医療機関向けＩＳＭＳユーザーズガイド

-JIS Q 27001:2006（ISO/IEC 27001:2005）対応-

ISMS：Information Security Management System
情報セキュリティマネジメントシステム

2008 年 5 月 31 日

財団法人　日本情報処理開発協会

監修：財団法人　医療情報システム開発センター

はじめに

我が国における情報セキュリティマネジメントシステム（ISMS）適合性評価制度は、2002年 4 月より本格運用を開始しました。本制度は、我が国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られるレベルの情報セキュリティを達成し、維持することを目的としています。

本制度に適用される認証基準である JIS Q 27001:2006（ISO/IEC 27001:2005）（以下、ISMS認証基準）は、多くの企業が情報セキュリティマネジメントの実践に活用し、これにより認証を取得している事業者も増えています。

財団法人日本情報処理開発協会及び ISMS 適合性評価制度技術専門部会においても、ISMS認証取得を目指す事業者の理解を深めるために、2003 年 9 月に ISMS ユーザーズガイドを、2004 年 7 月に ISMS ユーザーズガイドーリスクマネジメント編ーを公表してきました。また、2004 年 11 月に顧客情報を多く取り扱う医療機関を対象とした医療機関向け ISMS ユーザーズガイドを公表し、さらに今回、従来の認証基準である ISMS 認証基準（Ver.2.0）から JIS Q 27001:2006 への移行を機に、本ガイドを改訂いたしました。

本ガイドの主な読者として想定しているのは、医療機関の経営層のほか、ISMS の構築または ISMS 認証取得を検討している医療機関において、実際に ISMS の構築に携っている担当者あるいはその責任者です。本ガイドが医療機関における ISMS を理解する上での一助となり、ISMS を構築・運用する上で参考になることを期待しています。

本ガイドの作成にあたり、ご協力頂いた財団法人医療情報システム開発センター（MEDIS-DC）の医療情報セキュリティ委員会の委員の皆様、IMS 適合性評価制度運営委員会の委員の皆様をはじめご協力頂いた関係各位に対し厚く御礼申し上げます。

2008 年 5 月

ISMS 適合性評価制度技術専門部会
財団法人日本情報処理開発協会

目　次

はじめに 1

１．位置付け 4
１．０　はじめに 4
１．１　本ガイドの位置付け 7
１．２　本ガイドの記述上のポイント 7
１．３　ISMS 構築ステップ 8
１．４　プロセスアプローチと PDCA モデル 9

２．引用規格 14
２．１　JIS Q 27002 14
２．２　ISO 27799 15
２．３　JIS Q 9001 15
２．４　TR Q 0008 15
２．５　その他の参考規格 18

３．用語及び定義 19
３．１　情報セキュリティとは 20
３．２　リスクマネジメントとは 23
３．３　マネジメントシステムとは 24
３．４　情報セキュリティ事象・情報セキュリティインシデントについて 24

４．情報セキュリティマネジメントシステム 27
４．０　医療情報セキュリティの重要性とセキュリティマネジメントの必要性 27
４．１　ISMS の確立と運用管理（医療機関における情報セキュリティマネジメントシステム（ISMS）の実践） 33
４．２　ISMS の確立（Plan-計画） 34
４．３　ISMS の導入及び運用（Do-実行） 71
４．４　ISMS の監視及びレビュー（Check-点検）・ISMS の維持及び改善（Act-処置） 75
４．５　文書化に関する要求事項 79
４．６　文書管理 81
４．７　記録の管理 81
４まとめ 82

５．経営陣の責任 83
５．１　経営陣のコミットメント 84
５．２　経営資源の運用管理 85
６．ISMS 内部監査 89
７．ISMS のマネジメントレビュー 91
７．１　一般 91
７．２　マネジメントレビューへのインプット 91
７．３　マネジメントレビューからのアウトプット 93
８．ISMS の改善 95
８．１　継続的改善 95
９．有効性の測定 98
９．１　有効性測定の目的 98
９．２　有効性測定のプロセス 100
９．３　有効性測定の PDCA 101
９．４　有効性測定手順書の概要例 110
ANNEX A.　参考文献 111
１　参考文献 111
２　法令等 120
ANNEX B.　医療機関向けｶﾞｲﾄﾞﾗｲﾝ（一部）と JIS Q 27001 及び JIS Q 27002 の位置付け 127
Annex C.　補足資料：情報漏洩等の事故に関する損害賠償と ISMS 適合性評価制度 129
おわりに 131

