医療情報システムの安全管理に関するガイドライン第5.1版（案）について

2020年10月2日

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

医療情報システムの安全管理に関するガイドライン第5.1版の改定概要

改定の背景

サイバー攻撃の手法の多様化・巧妙化、地域医療連携や医療介護連携等の推進、「IoT（モノのインターネット）」と称される新技術やサービス等の普及、各種ガイドライン等の変更等、医療情報システムを取り巻く環境の変化に対応するため、「医療情報システムの安全管理に関するガイドライン」（以降、安全管理ガイドライン）の中で関連章を改定するとともに、第5版の公表以降に追加された標準規格等への対応等を行う。

改定概要

【4章】
- クラウドサービスを利用する場合の責任分界の考え方等について、追記する。

【5章】
- 新たに加わった厚生労働省標準規格の内容を更新する。

【6章】
- 「6.5 技術的安全対策」において、二要素認証の導入促進に関する対応、パスワード要件の明確化、サイバー攻撃に対する考え方、Bluetoothなどの近距離無線を利用した機器に関するセキュリティなどについて追記、更新を行う。
- 「6.10.　災害、サイバー攻撃等の非常時の対応」において、非常時に備えたセキュリティ体制の整備、医療情報システムに障害が発生した場合の医療機関等における報告等に関する責務について、追記、更新を行う。
- 「6.11 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」において、内部ネットワークの監視等、無害化対応についての考え方等について、追記更新を行う。また暗号鍵に関する対応について、「④　暗号化を行うための適切な鍵管理」を新設し、その考え方を示す。また医療機関等がクラウドサービスを用いた場合についての対応についても、追記を行う。

【8章】
- 「8.1.2　外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」において、外部事業者の運営組織形態の違いによって定められていた要求事項等を、全ての運営組織形態で一本化した。また選定時において確認すべき事項について明示するほか、委託先となる外部事業者における国内法の適用等の確認を行う旨についても、明確化した。

上記の改定に加え、分かりやすさの観点から全般的に表現の修正を行い、本ガイドラインが参照している資料について、最新の版に合わせ名称等を更新する。

改定テーマ一覧

第5.1版では、下記の7テーマを軸に所要の改定を行う。次頁以降、改定テーマごとに改定内容を説明する。

項番	改定テーマ
1	クラウドサービス利用の拡大への対応
2	二要素認証の必要性及びパスワードの要件の明確化
3	Bluetooth等に関する安全対策への対応
4	サイバーセキュリティ事故情報の報告スキームの明確化
5	暗号鍵の管理要件への対応
6	近時のサイバー攻撃への対応
7	外部保存を受託する機関の選定基準への対応

1．クラウドサービスの利用の利用拡大への対応

改定方針

- クラウドサービスの拡大に伴い、クラウドサービスを利用する場合の責任分界点のあり方等を追記する。

改定の意図

① オンライン外部保存を委託する場合の責任分界の考え方に関して、クラウドサービスを利用する場合の責任分界点のあり方等を追記する。

改定案

- クラウドサービスを利用した責任関係を明らかにするために、「4.3　例示による責任分界点の考え方の整理」のB項においてクラウドサービスの概要説明を追記する。（P30）
- 同B項において、クラウドサービスの提供形態に則した管理方法に基づく責任分界の設定が必要な旨を追記する。（P30）
- クラウドサービスの利用において、サービス間相互に依存関係（垂直連携、水平連携）がある場合の責任分界等の取決めの重要性を示す。（P30-31）

1．クラウドサービスの利用の利用拡大への対応

改定の意図	改定案
② 医療機関等が、外部のネットワーク上で提供される複数のサービスを利用する場合等における安全性確保のための対応を明記する。	「6.11 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」のB項「B-2. 選択すべきネットワークのセキュリティの考え方」において、複数のクラウドサービスの利用などの場合に、各利用サービスの内容等を踏まえ、必要に応じてネットワーク分離を図ることや、データ交換の管理を行う旨の考え方を追記する。（P84、P86-P87）
③ 医療機関等で管理する医療情報を、患者の依頼に基づき医療機関等から第三者（クラウドさサービス事業者等）に提供する際の責任分界等を整理する。	「6.11 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」のB項「B-4.患者等に診療情報等を提供する場合のネットワークに関する考え方」において、医療機関等が、患者が契約するクラウドサービス事業者に診療情報等の患者情報を送信等するよう患者から依頼された場合の対応や、責任分界の取決め等を行う必要性等について明記する。（P93）
④ 医療機関等がクラウドサービス等を利用する際に、サービス利用上必要なCookie情報で、患者に関するものを受託事業者に提供した場合の対応を明記する。	「8.1.2 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」のB項「3.情報の提供」において、受託事業者が取得した患者に関するCookie情報について、受託事業者において第三者提供等を禁止する取り決めを行う必要性を明記する。（P121）

