画像枚数、例えば40)とInstance Number(0020,0013)(画像通し 番号、例えば150)を参照して、Instance Number / Images In Acquisitionを計算、商(上の例では3)が何ブロック目かを、余り(30)がそのブロックで何枚目 の画像かを表す。ブロック単位で画像を分ける。

- PETでは、ダイナミック撮像といって長い時間同じ画像を何ブロックにも分けて撮る場合、ブロックを仕分けるにはSeries Numberに加 えてNumber of Time Slices(0054,0101)の数値でもグルーピ ングが必要。仕分けた後何枚目かはAcquisition Number。

3.2 画像データ登録機能

- DICOMデータは、アップロード完了後、サーバが自動的に任意の形式に変換すること。変換する形式は、以下の2種類である。
  - NIfTI
  - Analyze
- 変換元となるDICOMデータ形式は、テスト用データセットに含まれる形式とする。
- DICOMデータが1枚しかアップロードされない場合でも、ファイル形式の変換を行う。(表示できるのは2次元の静止画1枚のみ)
- アップロードされたファイルのヘッダー情報及び被験者コードをデータベースに登録し、検索可能な状態で保存すること。

3.3 画像閲覧機能

閲覧権限のある画像をリスト形式で表示できる。

一覧表は以下の項目で絞込みができる。
- 被験者コード
- 日付範囲
- 画像モダリティ

リスト表示の項目は撮像日、撮像施設名、撮像装置など5～10項目。
※詳細はプロトタイプで確認・決定する。

元データ(DICOM画像)のひとまとまり(基本的にはシリーズごと)に対して解析結果の画像(NIfTI、Analyzeなど)が対応付けられていればアイコンなどでファイルの存在を表現する。

ビューワが起動できるファイルの場合(NIfTI、Analyze、PDFやjpgなど)ビューワを起動し閲覧できるようにする。

権限が与えられている利用者が、画像データや解析データをダウンロードできるようにする。

3.4 品質管理機能

- NIfTIビューワを使用し、被験者またはひとまとまりの画像に対して品質チェックを行い、結果を登録、閲覧、修正、削除できる。
- 選択した一人の被験者、もしくはさらに細かくひとまとまりの画像に対してそれぞれチェック項目があり、入力、閲覧、変更ができる。(権限があるユーザーのみビューワから起動できる。)
- 登録、閲覧、修正、削除は権限を与えられた利用者に限る。

3.5 読影管理機能

NIfTIビューワを使用し、被験者またはひとまとまりの画像に対して読影レポートを登録、閲覧、削除できる。

- 読影レポートはフリーのテキストコメントである。
- 登録、閲覧、修正、削除は権限を与えられた利用者に限る。

3.6 解析データ管理機能

任意のフォーマットのファイルを選択し、被験者と対応付けて解析データファイルをサーバにアップロードできる。

- ファイルの種類にはNIfTIやAnalyzeフォーマットのものやPDF、jpg、csvなどが見込まれる。
- アップロードされた解析データファイルは、被験者に対してだけではなく、DICOM画像の1まとまりごとに対しての対応付けも行われ、閲覧とダウンロードの対象となる。
- NIfTIやAnalyzeの場合は.hdrと.imgの2ファイルに分かれてしまう可能性があるため、ワンセットとして対応付けできるようにする。
- 登録、閲覧、修正、削除は権限を与えられた利用者に限る。

3.7 撮像装置品質情報管理

撮像装置情報及び品質管理情報の登録、変更、変更履歴表示、削除ができ、プロジェクト毎に、撮像装置の情報を一覧表示できる。る。

撮像装置情報とは以下の通りである。

- メーカー名
- 装置名
- 画像モダリティ
- ソフトウェアバージョン
- 設置日

品質管理情報とは以下の通りである。

- 登録日(システム日付)
- 登録者(ログインIDの利用者名)
- コメント(テキスト形式)

3.8 システム管理

3.8.1 ユーザ管理

登録申請画面より必要な情報を入力して、登録申請できる。
登録に必要な情報は以下の通りである。

- ユーザ名
- ユーザID(e-Mailアドレス)
- パスワード
- 施設名
- 連絡先(電話番号 内線番号 FAX番号)

3.8.2 プロジェクト管理

プロジェクトの登録、変更 、削除でき、登録された情報を一覧表及び詳細画面で閲覧できる。
登録されるプロジェクト情報は以下の通りである。

- プロジェクト名
- プロジェクト内容
- 責任者名
- 責任者連絡先(電話番号 FAX番号 e-Mailアドレス)

