資料1

「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」のパフリックコメント結果概要

パブリックコメントの実施結果概要

実施期間：令和2年10月2日～令和2年11月2日
受付件数：27件　うち　個人　20件
法人　5件
その他（匿名等）　2件

意見対象

意見箇所		意見対象のテーマ	件数
第4章関係	4.3	例示による責任分界点の考え方の整理（クラウドサービスの責任分界）	2件
第6章関係	6.1	医療情報システム安全管理責任者	2件
	6.2	医療機関等における情報セキュリティマネジメントシステム(ISMS）の実践	2件
	6.5	不正アクセス	3件
		利用者の識別・認証	6件
		IoTセキュリティ	1件
	6.7	情報の破棄の管理者	1件
	6.10	非常時に備えたセキュリティ体制の整備	3件
	6.11	サイバー攻撃対策	3件
		オープンなネットワークで接続する場合	3件
	6.12	法令で定められた記名・押印を電子署名で行うことについて	3件
第8章関係	8.1.2	外部保存を受託する事業者の選定基準	10件
		ガイドラインの対象	1件
		その他（国外法不適用確認等）	2件
第9章関係	9.5	原本管理関係	1件
全般		表現、誤字等の修正	101件
計			144件（延べ件数）

（※）1個人又は1法人が複数箇所意見出ししているため、受付件数と意見件数は一致しない。

パブリックコメントにおける主なご意見とその対応（1/2）

ご意見の対象箇所		ご意見内容	対応内容
第4章	クラウドサービスの責任分界	IaaSやPaaS事業者については、医療機関との直接の契約関係に立たないこともあるので、委託と整理しえないのではないか。	◆医療機関と、IaaSやPaaS事業者の間に直接の契約関係がない場合でも、外部受託事業者を通じて再委託に類似する関係が生じるため、原案の通りとした。
第6章	6.2 医療機関等における情報セキュリティマネジメントシステム(ISMS)の実践	2省ガイドラインを踏まえて、受託事業者がシステム・サービスに係る情報を提供した場合には、医療機関等にリスクコミュニケーションを義務付けるべきではないか。	◆C.最低限のガイドラインにおいて、ベンダから技術的対策等の情報収集することや、リスク分析や対策を実施する活動を求めていることから、原案の通りとした。
	6.5 利用者の識別・認証	令和9年度に稼働していることが予定されている医療情報システムの新規導入・更新に関する二要素認証対応につき、例外的なケースはないか。	◆ベンダ製品が未対応等により、やむを得ない場合には、入室管理をする等により、全体として二要素認証に相当する対策を講じるべき旨を、QAに示した。
	6.10 非常時に備えたセキュリティ体制の整備	CISOの設置やCSIRTの整備に関して、具体的な数値による設置基準を示すべきではないか	◆CISOの設置やCSIRTの整備については、医療機関等の規模や法人組織形態、地域における機能等が様々であり、一律の基準を示すことで適切な体制を講じられなくなる可能性があるため、原案通りとした。

パブリックコメントにおける主なご意見とその対応（2/2）

ご意見の対象箇所		ご意見内容	対応内容
第6章	6.11 オープンなネットワークで接続する場合	6.11省C項10において「いわゆるSSL-VPNは偽サーバへの対策が不十分なものが多いため、原則として使用しないこと。」とあるが、例外を示すべきではないか。	◆例外的な対応として、やむをえない場合には、偽サーバへの接続リスクが低い、クライアント型のSSL-VPNによるべき旨をQAに示した。
	6.12 電子署名	令和2年度診療報酬改定を踏まえて、本ガイドラインにおける電子署名の要件を緩和すべきではないか。	◆ガイドラインでは、法令で署名又は記名・押印が義務付けられた文書等について、e-文書法で定められた要件を踏まえて「電子署名及び認証業務に関する法律」の電子署名によることを規定しております。タブレットやスマートフォン上で行う手書きサイン等ではその要件を満たさないことになりますので、原案通りとした。
第8章	8.1.2 外部保存を受託する事業者の選定基準	8.1.2のC項2.(9)eで示す、外部保存を委託する事業者選定に際しての確認項目に、JIS Q 15001、JIS Q 27001を加えるべきではないか。	◆JIS Q 15001及びJIS Q 27001は、既にD項において”取得している事業者を選択”することを推奨していることも踏まえて、JIS Q 15001、JIS Q 27001の認証の有無を確認すべき内容を追加した。

QA集の主な変更・新設点

分類	変更箇所	概要
利用者の識別・認証（パスワード要件）	今回の改定でID/パスワードに関する要求事項を変更したため、Q-27（パスワード要件の根拠）の見直し	◆ID/パスワードのみ認証について、パスワードの文字数の根拠や適切な管理方法の例を示した。 ◆QAにおいても、ID/パスワードのみの認証では、安全性に限度があるため、できるだけ早く二要素認証の導入へ誘導する考え方を示した。
利用者の識別・認証（二要素認証）	二要素認証を用いる場合に、認証要素にPINが設定されている場合の解説として、Q-28を新設	◆パスワードとPINの違いを示して、認証要素に設定されるPINに文字数の要件は求めないことを解説した。 例．HPKIカードのPINは8文字より短くて良い
オープンなネットワークで接続する場合（SSL-VPN）	TLS暗号設定ガイドライン（IPA策定）を踏まえて、SSL-VPNを用いる場合の原則禁止の解説として、Q-34を新設	◆SSL-VPNには、「クライアントレス型」「on-demandインストール型」「クライアント型」の3つの実現形態があることを示し、やむを得ず医療情報システムにおいてSSL-VPNを用いる場合には、「クライアント型」のSSL-VPNを利用すべきという考え方を示す。
外部保存を受託する事業者の選定基準	パブコメ版で例示した以外の資格による対応についての考え方を示すためQ-62を新設	◆医療機関が適切なクラウドサービスを選択できるように、外部保存を委託する事業者や利用するクラウドサービスが取得している第三者認証の有無の確認を8.1.2C項2(9)fに示したところ、他の第三者認証で代替できないか意見があった。 ◆そのため、本文記載の第三者認証は例示であり、その他の資格により、技術や運用管理能力の有無の確認も可能であるという考え方を示す。