

項番	アンケート内容	回答	ガイドライン	
			頁	項番
2. 3. 5.(4)	常時、コンピュータウイルス対策を講じていますか。	※ガイドライン6章5.D.3(アンケート項番1.3.2.(3))に同じ。 1. すべてのパソコンにアンチウイルスソフトを導入している 2. アンチウイルスゲートウェイを導入している 3. その他のウイルス対策を行っている(具体的に:) 4. ウィルス対策は行っていない	52	73D(1)2
2. 3. 5.(5)	常にウィルスパターンファイルを最新の状態にしていますか。	※ガイドライン6章5.D.3(アンケート項番1.3.2.(4))に同じ。 1. 常時インターネットから最新パターンファイルをダウンロードしている 2. 院内にウィルスパターンファイル更新用サーバを用意している 3. ウィルスパターンファイルは不定期に更新している 4. パターンファイルを更新していないパソコンがある(複数回答可)	52	73D(1)2
2. 3. 6.不適切な保管・取扱いによる情報の滅失、破壊の防止			52	
2. 3. 6.(1)	サーバ室の入退室履歴を残し、作業履歴を関連づけて保存していますか。	はい/いいえ	52	73D(2)1
2. 3. 6.(2)	サーバ室には、許可を受けた担当者以外が立ち入ることができないような対策を講じていますか。	※ガイドライン7章3.G.2(3)(アンケート項番2.3.2.(3))に同じ。 1. 業務時間外は施錠している 2. ICカードで入室ができるようになっている 3. 生体認証で入室ができるようになっている 4. その他の方法で入室者を制限している(具体的に:) 5. 上記いずれの方法もとっていない	52	73D(2)2
2. 3. 6.(3)	診療録等のバックアップデータを定期的に検査し、改ざんなどによる情報の破壊が行われていないことが分かる機能を備えていますか。	はい/いいえ	52	73D(2)3
2. 3. 7.記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止			52	
2. 3. 7.(1)	品質が保証された記録媒体を利用していますか。	はい/いいえ	52	73D(3)1
2. 3. 7.(2)	ハードディスクに記録する場合、RAID-1もしくはRAID-5相当のシステムを導入していますか。	1. RAID-1を導入している 2. RAID-5を導入している 3. その他の方式を導入している(具体的に:) 4. ハードディスクの障害対策は行っていない(複数回答可)	52	73D(3)2
2. 4 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			53	
2. 4 最低限のガイドライン			53	
2. 4. 1.認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと。			53	
2. 4. 1.(1)	その電子証明書は、電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いていますか。	1. 認定特定認証事業者の発行する電子証明書を用いている 2. 同等の厳密さを有する電子証明書を用いている(具体的に:) 3. 公的個人認証サービスを用いている 4. 電子証明書は利用していない(いずれかに○)	53	74C(1)
2. 4. 2.電子署名を含む文書全体にタイムスタンプを付与すること。			54	
2. 4. 2.(1)	タイムスタンプは、「タイムビジネスに係る指針—ネットワークの安心な利用と電子データの安全な長期保存のために—」(総務省、平成16年11月)等で示されている時刻認証業務の基準に準拠し、財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能ですか。	はい/いいえ	54	74C(2)1
2. 4. 2.(2)	法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じていますか。	はい/いいえ	54	74C(2)2
2. 4. 2.(3)	タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容に留意しながら適切に対策を講じていくことができますか。	はい/いいえ	54	74C(2)3
2. 4. 3.上記タイムスタンプを付与する時点で有効な電子証明書を用いること。			54	
2. 4. 3.(1)	タイムスタンプの時点で有効な電子証明書を用いていますか。	はい/いいえ	54	74C(3)1
3. 診療録等をスキャナ等により電子化して保存する場合について				
3. 1 共通の要件			90	
3. 1. 1.最低限のガイドライン			90	
3. 1. 1.(1)	フィルムデジタルサイズについては、次の特性を満たしていますか。 (1)サンプリングピッチ: 200 μ m以下 (2)空間分解能: CTF(0.25) \geq 0.9、CTF(0.5) \geq 0.8、CTF(1.0) \geq 0.7 ここでCTF(n)は、 nlp/mmのContrast Transfer Functionを示す。 (3)濃度階調数: 1024以上(10ビットグレイスケール以上) (4)デジタルサイズ濃度範囲: 0.0D~3.0D以上	はい/いいえ	90	91C1
3. 1. 1.(2)	フィルムデジタル化した画像ファイルはDICOM形式で保存していますか。	1. DICOM形式で保存している 2. その他の形式で保存している(具体的に:)	90	91C1
3. 1. 1.(3)	紙媒体については、300dpi、RGB各8ビット以上でスキャンを行っていますか。	はい/いいえ	90	91C1