3.8.3 権限管理

管理者は、ユーザに対してアクセス権限を設定することができる。
各権限は以下の通りである。

	Project Director	施設責任者	DICOMデータアップロード担当者	画像閲覧者	画像品質チェック担当者	読影担当者	解析担当者	撮像装置品質管理担当者
画像リスト閲覧	○	○	△	○	○	○	○	○
画像閲覧	○	○	△	○	○	○	○	○
DICOMデータアップロード			○					
DICOMデータダウンロード	○						○	
品質チェック登録					○			
品質チェック閲覧	○	○		□	△		○	○
読影レポート登録						○		
読影レポート閲覧	○	○		□		△		
解析データアップロード							○	
解析データ閲覧・ダウンロード	○	○		□			△	
解析レポートアップロード							○	
解析レポート 閲覧・ダウンロード	○	○		□			△	
撮像装置品質レポートアップロード								○
撮像装置品質レポートダウンロード	○	○						△

○　：権限あり
△　：自分で登録したものの確認のみ
□　：特別に権限を与えられた者のみ

4.非機能要求

非機能要求を定義するにあたり、前提となる条件は以下の通りである。

- 最大プロジェクト数:50
- 最大アカウント数:1000
- 研究プロジェクト終了までの期間:2008年12月1日～2013年03月31日
- データ保管期間:最大8年
- データ件数:以下の表の通り

	2009/03	2010/03	2011/03	2012/03	2013/03
アップロード件数/日	3	4	8	13	13
ダウンロード件数/日	8	10	20	25	25
閲覧数/日	8	10	20	25	25

	2009/03	2010/03	2011/03	2012/03	2013/03
最大アップロード数/時	5	5	10	10	10
最大ダウンロード数/時	5	5	20	25	25
最大同時閲覧数/時	5	10	20	25	25

- データ容量:最大100MB/ファイル
- サーバメンテナンス時間は、事前に計画すれば任意で設けることができる。
- デイリーメンテナンスが必要な場合は3:00AM - 5:00AMの間であればサーバを停止する事が可能。
- 利用者がサーバにアクセスする回線は、基本的に光回線またはADSL回線によるベストエフォート型インターネット経由での接続である。
- サーバは、ベストエフォート型光回線でインターネットに接続される。

4.1 可用性

運用に対する可用性は、毎月1回、2時間の定期メンテナンスを行う場合、稼働時間が8736時間となり、稼働率は99.7%となります。メンテナンスについては、運用計画で定める。

故障に対する可用性は、使用するハードウェア及びネットワーク、及びソフトウェアの品質によって決まる。

4.2保守性

保守性は復旧までの目標時間ですが、故障の内容によって異なり、リスクは、ハードウェア、ソフトウェア、ネットワークに区別できる。それぞれの障害発生時の復旧目標は以下の通りである。

- ハードウェア　:24時間以内
- ソフトウェア　:24時間以内
- ネットワーク　:24時間以内

4.3 保全性

障害発生時のデータ保全メカニズムは、以下の通りである。

- サーバのクラスタ化、
- ディスクのミラーリング
- ファイル及びデータベースの自動バックアップ

4.4 セキュリティ

- ID、パスワードによるログイン認証管理ができること
- 権限規定に基づくアクセス管理ができること

4.5 レスポンス

サーバ応答速度は2秒以内

4.6 スループット

サーバスループット:100Mbps以上
回線スループット:回線品質及びサービス内容に依存するが、平均スループットで5Mbps以上を確保したい。

4.7 キャパシティ

画像用ストレージスペース:400GB
システム領域及びデータベース:100GB

4.8 拡張性

サーバ仮想化及びスケールアウトによる拡張に対応する。

仮想化とは、I 台のサーバを論理的に分割し複数のOSとアプリケーションを同時に使用できるようにする技術。

スケールアウトとは、1台のサーバのパフォーマンスを向上させるのではなく、複数台のサーバで処理を分散することでパフォーマンスを向上させる拡張方法。

5. 将来に備えて

脳画像センターのサービスは、Ⅰ.の業務機能概要書にあるように、将来中核病院として高度化すると考えた時、今回の要求では補えない部分が発生する。

今後の開発は、運用管理規定を定め、チェックリストによってガイドライン等の安全管理項目に漏れがないように管理していく必要がある。

以下の表は、今回のシステムを安全管理ガイドラインに関連する要求と対応させた表である。

付表1:医療情報システム安全管理ガイドライン項目の内容
付表2:医療情報システム安全管理ガイドラインと脳画像センターシステム機能対比表

Ⅲ. 脳画像センター運用計画書

目次

【参考資料】

1 医療情報システムの安全管理に関するガイドライン
ファイル名:安全管理外ドライン.pdf

2 診療録等の保存を行う場所について
ファイル名:診療録等保存について.pdf

3 政府機関と重要インフラの情報セキュリティに係る行動計画
ファイル名:重要インフラセキュリティ行動計画.pdf

4 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」技術・運用基準チェックシート使用説明書(チェックシート第3版についても説明書は第2版と同じ)
ファイル名:チェックシート説明書.pdf

