医療情報システムの安全管理に関するガイドライン　第2版
最低限のガイドライン遵守チェックリスト

本遵守チェックリストは、平成19年3月「医療情報システムの安全管理に関するガイドライン　第2版」の1章～6章における「最低限のガイドライン」の遵守状況のチェックリストである。

＊代行機関の業務を実施する者は、本資料を作成しホームページ（自機関のWebサイトでも他のサイトでも可）に掲出すること。

＊選択肢の項目については、「実施済」「実施予定」より一つ選び、□を■にすること。「実施予定」を選択した場合は、実施予定時期を明記すること。

更新情報	最終更新日	2008年　3月　1日

＊下記事項に変更があった場合は速やかに変更し、掲載しているホームページを更新し、更新日を明示すること。

組織的安全管理対策

No	チェック項目	実施済	実施予定（実施時期）
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）の限定を行っている。	■	□（　　）
2.	個人情報が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ている。	■	□（　　）
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定を作成している。	□	■（　　）
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ている。	■	□（　　）
5.	運用管理規程等において、次の内容を定めている。 (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	■	□（　　）

物理的安全対策

No	チェック項目	実施済	実施予定（実施時期）
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場所には施錠している。	■	□（　　）
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ている。もしくは、同等レベルの他の取りうる手段がある。	■	□（　　）
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している。	■	□（　　）
4.	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している。	■	□（　　）
5.	入退者の記録を定期的にチェックし、妥当性を確認している。	■	□（　　）
6.	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している。	■	□（　　）
7.	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している。	■	□（　　）

技術的安全対策

No	チェック項目	実施済	実施予定（実施時期）
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っている。	■	□（　　）
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、漏洩等に十分留意している。注1）	■	□（　　）
3.	関係職種ごとに、アクセスできる情報の範囲を定め、そのレベルに沿ったアクセスを行っている。	■	□（　　）
4.	アクセスの記録及び定期的なログを確認している。注2）	□	■（　　）
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。注3）	■	□（　　）
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している。	■	□（　　）
7.	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ている。注4）	■	□（　　）
8.	利用者がパスワードを忘れたり、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している。	■	□（　　）
9.	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している。注5）	■	□（　　）

注１：動作確認用データの情報管理を厳格に行い、動作確認終了後は適切に破棄を行うことを指す。

注２：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情報が特定できることを指す。また、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）を持って代えることができる。

注３：代行機関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操作事実の記録として問題のない範囲の精度を保つことを指す。

注４：利用者識別にＩＣカード等也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を持って代えることができる。

注５：例として設定ファイルにパスワードを記載しないようにする等があげられる。

人的安全対策（従業者に対する人的安全管理措置）

No	チェック項目	実施済	実施予定（実施時期）
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っている。	■	□（　　）
2.	定期的に従業者に対し教育訓練を行っている。	■	□（　　）
3.	従業者の退職後の個人情報保護規定を定めている。	■	□（　　）

人的安全対策（事務取扱委託業者の監督及び守秘義務契約）

No	チェック項目	実施済	実施予定（実施時期）
1.	外部受託業者を採用する場合は、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義務を締結している。	□	■（　　）

2.	外部受託業者を採用する場合で、保守作業等の情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行っている。	□	■（　　）
3.	外部受託業者を採用する場合は、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っている。	□	■（　　）
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している。	■	□（　　）

情報の破棄

No	チェック項目	実施済	実施予定（実施時期）
1.	情報種別ごとに破棄の手順を定めている。注6）	■	□（　　）
2.	情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認している。	■	□（　　）
3.	破棄を外部事業者に委託した場合は、委託元の医療機関等が確実に情報の破棄が行なわれたことを確認している。	■	□（　　）
4.	運用管理規程において不要になった個人情報を含む媒体の破棄を定める規程の作成を定めている。	■	□（　　）