１．位置付け

１．０　はじめに

（１）　情報セキュリティの背景

「情報」が個人や組織が活動するための貴重なものであり、安全に管理する事の重要性は、情報技術の進展に伴い益々高まっています。情報がコンピュータで取り扱われるか否かにかかわらず、自らが保有する情報を安全に管理する事は、当然の責務である事は論を待ちません。特に医療機関などの組織においても、多数の関係者が情報に関与するため、安全な管理は組織として行わなければ効果的ではありません。情報セキュリティマネジメントを怠ると、その被害は自らに及ぶのみならず、他者にも及ぶことが考えられます。個人の医療情報が漏洩した場合はこれに当たります。

2005 年 10 月に ISMS 認証基準として国際規格 ISO/IEC 27001:2005 が、2006 年 5 月に国内規格 JIS Q 27001:2006 が、それぞれ発行され、金融サービス、製造業を始め各業種で普及が広がっています。医療分野においても、ISO/IEC 27002 は既に、オーストラリア、カナダ、オランダ、ニュージーランド、南アフリカ、英国の各国でローカルガイドラインとして医療情報セキュリティマネジメントに使われていますし、その他の国での関心も同様に高まって来ています。ISO/TC215 でも、ISO/IEC 27002 に基づく情報セキュリティマネジメントガイドの作成に着手しています。

各分野においてはそれぞれ独自なセキュリティ要件があります。個人情報の保護と安全性は全ての個人、企業、研究機関、政府において重要でありますが、医療分野でのセキュリティ要件(機密性、完全性、可用性)には独自な要求があります。医療機関は医療提供の必要性から個人的情報(家系や宗教、思想信条など)に触れることもありえますので、個人医療情報は全ての個人情報の中でもっとも機密性があると見なされており、その機密性を保護することは患者のプライバシーを守る為には基本的なことです。

医療情報の完全性を確保するために、その情報の取得から保存、更新、提供、廃棄までの完全なライフサイクル管理が検証可能であることもまた重要です。医療情報の可用性もまた、効果的な医療提供のためには肝要な点です。セキュリティ管理に重きを置き過ぎる余り医療行為に支障が出るような事があってはなりません。医療情報システムはまた、自然災害やシステム故障時に当たっても運用性が確保されることが必要不可欠な要請です。それゆえ、医療情報の機密性、完全性、とりわけ可用性を保持することは、医療分野での特徴的な点です。

医療分野での効果的な情報セキュリティマネジメントの必要性は、医療提供におけるワイヤレス（wireless)、インターネット技術の利用増大を通じてより緊急性を持っています。これらの技術は適切に扱われないと医療情報の機密性、完全性、可用性の危険性を増やします。多くの医療行為は、個人経営の診療所あるいは小規模診療所で提供されています。そこではセキュリティを管理するための体制が不十分になりがちです。医療施設の規模、場所、

医療提供形態に関係なく、全ての医療機関は医療情報の保護のために厳重な管理をしなければなりません。従って、医療機関はそのような管理の選択と実装の、明快で簡潔な医療独自の指標を必要としています。つまり、医療機関間の患者情報の電子的データ交換が増えるに連れて、医療における情報セキュリティマネジメントの共通規約を採用することは、医療機関にとって明らかに利点となります。

（２） ISMS の構築

医療情報は様々な様式で存在します。言語や数字で表現されたものだけでなく、写真、図、ビデオ、医療画像の形態をとるものもあります。また保管様式も、紙、フィルムや電子的媒体があり、伝送に当たっても、手渡し、FAX、郵便、コンピュータネットワーク等が利用されます。医療情報がどんな形を取り、どんな手段で転送や保管されたとしても、適切に保護されなければなりません。

医療機関向け ISMS ユーザーズガイド（以下、本ガイド）は、JIS Q 27001（以下、ISMS 認証基準）に従った情報セキュリティマネジメントシステム(Information Security Management System：ISMS)の医療情報分野における解釈と実装のためのガイドです。医療機関は、医療情報のセキュリティマネジメントが本ガイドに従って実施することにより、個人医療情報の機密性、完全性、可用性を保持するための安全性について、最低レベルの必要条件を満たすことになります。