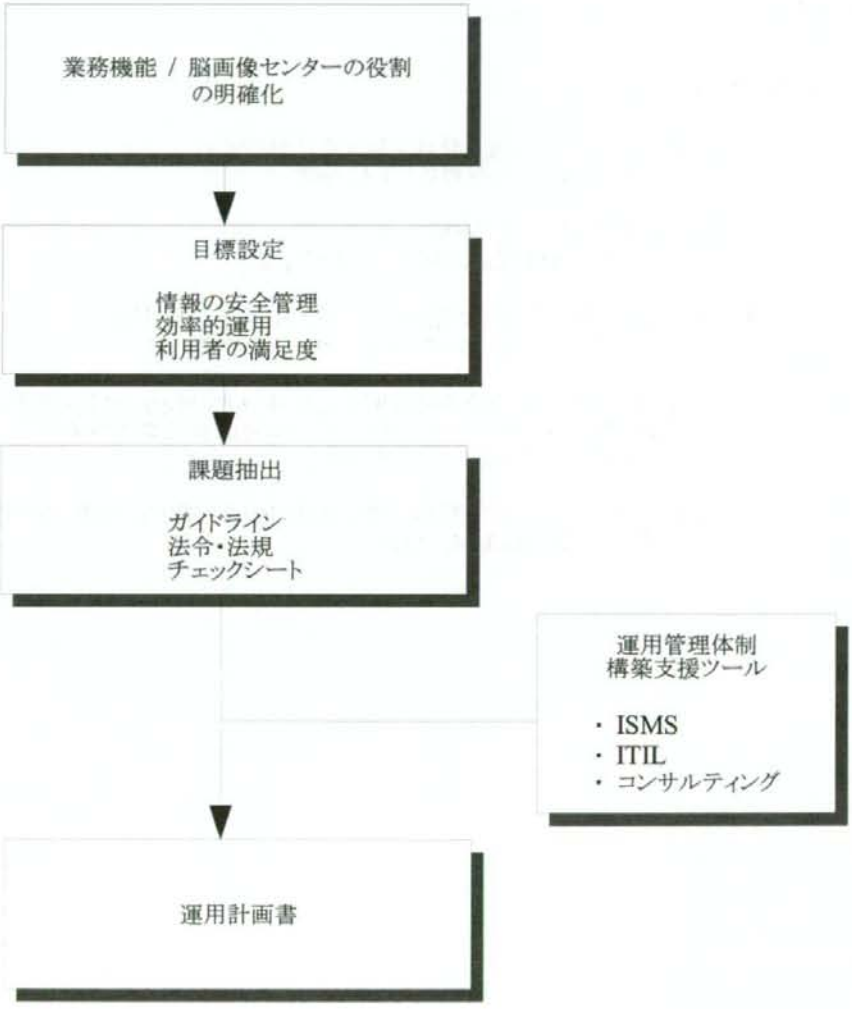
5 医療情報システムの安全管理に関するガイドライン第2版」技術・運用基準チェックシート
ファイル名:check_sheet.xls

1.脳画像センター運用管理に関する基本的な考え方

脳画像センターの運用管理において重要な達成ポイントが 3 つある。
「情報の安全管理」、「 効率的運用」、「利用者の満足度」である。
この 3 つの課題は、脳画像センターの業務目的に大きなく関係しており、計画段階から永続的に取り組まなければならない課題である。

脳画像センターの業務機能として、日々の運用を通して様々なサービスを提供するだけでなく、ノウハウを蓄積し、体系化し、効率的な治験コンサルティングにつなげていく取り組みを行う基盤として、運用計画策定及び運用業務を捉えていただければ幸いである。

【脳画像センター 運用計画策定手順イメージ】



1.1 運用計画書 項目一覧(サンプル)

1. 運用計画書概要
    - 1.1 計画書の対象となる範囲
    - 1.2 用語の定義
    - 1.3 運用責任について
    - 1.4 情報の相互利用性について

2.運営戦略
    - 2.1 運用計画
    - 2.2 サービスレベル高度化計画

3.サービス業務設計
    - 3.1 情報の安全管理(セキュリティポリシー)
        - 3.1.1 組織的安全管理
        - 3.1.2 物理的安全管理
        - 3.1.3 技術的安全管理
        - 3.1.4 人的安全管理
        - 3.1.5 情報の破棄
        - 3.1.6 外部との情報交換に関する安全管理
        - 3.1.7 電子保存の要求事項
        - 3.1.8 電子署名について
        - 3.1.9 電子データの外部保存に関する基準の明確化
    - 3.2. サービスレベル管理
    - 3.3 キャパシティ管理
    - 3.4 可用性管理
    - 3.5 継続性管理
    - 3.6 サプライヤ管理