調査結果(はい/いいえ:Y/N、択一選択:選択番号、複数選択:選択=選択番号、非該当:NA)																	アンケート項目別評価基準				
回答	病院					クリニック			調剤・薬局			回答項目別評価	評価方法追記								
	病院01	病院02	病院03	病院04	病院05	医院06	医院07	医院08	薬局09	薬局10	薬局11										
選	1,2,3	○	一部	NA	1	NA	1	NA	1	NA	3	NA	4	×	4	×	2	○	4	×	2は可。 1,3は評価対象外 4は不可。
1	0		NA		0		0		0		NA		0		0		0		0		可
2	2	○	NA	NA	0	×	2	○	2	○	0	○	0	×	0	×	0	×	0	×	可
3	0		NA		3		0		0		3		0		0		0		0		不可
4	0		NA		0		0		0		0		NA		4		4		4		不可
Y/N	Y	○	Y	○	N	×	Y	○	Y	○	N	×	N	×	N	×	N	×	N	×	Y:可
1	0		0		1		0		0		0		1		1		0		1		不可
2	2	○	0		0		2	○	2	○	0	○	0		0		0		0		可
3	0		3	○	0	×	0	○	0	○	0	×	0	×	0	×	0	×	0	×	可
4	0		0		0		4		0		0		0		0		0		0		具体的内容によって判
5	0		0		0		0		5		5		0		0		5		0		不可
Y/N	N	×	NA	NA	N	×	N	×	N	×	Y	○	N	×	N	×	N	×	N	×	Y:可
Y/N	Y	○	Y	○	Y	○	Y	○	Y	○	Y	○	Y	○	Y	○	Y	○	Y	○	Y:可
1	1		0		0		0		0		0		0		0		0		0		可
2	2	○	2	○	2	○	2	○	2	○	2	○	0	×	0	×	2	○	0	×	○
3	0		0		0		0		0		0		0		0		0		0		具体的内容によって判
4	0		0		0		0		0		4		4		0		4		4		不可
RAID-1もしくはRAID-5 相当の障害対策であること。																					
選	4	×	4	×	4	×	4	×	4	×	4	×	4	×	4	×	4	×	4	×	1,2,3は可。4は不可。
Y/N	NA	NA	NA	NA	NA	NA	N	×	N	×		×	N	×	N	×	N	×	N	×	Y:可
Y/N	NA	NA	NA	NA	NA	NA	N	×	N	×		×	N	×	N	×	N	×	N	×	Y:可
Y/N	NA	NA	NA	NA	NA	NA	Y	○	N	×		×	N	×	N	×	N	×	N	×	Y:可
Y/N	NA	NA	NA	NA	NA	NA	N	×	N	×		×	N	×	N	×	N	×	N	×	Y:可
Y/N	NA	NA	NA	NA	Y	○	Y	○	Y	○	NA	NA	NA	NA	Y	NA	NA	NA	NA	NA	Y:可
選	NA	NA	NA	NA	NA	NA	1	○	1	○	NA	NA	NA	NA	1	NA	NA	NA	NA	NA	具体的内容によって判
Y/N	NA	NA	NA	NA	Y	○	N	×	N	×	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Y:可
DICOM等の適切な形式であること。																					