一医療機関内に限っての ISMS を独自の手法で構築することは可能ですが、(1) に述べたように、複数の医療機関同士が電子的データ交換をするような場合には、全体として同じマネジメントシステムでセキュリティ管理を行っていることにより、漏れが無く有効な管理策を短期に構築できます。

また、ISMS は一度構築してからも継続的な見直しが必要です。その点からも標準的な手法に準拠して構築することが得策といえます。

本ガイドでは、医療情報のセキュリティにおいて要求されている事項を整理し、いかに管理運用するかのアプローチを示しています。本ガイドで記述されている要求事項は、長期間に渡って普遍的なものです。

一方、セキュリティ技術は今も急速に進歩し続けており、実装技術については例示しているものであっても利用者が実装するに当たってはこれに拘束されるものではありません。新たに開発され進歩している技術に対して偏見無く要求に合致する必要な技術を自由に採用できます。また、厚生労働省発行の「医療情報システムの安全管理に関するガイドライン第 3 版（案)」においても、医療情報の保管を委託される民間のデータセンターには、プライバシーマークや ISMS の認証を求めています。医療情報の外部保管を求める医療機関自身においても、ISMS 適合性評価制度についての知識・経験を持つことが、安全で有効な情報セ

キュリティマネジメントにつながります。

一般的論としての ISMS 構築とは、組織の目標を達成するために、事業領域のリスクマネジメントを効率的、効果的に行うための仕組みです。このことを ISMS 認証基準では以下の様に説明しています。

> 3.7 情報セキュリティマネジメントシステム，ISMS（Information security management system）
> マネジメントシステム全体の中で，事業リスクに対する取組み方に基づいて，情報セキュリティの確立，導入，運用，監視，レビュー，維持及び改善を担う部分。
> 注記 マネジメントシステムには，組織の構造，方針，計画作成活動，責任，実践，手順，プロセス及び経営資源が含まれる。
>
> （JIS Q 27001:2006 3 用語及び定義 より引用）

また、ISMS の構築で、以下のような効果が期待されます。

- 組織の目標を明確にし、確実に伝達し実施されるようにする
- 実施の状況を継続的に管理し、適正な水準に保つ
- 定期的な見直しを実施し、対策や実施の体制等を柔軟に改善する
- 社会環境や要請を認識し、組織の目標に反映する

ISMS は、情報セキュリティの分野にかかるマネジメントが対象です。情報セキュリティに関するマネジメントシステムの構築とは、組織が所有し、管理、運用する資産の価値に見合う対策の実施や、コンプライアンスの観点から法令等を遵守し、それを維持するための枠組みを構築することを意味します。

（注記）本ガイドにおける資産とは、情報に関連した資産のことをいいます。ISMS 認証基準(Ver.2.0)対応のユーザーズガイドでは情報資産と呼んでいましたが、JIS Q 27002:2006 で用語が「資産」に変更されたため本ガイドでは、一部の箇所を除き以下、資産と呼びます。

> この ISMS は，情報資産を保護し，また，利害関係者に信頼を与える，十分で，かつ，均整のとれたセキュリティ管理策の選択を確実にするために設計される。
>
> （JIS Q 27001:2006 1 適用範囲 1.1 一般 より引用）

従って、ガイドの要求事項を適切に実施することは、患者を始めとする利害関係者からの信頼を確保するために十分なバランスのとれた情報セキュリティを構築し、維持していくことにつながります。

１．１　本ガイドの位置付け

本ガイドの目的は、医療機関が情報セキュリティマネジメントを行うにあたり、運用規約と ISMS を効果的に構築する手助けとなるガイドとして作成されたものです。本ガイドに沿って ISMS を構築することが、唯一の ISMS 構築手段ではありません。ISMS に馴染みの無い医療機関にとって、ISMS 構築に取組むにあたってのガイドを目指しています。

本ガイドでは、ISMS 構築に必要な条項を紹介し、要求する内容や要求の意図、コンセプトなどについて解説しています。前述した ISO/IEC 27002、ISO/TC215 での議論を意識して記述されてはいますが、この国際標準（規格）に基づく「ISMS 認証」取得用ガイドラインではありません。しかし、ISMS を構築した医療機関にとって、更に第三者の評価を得るための「ISMS 認証」取得を目指す事は、本ガイドの延長線上にあります。