4. サービス業務移行
    - 4.1 変更管理
    - 4.2 資産管理
    - 4.3 構成管理
    - 4.4 ナレッジ管理
    - 4.5 リリース管理

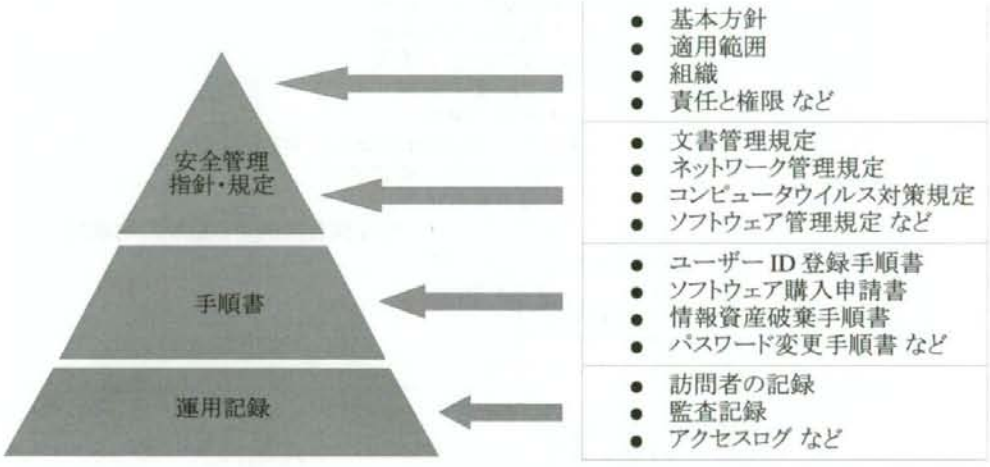
5. サービス業務運用
    - 5.1 イベント管理
    - 5.2 インシデント管理
    - 5.3 アクセス管理
    - 5.4 問題管理

6. 継続的改善
    - 6.1 監査
    - 6.2 サービスレポート
    - 6.3 フィードバック会議

2.情報の安全管理体制構築のための ISMS によるアプローチ

2.1 ISMS とは

ISMS（Information Security Management System)とは、組織の情報資産*1 の「機密性*2」、「安全性*3」、「利用可能性*4」を維持するための取り組みと定義されている。医療情報の安全管理面での適切な運用と説明責任を果たすための方法論として ISMS を活用することは有益であると言える。ISMS は、安全管理に関する指針、規定、手順、記録といった文書を基本に運用するフレームワークである。その文書の一般的な構成例は以下の通りである。