項番	アンケート内容	回答	ガイドライン	
			頁	項番
3. 1. 1. (4)	スキャンした画像ファイルの保存形式。	1. TIFF形式 2. PDF形式 3. JPEG形式 4. BMP形式 5. その他の形式 (いずれかに○)	90	91C1
3. 1. 1. (5)	スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保する対策を施していますか。	1. 光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いている 2. 紙媒体については、300dpi、RGB各8ビット以上でスキャンを行っている 3. その他(具体的に:) 4. 特に対策を施していない (複数回答可)	90	91C1
3. 1. 1. (6)	スキャナによる読み取りに係る運用管理規程を定めていますか。	はい/いいえ	91	91C2
3. 1. 1. (7)	スキャナで読み取ったファイルの登録の際、作成責任者の氏名またはID番号、信頼できる時刻による作成日時が記録されていますか。	1. 作成責任者の氏名が登録される 2. 作成責任者のIDが登録される 3. 時刻が登録される 4. 登録時刻は「タイムビジネスに係る指針」適合のタイムスタンプを用いている 5. 上記のいずれも登録されない (複数回答可)	91	91C2
3. 1. 1. (8)	スキャナにより読み取った電子情報ともの文書等から得られる情報との同一性を担保する情報作成管理者を定めていますか。	はい/いいえ	91	91C3
3. 1. 1. (9)	緊急に診療録などの閲覧が必要になったときに迅速に対応できるような対策を施していますか。	1. 停電時の補助電源を確保している 2. システムトラブルに備えたミラーサーバーを用意している 3. その他の緊急用対策を施している(具体的に:) 4. 障害対策を施していない (複数回答可)	91	91C4
3. 1. 1. (10)	電子化後のもの紙媒体やフィルムを破棄する場合、シュレッダー等で個人識別不可能な状態にしたうえで破棄していますか。	はい/いいえ	91	91C5
3. 2 診療等の都度スキャナ等で電子化して保存する場合			92	
3. 2 .1.最低限のガイドライン			92	
3. 2. 1. (1)	改ざんを防止するため情報が作成されてから、または情報を入手してから一定期間以内にスキャンを行う規定は設けていますか。(一定期間とは改ざんの機会が生じない程度の期間)	はい/いいえ	92	92C
3. 3 過去に蓄積された紙媒体等をスキャナ等で電子化保存する場合			93	
3. 3 .1.最低限のガイドライン			93	
3. 3. 1. (1)	実施計画書には、患者等への通知の手段が明記されていますか。	はい/いいえ	93	93C1
3. 3. 1. (2)	実施計画書には、患者等からの異議の申し立てがあった場合、電子化を行わないこととしていますか。	はい/いいえ	93	93C1
3. 3. 1. (3)	電子化の実施前に実施計画書を作成していますか。	はい/いいえ	93	93C2
3. 3. 1. (4)	実施計画書は、運用管理規程の作成と妥当性の評価を行っていますか。この評価は大規模医療機関等にあつては外部の有識者を含む、公正性を確保した委員会等(倫理委員会など)でおこなっていますか。	はい/いいえ	93	93C2
3. 3. 1. (5)	実施計画書には、作業責任者が特定されていますか。	はい/いいえ	93	93C2
3. 3. 1. (6)	実施計画書には、患者等への通知の手段が明記されていますか。	※ガイドライン9章3.C.1(アンケート項番3.3.1.(1))に同じ。 はい/いいえ	93	93C2
3. 3. 1. (7)	実施計画書には、相互監視を含む実施の体制が明記されていますか。	はい/いいえ	93	93C2
3. 3. 1. (8)	実施計画書には、実施記録の作成と記録項目が明記されていますか。	はい/いいえ	93	93C2
3. 3. 1. (9)	実施計画書には、事後の監査人の特定されていますか。	はい/いいえ	93	93C2
3. 3. 1. (10)	実施計画書には、事後の監査項目が明記されていますか。	はい/いいえ	93	93C2
3. 3. 1. (11)	スキャナ等で電子化をおこなってから紙やフィルムを破棄するまでの期間、及び破棄の方法を明記していますか。	1. 破棄条件を明記している 2. 破棄担当者を明記している 3. 破棄手順を明記している 4. 上記のいずれも行っていない (複数回答可)	94	93C2
3. 3. 1. (12)	スキャナ等で電子化をおこなう場合の監査をシステム監査技術者やCertified Information Systems Auditor (ISACA認定)等の適切な能力を持つ外部監査人によっておこなっていますか。	1. 外部監査人によって行っている 2. 内部監査を行っている 3. 監査は行っていない (複数回答可)	94	93C3

