第11回　病院情報システムの運用

日紫喜　光良

病院情報システムの運用

- １．資産管理
- ２．ハードウェア・ソフトウェアの維持管理
- ３．利用面での維持管理
- ４．病院情報システムのトラブル対応
- ５．運用管理規程
- ６．システム評価
- ７．システム監査
- ８．労働衛生管理

資産管理

- ハードウェア
- ソフトウェア
- 周辺機器

- インベントリー収集
  - インベントリー：企業などで使用されている情報機器の資産情報のこと。
    - 例：PC本体の機種、そこに搭載されているCPU、メモリー、ハードディスクなどの部品、印刷機(プリンター)、ネットワーク機器などに関する情報
  - ネットワークを利用
    - Simple Network Management Protocol (SNMP)

ハードウェア管理

- システムを構成する機器の種類・役割・設置場所
- 故障発生時の対応方法
- 修理に要する時間
- →これらを考慮し、障害発生時のリスクを分析し、事前に対策を講じる
  - リスク表の作成
- 個々のシステムの管理者と、管理手順（正常、異常時）について定期的に確認

ソフトウェア管理

- 日常管理
  - システム関連ドキュメントの整備
  - プログラムなどの改修履歴の管理
- クライアントにおけるバージョン管理
  - 資源管理サーバ
  - ソフトウェア配信ツール
- データ(ファイル)管理

データ管理

- データファイルの種類
  - マスタ
  - トランザクションファイル
    - 一連の分断できない処理、一連の長い処理
    - （例）処方オーダのトランザクション：オーダ情報の入力におけるデータベースへの書き込みでは、オーダ内の全ての情報がデータベースに書き込まれるまで）
  - ログファイル
  - バックアップファイル
- マスタの維持管理
- データのバックアップと維持管理
  - すべてのステップを確実にする。
  - バックアップ作業時間の設定と関係部署への徹底周知

マスタの維持管理（1）

- (a) 素データ（病名や医薬品マスタなど）:
- 基本的には標準コードを利用（病名、手術・処置、医薬品、医療材料など）。
- ダウンロード、バージョン管理

- 独自コードとの折り合い。
- 旧コードとの整合性
- 旧コードから新コードに移行する際に、過去に蓄積されたデータをどうするか？
- 医師による、独自コード/旧コード→標準コードへの変換環境を整備する。

マスタの維持管理(2)

- (b) 運用データ(点数マスタなど)
- 解釈の変更多い。
- マスタに含まれる項目の意味、関連するプログラムや変更した場合の影響範囲を詳細に管理する必要。

３．利用面での維持管理

- 紙ベースの運用体制確保
- システム運用記録
- 利用者管理
- 業務運用上の問題点抽出と改善

紙ベースの運用体制

- システムダウン時は紙伝票で情報伝達。
- 障害時の運用手順について関係部署と詳細を詰め、使用する伝票類を統一して事前に準備
- 緊急時対策マニュアルに記載、徹底周知
  - どの段階で伝票システムに切り替えるか
  - 院内の連絡体制
  - 患者に動揺を与えない院内放送の方法、など

システム運用記録の重要性

- システムの運用記録：(a) レセプト作成など事前に綿密なスケジュールを立てておこなわれるシステム運用に関するもの、(b) 個々の機器のトラブルなど突発的事項

- おこなったことの内容
- それが正常に終了していることの確認

- トラブル発生時、一連のリカバリー手順の中でそれぞれのステップでの記録を残すことやトラブル報告を書いて病院長など責任者へわかりやすく説明することが重要。
- 機器の故障の場合には機器ごとに故障記録を記録簿に記載して管理すること。

利用者管理

- 原則
  - AccountabilityとTraceability
- 利用者登録
  - アクセス権限（ユーザ権限）の設定・変更
- ユーザによる正しいログイン
  - 自分のIDでおこなわなくてはならない

利用者管理の原則

- Accountability：
  - 個々の情報に対する責任の所在を明確にし、誰が(who)、いつ(when)、何を(what)、誰に(to whom)、何の目的で(why)、どのような方法で(how)、といった5W1H条件を保存すること。
- Traceability：
  - 責任の所在を過去にさかのぼって明確化できる環境を整えること

