資料 2

徳島県個人情報保護審査会会議資料(オンライン結合による個人情報の提供の制限の例外に関する事項
1　実施機関に関する基準
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、毀損及び漏洩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。

基準	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。	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。 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。 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。	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。	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。	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。	送信データの暗号化を実施する。 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。	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。	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。	

徳島県個人情報保護審査会会議資料(オンライン結合による個人情報の提供の制限の例外に関する事項

1　実施機関に関する基準

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、毀損及び漏洩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。

基準	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。	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。	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。
（相手方に関する基準）	
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。	「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 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。 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。
ア　目的外の利用及び提供の禁止	
イ　個人情報を取り扱う職員の責務	
ウ　不用となった個人情報の確実な廃棄	
エ　その他個人情報保護のための必要な措置	
（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。	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。	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。	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。	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。

徳島県個人情報保護審査会会議資料(オンライン結合による個人情報の提供の制限の例外に関する事項
1　実施機関に関する基準
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、毀損及び漏洩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。

基準	対応策
（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。	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。 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）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。	パスワードの変更は随時可能とする。 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。
ａ適宜変更し，かつ推測が困難なものとすること。	
ｂ他人に教えないよう徹底すること。	
ｃ書き留めておかないよう徹底すること。	