回答	調査結果(はい/いいえ:Y/N、択一選択:選択番号、複数選択:選択=選択番号、非該当:NA)															アンケート項目別評価基準								
	病院					クリニック			調剤・薬局			回答項目別評価	評価方法追記											
	病院01	病院02	病院03	病院04	病院05	医院06	医院07	医院08	薬局09	薬局10	薬局11													
選	NA	NA	NA	NA	3	×	3	×	3	×	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1,2は可。その他は雑	非可逆圧縮で業務に支障がない精度であることを確認。
1	NA	NA	NA	0	0		1		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	可	
2	NA	NA	NA	2	0	○	0	○	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	可	
3	NA	NA	NA	0	0		3		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	具体的内容によって	
4	NA	NA	NA	0	0		0		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	不可	
Y/N	NA	NA	NA	NA	N	×	N	×	Y	○	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Y:可	
1	NA	NA	NA	1	0		1		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		電子署名およびタイムスタンプが付与されること。それぞれ単独では不可。
2	NA	NA	NA	0	0		0	2	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
3	NA	NA	NA	0	×	3	×	3	○	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
4	NA	NA	NA	0	0		0		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
5	NA	NA	NA	0	0		0		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	不可	
Y/N	NA	NA	NA	NA	N	×	Y	○	Y	○	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Y:可	
1	NA	NA	NA	1	1		1		NA	NA	NA	1	1	NA	NA	NA	NA	NA	NA	NA	NA	NA	可	
2	NA	NA	NA	0	0	○	0	2	NA	NA	NA	2	NA	0	NA	NA	NA	NA	NA	NA	NA	NA	可	
3	NA	NA	NA	0	3		3		NA	NA	NA	0	0	0	NA	NA	NA	NA	NA	NA	NA	NA	具体的内容によって	
4	NA	NA	NA	0	0		0		NA	NA	NA	0	0	0	NA	NA	NA	NA	NA	NA	NA	NA	不可	
Y/N	NA	NA	NA	NA	Y	○	Y	○	Y	○	NA	NA	NA	NA	Y	NA	Y	NA	NA	NA	NA	NA	Y:可	
Y/N	NA	NA	NA	NA	N	×	Y	○	N	×	NA	NA	NA	NA	N	NA	NA	NA	NA	NA	NA	NA	Y:可	
Y/N	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	N	NA	NA	NA	NA	NA	NA	NA	Y:可	
Y/N	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	N	NA	NA	NA	NA	NA	NA	NA	Y:可	
Y/N	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	N	NA	NA	NA	NA	NA	NA	NA	Y:可	
Y/N	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	N	NA	NA	NA	NA	NA	NA	NA	Y:可	
Y/N	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	N	NA	NA	NA	NA	NA	NA	NA	Y:可	
Y/N	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	N	NA	NA	NA	NA	NA	NA	NA	Y:可	
Y/N	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	N	NA	NA	NA	NA	NA	NA	NA	Y:可	
Y/N	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	N	NA	NA	NA	NA	NA	NA	NA	Y:可	
1	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	可	
2	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	可	
3	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	可	
4	NA	NA	NA	4	NA	NA	NA	NA	NA	NA	NA	4	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	不可	
1	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	不可	
2	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	可	
3	NA	NA	NA	3	NA	NA	NA	NA	NA	NA	NA	3	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	不可	

項番	アンケート内容	回答	ガイドライン	
			頁	項番
3. 3. 1. (13)	外部事業者に委託する場合は、適切な事業者を選定する規定が明記されていますか。	1. プライバシーマークを取得している事業者を選定する 2. 過去に情報の安全管理や個人情報保護上の問題を起こしていない事業者であることを確認している 3. 外部監査人の監査を受けている 4. 契約上に十分な安全管理をおこなうことを具体的に明記している 5. 上記いずれも行っていない (複数回答可)	94	93C4
3. 4	(補足)運用の利便性のためにスキャナ等で電子化をおこなうが、紙等の媒体もそのまま保存をおこなう場合		95	
3. 4	1. 最低限のガイドライン		95	
3. 4. 1. (1)	紙媒体については、300dpi、RGB各8ビット以上でスキャンを行っていますか。	※ガイドライン9章1.C.1(アンケート項番3.1.1.(3))に同じ。 はい/いいえ	95	94C1
3. 4. 1. (2)	医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぐため、光学解像度、センサ等の一定の規格・基準を設けていますか。	はい/いいえ	95	94C1
3. 4. 1. (3)	スキャンした画像ファイルの保存形式。	※ガイドライン9章1.C.1(アンケート項番3.1.1.(4))に同じ。 1. TIFF形式 2. PDF形式 3. JPEG形式 4. BMP形式 5. その他の形式 (いずれかに○)	95	94C1
3. 4. 1. (4)	CT、MRI画像、X線画像の診断に使用するCRTモニタの表示マトリックスは、1,000 X 1,000 以上ですか。	1. 1,000 X 1,000 以上 2. 1,000 X 1,000 未満 3. 特に規定していない	95	94C1
3. 4. 1. (5)	CT、MRI画像、X線画像の診断に使用するCRTモニタの輝度劣化の程度を、チェックしていますか。	1. 毎日チェックしている 2. 不定期にチェックしている 3. チェックしていない	95	94C1
3. 4. 1. (6)	スキャナによる読み取りに係る運用管理規程を定めていますか。	※ガイドライン9章1.C.2(アンケート項番3.1.1.(6))に同じ。 はい/いいえ	96	94C2
3. 4. 1. (7)	緊急に閲覧が必要になったときに迅速に対応できるよう、保存している紙媒体等の検索性も必要に応じて維持していますか。	1. 紙媒体等の検索性を維持している 2. とくに管理していない	96	94C3
3. 4. 1. (8)	個人情報の保護のため個人情報保護関連各法を踏まえた所要の取り扱いについて、明記されていますか。	はい/いいえ	96	94C4
4.	運用管理について		98	
4. 1. 1. (1)	運用管理規定があれば、ご提供下さい。	1. 提供可 2. 提供不可		