利用者登録の問題点

- 迅速な対応が困難な場合がある
  - 利用者の採用、退職
    - 大学病院など多くの研修病院では医師の出入りが激しいので、タイムリーな利用者の登録が難しい
    - 看護学生や医学生の実習への対応
    - 非常勤職員や臨時職員の取り扱い
    - 非常勤医師の都合で別の医師が来て診療をおこなうこと（代診）への対応
  - 人事システムとの連携の問題
    - 人事システムと病院情報システムの利用者管理情報との目的の違い→単純にデータを取り込んでも役にたたない。

アクセス権限の設定・変更

- アクセステーブル
  - 職種、利用者ごとに利用範囲を定義
  - ミリタリーモデル
    - 緊急時に、当直医が担当外の患者を診察する場合もあるが、平時はアクセス禁止で緊急時にはアクセスを許すことはこのモデルでは対応できない。
    - 診療チームに属するすべての医師が担当患者のデータを共有するのが一般的であるが、患者の希望で特定の医師にのみデータ参照を許さなければならない場合もこのモデルでの実現は不可能
- 緊急の場合への対応が必要
  - アクセス制限を解除する機能
  - アクセス制限を広めに設定→不必要なアクセスをアクセスログなどから監視

アクセスログ

- 誰が
- いつ
- どの端末から
- どの患者の
- どのような情報に　アクセスしたか

パスワード

- 定期的な変更
- 平易なパスワードの設定をさせない
- パスワード管理の重要性についての利用者教育

- パスワードの補助機能
  - 生体認証
  - ICカード
    - 利用者が端末に近づいただけで本人認証をおこない、本人専用のシステムが自動的に立ち上がり、場所を離れると自動的にログオフするといった機能が本来は必要。

- 病院情報システムの利用者管理について明らかに誤っているのは？
  - １） 職種毎に設定する操作権限の範囲は医療機関全体で決定する
  - ２） 同一職種の同僚のIDを借りても医療関係資格に関わる守秘義務には違反しない
  - ３） 利用者に対する生体認証を完備していてもセキュリティに係るユーザ教育は不可欠である
  - ４） 職員本人の同意なしにアクセスログを監視する行為は個人情報保護法に違反している
  - ５） IDとパスワードによる電子カルテのアクセス管理は、真正性の確保を担保する意味がある。

４．トラブル対応

- システム障害
  - ハードウェアの故障
    - サーバ
    - クライアント、周辺機器
  - ソフトウェアのバグ
  - ネットワーク障害　など
- 運用障害
  - 運用手順ミスによるデータ破壊など
    - システム復旧時の伝票からシステムへの切り替えに関して

ソフトウェアのバグ対策

- 発見が困難
  - 「十分なシステム検証を経た保証」は難しい
- 対策:
  - 十分なテストを経たソフトウェアを採用
  - 他の施設での導入・稼動実績のあるソフトウェアを採用

- ベンダ企業との協同作業が必要
  - テストデータの整備
  - チェック体制の確立と標準化

ハードウェア障害への対策

- ある確率で必ず発生するものとして対策を立てる
  - 障害発見のスピード：日常の監視体制
  - 障害の程度や診療への影響の迅速な把握：情報収集体制
  - 素早い対処：ログファイル（ジャーナル）のバックアップなど、データを元に戻すための作業を確実におこなうための訓練
- 障害が広がらない工夫
  - それぞれの部署には複数の端末を配置する

監視体制

- オンライン監視
  - コンソールのログ情報、端末稼動状況
  - ハードウェアからのアラーム
- ネットワーク監視
  - 動作確認
  - ネットワーク監視パネル
- 日常処理監視
  - 処理の正常終了の確認
  - データ量などの確認
  - 業務日誌への記載
- オンライン環境監視
  - ディスク残量監視、一日の減少率の把握

システム障害発見の契機

- 発見者からのクレーム電話
- アラームランプ点灯
- 処理の異常終了
- コンソールのエラーメッセージ・ログ情報
- データ処理量が異常に少ない（または多い）
- オンライン業務の異常終了

システム障害時の対応（1）

- 情報収集（収集目的：発生源の特定、影響範囲の特定、トラブルの種類の特定、原因追及・原因分析のためのデータ保全）
- 関係部署への連絡/院内放送など（第1報）
- 対策の決定（対策選択の因子：診療への影響、代替案の有無、復旧見通し、復旧後の作業量）

- システムを復旧させ再起動する前に、データ・ロスが発生しないことの確認を忘れてはならない。

システム障害時の対応（2）対策決定後

- 関係部署への連絡/院内放送など（第2報）
- バックアップ作業の正常終了確認
- システム復旧（データの復旧作業は、夜間などにおこなうことが多い）
- 管理者（病院長など）への報告