表 1-1　本 ISMS ガイドの位置付け

	ISMS ユーザーズガイド
対象組織	医療機関
対象者	主として医療機関の経営層、ISMS 構築要員

１．２　本ガイドの記述上のポイント

本ガイドの記述上のポイントは以下の点です。

本ガイドは、

- 医療機関向けに記述されている
- ISMS の認証標準である「JIS Q 27001:2006」を参照している
- 実践のための規範(ベストプラクティス)として「日本工業規格 情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範 JIS Q 27002:2006」(以下、JIS Q 27002:2006)を参照している。
- ISMS 適合性評価制度の、国際的な動向、国内の標準化の動向を視野に入れて記述されている
- 効果的な情報セキュリティマネジメントの確立及び維持を確実なものとするために、継続的改善プロセスが必要であることから、Plan-Do-Check-Act(PDCA)モデルを採用している
- PDCA モデルに基づいたプロセスアプローチを採用している
- リスクアセスメントプロセス、管理策の選択、適用宣言書(Statement of Applicability；SoA)の関係を記述している

１．３　ISMS 構築ステップ

ISMS 認証基準の改訂において、その意味する所は大きく変更していない事を、各 ISMS 認証基準に規定されている ISMS 構築のステップを比較検討し確認します。

情報セキュリティマネジメントの枠組みについては、ISMS 認証基準(Ver.2.0)では「9 ステップ」が規定されていました（図 1-1 参照）。

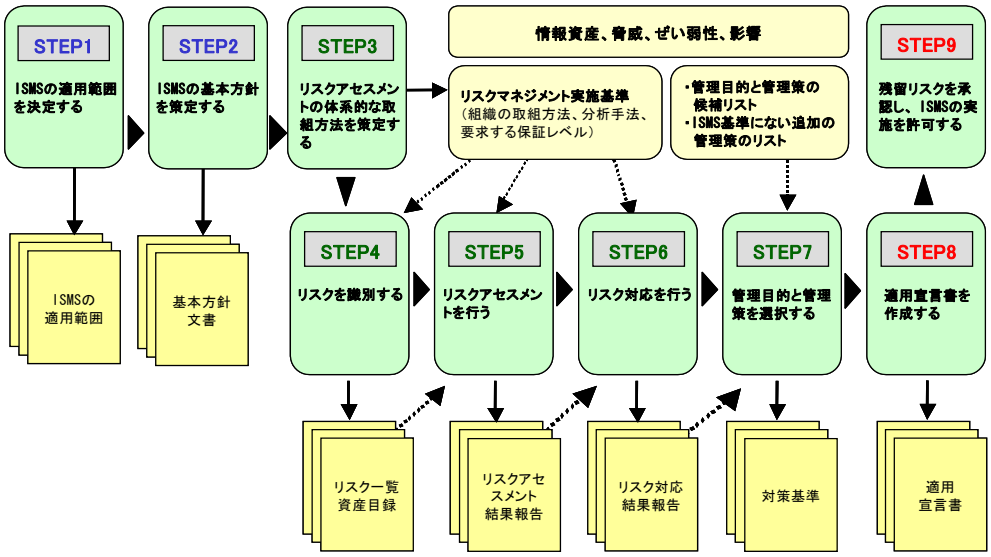


図 1-1　ISMS 構築のステップ(ISMS 認証基準(Ver.2.0))