回答	調査結果(はい/いいえ:Y/N、択一選択:選択番号、複数選択:選択=選択番号、非該当:NA)																		アンケート項目別評価基準	
	病院					クリニック					調剤・薬局			回答項目別評価	評価方法追記					
	病院01	病院02	病院03	病院04	病院05	医院06	医院07	医院08	薬局09	薬局10	薬局11									
1	NA	NA	0	NA	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	NA	1,2,3,4の組合せで可。	1,2,3,4の組合せで可。 いずれかがない場合は不可。		
2	NA	NA	0	NA	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	NA	1,2,3,4の組合せで可。			
3	NA	NA	0	NA	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	NA	1,2,3,4の組合せで可。			
4	NA	NA	0	NA	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	NA	NA	1,2,3,4の組合せで可。			
5	NA	NA	5	NA	NA	NA	NA	5	NA	NA	NA	NA	NA	NA	NA	NA	不可			
Y/N	NA	NA	Y	○	N	×	N	×	NA	NA	NA	NA	NA	NA	NA	NA	NA	Y:可		
Y/N	NA	NA	N	×	Y	○	N	×	NA	NA	NA	NA	N	NA	NA	NA	NA	Y:可		
選	NA	NA	3	×	3	×	3	×	NA	NA	NA	NA	NA	NA	NA	NA	NA	1,2は可。その他は確認	非可逆圧縮で業務に 支障がない制度である ことを確認。	
選	NA	NA	1	○	1	○	1	○	NA	NA	NA	NA	3	NA	NA	NA	NA	NA	1は可2,3は不可。	
選	NA	NA	1	○	2	○	2	○	NA	NA	NA	NA	2	NA	NA	NA	NA	NA	1,2は可3は不可。	
Y/N	NA	NA	N	×	N	×	Y	○	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Y:可	
選	NA	NA	2	×	1	○	1	○	NA	NA	NA	NA	2	NA	NA	NA	NA	NA	1は可2は不可。	
Y/N	NA	NA	N	×	Y	○	Y	○	NA	NA	NA	NA	Y	NA	NA	NA	NA	NA	Y:可	
選	NA	NA	1	○	1	○	2	○	NA	NA	NA	NA	2	NA	NA	NA	NA	NA	評価対象外	

1. 4 最低限のガイドラインに関する考察

「医療情報システムの安全管理に関するガイドライン」の「最低限のガイドライン」に該当する項目の調査結果に対する考察を行った。各々の考察の項番は「医療情報システムの安全管理に関するガイドライン」の章・項目番号と同じである。

考察では、大規模な医療機関である病院（5箇所）と比較的小規模であるクリニック・薬局（6箇所）に分け、各々の傾向、背景、対策案について記述している。

6 情報システムの基本的な安全管理

6.3 組織的安全管理対策（体制、運用管理規程）

6.3.C.1 情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。

◇ 『病院』

【傾向】

- ・管理体制に係わる安全管理規定などは整っている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

◇ 『クリニック・薬局』

【傾向】

- ・組織的安全管理対策がとられていない所(3/6箇所)がある。

【背景】

- ・情報に対してアクセスできるスタッフが少数であるため、規定集を設けていないと思われる。

【対策案】

- ・小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。

6.3.C.2 個人情報参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。

◇ 『病院』

【傾向】

- ・入退室管理規定に係わる安全管理規定などは整っている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

◇ 『クリニック・薬局』

【傾向】

- ・入退室管理対策がとられていない所(5/6箇所)がある。

【背景】

- ・情報に対してアクセスできるスタッフが少数であるため、入退管理を定めていないと思われる。

【対策案】

- ・入退室管理規定に係わる安全管理規定などを整備する。

6.3.C.3 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。

◇ 『病院』

【傾向】

- ・アクセス管理規定に係わる安全管理規定などは整っている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

