参考資料5

「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

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の背景

第1回医療等情報利活用WG資料抜粋

医療情報システムの安全管理に関するガイドライン（平成29年5月）第5版

新たな状況の発生

技術的な動向

【スマートフォンや各種クラウドサービス等の医療現場での普及】
- スマートフォン・タブレット端末がモバイル端末の主流へ
- 医療分野におけるクラウドサービスの多様化と普及
- PaaSなどクラウドサービスのさらなる普及とサプライチェーンの複雑化

【サイバー攻撃の多様化・巧妙化】
- 標的型攻撃による被害、ビジネスメール詐欺による被害、ランサムウェアによる被害が外部からの攻撃として増加
- 国内医療機関におけるランサムウェアによる被害の発生

【各種ネットワークサービスの動向への対応】
- ISDN、PHSのサービス停止への対応
- ５Gサービスの開始

制度的な動向

【各種ガイドラインとの整合性の確保】
- 重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）等、他のガイドラインへの対応
- 「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」と「クラウドサービス事業者が医療情報を取り扱う際の安全管理ガイドライン」の一本化の検討

【個人情報保護法制への対応】
- GDPR（欧州）への対応要否の確認
- Cookie等、非個人情報に対する対応の要請

新たな課題への対応

安全管理ガイドラインの改定（第５・Ｘ版）

安全管理ガイドラインの主な改定検討内容

- 新しい動向の中から論点を抽出し、安全管理ガイドライン第5版への影響などを検討したうえで、追記の要否およびその具体的な内容を決定して、改定案等を作成する。

主な論点	具体的な検討内容
• ネットワークサービスの動向	• 近時のサイバー攻撃への対応」 • パスワードに関する記述対応 • 暗号鍵の管理要件に関する記述対応」 • サイバーセキュリティ事故情報の報告スキーム
• 端末等の動向	• Bluetooth等に関する安全対策 • Cookieに関する対応
• クラウドサービス利用の拡大	• ネットワーク上の複数サービス間の安全性確保のためのセキュリティ要件等 • サプライチェーンを踏まえた責任分界の検討 • 患者の依頼に基づき医療機関等から患者情報を提供する際の責任分界等の整理
• 重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）等、他のガイドラインへの対応	• 「近時のセキュリティに関連するガイドライン等との整合性の確認」
• 表現の全般的な見直し	• わかりにくい表現の見直し • 表現の正規化・標準化

検討を踏まえた改定の対応方法

- **必要性が高いものは対策項目（C項・D項）に記述**
- **特に留意すべき内容の喪については考え方（B項）等で対応**
- **具体的な対応に関するものはQAなどで対応**

検討結果に関する安全管理ガイドラインの改定素案の記載個所

第1回医療等情報利活用WG資料抜粋

- ガイドラインの以下の記載個所に、今回の検討結果を反映することとした。

4．3　例示による責任分界点の考え方の整理	• サプライチェーンを踏まえた責任分界の検討
6．5　技術的安全対策	• パスワードに関する記述対応 • 近時のサイバー攻撃への対応 • Bluetooth等に関する安全対策
6．10　災害、サイバー攻撃等の非常時の対応	• サイバーセキュリティ事故情報の報告スキーム
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	• 暗号鍵の管理要件に関する記述対応 • 近時のサイバー攻撃への対応 • ネットワーク上の複数サービス間の安全性確保のためのセキュリティ要件等 • 患者の依頼に基づき医療機関等から患者情報を提供する際の責任分界等の整理
8．1．2	• 近時のセキュリティに関連するガイドライン等との整合性の確認 • 近時のサイバー攻撃への対応

4.3　例示による責任分界点の考え方の整理

ガイドライン記載個所	論点	改定素案における対応
オンライン外部保存を委託する場合	「サプライチェーンを踏まえた責任分界の検討」	◆クラウドサービスの概要説明を追記 ◆クラウドサービス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 ◆クラウドの利用方法により、ポリシーの自動適用を講じていることの確認について追記 ◆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について追記

6.5　技術的安全対策

ガイドライン記載個所	論点	改定素案における対応
（1）利用者の識別及び認証	「パスワードに関する記述対応」	◆パスワードの定期変更については、引き続き対策項目に残す。 ◆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は二要素認証又はこれに相当する対応を図る旨の項目をC項に新設
（3）アクセスの記録（アクセスログ）	「近時のサイバー攻撃への対応」	◆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、 B 項に追記
（5）ネットワーク上からの不正アクセス		◆医療関係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）を推奨する考えをB項に追記
(7) 医療等分野におけるIoT機器の利用	Bluetooth等に関する安全対策	◆Bluetoothなどの近距離無線機器の脆弱性を確認すべき旨をB項に追記

6.10　災害、サイバー攻撃等の非常時の対応

ガイドライン記載個所	論点	改定素案における対応
	「サイバーセキュリティ事故情報の報告スキーム」	◆Ｂ項に「(4) 非常時に備えたセキュリティ体制の整備」を新設し、緊急時対応に必要な体制の構築の必要性を追記。 ◆一定の医療機関等において、CISOやCSIRTの設置の必要性を追記
		◆現状の報告に関する規定を、「医療機関等における医療情報システム障害等が発生した場合の対応について」（医政局※策定中）に示す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（C項）

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

ガイドライン記載個所	論点	改定素案における対応
B-1 医療機関等における留意事項	「暗号鍵の管理要件に関する記述対応」	◆「④暗号化を行うための適切な鍵管理」を新設し、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B項に記載。 ◆電子署名に用いる秘密鍵については、認証局のポリシーに基づいて管理すべき旨の項目をC項、格納機器の要件等については、D項に、それぞれ対策項目を新設。
B-2 Ⅱ．オープンなネットワークで接続されている場合	「近時のサイバー攻撃への対応」	◆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B項に追記
	「ネットワーク上の複数サービス間の安全性確保のためのセキュリティ要件等」	◆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B項に追記
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	「患者の依頼に基づき医療機関等から患者情報を提供する際の責任分界等の整理」	◆診療情報につき、患者が契約する事業者に送信等を患者から依頼された場合の対応や、責任分界の取決めを行う旨をB項に追記

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

ガイドライン記載個所	論点	改定素案における対応
1.外部保存を受託する機関の選定基準	近時のセキュリティに関連するガイドライン等との整合性の確認	◆受託事業者のセキュリティ状況を確認すべき旨をB項及びC項に追記 ◆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旨をC項に新設。 ◆受託事業者選定基準策定に際して、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を追記
3. 3.情報の提供	「近時のサイバー攻撃への対応」	◆受託事業者が取得した患者に関するCookie情報の第三者提供を禁止する旨を追記