セキュリティポリシーとスタンダードにおいて、これらの各システムにおけるユーザＩＤの申請や承認ルールを明確に定める必要がある。

３　物理的セキュリティ

⑴ 電算機室の入退管理

（「オーダリングシステム（医事会計システムを含む）の患者情報のセキュリティ」及び「所内LANのセンター業務上のセキュリティ」）

電算機室には重要なデータを記録しているサーバ等ハードディスクを設置している。このサーバ等ハードウェアの損傷、盗難、データの漏洩等を防止する措置となる電算機室の常時入退管理が重要である。

電算機室は夜間施錠しているが、昼間勤務時間中は施錠管理せず衆人環視によっている。

昼間勤務時間中においても衆人環視によらず、施錠による入退管理が必要である。

⑵ ガス消火器の設置

（「オーダリングシステム（医事会計システムを含む)」及び「所内LANのセンター業務上のセキュリティ」）

サーバ等ハードウェアは水がかかると損傷する危険性が高いため、消火設備は水以外で消火するものを設置することが重要である。

電算機室は、天井にスプリンクラー、手前の部屋の廊下に消火栓が設置されているが、ガス消火器は設置されていない。

火災が発生した場合、スプリンクラーないし消火栓から水にて消火すると、ハードウェアが損傷する恐れがあるため、電算機室消火用にガス消火器を設置する必要がある。

⑶ 電算機の床固定

（「オーダリングシステム（医事会計システムを含む)」及び「所内LANのセンター業務上のセキュリティ」）

電算機は、地震が発生した場合、その振動により隣接しているサーバ等との衝突により損傷する危険性があるため、床への固定等保護措置が重要である。

電算機は、電算機室の床に固定されていないが、地震が発生した場合の損傷を防止するため、床に固定する必要がある。

⑷ 記録媒体の厳重な保管

（「オーダリングシステム（医事会計システムを含む)」及び「所内LANのセンター業務上のセキュリティ」）

カセットテープ等記録媒体は、小さく、鞄等に入れ容易に持ち出しが可能であるため、大型の金庫などによる厳重な保管が重要である。

マスタファイル等の重要なデータのバックアップを保管することに関する規程がなく、これらのバックアップは、鍵のある簡易な通常のロッカーに施錠されずに保管されている。

このため、バックアップを容易に持ち出すことが可能で、データが漏洩するおそれがある。

バックアップの記録媒体は、持ち運びが困難な大型の金庫等での施錠保管など、セキュリティを高める必要がある。

また、バックアップの持ち出しを防止するため、厳重な保管管理対策を検討すべきである。

(5) データ保管庫へのカセットテープ持ち出し検知機設置

（「オーダリングシステム（医事会計システムを含む）の患者情報のセキュリティ」及び「所内LANのセンター業務上のセキュリティ」）

バックアップの記憶媒体であるカセットテープは、小さく、鞄等に入れて持ち出すことが比較的容易であるため、媒体へのセンタータグ装着、持ち出しにより警報を鳴らす検知器の設置等が重要である。

バックアップテープの持ち出しに対して、センサータグを利用して警報が鳴る等の検知器は設置されていないため、カセットテープが持ち出され、データが漏洩するおそれがある。

バックアップの持ち出し検知器を設置し、持ち出しができないようにする必要がある。

4　情報セキュリティ教育

(1) システムのユーザ、システム要員、その他すべての職員の各々の特性を考慮したセキュリティ教育の実施

（「オーダリングシステム（医事会計システムを含む）の患者情報のセキュリティ」及び「所内LANのセンター業務上のセキュリティ」）

システムのユーザ、システム要員、その他の職員により各々の権限、取扱データの内容、重要性が異なるため、これらすべての職員に対する各々の特性を考慮したセキュリティ教育の実施が重要である。

セキュリティ教育として、システムのユーザその他すべての職員の各々の特性を考慮したセキュリティ教育は実施されていないため、個人情報を多く含む病院オーダリングシステムに係る電子データが漏洩するおそれがある。

すべての職員の各々の特性を考慮したセキュリティ教育を実施する必要がある。

5　個人情報保護

(1) 個人情報の持ち出し等に関するルールの明文化

（「オーダリングシステム（医事会計システムを含む）の患者情報のセキュリティ」）

患者の氏名、病名等個人情報は、個人にとって重要な情報である。この個人情報について、一定の保護措置が個人情報保護法等で定められている。これらの法律を遵守するために、個人情報の持ち出しや電子情報の学会持ち出し等に関する取扱ルールを明確に文書化することが重要である。

個人情報に該当する電子情報の学会持ち出し等に関する明文の取扱ルールがないため、個人情報の持ち出しや電子情報の学会持ち出し等に関する取扱ルールを明確に文書化する必要がある。

(2) 外部委託先からの個人情報保護に対する宣誓書入手

（「オーダリングシステム（医事会計システムを含む）の患者情報のセキュリティ」）

民法第715条第１項では、「ある事業のために他人を使用する者は、被用者がその事業の執行につき、第三者に加えたる損害を、賠償する責に任じる。但し、使用者が被用者の選任及びその事業の監督につき、相当の注意をなしたとき、または、相当の注意をしても損害が生じてしまったときは、この限りではない。」としている。