2．二要素認証の必要性及びパスワードの要件の明確化

改定方針

- より高いセキュリティが期待できる二要素認証の導入を促進するため、第5版の記載からさらに進めて記述する。
- パスワードの定期的変更を不要とする場面も含め、パスワードの利用方法等の違いによるリスクに応じた設定ルールを明記する。

改定の意図	改定案
① より高いセキュリティが期待できる二要素認証の導入を促進するため、第5版の記載からさらに進めた記述とする。	• 「6.5. 技術的安全対策」B項において、二要素認証の導入をさらに強く推し進める必要性に言及する。（P53） • 「6.5. 技術的安全対策」C項において、本ガイドライン改定後に、新規導入、あるいは更新する医療情報システムについて、二要素認証又はこれに相当する対応を図る必要があることを明記する。（P60）
② パスワードの定期的変更を不要とする場面も含め、パスワードの利用方法等の違いによるリスクに応じたパスワード要件を明記する。	• 「6.5. 技術的安全対策」B項において、パスワードを定期変更する場合については、従来のパスワードに関するルールを踏襲するとともに、定期変更しない場合のパスワード設定等のルールについて言及する。（P53） • 「6.5. 技術的安全対策」C項において、パスワードの定期的変更の有無や二要素認証を採用している場合等のリスクに応じたパスワード要件を明確化する。（P61）

3．Bluetooth等に関する安全対策への対応

改定方針

情報交換において用いられるBluetoothなどの近距離無線を利用した機器に関するセキュリティ上の対応を明記する。

改定の意図

情報交換において用いられるBluetoothなどの近距離無線を利用した機器に関するセキュリティ上の対応を明記する。

改定案

「6.5.　技術的安全対策」」のB項「(6)　医療等分野におけるIoT機器の利用」において、IoT機器に対するセキュリティ対策として、以下の3点について言及する。（P59）

- IoT機器が用いる通信規格の脆弱性を確認することが望ましい旨
- 不要な接続は行わない旨
- IoT機器の利用状況に関する状況を収集して不正に利用者を特定されるリスク

4．サイバーセキュリティ事故情報の報告スキームの明確化

改定方針

サイバー攻撃やセキュリティ事故が発生した場合に、必要な対応を講じるための体制の在り方や、報告のあり方について、明記する。

改定の意図	改定案
① 非常時に備えたセキュリティ体制の整備を行うために、緊急時対応に必要な体制の構築の必要性を明記する。	「6.10. 災害、サイバー攻撃等の非常時の対応」のB項において、非常時に備えたセキュリティ体制の整備を行うための解説項目を設け、緊急時対応に必要な体制の構築の必要性を明記する。（P75） 併せて、一定の医療機関等において、情報セキュリティ責任者(CISO)や緊急対応体制(CSIRT等)の設置の必要性を明記する。（P75）
② サイバー攻撃により医療情報システムに障害が発生し、個人情報の漏洩や医療提供体制に支障が生じるなどの事象が発生した場合の医療機関等における報告等に関する責務を明記する。	「6.10. 災害、サイバー攻撃等の非常時の対応」のC項4.における現状の報告に関する規定を、「医療機関等におけるサイバーセキュリティ対策の強化について（平成30年10月29日通知）」で示す、サイバー攻撃により医療情報システムに障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案について厚労省へ報告を行うこと、及びこれに必要な体制を整備する旨に変更する。（P75）