ISMS 証基準では、図 1-1 の 9 ステップに代わり「4　情報セキュリティマネジメントシステム」において図 1-2 の 10 ステップを規定しています。

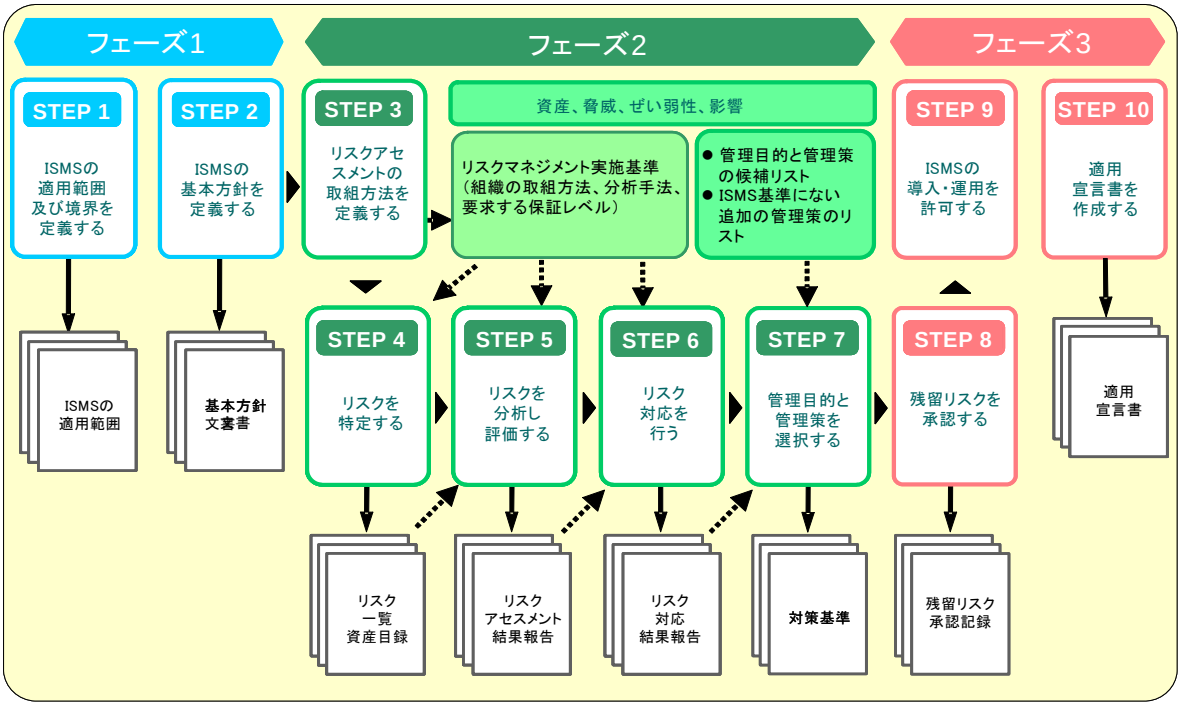


図 1-2　ISMS 構築のステップ(JIS Q 27001:2006)

（注記）STEP 6「リスク対応を行う」は、「リスク対応を行う（4 つの選択肢を明確にし、評価する)」を意味します。

構築のステップ数が 9 から 10 に増えてはいますが、これにより ISMS の構築の流れが大きく変更された訳ではありません（表 1-2 参照）。

表 1-2　ISMS 構築ステップの比較

ISMS 認証基準(Ver.2.0)	JIS Q 27001:2006
①ISMS の適用範囲を決定する －事業の特徴、組織、その所在地、資産及び技術の観点から	①ISMS の適用範囲及び境界を定義する －事業、組織、その所在地、資産及び技術の各特徴の観点から
②ISMS の基本方針を策定する －事業の特徴、組織、その所在地、資産及び技術の観点から	②ISMS の基本方針を定義する －事業上及び法的要求事項やリスクアセスメントなどから導かれる情報セキュリティに対する要求事項を考慮し、リスクマネジメント環境、ISMS を確立し維持する組織環境、情報セキュリティの全般的な方向性及び行動指針
③リスクアセスメントの体系的な取組方法を策定する ④リスクを識別する ⑤リスクアセスメントを行う	③リスクアセスメントの取組方法を定義する ④リスクを特定する ⑤リスクを分析し評価する
⑥リスク対応を行う	⑥リスク対応を行う
⑦管理目的と管理策を選択する	⑦管理目的と管理策を選択する
⑧適用宣言書を作成する	⑩適用宣言書を作成する
⑨残留リスクを承認し、ISMS の実施を許可する	⑧残留リスクを承認する ⑨ISMS の導入・運用を許可する

１．４　プロセスアプローチと PDCA モデル

本ガイドでは、医療機関が ISMS を確立、導入、運用、レビュー、監視、維持及び改善するためのモデルを提供することを目的として作成されています。従って、医療機関の業務環境を取り巻く情報リスクの変化に対応できる体制を構築する目的に適しています。

１．４．１　一般

一般に、業務改善はベンチマーキング(ベンチマーク基準)を活用すると成果が上がるといわれています。ここで、ベンチマーキングとは組織内外のベストプラクティス(最良の実践規範)に学ぶ手法のことを指します。

