資料５－１

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素案概要

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

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版（平成29年5月）

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）

医療情報システムの安全管理に関するガイドライン」改定に向けた調査一式
改定作業班構成員等

論点	氏名・所属等
座長・構成員 （五十音順・敬称略）	座長 • 山本　隆一　医療情報システム開発センター 理事長 構成員 • 秋山　祐治　医療ネットワーク岡山協議会 常任理事 • 小尾　高史　東京工業大学 科学技術創成研究院 准教授 • 河野　行満　日本薬剤師会 中央薬事情報センター 医療情報管理部 部長 • 児島　純司　民間病院を中心とした医療情報連携フォーラム 事務局長 • 武田　理宏　大阪大学大学院 医学研究科 准教授（日本病院会） • 玉川　裕夫　日本歯科医師会 嘱託（情報管理担当） • 野津　勤　日本画像医療システム工業会 セキュリティ委員会副委員長 • 樋口　範雄　武蔵野大学 法学部 特任教授 • 松元恒一郎　電子技術産業協会 医療用ソフトウェア専門委員会 委員長 • 松山　征嗣　トレンドマイクロ株式会社 業種営業推進グループ 医療担当 • 茗原　秀幸　保健医療福祉情報システム工業会 セキュリティ委員会 委員長 • 矢野　一博　日本医師会 総合政策研究機構 主任研究員
オブザーバー	• 総務省　情報流通行政局　情報流通振興課　情報流通高度化推進室 • 経済産業省　商務情報政策局　情報産業課 • 厚生労働省 医政局 研究開発振興課 医療情報技術推進室
事務局	• 株式会社エヌ・ティ・ティ・データ経営研究所

2019年12月～2020年3月に6回開催

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**

A～D項について

A項 制度上の要求事項
法律、通知、他の指針等を踏まえた要求事項。

B項 考え方
要求事項の解説及び原則的な対策。

C項 最低限のガイドライン
A項の要求事項を満たすために必ず実施しなければならない事項。

D項 推奨されるガイドライン
実施しなくても要求事項を満たすことは可能であるが、説明責任の観点から実施した方が望ましい対策。

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箇所

- ガイドラインの以下の記載箇所に、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　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	• 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

安全管理ガイドラインの主な改定検討内容（個別論点）1/5

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 記載箇所	論点	改定素案における対応
(4)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

安全管理ガイドラインの主な改定検討内容（個別論点） 2/5

6.5　技術的安全対策

ガイドライン 記載箇所	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）を推奨する考えをB項に追記
(6)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

安全管理ガイドラインの主な改定検討内容（個別論点） 3/5

6.10　災害、サイバー攻撃等の非常時の対応

ガイドライン記載箇所	論点	改定素案における対応
(4)を新設	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、情報セキュリティ責任者(CISO)や緊急対応体制(CSIRT等)の設置の必要性を追記
		◆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（C項）

（※）CISO（シーアイエスオー）・・・Chief Information Security Officerの略。組織内において情報管理およびその運用を担当し、情報セキュリティを統括する責任者。最高情報セキュリティ責任者。

CSIRT（シーサート）・・・Computer Security Incident Response Teamの略。情報セキュリティインシデントの報告を受け取り、その調査・連絡の対応を行う組織体。

安全管理ガイドラインの主な改定検討内容（個別論点） 4/5

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

ガイドライン記載箇所	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

安全管理ガイドラインの主な改定検討内容（個別論点） 5/5

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 記載箇所	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