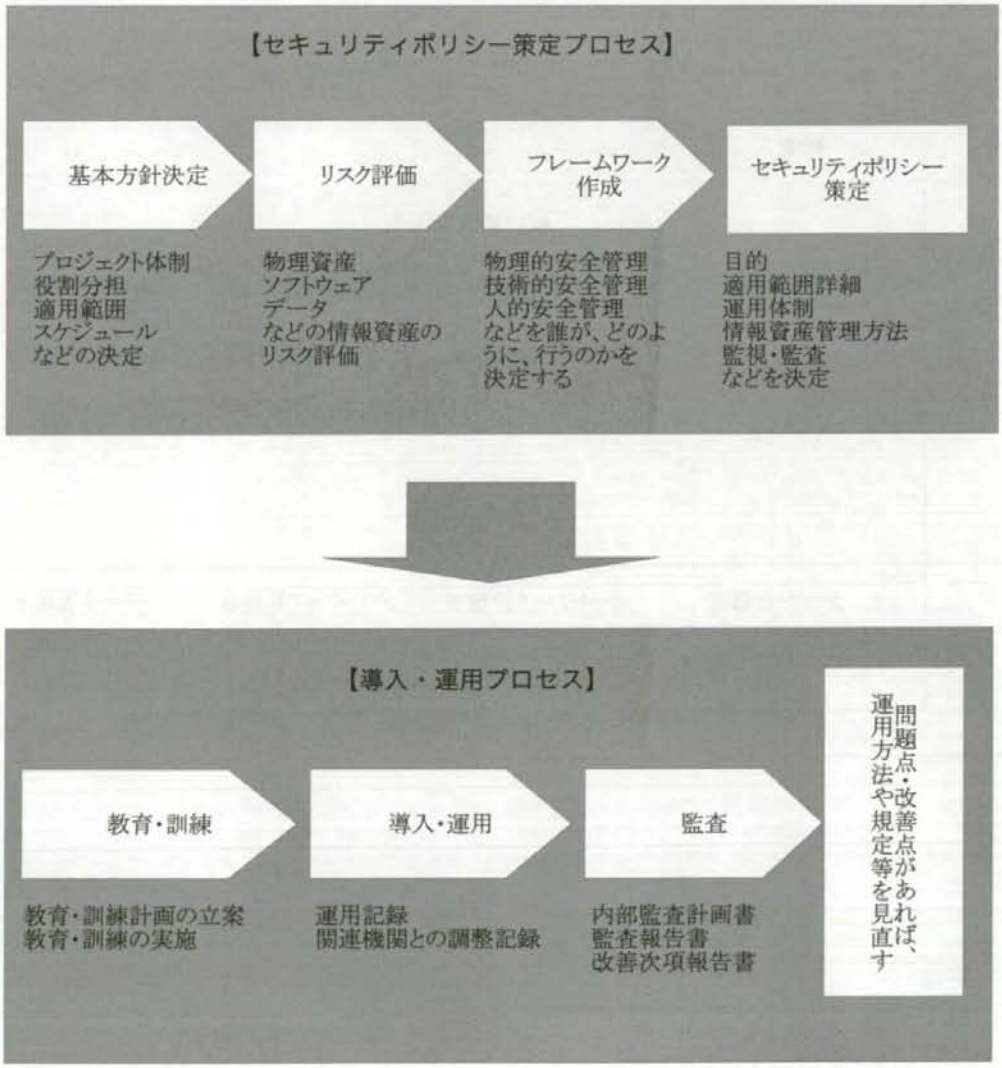
*1 情報資産　:組織が価値のあるものとして考え、保護する必要があるもの。
*2 機密性　:アクセスを許可された者だけがアクセスできることを保証すること。
*3 完全性　:情報及び処理方法の正確さ及び完全である状態を安全防護すること。
*4 利用可能性 :許可されたユーザーが必要時に、情報及び関連資産にアクセスできる事を保証すること。

2.2 安全管理体制の構築手順

ISMSを活用して、医療情報の安全管理体制を構築する場合、まず基本となる情報安全管理指針(以下セキュリティポリシー)を定め、その中で運用体制、指針、規定、手順といった個別の項目を策定する。策定作業は「セキュリティポリシー策定」と「導入・運用」の2つのプロセスがある。

以下の図は、プロセス項目と概要を示すものである。

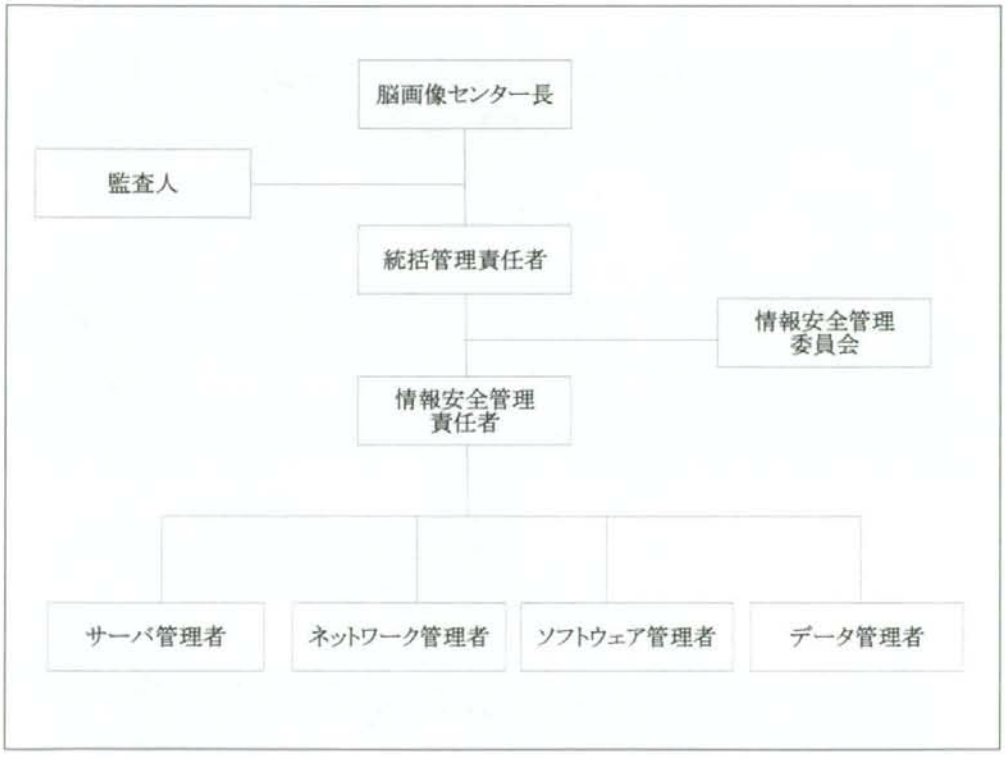
方針や規定の策定(Plan) → 教育・訓練 導入・運用(Do) → 監査(Check) → 改善(Action)のPDCAサイクルに合わせて設計されている。