◇ 『クリニック・薬局』

【傾向】

- ・アクセス管理規程を定めていない所(4/6箇所)がある。

【背景】

- ・情報に対してアクセスできるスタッフが少数であるため、アクセス管理規程を定めていないと思われる。

【対策案】

- ・アクセス管理規程に係わる安全管理規定などを整備する。

6.3.C.4 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。

◇ 『病院』

【傾向】

- ・委託契約に係わる安全管理規定などは整っている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

◇ 『クリニック・薬局』

【傾向】

- ・委託契約において安全管理に関する条項を含めていない所(3/6箇所)がある。

【背景】

- ・特になし。

【対策案】

- ・委託契約書の安全管理に関する条項を見直す。

6.3.C.5

運用管理規程等において次の内容を定めること。

- (a) 個人情報の記録媒体の管理（保管・授受等）の方法
- (b) リスクに対する予防、発生時の対応の方法

◇ 『病院』

【傾向】

- ・リスク予防策・発生時の対処に関する管理規定が設けられていない所(2/5箇所)がある。
- ・記録メディアの管理規定が設けられていない所(2/5箇所)がある。

【背景】

- ・特になし。

【対策案】

- ・リスク予防策・発生時の対処に関する管理規定を整備する。
- ・記録メディアの管理規定を整備する。

◇ 『クリニック・薬局』

【傾向】

- ・組織的安全管理対策がとられていない所(5/6箇所)がある。

【背景】

- ・情報に対してアクセスできるスタッフが少数であるため、規定集を設けていないと思われる。
- ・小規模なことからリスクの認識が不足していると思われる。

【対策案】

- ・リスク分析を行い、リスク予防策・発生時の対処に関する管理規定を整備する。
- ・記録メディアの管理規定を整備する。

6.4 物理的安全対策

6.4.C.1

個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。

◇ 『病院』

【傾向】

- ・ 個人情報が入力されている機器の設置場所及び記録媒体の保存場所は施錠されている。

【背景】

- ・ 特になし。

【対策案】

- ・ 特になし。

◇ 『クリニック・薬局』

【傾向】

- ・ ハードウェアや記録メディアの設置場所の施錠が不十分な所(4/6箇所)がある。

【背景】

- ・ 設置場所、設置スペースに問題がある。
- ・ 少人数の運用であるためと考えられる。

【対策案】

- ・ 個人情報が入力されている機器の設置場所及び記録媒体の保存場所には施錠する。

6.4.C.2

個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、権限者以外立ち入ることが出来ない対策を講じること。ただし、本体策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。

◇ 『病院』

【傾向】

- ・ 業務時間帯以外は施錠等、権限者以外立ち入ることが出来ない対策が講じられている。

【背景】

- ・ 特になし。

【対策案】

- ・ 特になし。

◇ 『クリニック・薬局』

【傾向】

- ・ 入退室管理、窃視防止対策が不十分な所(2/6箇所)がある。

【背景】

- ・ 設置場所、設置スペースに問題がある。
- ・ 少人数の運用であるためと考えられる。

【対策案】

- ・ 施錠などの管理できる仕組みを整備する。

6.4.C.3

個人情報の物理的保存を行っている区画への入退管理を実施すること。

- ・入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録すること。
- ・入退者の記録を定期的にチェックし、妥当性を確認すること。

◇ 『病院』

【傾向】

- ・個人情報を参照できる区画に対して入退室管理記録の整備が不十分である所(2 / 5箇所)がある。

【背景】

- ・特になし。

【対策案】

- ・入退室を記録し、その記録をチェックする運用を整備する。

◇ 『クリニック・薬局』

【傾向】

- ・入退室管理が不十分な所(4 / 6箇所)がある。

【背景】

- ・設置場所、設置スペースに問題がある。
- ・少人数の運用であるためと考えられる。

【対策案】

- ・入退室を記録し、その記録をチェックする運用を整備する。

6.4.C.4

個人情報が存在する PC 等の重要な機器に盗難防止用チェーンを設置すること。

◇ 『病院』

【傾向】

- ・盗難防止用チェーンの設置、もしくはPCに個人情報を蓄積しない仕組みが施されていない所(1 / 5箇所)がある。

【背景】

- ・特になし。

【対策案】

- ・盗難防止用チェーンを設置する。
- ・PCなどに個人情報を蓄積しない仕組みを整備する。

◇ 『クリニック・薬局』

【傾向】

- ・盗難防止用チェーンの設置、もしくはPCに個人情報を蓄積しない仕組みが施されていない所(3 / 5箇所)がある。

【背景】

- ・少人数の運用であり、常に目が届く範囲にPCなどが設置されているためと考えられる。

【対策案】

- ・盗難防止用チェーンを設置する。
- ・PCなどに個人情報を蓄積しない仕組みを整備する。

6.4.C.5 離席時にも端末等での正当な権限者以外の者による窃視防止の対策を実施すること。

◇ 『病院』

【傾向】

- ・パスワード付きのスクリーンセーバなどによる窃視防止の対策が施されている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