注6：手順は、破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含む必要がある。

情報システムの改造と保守

No	チェック項目	実施済	実施予定（実施時期）
1.	動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めている。	■	□（　　）
2.	メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、およびアクセスした場合は対象個人情報を含む作業記録を残している。	□	■（　　）
3.	保守要員個人の専用アカウントは外部流出等による不正使用の防止の観点から適切に管理することを求めている。	□	■（　　）
4.	保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えている。	□	■（　　）
5.	保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認している。	□	■（　　）
6.	保守会社と守秘義務契約を締結し、これを遵守させている。	■	□（　　）
7.	保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむ得ない状況で組織外に持ち出さなければならない場合には、置き忘れに対する十分な対策を	□	■（　　）

	含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認している。		
8.	リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずメッセージログを採取し、当該作業の終了後速やかにメッセージログの内容を医療機関等の責任者が確認している。	□	■（　　）
9.	再委託が行われる場合は再委託先にも保守会社と同等の義務を課している。	■	□（　　）

注7：判断するための基準、手順、判断者、をあらかじめ決めていることを指す。

災害時の非常時の対応

No	チェック項目	実施済	実施予定（実施時期）
1.	医療サービスを提供し続けるためのBCPの一環として”非常時”と判断する仕組み、正常復帰時の手順を設けている。注7）	□	■（　　）
2.	正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意している。	□	■（　　）
3.	非常時のユーザアカウントや非常時用機能の管理手順を整備している。	□	■（　　）
4.	非常時機能が定常時に不適切に利用されることがないようにし、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理および監査を行っている。	□	■（　　）
5.	非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更している。	□	■（　　）
6.	サイバー攻撃で広範な地域での一部業務の停止など業務提供体制に支障が発生する場合は、所管官庁への連絡を行っている。	□	■（　　）

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

No	チェック項目	実施済	実施予定（実施時期）
1.	ネットワーク経路でのメッセージ挿入、ウイルス混入などの改ざんを防止する対策、施設間の経路上においてクラッカーによりパスワード盗聴、本文の盗聴を防止する対策、セッション乗っ取り、ＩＰアドレス詐称などのなりすましを防止する対策をとっている。注8）	■	□（　　）
2.	データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者の必要な単位で、相手の確認（認証）を行っている。	■	□（　　）
3.	施設内において、正規利用者への成りすまし、許可機器への成りすましを防ぐ対策をとっている。	□	■（　　）
4.	ルータなどのネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶＶＰＮの間で送受信ができないように経路設定されている。注9）	■	□（　　）
5.	送信元と相手先の当事者間で当該情報そのものに対する暗	■	□（　　）

	号化などのセキュリティ対策を実施している。注10）		
6.	通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社などと、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にしている。 ・診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に係わる操作を開始する動作の決定 ・送信元の医療機関等がネットワークに接続できない場合の対処 ・送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ネットワークの経路途中が不通または著しい遅延の場合の対処 ・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 ・伝送情報の暗号化に不具合があった場合の対処 ・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 ・障害が起こった場合に障害部位を切り分ける責任 ・送信元の医療機関等または送信元の医療機関等が情報交換を中止する場合に対処	■	□（　　）
7.	医療機関内において次の事項において契約や運用管理規程等で定めている。 ・通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。 ・患者等に対する説明責任の明確化。 ・事故発生時における復旧作業・他施設やベンダとの連携に当たる専任の管理者の設置。 ・交換した医療情報等に対する結果責任の明確化。 ・個人情報の取扱いに関して患者から紹介等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。	□	■（　　）
8.	リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止している。	■	□（　　）
9.	回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認している。	■	□（　　）

注8：例として IPSec と IKE を利用することによりセキュアな通信路を確保することがあげられる。

注9：安全性が確認できる機器とは、例として ISO15408 で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が医療情報システムの安全管理に関するガイドライン第２版に適合していることを確認できるものをいう。

注 10：例として、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化などの対策があげられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用していなければならない。