5．暗号鍵の管理要件への対応

改定方針

医療情報システムにおいて用いられる暗号化を行うための各種の鍵を管理するための対策を明記する。

改定の意図	改定案
①暗号化を行うための各種の鍵を管理するための対策を明記する。	「6.11　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」のB項に、「④　暗号化を行うための適切な鍵管理」を新たに設け、暗号鍵について、利用場面に応じた適切な管理を求める旨の考え方を明記する。 またD項において、同内容について、対策項目として規定する。（P80,P96）
②　電子署名に用いる秘密鍵の管理における対応を明記する。	「6.11　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」のB項に、「④　暗号化を行うための適切な鍵管理」を新たに設け、電子署名に用いる秘密鍵について、認証局のポリシーに基づいて管理すべき旨と、格納機器の要件について対策項目等で明記する。 またC項において、同内容について、対策項目として規定する。（P80,P96）

6．近時のサイバー攻撃への対応

改定方針

近時のサイバー攻撃の高度化・多様化を踏まえた対応措置の必要性、対応策等について明記する。

改定の意図	改定案
① サイバー攻撃が行われた場合に、迅速にこれを検知し、アラートを上げるための仕組みの必要性を明記する。	「6.5 技術的安全対策」B項の「(3)アクセスの記録(アクセスログ)」において、サイバー攻撃等が行われた場合に、迅速にこれを検知するために、ログ分析を行い、緊急時にアラートをあげる仕組みの必要性について追記する。(P56)
② クローズドネットワークにおける不正な通信等による攻撃への対応を明記する。	• 「6.5 技術的安全対策」B項の「(5)ネットワーク上からの不正アクセス」において、近時のサイバー攻撃に対応するため、医療機関等の内部における不正な通信等のモニタリング(内部脅威監視)を推奨することの必要性について、明記する。(P57) • また「6.11 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」のC項において、内部トラフィックにおける脅威の拡散等を防止するための措置を講じるべき旨を規定する。(P96)

6．近時のサイバー攻撃への対応

改定の意図	改定案
③ 外部からのデータ取り込み等において、標的型攻撃等からのリスクを低減するための措置の必要性を明記する。	「6.11 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」B項の「B-2. 選択すべきネットワークのセキュリティの考え方」において、外部からのデータ取り込み等において、標的型攻撃等からのリスクを低減するために、無害化等の措置を講じることを明記する。（P86）
④ 「TLS暗号設定ガイドライン3.0.1版」の公表を踏まえ、同ガイドラインで求める高セキュリティ型に関する変更内容を反映する。	「6.11 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」B項の「B-2. 選択すべきネットワークのセキュリティの考え方」及びC項において、オープンネットワークにおいてHTTPSを利用する場合のTLSのプロトコルバージョンをTLS1.2のみに限定している第5版の記載から、TLS1.3に限定し、システム・サービス等の対応が困難な場合にはTLS1.2の設定によることも可能であることと変更した。（P85、P95）

7．外部保存を受託する機関の選定基準への対応

改定方針

外部保存を行う事業者の実態の反映や、必要なリスク管理を行う観点から、外部保存を受託する機関の選定基準の整理等の対応を行う。

改定の意図	改定案
① データセンター等の運営組織形態の違いによって定められていた要求事項等を、全ての運営組織形態で一本化した要求事項等とする等の対応を行う。	「8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」のB項において行政機関が設置するデータセンターと民間事業者が設置するデータセンターの選定基準を整理し、統合する。 またC項における対策項目についても、統合する。 （P119-P124）
② 外部保存する医療情報を格納するシステム等について、国内法が適用されることを確認する必要があることを明記する。	「8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」のB項「1.外部保存を受託する事業者の選定基準」において、外部保存する医療情報を格納するシステム等について、国内法が適用されることを確認する必要がある旨の考え方を示すとともに、同C項において上記内容を要求事項として明記する。（P120、P123）

7．外部保存を受託する機関の選定基準への対応

③　受託事業者における情報管理に係るリスク判断をするのに必要な情報を確認する必要があることを明記する。

- 「8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」のC項において、受託事業者における情報管理等の状況や、認証の取得状況などを確認すべき旨を明記する。（P123）
- 「8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」のB項「1.外部保存を受託する事業者の選定基準」において、外部保存する医療情報を受託する事業者に国外法が適用される可能性を確認する旨の考え方を示すとともに、同C項において上記内容を要求事項として明記する。（P120、P123）。