- 伝票など別の運用で一時しのぎした場合、
  - システム復旧後にデータを復旧させる作業（通常、その日の夜間にシステムを停止させておこなうこととなる）で
  - 完全にデータの整合性がとれる状態にもどす。
  - 対策についてベンダのSEとも協議し、万全の体制で臨む。

システム障害時の対応（3）システム復旧後

- 関係部署への連絡/院内放送など（第3報）
- データの復旧作業
- 管理者（病院長など）への完了報告

障害記録簿

- トラブルの発生から復旧にいたるまでのプロセスを記録（障害記録簿）として残し、いつでも参照できるようにしておく必要がある。
- 記録簿に記入した日
- 記入者
- 障害発生日時（できるだけ時刻も）
- 障害ホスト名とそのOS
- 障害の内容
- 原因
- そのときおこなった対処
- 関連資料
- ユーザにどのようなアナウンスをおこなったか
- サーバの停止をおこなったのであれば、その時間も

- システム障害への対応で誤っているのは？
  - １） 障害の原因がわかるまでは、院内全体への放送はしない
  - ２） 障害時の連絡先などの体制を決め、院内全体に周知しておく
  - ３） 端末等の予備機を用意し、すぐに交換できるように準備しておく
  - ４） 障害の復旧見込み時刻によっては、伝票での運用に切り替える
  - ５） 障害を発見したとき、診療への影響判断のための情報収集をおこなう。

- 電子カルテを操作しているPCでウイルス検知のメッセージが表示された場合、利用者の最適な行動はどれか
  - １） PCはそのままにして、セキュリティの管理部門に連絡する
  - ２） PCの電源をOFFにして、セキュリティの管理部門に連絡する
  - ３） PCをネットワークから切り離して、セキュリティの管理部門に連絡する
  - ４） PCの画面のハードコピーを印刷して、セキュリティの管理部門に連絡する
  - ５） アンチウイルスツールでウイルスを駆除して、セキュリティの管理部門に連絡する

障害対策ならびに運用マニュアルの作成

- （1）システム全体に関わる事項
  - (a)機器構成
  - (b) システム構成
- （2）保守体制に関する事項
  - (a) 保守契約書関係
  - (b) 保守報告書関係
- （3）バックアップに関する事項
  - (a) データバックアップ・リストア（再編成）手順書
  - (b) データバックアップ確認チェックリスト
  - (c) バックアップデータの保管
- （4）監視体制に関する事項
- （5）周辺機器の故障に関するユーザ向け説明書
  - (a) ユーザ向け機器の取り扱い説明書
  - (b) 機器の故障の見分け方
- （6）トラブル時のチェック項目
- （7）システム障害時の対応
- （8）教育に関する事項

- 病院情報システムのトラブルについて誤っているものは？
  - １） 発生を完全に防ぐことは難しい
  - ２） 順調に稼動しているシステムに突然発生することがある
  - ３） 発生防止に十分なコストをかければバックアップは不要である
  - ４） 発生に十分備えるためにはシステム担当職員の育成が必要である
  - ５） 発生防止にかけるコストが不十分であれば生じる損失が大きくなることが多い

５．運用管理規程

- 趣旨
- 利用目的
- 用語の定義
- 責任体制
- 情報のコントロール権
- 個人情報のアクセス権
- 情報の作成責任
- 情報の利用責任
- 利用者の資格
- 利用の申請、内容の変更、中止
- 利用の承認
- 利用の制限
- 他の情報システムの接続条件
- 守秘義務
- 利用の監査
- 利用の承認の取り消し権
- など

最低限必要な項目

- システム利用者の権利･義務･責任
  - システム利用者のアクセス範囲
- 管理責任者の役割･権限･義務･責任
- システム利用者の規約違反への対応

運用管理規定の実施

- アクセスログ収集・解析機能等のセキュリティシステムの実装
  - 管理者がアクセスログをチェック
- 監査委員会に報告

セキュリティポリシーの公開

- セキュリティポリシーの作成管理について誤っているのは？
  - １） リスク分析をおこなった
  - ２） セキュリティ確保のための組織を作った
  - ３） 基本方針や対策方法と実施手順を決めた
  - ４） ポリシーを第三者に知られないように厳重に保管した
  - ５） どのような情報があるか調査し、その重要性を決めた。

