資料 1

| オンライン結合の基準(徳島県個人情報保護条例) | 医療情報システムの安全管理に関するガイドライン第4.3版(厚生労働省) | 対応策 |
|---|---|---|
| (実施機関に関する基準) | | |
| 4 オンライン結合を行うことにより個人情報の改ざん，滅失，毀損及び漏えい等の危険が生じないようにするために，実施機関において，次のようなハードウェア上及びソフトウェア上適切な技術的措置が講じられていると認められること。 | | |
| (1) 不正なアクセスを防止するための適切な技術的措置が講じられていること。 | | |
| ア 無資格者によるアクセスを制限するためパスワード，IDカード等が必要なシステムとすること。 | 6.5 C-1(P48)<br>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。<br>6.11 C-2(P78)<br>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、<br>利用者等の必要な単位で、相手の確認を行う必要がある。 | 利用者毎にユーザーIDとパスワードを設定し、システムのアクセス権限を制限する。<br>ファイア」ウオールを設置し、外部からの不正アクセスを制限する。<br>デジタル証明書を使用するPKI認証により、端末機器の確認を行う。(暗号技術が用いられた偽造が不可能なデジタル証明書(電子署名)を利用して、外部からのアクセスが真正であるかを確認する仕組み。) |
| イ パスワードが画面に表示されないようにすること。 | 6.5 C-2(P48)<br>本人の識別・認証にユーザID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。 | パスワードは画面に表示できない機能とする。 |
| ウ 公衆回線により接続している場合は，端末機の確認機能を設けること。 | 6.11 C-2(P78)<br>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、利用者等の必要な単位で、相手の確認を行う必要がある。(再掲) | デジタル証明害を使用するPKI認証により、端末機器の確認を行う。(再掲) |
| エ 相手方のアクセスを必要な情報のみに制限する機能を設けること。 | 6.5 C-5(P48)<br>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。 | カルテ参照機能については、患者の同意に基づき、必要な情報のみにアクセスを制限する機能を有する。 |
| オ 特に重要なデータを提供する場合には，専用回線の利用，送信データの暗号化等，より厳重なデータ保護機能を設けること。 | 6.11 C-1(P48)<br>ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策をとること。施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策をとること。セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策をとること。<br>上記を満たす対策として、例えば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。 | 送信データの暗号化を実施する。<br>IPSecVPNによるセキュリティが確保された通信路を使用する。(IPSecとは暗号技術を用いてデータの改鼠防止や秘匿する技術のこと。VPNとは認証や暗号化により専用線の機能を提供するサービス。) |
| (2) 障害時の安全性を確保するために適切な措置が講じられていること。 | | |
| ア 機器の能力，容量を超えないように負荷状態を監視し，または制御する機能を設けること。 | 7.2 C-2(P93)<br>見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。 | 管理画面でデータベース容量を確認でき、容量のチェックが可能な機能を有する。 |
| イ 更新が終わるまで同一ファイルに対する他のアクセスを禁止する(排他制御)機能を設けること。 | 7.1 C-2-a-3(P89)<br>確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと。 | 同一ファイル内の同一レコードの更新作業は、同時にはできない排他制御の機能を有する。 |
| (3) 障害を速やかに回復するために適切な措置が講じられていること。 | | |

| オンライン結合の基準（徳島県個人情報保護条例） | 医療情報システムの安全管理に関するガイドライン第4.3版（厚生労働省） | 対応策 |
| --- | --- | --- |
| ア　障害を早期に発見できるように，システムの運転状況を監視する機能を設けること。 | 6.10　C-1(P61)<br>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ること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。 | ディスク容量のチェック及びシステムが停止していないかの確認機能を有する。トラブルシューティングの手順書を作成する。 |
| イ　定期的にデータのバックアップを行うとともに，障害発生時にはこれらのデータを元に速やかにシステムを回復させる機能を設けること。 | 7.3　C-2-5(P97)<br>各保存場所における情報がき損した時に、バックアップされたデータを用いてき損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと。 | 定期的にバックアップを行っており、ディスク障害発生時に復元させる機能を有する。 |

