の機能に関し、本年度から検討を行い2026年度中に具体的な対応方針を決定する。

今後の主な対応方針

- 標準型電子カルテ（デジタル庁で開発中）について、本格運用の具体的内容を2025年度中に示した上で、**必要な支援策の具体化を検討**するとともに、**2026年度中目途の完成**を目指す。
- 併せて、標準型電子カルテの要件※3を参考として、**医科診療所向け電子カルテの標準仕様（基本要件）を2025年度中に策定**する。

※３ 小規模な医療機関でも過度な負担なく導入が可能となるよう、①共有サービス・電子処方箋管理サービスへの対応、②ガバメントクラウドへの対応が可能となり、かつ、１つのシステムを複数の医療機関で共同利用することで廉価なサービス提供が可能となるマルチテナント方式（いわゆるSaaS型）のクラウド型サービスとする、③関係システムへの標準APIを搭載する、④データ引き継ぎが可能な互換性を確保すること等を要件とする方向。

- **2026年夏までに、電子カルテ／共有サービスの具体的な普及計画**を策定する。

（参考） Project YATA-Shield

● フロンティアAIモデルによるサイバーセキュリティ性能が向上する中においても、我が国のサイバーセキュリティが確保されるよう、**政府全体としての対策パッケージを取りまとめ**。

基本的な認識・考え方

重要インフラ事業者等・政府機関等が取るべき対応

- **発見された脆弱性のパッチ適用やリスク緩和措置**を速やかに実施（リスクベース）
- **基本的な対策**、**多層防御の実施**、**インシデント発生時の備え**　等

※英国・米国政府の注意喚起も参考に

脆弱性を発見するAIの進化

- **Anthropic（Project Glasswing）**：Mythosへのアクセスを、**ビッグテックや重要インフラ等**に限定。
- **OpenAI**：GPT-5.5-Cyberへのアクセスを、**一部の認証者**に限定して付与。

実施する施策

重要インフラ事業者等・政府機関等への対応

① **重要インフラ事業者等への注意喚起等**

② **金融分野での先行的な取組及び 他分野への展開**

③ **人材育成支援**

④ **政府機関等の情報システムにおける対応**

脆弱性の発見・修正等への対応

① **外国政府機関やビッグテック等との更なる連携**

② **ソフトウェア・ベンダへの注意喚起**

③ **AISIによる技術支援等**

④ **技術開発の推進**

⑤ **高性能AIを活用したサイバー対処能力強化**

関係機関への注意喚起

AI によるサイバー攻撃に関する情報共有と
医療機関等におけるサイバーセキュリティ対策に関する
厚生労働省との意見交換（令和８年５月22日）資料１

● 対策パッケージ「Project YATA-Shield」の取りまとめ・公表を行い、**重要インフラ事業者等、政府機関等、ソフトウェア・ベンダへの注意喚起**を公表・実施。

重要インフラ事業者等

●**経営層のリーダーシップの下での対策の実施**

→ 必要な投資と捉えて、組織のリスクマネジメントとして実施

●**基本的な対策の確実な実施等**

英：基本的な対策
米：隔離・復旧
} が重要

→ 資産管理、脆弱性対策、インシデント対応・復旧など（重要インフラ統一基準）

→ 実施状況の機動的な確認

●**高速化する脆弱性の発見・修正等への対応**

→ 脆弱性のリスク評価、パッチ適用・リスク緩和措置の速やかな実施

政府機関等

●**組織トップのリーダーシップの下、対応の徹底を要請**

●**基本的な対策の徹底**

英：基本的な対策
米：隔離・復旧
} が重要

→ 資産管理、脆弱性対策、インシデント対応・復旧など（政府統一基準）

→ 実施状況の機動的な確認（各機関・NCOによる監査）

●**脆弱性対策の強化**

→ パッチ管理・適用の運用設計の見直し、パッチ適用・リスク緩和措置の速やかな実施

ソフトウェア・ベンダ

●**高性能AIも活用**しながら、**脆弱性の早期発見・対応**

① リリース前のソフトウェア

→ 脆弱性を低減させた上でリリース

② リリース後のソフトウェア

→ 脆弱性の把握、パッチの早期作成、顧客への早期提供

（参考）医療機関等において改めてご確認いただきたい事項

AI によるサイバー攻撃に関する情報共有と医療機関等におけるサイバーセキュリティ対策に関する厚生労働省との意見交換（令和８年５月22日）資料３

「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」を用いて
皆様の医療機関等におけるサイバーセキュリティの取組をご確認ください。

経営層の関与と意思決定体制の確立

経営層の主体的関与
サイバーセキュリティは経営課題。経営層の積極的関与が不可欠

ガバナンス体制の確立
ガバナンス体制を構築し、方針や資源配分を明確化

責任者の任命と役割定義
責任者を明確化→権限と責任範囲を定め→迅速な意思決定

意思決定フローと訓練
インシデント時の連絡系統や意思決定フロー整備→机上訓練

インシデント対応体制と教育・訓練

初動対応手順の明確化（インシデント対応の基本）
感染端末の隔離や影響範囲の迅速な確認

報告・連携体制の整備
厚生労働省や関係機関への連絡先を事前に確認

事後対応と再発防止
原因分析と継続的な技術・運用・組織改善→再発防止

教育・訓練の重要性
全職員対象の定期的な教育やフィッシング訓練で対応力を強化

リスク管理・脆弱性対策・ランサムウェア対策

リスク管理の重要性
医療情報システム全体を把握し、資産ごとのリスク評価を行う

多層的な防御策
ネットワーク分離、多要素認証、アクセス制御などの段階的防御で侵入と拡大を防ぐ

脆弱性発見と更新管理
脆弱性の早期発見と迅速なセキュリティパッチ適用が不可欠

ランサムウェア対策
オフラインバックアップや復旧訓練、不審メール対策→被害を最小化

サプライチェーン対策とBCPの確保

サプライチェーン全体の連携
医療機器メーカーやシステムベンダーと連携し、脆弱性やインシデント情報を共有する体制の構築

調達段階のセキュリティ要件
調達時にセキュリティ要件を契約条件として明確化→リスクを未然に抑制

事業継続計画（BCP）の策定と代替手段準備
サイバー攻撃を想定したBCPを策定→紙運用等代替手段用意

訓練と継続的改善
「サイバー攻撃を想定したBCP策定のための確認表」を用いてBCPを策定→定期的な訓練で実行性を検証、改善