◇ 『クリニック・薬局』

【傾向】

- ・窃視防止対策が不十分な所(4 / 6箇所)がある。

【背景】

- ・少人数の運用であるためと考えられる。

【対策案】

- ・パスワード付のスクリーンセーバを導入する。

6.5 技術的安全対策

6.5.C.1 情報システムへのアクセスにおける利用者の識別と認証を行うこと。

◇ 『病院』

【傾向】

- ・利用者の識別と認証は行われている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

◇ 『クリニック・薬局』

【傾向】

- ・利用者の識別と認証は行われていない所(1 / 6箇所)がある。
- ・対策がとられていない所(1 / 6箇所)は電子保存の対象ではない。

【背景】

- ・医師1名のみ利用のためと思われる。

【対策案】

- ・特になし。

6.5.C.2 動作確認等で個人情報を含むデータを使用するときは、漏洩等に十分留意すること。

◇ 『病院』

【傾向】

- ・漏洩等に留意されている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

◇ 『クリニック・薬局』

【傾向】

- ・漏洩等に留意していない所(2 / 6箇所)がある。

【背景】

- ・特になし。

【対策案】

- ・動作確認に関する運用管理規定を整備する。

6.5.C.3 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。
複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、現状でそのような機能がない場合は、システム更新までの期間、運用管理規定でアクセス可能範囲をさだめ、次項の操作記録を行なうことで担保する必要がある。

◇ 『病院』

【傾向】

- ・医療従事者、関係職種ごとに、アクセス管理が行われている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

◇ 『クリニック・薬局』

【傾向】

- ・関係職種ごとに、アクセス管理が行われている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

6.5.C.4

アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録はすくなくとも利用者のログイン時刻および時間、ログイン中に操作した患者が特定できること。情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容）を必ず行うこと。

◇ 『病院』

【傾向】

- ・情報システムでアクセスの記録をしていない所(1 / 5箇所)がある。
- ・アクセス記録の定期的な確認は行われていない。

【背景】

- ・特になし。

【対策案】

- ・アクセス記録の定期的な確認を行う。

◇ 『クリニック・薬局』

【傾向】

- ・情報システムおよび業務日誌などでアクセスを記録していない所(3 / 6箇所)がある。

【背景】

- ・少人数での運用であるためと思われる。

【対策案】

- ・情報システムにアクセス記録機能を設ける。
- ・アクセス記録の定期的な確認を行う。

6.5.C.5 アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。

◇ 『病院』

【傾向】

- ・システム内のハードウェアは全て時刻が同期されている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

◇ 『クリニック・薬局』

【傾向】

- ・薬局ではハードウェアの時刻の同期を行っていない。

【背景】

- ・システム的な対応がなされていないためと思われる。

【対策案】

- ・全てのハードウェアの時刻を同期する対応を行う。

6.5.C.6 システム構築時や、適切に管理されていないメディアを使用したり、外部からの情報を受け取る際にはウイルス等の不正なソフトウェアの混入がないか確認すること。

◇ 『病院』

【傾向】

- ・管理されていないメディアを使用している所(3 / 5箇所)がある。

【背景】

- ・特になし。

【対策案】

- ・外部メディアの使用に関する運用規定を整備する。

◇ 『クリニック・薬局』

【傾向】

- ・薬局は適切に管理されたメディアのみ使用している。
- ・クリニックでは管理されていないメディアを使用している。

【背景】

- ・特になし。

【対策案】

- ・外部メディアの使用に関する運用規定を整備する。

6.5.C.7

パスワードを利用者識別に使用する場合システム管理者は以下の事項に留意すること。

- (1) システム内のパスワードファイルでパスワードは必ず暗号化(不可逆)され、適切な手法で管理及び運用が行われること。(利用者識別にICカード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用規程にて定めること)
- (2) 利用者がパスワードを忘れてたり、盗用される恐れがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知りえない方法で再登録を実施すること。
- (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること。(設定ファイルにパスワードが記載される等があってはならない。)また、利用者は以下の事項に留意すること。