| オンライン結合の基準（徳島県個人情報保護条例） | 医療情報システムの安全管理に関するガイドライン第4.3版（厚生労働省） | 対応策 |
|---|---|---|
| 5 提供の相手方が特定できる場合は，相手方に，次のような個人情報保護のための制度が整備されている，又は提供された個人情報を保護するための適切な措置が講じられていると認められること。 | | |
| (1) 相手方が，電子計算機処理される個人情報に関して次の事項を定めた条例，規則，要綱等の規程を制定していること又は同等の運用を行っていること。<br>ア 目的外の利用及び提供の禁止<br>イ 個人情報を取り扱う職員の責務<br>ウ 不用となった個人情報の確実な廃棄<br>エ その他個人情報保護のための必要な措置 | 6.11 C-6(P79)<br>医療機関内においても次の事項において契約や運用管理規定等で定めておくこと。<br>・通信機器、暗号化装置、認証装置等の管理責任の明確化。<br>・患者等に対する説明責任の明確化。<br>・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。<br>・交換した医療情報等に対する管理責任及び事後責任の明確化。 | 「徳島県立中央病院地域連携医療情報ネットワーク（仮称）」の運用規程<br>および運用規程細則により目的外利用の禁止、職員の責務、確実な廃棄を定めている。<br>また機器の管理責任、患者への説明、事故発生時の対応者、交換した医療情報の管理責任について定める。 |
| (2) 端末機の管理について適切な措置が講じられていること。 | | |
| ア 端末機の管理責任者を定めること。 | | 端末機の管理責任者を定める。 |
| イ 端末機の使用状況を監視し，及び記録すること。 | 6.5 技術的安全対策 C-6(P48)<br>アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時間、ならびにログイン中に操作した患者が特定できること。 | アクセスログにより、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可能となっている。（ログイン時間はログアウト時刻から算出）定期的にアクセス記録を確認する。 |
| (3) 個人情報への不当なアクセスを防止するため，適切な措置が講じられていること。 | | |
| ア 個人情報へのアクセス資格を定めること。 | 6.5 C-5(P.48) 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。 | カルテ参照機能については、患者の同意に基づき、利用者ごとに必要な情報のみアクセスできる仕様となっている。 |
| イ アクセス資格を確認するためのパスワード，IDカード等が不正に使用されることがないように次のような措置をとること。 | | |
| (ア) パスワード，IDカード等の管理者を指定すること。 | 6.3 組織的安全管理対策 C-1(P40)<br>情報システム運用責任者の設置及び担当者の限定を行うこと。 | 医療情報システムの管理者を定めている。 |
| (イ) 依頼，承認，発行手続きを明確にすること。 | | 院内規程により、依頼、承認、発行手続きを定めている。 |
| (ウ) 有資格者が資格を失ったときは，直ちに資格を抹消すること。 | 6.5 C-5(P48)<br>アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規定で定めていること。 | 運用規定で利用者に変更があった場合は、直ちに届け出るように規定し、資格を抹消する。 |
| (エ) パスワードを他人に知られ，またはIDカードを紛失する等の事故があったときは直ちに無効とする手続きを定めておくこと。 | 6.5 C-10(P49)<br>利用者がパスワードを忘れたり、盗用されたりす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。 | システム管理者が該当利用者の権限を無効とすることが可能である。<br>パスワードを他人に知られる等の事故があった場合の対応として、直ちに無効とする手続きを定める。 |

| オンライン結合の基準（徳島県個人情報保護条例） | 医療情報システムの安全管理に関するガイドライン第4.3版（厚生労働省） | 対応策 |
| --- | --- | --- |
| (オ) その他パスワードについては，次のような措置をとること。<br>a適宜変更し，かつ推測が困難なものとすること。<br>b他人に教えないよう徹底すること。<br>c書き留めておかないよう徹底すること。 | 6.5 C-10(P49)<br>(1)パスワードは定期的に変更し（最長でも2ケ月以内）、極端に短い文字列を使用しないこと。英数字、記号を混在させた8文字以上の文字列が望ましい。<br>(2)類推しやすいパスワードを使用しなこと。<br>6.5 C-2(P48)<br>本人の識別・認証にユーザIDとパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知りえない状態に保つよう対策を行うこと。 | パスワードの変更は随時可能とする。<br>パスワードは画面に表示できない機能とする。運用にて、定期的な変更、他人に教えない、利用者IDの共用の禁止、パスワードを書いたメモの貼付の禁止等ID・パスワードの漏洩することがないよう研修会等で徹底していく。 |

医療情報システムの安全管理に関するガイドライン第4．3版 （厚生労働省）への対応について

| 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 |
|---|
| 1. ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策をとること。<br>施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策をとること。<br>セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策をとること。上記を満たす対策として、例えば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。チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者に確認すること。 |
| 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・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。認証手段としてはPKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法を用いるのが望ましい。 |
| 3. 施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策をとること。これに関しては、医療情報の安全管理に関するガイドライン「6.5技術的安全対策」で包括的に述べているので、それを参照すること。 |
| 4. ルータ等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こと。安全性が確認できる機器とは、例えば、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本ガイドラインに適合していることを確認できるものをいう。 |
| 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等のセキュリティ対策を実施すること。たとえば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。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すること。 |
| 6. 医療機関等の間の情報通信には、医療機関等だけでなく、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等多くの組織が関連する。そのため、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すること。<br>・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関わる操作を開始する動作の決定<br>・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<br>・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<br>・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<br>・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<br>・伝送情報の暗号化に不具合があった場合の対処<br>・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<br>・障害が起こった場合に障害部位を切り分ける責任<br>・送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対処また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。<br>・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。<br>・患者等に対する説明責任の明確化。<br>・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。<br>・交換した医療情報等に対する管理責任及び事後責任の明確化。<br>個人情報の取扱いに関して患者から照会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。 |
| 7. 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すること。また、メンテナンス自体は「6.8 情報システムの改造と保守」を参照すること。 |
| 8. 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すること。<br>また上記1 及び4 を満たしていることを確認すること。 |
| 9. 患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI 個人認証等の技術を用いた対策を実施すること。また、情報の主体者となる患者等へ危険性や提供目的の納得できる説明を実施し、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にすること。 |

※厚生労働省の「医療情報システムの安全管理に関するガイドライン」については、すべての項目についてシステム稼働までに検証し、ガイドラインに沿った運用を行います。