> 民法
> 第七百十五条
> 或事業ノ為メニ他人ヲ使用スル者ハ被用者カ其事業ノ執行ニ付キ第三者ニ加ヘタル損害ヲ賠償スル責ニ任ス但使用者カ被用者ノ選任及ヒ其事業ノ監督ニ付キ相当ノ注意ヲ為シタルトキ又ハ相当ノ注意ヲ為スモ損害カ生スヘカリシトキハ此限ニ在ラス
> ２使用者ニ代ハリテ事業ヲ監督スル者モ亦前項ノ責ニ任ス
> ３前二項ノ規定ハ使用者又ハ監督者ヨリ被用者ニ対スル求償権ノ行使ヲ妨ケス

最近の判例（事件名：宇治市住民基本台帳データ大量漏洩事件控訴審判決、大阪高等裁判所平成13（2001）年12月25日）で、その実質が業務委託契約であるか、請負契約であるかは契約形態の相違にすぎず、いずれにせよ、使用者責任の有無については，実質的な指揮・監督関係の有無が問題であるとして、委託した地方公共団体の使用者責任を認めた。

「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」第５条では、行政機関の長は、個人情報の安全確保等を講ずるよう努めなければならないとされている。

> 行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律
> （個人情報の安全確保等）
> 第五条　行政機関が個人情報の電子計算機処理又はせん孔業務その他の情報の入力のための準備作業若しくは磁気テープ等の保管（以下「個人情報の電子計算機処理等」という。）を行うに当たっては、当該行政機関の長（第二条第一号ロの政令で定める特別の機関にあっては、その機関ごとに政令で定める者をいう。以下同じ。）は、個人情報の漏えい、滅失、き損の防止その他の個人情報の適切な管理のために必要な措置（以下「安全確保の措置」という。）を講ずるよう努めなければならない。
> ２　個人情報ファイルを保有する行政機関（以下「保有機関」という。）の長は、ファイル保有目的に必要な範囲内で、処理情報が過去又は現在の事実と合致するよう努めなければならない。

医事業務（医療会計事務）の委託先は、脳血管研究センターとの契約の別記として個人情報保護を規定しているが、担当者から個人情報の保護に係る宣誓書を入手していない。情報システム保守の委託先と脳血管研究センターとの保守契約には一般的な秘密の保持の規定があるが、個人が類推される情報を含む範囲の広い個人情報の保護の規定はなく、情報システム保守の委託先は担当者から個人情報の保護に係る宣誓書を入手していない。脳血管研究センターはこれらの委託先から担当者個人の宣誓書の写しを入手していない。

このため、以下のおそれがある。

・委託先の担当者の個人情報の保護について認識がないこと
・この認識がないことにより、情報システム保守の委託先から個人情報が漏れること
・この漏れにより、患者のプライバシー権（自己の個人情報をコントロールする権利）が侵害されること
・この侵害により、脳血管研究センターが民法715条による損害賠償の責めを負うこと

個人情報の保護については委託先の管理が法律上必要とされており、脳血管研究センターは委託先から担当者個人の誓約書の写しを入手する必要がある。

(3) 委託契約書における個人情報持ち出し禁止規定の記載

（「オーダリングシステム（医事会計システムを含む）の患者情報のセキュリティ」）

個人情報は、情報の複写、漏洩等を防止する面で、常時その管理下に置いておく必要がある。このことから、この個人情報の外部持ち出しを禁止することが重要である。

医事業務の委託契約書及び情報システムの保守委託契約書には、個人情報の外部への持ち出しの禁止規定がないため、個人情報を外部に持ち出して業務を行うおそれがあり、この外部に持ち出しにより、個人情報が漏洩するリスクがある。

委託契約書に個人情報の外部への持ち出しを禁止する規定を定める必要がある。

6　事業継続の計画策定

(1) プログラムのバックアップ管理

（「オーダリングシステム（医事会計システムを含む）」）

電算機のディスク等が損傷を受け、情報システムを復旧する場合、ディスク等を交換する。その後、ＯＳ、プログラム及びデータのバックアップによりリカバーする。これに備え、プログラムのバックアップ等は、最新のものを外部媒体に保存することが重要である。

病院オーダリングシステムが稼動する電算機は、データ部分のバックアップをシステムで自動的に実施している。月曜日から金曜日に医事課の職員がバックアップテープを入替え、この入替により、5世代データのバックアップ保存が行われている。

しかし、病院オーダリングシステム（適用業務システム）の実行可能な形式のプログラムについて、脳血管研究センターでは一部を除きバックアップを保有しておらず、情報システムの委託先が保有している。

このため、もしハードウェアが損傷し、かつ、委託先がその実行可能な形式のプログラムを紛失等すると、ハードウェアを再度購入しても情報システムを復旧できないおそれがある。