本ガイドは、「JIS Q 27002:2006」に規定された情報セキュリティマネジメントのベスト

プラクティスを参照して作成されているため、組織における「リスクの識別とその対応」の向上が期待されます。

ISMS におけるベンチマーキングの目的は、リスクアセスメントにより明らかになった適用範囲内のリスクに対して情報セキュリティを向上させることです。そのためには、適用範囲内の業務を取り巻く環境を分析し、影響を及ぼすリスクの状態を適切に捉えることが重要です。このリスク及びリスクの変化を的確に認識するためには、管理対象を明確に規定したマネジメントが必要になります。

マネジメントを実施することによって組織の方向性や方針が明確となり、これにより組織全体に情報セキュリティに対する期待やその測定等が徹底されます。更に、測定した結果をフィードバックすることにより改善が行われ、本質的な情報セキュリティ管理へとつながります。このことは、次のプロセスアプローチという考え方を採用することでより明確になります。

１．４．２　プロセスアプローチ

このプロセスアプローチという考え方は、品質マネジメントシステムの規格(JIS Q 9001:2000)等で紹介され、日本においても多くの組織で活用されています。プロセスアプローチでは、インプットをアウトプットに変換するために、経営資源を使用して運営管理されるあらゆる活動をプロセスとみなします。そして、組織内に存在する業務(プロセス)を明確にし、それらの相互関係を把握し、これら一連のプロセスをシステムとして適用して、運営管理する考え方のこと(アプローチ)を言います(図 1-3 参照)。

本ガイドでは、組織の情報セキュリティを管理するため、多くの活動を明確にした「プロセスアプローチ」を採用することを推奨しています。

> この規格は，組織の ISMS の確立，導入，運用，監視，レビュー，維持及び改善のために，プロセスアプローチを採用する。
> 組織が有効に機能するためには，多くの活動を明確にし，また，それらを運営管理する必要がある。インプットをアウトプットに変換することを可能にするために経営資源を使用して運営管理するあらゆる活動は，プロセスとみなすことができる。多くの場合，一つのプロセスからのアウトプットは，次のプロセスへの直接のインプットとなる。
> そのようなプロセスを明確にし，かつ，相互作用させることと合わせて，それらのプロセスをシステムとして組織内に適用し，かつ，運営管理することを“プロセスアプローチ”と呼ぶ。
>
> （JIS Q 27001:2006　0.2 ISMS の採用　0.2.2 プロセスアプローチ　より引用）

図 1-3 プロセスアプローチ

プロセスアプローチでは、それぞれのプロセスにおいて「インプット」されるものが何で、処理結果として「アウトプット」されるものが何かを多角的に検討し、明確にする必要があります。

ISMS の構築では、ここで検討され明確にされた情報セキュリティに関する項目からプロセスに関与する資産のリスクを識別し、適切に管理策を実施し運用していくことに繋がります。

本ガイドでは、医療機関がプロセスアプローチを採用した場合のメリットを以下の「ISMS 認証基準」をそのまま使用しています。

この規格が規定する情報セキュリティマネジメントのためのプロセスアプローチでは，利用者が次の点を重視することを期待する。

a) 組織の情報セキュリティ要求事項を理解し，かつ，情報セキュリティのための基本方針及び目的を確立する必要性を理解する。
b) その組織の事業リスク全般に対する考慮のもとで，組織の情報セキュリティリスクを運営管理するための管理策を導入し，運用する。
c) その ISMS のパフォーマンス及び有効性を監視し，レビューする。
d) 客観的な測定に基づいて継続的に改善する。

（JIS Q 27001:2006　0.2 ISMS の採用　0.2.2 プロセスアプローチ　より引用）

つまり、ISMS の構築を一連のプロセスとして捉え、各々のプロセスをプロセスアプローチに従って明確化し、その相互関係にあるインプットとアウトプットを把握することで、上記に示した ISMS の構築に要求される重要な事項が認識できます。

本ガイドでは、ISMS における管理手法としてプロセスアプローチを採用することを奨励し、それを実現するための考え方として次に述べる「PDCA モデル」を提示しています。

１．４．３　PDCA モデル

本ガイドでは、図 1-4 に示す「PDCA モデル」を採用しています。

後に触れる利害関係者の情報セキュリティ要求事項及び期待をインプットに、これらの要

求事項及び期待を満たす情報セキュリティの結果(運営管理された情報セキュリティ)をアウトプットとして導くために必要な活動及びプロセスを ISMS プロセスとします。