2.3 運用体制

各情報安全管理の責任者は法令、規則及び規定要求事項に合致した行動をとる事の重要性と継続的な改善が必要であることを組織に伝達し周知させなければんばらない。また、組織の責任者は、ISMS を確立し、実施、維持していくために必要なリソースを提供、確保しなければならない。

ISMS の運用体制イメージを以下に示す。



2.4 安全管理規定内容参考例

規定名	規定の適用範囲
全般管理規定	情報資産を不正アクセスから保護するため、情報機器の取り扱い及び施設へのアクセス全般について定めるものである。
機密情報取扱管理規定	情報資産に対して、機密の重要度合い応じた取り扱いについて定めるものである。
リスクアセスメント管理規定	情報資産のリスクを評価するための目標及び評価方法を定めるのである。
職員管理規定	職員等が遵守しなければならないISMSの定めるものである。
物理アクセス管理規定	脳画像センターの入退室ルールを定義したもの
業務委託管理規定	業務委託先に対する情報安全管理水準を定めるものである。
ネットワーク管理規定	情報資産の適せるな活用のため、ネットワーク環境に関する取り扱いについて定めるものである。
コンピュータウイルス管理規定	コンピュータウイルスによる被害を未然に防止または最小限にとどめるため、コンピュータウイルスの感染に対する諸対策について定めるものである。
情報セキュリティ倫理規定	情報資産利用者の情報の取り扱いに対する意識向上のため、情報セキュリティに関する倫理的事項について定めるものである。
ソフトウェア管理規定	ソフトウェアのライセンス保護のため、ライセンス使用に関する取り扱いについて定めるものである。
システム開発管理規定	システム開発時における情報保護のため、開発環境での情報の取扱について定めるものである。
事業継続管理規定	業務の継続に対する重大な障害の影響から業務のプロセスを保護するため、組織全体にわたる事業継続管理について定めるものである。

3.業務効率化推進とサービスレベル向上のための ITIL アプローチ

脳画像センターの業務目的に、業務効率化推進と新たなサービスの開発がある。これらの要件を満たすには、運用によるノウハウの蓄積や安全管理を適切に行うという事以外に、これまでにない新しい価値を創造するという事が重要である。そのためには、日々の業務のサービスレベルを向上されるとともに、利用者のニーズを継続的にキャッチアップできる仕組みが必要となる。

ITIL(Information Technology Infrastructure Library)は、運用管理におけるベストプラクティス群であり ISMS のような方法論ではないので、自らがそのベスとプラクティスを参考に、運用改善策を構築していかなければならない。

しかしながら、手探りの運用改善と方向性を定めた運用改善ではその効果に差が生じることは明らかである。利用者のニーズや要求が絶え間なく変化する環境において、最も重要なリソースは時間であり、いかに効率的にサービスレベルの改善と高度化を達成できるかが、脳画像センターの成功要因になると言える。