また、利用者は以下の事項に留意すること。

- (1) パスワードは定期的に変更し(最長でも2ヶ月以内)、極端に短い文字列を使用しないこと(8バイト以上の可変長の文字列が望ましい)。
- (2) 類推しやすい、不注意によるパスワードの盗用は、盗用された本人の責任になることを認識すること。

◇ 『病院』

【傾向】

- ・パスワードの不可逆暗号化がなされていない所(3/5箇所)がある。
- ・システム管理者がパスワードを変更する場合に、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知りえない方法で再登録を実施していない。
- ・パスワードの定期的な変更がなされていない所(4/5箇所)がある。
- ・パスワードの文字数が極端に短い文字列を使用しないように規定されていない所(2/5箇所)がある。
- ・パスワード盗用が本人の責任になることが認識されている。

【背景】

- ・パスワードの不可逆暗号化はシステムが対応していないためと考えられる。
- ・頻繁なパスワード変更による担当者の負荷が考えられる。

【対策案】

- ・パスワードを不可逆暗号化できるようにシステムを改善する。
- ・システム側で、一定期間同じパスワードを利用していたら警告メッセージを表示するようにシステムを改善する。
- ・システム側で、パスワード文字数のチェックをするようにシステムを改善する。
- ・パスワード変更に関する運用管理規定を整備する。

◇ 『クリニック・薬局』

【傾向】

- ・パスワードの不可逆暗号化がなされていない所(2 / 5 箇所)がある。
- ・システム管理者がパスワードを変更する場合に、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知りえない方法で再登録を実施していない。
- ・パスワードの定期的な変更がなされていない所(4 / 6 箇所)がある。
- ・パスワードの文字数が極端に短い文字列を使用しないように規定されていない所(5 / 6 箇所)がある。
- ・パスワード盗用が本人の責任になることが認識されていない所(3 / 6 箇所)がある。

【背景】

- ・パスワードの不可逆暗号化はシステムが対応していないためと考えられる。
- ・頻繁なパスワード変更による担当者の負荷が考えられる。

【対策案】

- ・パスワードを不可逆暗号化できるようにシステムを改善する。
- ・システム側で、一定期間同じパスワードを利用していたら警告メッセージを表示するようにシステムを改善する。
- ・システム側で、パスワード文字数のチェックをするようにシステムを改善する。
- ・パスワード変更に関する運用管理規定を整備する。

6.6 人的安全対策

(1) 従業者に対する人的安全管理措置

6.6. (1). C. 1 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。

◇ 『病院』

【傾向】

- ・従業者に対する人的安全管理措置がとられている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

◇ 『クリニック・薬局』

【傾向】

- ・従業者に対する人的安全管理措置がとられていない所(2 / 6 箇所)がある。

【背景】

- ・特になし。

【対策案】

- ・従業者に対して守秘・非開示契約を締結すること等の人的安全管理措置を講じる。

6.6. (1). C. 2 定期的に従業者に対し教育訓練を行うこと。

◇ 『病院』

【傾向】

- ・定期的に従業者に対し教育訓練を行っていない所(1 / 5 箇所)がある。

【背景】

- ・特になし。

【対策案】

- ・従業者への定期的な教育訓練を実施する。

◇ 『クリニック・薬局』

【傾向】

- ・定期的に従業者に対し教育訓練を行っていない所(4 / 6 箇所)がある。

【背景】

- ・特になし。

【対策案】

- ・従業者への定期的な教育訓練を実施する。

6.6.(1).C.3 従業者の退職後の個人情報保護規程を定めること。

◇ 『病院』

【傾向】

- ・退職後の個人情報保護規程は定められている。

【背景】

- ・特になし。

【対策案】

- ・特になし。

◇ 『クリニック・薬局』

【傾向】

- ・退職後の個人情報保護規程は定められていない所(4/6箇所)がある。

【背景】

- ・特になし。

【対策案】

- ・退職後の個人情報取扱規程を整備する。

(2) 事務取扱委託業者の監督及び守秘義務契約

6.6.(2).C.1 プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で病院事務、運用等で、外部受託業者を採用する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。

- ①包括的な委託先の罰則を定めた就業規則等で裏づけられた守秘契約を締結すること
- ②保守作業等の医療情報システムに直接アクセスする作業の際には、作業員・作業内容・作業結果の確認をおこなうこと。
- ③清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。
- ④委託先事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託先と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。

◇ 『病院』