この ISMS プロセスは、PDCA モデルを採用することで整理され、組織の情報セキュリティ管理体制に継続的な学習と改善の機会を提供します。このことは、ISMS 認証基準では以下のように説明しています。

この規格は，“Plan-Do-Check-Act（計画－実行－点検－処置）”（PDCA）モデルを採用し，これを ISMS プロセスすべての構築に適用する。図 1 は，ISMS が，利害関係者からの情報セキュリティ要求事項及び期待をインプットとしてどう取り入れ，必要となる活動及びプロセスを経て，その要求事項及び期待を満たした情報セキュリティの成果をどう生み出すかを表している。また，図 1 は，箇条 4，5，6，7 及び 8 に規定するプロセス間のつながりも表している。

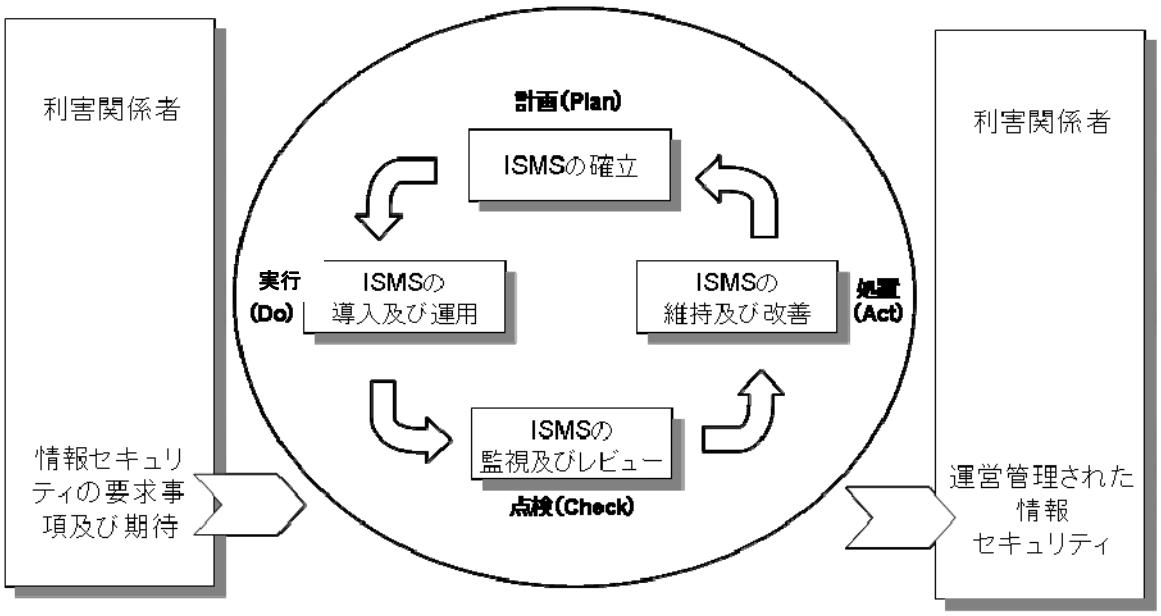


図1 ― ISMSプロセスに適用されるPDCAモデル

（JIS Q 27001:2006　0.2 ISMS の採用　0.2.2 プロセスアプローチ　より引用）

図 1-4 PDCA モデル

図 1-4 における利害関係者について、医療機関には多数の関係者が存在します。因みに、保険医療分野の公開鍵基盤の技術仕様書である ISO/TS 17090 には、ITU-T(国連の機関である国際電気通信連合の電気通信標準化部門)が定めた X.509(公開鍵証明書構造)の属性としての hcRole（helth care Role）で記述する資格として、医師、歯科医師、薬剤師、臨床検査技師、診療放射線技師、看護師、などが挙げられています。

「JIS Q 9000:2006」の定義を医療機関に当てはめると、「組織」とは各種形態の医療機関、

上記の資格者、その他の医療機関で働く人々と言えます。「顧客」とは言うまでも無く患者、患者団体および家族です。「供給者」とは、医療機関への物品、サービスの提供業者です。「利害関係者」とは前記全ての他に、医療機関の設立組織、保険者、薬局、資格者の団体、医療機関を監督する行政組織が含まれます。