変化の激しい環境においては、ITIL のような運用改善にフォーカスを当てたフレームワークを参考にすることは、非常に有益であると考える。

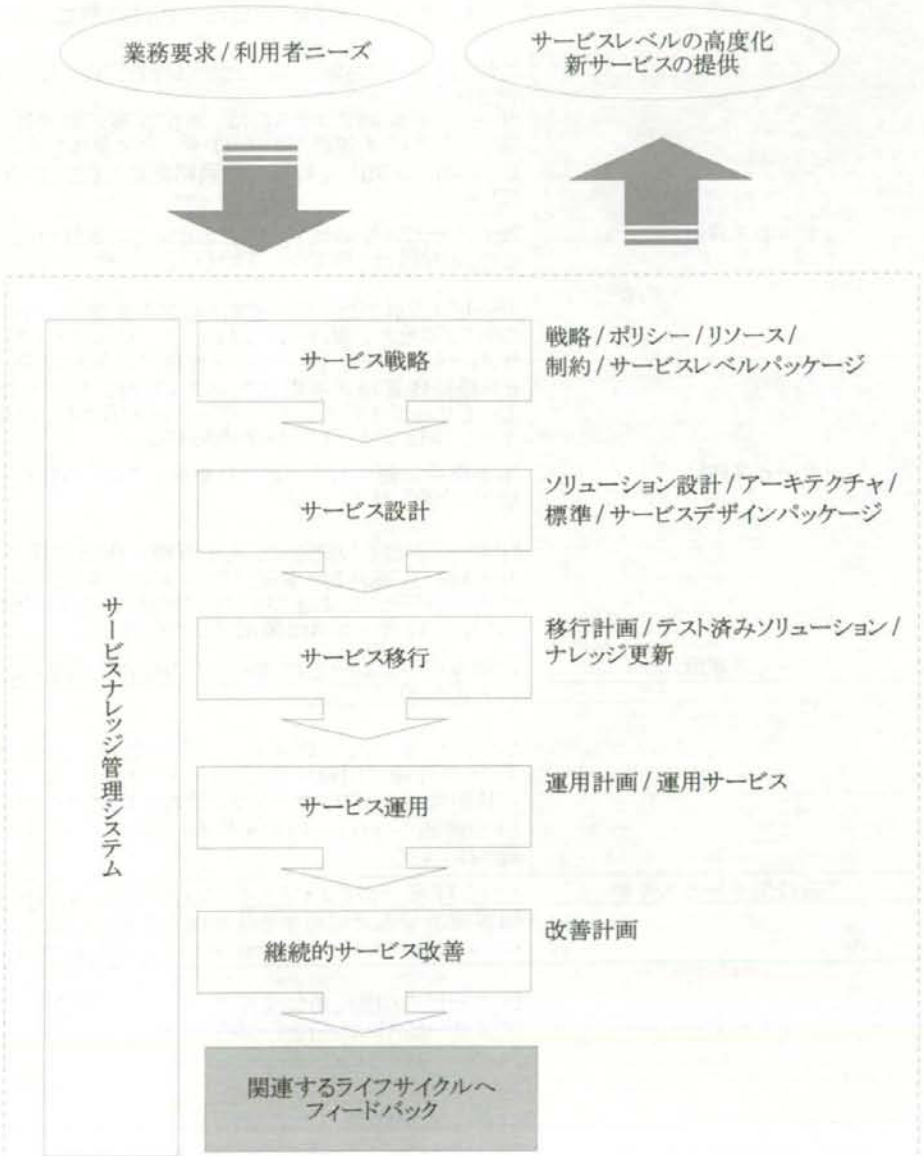
3.1 ITIL のフレームワーク

ITIL は現在バージョン3(ITIL V 3)となっており、5冊の書籍として提供されている。
その項目を以下に示す。

サービス戦略	サービス設計	サービス移行	サービス運用	継続的サービス改善
財務管理	サービスカタログ管理	変更管理	イベント管理	ステップ改善
需要管理	サービスレベル管理	サービス資産及び構成管理	インシデント管理	サービス測定
サービスポートフォリオ管理	キャパシティ管理	ナレッジ管理	リクエスト対応	サービスレポート
	可用性管理	移行計画及び支援	アクセス管理	
	IT サービス継続性管理	リリース及びデプロイ管理	問題管理	
	情報セキュリティ管理	サービスバリデーション及びテスト	サービスデスク	
	サプライヤ管理	評価	技術管理	
			アプリケーション管理	
			IT オペレーション管理	

3.2 ITIL V3 のライフサイクル

ITIL V3 では、すべてのサービス(インフラやアプリケーションを含む)活動は、業務からの要求によって実行されるとの考え方をとっている。以下の図は、そのライフサイクルを示したものである。



3.3 ライフサイクルの概要

ライフサイクル	概要
サービス戦略	どのようにしてサービスを設計、開発、実装をしていくべきかということを戦略としてまとめたもので以下の3項目を含む。 1. サービス提供先となる業務領域の特定 2. 提供サービスの決定 3. サービス提供に必要なアセットの準備に関する説明 これらはサービスレベルパッケージとしてサービス設計に引き渡される。 サービス戦略のプロセスには、財務管理／需要管理／サービスポートフォリオ管理があり、IT サービス全体をビジネスと同じレベルから俯瞰して長期的な戦略を立てることに重きを置いている。
サービス設計	既存サービスや新規サービスのビジネス要件を満たすためにどのような設計、開発をしていくべきか、その方法に関すること。 サービス設計では、サービスに必要な要素が一通り含まれるようにプロセスが設けられており、サービスカタログ管理／サービスレベル管理／キャパシティ管理／可用性管理／IT サービス継続性管理／情報セキュリティ管理／サプライヤ管理によってサービスデザインパッケージが定義され、以後はこのパッケージ単位でサービスが管理される。
サービス移行	本番環境に対するサービスの変更をスムーズに行うための方法がまとめられている。 IT サービスはこの段階で、変更管理／構成管理／ナレッジ管理／移行計画および支援／リリースおよびデプロイ管理／サービスバリデーションおよびテスト／評価というプロセスを経ることになり、IT サービスは運用フェイズとなる。
サービス運用	定常運用下における IT サービスの提供を効果的に行うための方法をまとめている。 ここでは、イベント管理／インシデント管理／リクエスト対応／アクセス管理／問題管理というプロセス群と、サービスデスク／技術管理／アプリケーション管理／IT オペレーション管理という機能が存在し、PDCA サイクルのベースとなる活動が定義されている。
継続的サービス改善	これら IT サービスライフサイクルのいずれの段階においても、障害個所や弱点に対する改善機会を見つけ出し、顧客に対してより良い IT サービスを提供する方法をまとめている。 IT サービスの継続的な改善は、7ステップ改善／サービス測定／サービスレポートというプロセスによって成り立っている。