6. システム評価

- 複数の視点が可能
- システム導入効果
  - 業務の効率化
  - 医療の質向上
  - 患者サービス向上
- システム品質・性能効果
  - 機能性
  - 安定性
  - 操作性
- システムのコストパフォーマンス評価
  - コスト：初期投資＋ランニングコスト
  - パフォーマンス：機能による処理量

システム導入効果の測定

- 業務の効率化
  - 職員の業務時間調査（タイムスタディ）
- 医療の質向上
  - 処方・注射などの疑義照会件数
  - 指示受け部門の確認・問い合わせ件数
- 患者サービス向上
  - 患者動態調査（到着時間、帰宅時間）による待ち時間の測定

7. システム監査

- 病院情報システムおよび業務に対する、第三者による点検・評価
  - 信頼性、安全性、効率性
  - 企画、開発、運用、保守　というシステムライフサイクル全過程が対象
  - 共通業務：企画、開発、運用及び保守業務に共通
    - ドキュメント管理
    - 進捗管理
    - 要員管理
    - 外部委託
    - 災害対策

システム監査基準

- (1) 一般基準（9項目）
  - 一般基準は、システム監査において基本となる監査計画及びシステム監査人に求められる要件等の原則を定めている。
- (2) 実施基準（191項目）
  - 実施基準は、システム監査の対象である情報システムの企画、開発、運用及び保守業務並びに共通業務に対する監査項目を定めている。
- (3) 報告基準（8項目）
  - 報告基準は、システム監査の結果をとりまとめるに当たっての必要事項及び結果に基づく措置を定めている。
    - 組織体の長に報告する

- 情報システム監査について、監査請負者が作成する監査報告書の提出先は？
  - １） 依頼組織の長
  - ２） 依頼組織の経営陣
  - ３） 依頼組織の監査依頼者
  - ４） 依頼組織の会計部門責任者
  - ５） 依頼組織の情報システム管理部門責任者

８．労働衛生管理

- VDT：Visual Display Terminals
  - ディスプレイとキーボードを備えた情報処理端末

快適なVDT作業のための作業環境

- 照明はディスプレイ面で500ルクス以上、照明器具にはルーバー、窓にはブラインドを
- ディスプレイは下向きに見る（ドライアイ防止）
- 視距離は40cm以上
- キーボードには傾斜を
- 筐体は邪魔にならない場所に
- 机の高さは、脚が窮屈でないように
- 椅子
  - 背あて角度調節ができる
  - 座面高さ調節ができる
  - 移動可能、5本足
  - 足裏全体がつくように

質問

- 医療情報技師の役割のうち誤っているものを1つ選べ
  - 1） 常日頃から各部署とのコミュニケーションを円滑に行なっておく
  - 2） システムの障害が発生した場合、診療業務に影響が出ないよう努める
  - 3） 各種マスタの維持管理を行なう際は、必ずベンダの許可を得た上で行なう。
  - 4）ハードウェアの維持管理だけでなくソフトウェアの維持管理も行う必要がある
  - 5） システムの障害が発生した場合に備え、緊急時の対応についてベンダと決定しておく。

システム（ハードウェア）の調達方式

	月賦購入	購入	レンタル	リース
所有権	完済でユーザ	ユーザ	レンタル会社	リース会社
保守管理	ユーザ	ユーザ	レンタル会社	ユーザ
契約期間	物件による		主に短期	通常3年以上
中途解約	原則不可		解約可能	原則不可
費用	物件代金と金利	一時金が割高	リースより割高	レンタルより割安

保守管理における契約形態

- 業務委託（アウトソーシング）
  - スタッフは受託会社との雇用関係のもと、指揮命令も受ける。
- 人材派遣（運用委託）
  - 派遣されるスタッフは派遣業者に雇用される
  - 医療機関側の指揮命令下に業務を行う。

業務委託と業務派遣

- 医療情報システムの開発をベンダに業務委託し、病院内に作業場所を確保して開発を行わせる場合、病院の情報システム担当者の行為として適切でないものを1つ選べ
  - １） 個人情報保護を含む機密保持契約を締結する
  - ２） 開発用のパーソナルコンピュータを無償で貸し出す
  - ３） 病院の情報システム担当者が持っていないノウハウや専門知識を提供してもらう
  - ４） 病院情報システムの開発について、ベンダの担当者と打ち合わせを行いながら開発をすすめる
  - ５） 病院情報システムの開発について、病院の情報システム担当者の指揮命令下で開発をおこなう。