病院オーダリングシステムのプログラムのバックアップを脳血管研究センターにおいても保存する必要がある。

(2) ハードウェア障害等により情報システム停止時における手作業マニュアル作成

（「オーダリングシステム（医事会計システムを含む）」）

ハードウェア障害等による情報システム停止時に事務を円滑に継続するため、これに備え伝票の手書き起票方法、業務フロー、承認ルール等を記載した作業マニュアルを作成し、必要な伝票類を常時保管しておくことが重要である。さらに、この作業マニュアル及び伝票類により、定期的にリハーサルを実施し、事務担当者の訓練及び作業マニュアルの見直しをすることが重要である。

医事会計システム及び病院オーダリングシステムを導入した平成12（2000）年12月時点で、システムが停止したときの対策として、伝票類を保存しておくことが各部門の代表者によって合意確認されている。

しかし、その伝票があれば運用ができるとして、コンティンジェンシー・プランの一環としてハードウェア障害等により情報システムが停止した時における手作業マニュアルが作成されていない。

このため、システム停止時の伝票類の手書きによる起票方法、業務処理フロー等が明確でない。

作業マニュアルを作成し、定期的にリハーサルを実施することにより、事務担当者の訓練及び作業マニュアルの見直しを実施する必要がある。

(3) 情報システム停止時、システムの復旧等に係る危機管理対応マニュアル等に基づく管理

（「オーダリングシステム（医事会計システムを含む）」）

情報システム停止時に円滑なシステムの復旧を図るため、①対応する組織、バックアップ等の資源の確保、停止時の病院事業運営・事務方法、復旧方法、教育・訓練、計画の維持管理等の危機管理計画を策定すること、②その復旧方法については危機管理対応マニュアル等に基づくこと、③外部の保守委託先の対応を契約で確保することが重要である。

24時間365日稼動する医事会計システム及び病院オーダリングシステムは停電時用の自家発電装置を備え、それが停止時においても救急医療を含め、全ての医療とその事務処理を継続する必要がある。

しかし、そのシステムの復旧手続は、外部委託先を呼んで復旧を依頼することとなっているのみである。情報システム停止時のシステムの復旧等に係る危機管理対応マニュアル等に基づく管理体制が整備されていない。外部委託先との契約では、保守を受けることができる時間が定められていない。これは、契約書に明記すると、脳血管研究センターが不利になることを理由としている。

このため、常識的な時間以外の時間において、その委託先の担当者がいない場合、復旧が遅れるおそれがある。

システムの復旧等に係る危機管理対応マニュアル等によって、委託先の担当者がいない場合の対策を定めておくこと、その対策がもし不可能であれば24時間365日の保守を委託契約で明記し、外部委託先の体制整備を促すことが必要である。

7　バックアップとリカバリー

(1) バックアップテープ交換の管理

（「オーダリングシステム（医事会計システムを含む)」）

情報システム障害時に常時可能な限り最新のバックアップからリカバリーによりその復旧を図るため、そのテープ交換を管理簿等により管理し、常時最新のものを一定世代確保することが重要である。

医事会計システム及び病院オーダリングシステムは、自動運用によりデータを日次に夜間バックアップしている。その完了により飛び出たテープを手作業により、テープ交換することで5世代保存されている。

バックアップテープの交換履歴が管理簿等により記録されておらず、システム管理者がテープ交換状況をモニタできないため、もしテープを交換せず、ハードディスクの損傷、その交換、バックアップデータによるリカバリーで､最新の前日分のバックアップデータが使用できないとき、その前々日のものがないおそれがある。

バックアップの実施を管理簿等により管理し、最新のもの5世代保存を確実なものとする必要がある。

(2) バックアップテープからの電算機のディスクへのリカバリー対策

（「オーダリングシステム（医事会計システムを含む)」及び「センター業務」）

電算機の障害時にはバックアップからディスクへのリカバリーにより情報システムを復元する。この復元を確実なものとするため、定期的に復元テストを実施することが重要である。

電算機は、24時間365日稼動の本番系1台のみであり、復元テストの実施には稼動を停止させる必要があるため、バックアップテープからの電算機のディスクへのリカバリーによる復元テストが実施されていない。

このため、もし、ハードディスクの損傷、その交換、データのバックアップテープからのリカバリーによる復元をしたとき、システムを復旧できないおそれがある。

予備系の電算機設置等を検討するとともに、バックアップのリカバリー体制の構築が必要と考える。

(3) バックアップテープの電算機隣接キャビネへの保管と遠隔地保管

（「オーダリングシステム（医事会計システムを含む)」及び「センター業務」）

バックアップ媒体は、熱に弱く火災発生時にはハードウェアと共にそれらを火災等で失う危険性がある。このため、バックアップ媒体は耐火金庫に保管し、さらに、重要なデータのバックアップは、電算機室や建物における大規模な災害発生時の対策として、遠隔地に保管することが重要である。

バックアップテープは電算機に隣接したキャビネの上段のガラス戸の中で保管している。

また、費用がかかること、セキュリティ上慎重を期すること、及び、建物が耐震構造で倒壊する危険性が少ないこと等から、バックアッププログラム及びデータの遠隔地（二重）保管を実施していない。