4. 確定項目について

現在開発に取り組んでいる脳画像センターシステムであるが、システムの運用に関しては未定となっている事項が多々あるのが現状である。上記に示してきたISMSやITILといった方法論やベストプラクティスを参考にした運用計画の策定の必要性については将来的な課題ということにしておくとして、提供するサービス業務の現実的な運用計画策定を急ぐ必要がある。

以下は、これまでNCNPと弊社で確認してきた運用に関する要求項目（要求仕様書に記載されている項目）以外に、医療機関として遵守すべきガイドライン等で定められた要求事項について、大規模医療機関用技術・運用基準チェックシートを参考にした確認項目である。

これらの要求は、実際にサービスを提供する場合に必須となる項目も多いため、確認漏れのないようにする必要がある。

確認項目	チェック内容概要
通信ポリシー	インターネット等の共有型ネットワークを経由している場合、事業者が検知できないデータの盗聴、改ざんなどのハッキング手法が知られており、セキュリティに関する脆弱性があるため、通信に関するセキュリティを担保する必要がある。 ※現在は暗号化等のセキュリティ対策については明確に定めていないので、暗号化するという方向で調整したい。
	IKE/IPSECのパラメータとして、最適な設定がされているかチェックする。
	アプライアンスに設定されたIKE/IPSecの設定が設定されているかチェックする。
	IKE/IPSecによる安全性をさらに向上させるため、オンデマンドにVPN接続が運用されているかチェックする。
	セキュリティ対策に必要なアプライアンスを導入しているかチェックする。
	ログによる監査、またはユーザからの提供要請に応じることが常に可能であるかチェックする。
	拠点間の不正侵入などの脅威から守るため、適切なリスク対策が行われているかチェックする。
拠点内の技術的セキュリティ	適切なウィルス感染対策が行われているかチェックする。
	接続合意がされていない通信を禁止しているかチェックする。
	接続の起点をHigh Secure Zoneとした Secure Zone、DMZへの代理接続についてチェックする。
	接続の起点をDMZとしたHigh Secure Zone、Secure Zoneへの代理接続についてチェックする。
	プロキシ機能の設定をチェックする。
	ログ収集機能をチェックする。
	患者データなど重要データのアップデート・閲覧において必要なアドレス・ポート・コンテンツに限定したフィルタによる制限が行われているかチェックする。
	IPアドレス・ポート・コンテンツの利用を制限する機能が正常に機能しているかチェックする。

確認項目	チェック内容概要
サービス種別	医療情報等の提供またはデータの格納を行っている機器へのアクセスにおけるプロキシ機能による外部ユーザからの遮蔽のためのプロキシ機能の設定をチェックする。
	医療情報等の提供またはデータの格納を行っているサーバ等の機器へのウィルスチェックが正常に行われているかチェックする。
	ユーザへの医療情報等の提供にあたってのインターネットからの攻撃(DoS 攻撃・不正形式パケットなど)に対する検知機能が動作するかファイアウォール等のセキュリティ機器のポリシー設定をチェックする。
	医療機関以外への重要情報を公開・提供する場合のロギングによるアクセス監視について、ログ収集機能をチェックする。
	情報提供サービスを利用するユーザの認証でどの技術を用いているかチェックする。
	外部 ASP に接続される機器が High Secure Zone に配置されているかチェックする。
	ログによる監査、またはユーザからの提供要請に応じることが常に可能であることをチェックする。
	サイト閲覧に関して閲覧制限を用いているかチェックする。
拠点内の物理セキュリティ	各ゾーンに配置・格納された機器・データに対する、破壊・盗難・事故・災害などの脅威への対策として、機器・データに対する、破壊・盗難・事故・災害などの脅威に対する次のセキュリティ対策についてチェックする。
	システムの設定や盗難、システム設定の変更、ネットワーク機器の改ざんへの対策として、破壊・盗難防止のための設置場所における入退室管理および管理者の ID/パスワード等による権限管理をチェックする。