これら関係者の情報への関与の仕方を明確にする事が重要です。

3.3.1　組織(organization)
責任、権限及び相互関係が取り決められている人々及び施設の集まり。
例　会社，法人，事務所，企業，団体，慈善団体，個人業者(sole trader)，協会，若しくはこれらの一部又は組合せ
注記 1　この取決めは，一般に秩序だっている。
注記 2　組織は，公的又は私的のいずれでもあり得る。
注記 3　この定義は，品質マネジメントシステム(JIS Q 9000：2006　3.2.3)規格の目的に対して有効なものである。ISO/IEC　Guide2 での用語“組織”の定義はこれとは異なる。

3.3.5　顧客(customer)
製品(JIS Q 9000：2006　3.4.2)を受け取る組織(JIS Q 9000：206　3.3.1)又は人。
例　消費者，依頼人，エンドユーザ，小売り業者，受益者及び購入者
注記　顧客は，組織の内部又は外部のいずれでもあり得る。

3.3.6　供給者(supplier)
製品(JIS Q 9000：2006　3.4.2)を提供する組織(JIS Q 9000：2006　3.3.1)又は人。
例　製品の生産者，卸売業者，小売り業者，納入業者，サービス提供者又は情報提供者
注記 1　供給者は，組織の内部又は外部のいずれでもあり得る。
注記 2　契約関係においては，供給者は“契約者”と呼ばれる。

3.3.7　利害関係者(interested party)
組織(JIS Q 9000：2006　3.3.1)のパフォーマンス及び成功に利害関係をもつ人又はグループ
例　顧客(JIS Q 9000：2006　3.3.5)，所有者，組織内の人々，供給者(JIS Q 9000：2006　3.3.6)，銀行家，組合，パートナ又は会社
注記　グループは，一つの組織，その一部又は複数の組織のこともある。

(JIS Q 9000:2006　3.3 組織に関する用語　より引用)

２．引用規格

ISMS 認証基準では、次の規格を引用規格として挙げています。ここでは、下記以外の規格も含めて情報セキュリティ及びマネジメントシステムについての規格を紹介します。

> 次に掲げる規格は，この規格に引用されることによって，この規格の規定の一部を構成する。これらの引用規格のうちで，西暦年を付記してあるものは，記載の年の版を適用し，その後の改正版（追補を含む。）には適用しない。
>
> JIS Q 27002:2006　情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範
>
> 注記　対応国際規格：ISO/IEC 17799:2005, Information technology－Security techniques－Code of practice for information security management (IDT)
>
> （JIS Q 27001:2006　2 引用規格　より引用）

２．１　JIS Q 27002

ISO/IEC 27002（ISO/IEC 17799）の制定発行に伴って、日本工業標準調査会(JISC)により日本工業標準(JIS)として制定された国内規格です。内容は、ISO/IEC 27002（ISO/IEC 17799）（※１）を忠実に日本語に翻訳し、国際規格との整合性が厳密に保たれたものとなっています。

※１　ISO/IEC 27002（ISO/IEC 17799）

情報セキュリティに対するマネジメントシステムの国際規格として、2000 年に ISO/IEC 17799 として制定発行されました。この規格は英国規格 BS 7799-1:1999（※２）を基にしており、実践のための規範をまとめたものです。現在使用されているのは、2005 年に改訂された版です。2007 年 7 月に規格番号が変更され、ISO/IEC 27002 となりました。

＜参考＞

ISO/IEC 27002 は、審査登録制度における認証基準ではありません。認証基準は、JIS Q 27001 です。

※２　BS 7799

1995 年に英国で制定発行された情報セキュリティに関する英国規格（British Standard）

で、情報セキュリティの技術的対策だけではなく、人及び組織の管理を含めたマネジメントに関する実践のための規範をまとめたものです。その後、1998 年に認証の基準となる第 2 部が制定されて 2 部構成になり、2006 年 3 月に第 3 部(Guidelines for information security risk management) が制定されました。なお、第 1 部と第 2 部は、BS ISO/IEC 17799:2005 及び BS ISO/IEC 27001:2005 に置き換わりました。

２．２　ISO 27799

ISO/IEC 27002 をベースに医療分野に特有の要件を規格化したものであり、2008 年発行の予定です。とりわけ医療情報に関する情報セキュリティマネジメントに有用な管理策を示すものです。

医療情報は、文字や数字以外にも、録音、画像、ビデオ、医学的なイメージなど多岐にわたります。また、それらが紙やフィルム、電子的に保存され、手渡し、FAX、ネットワーク、郵送などを介して伝達されています。ISO 27799 は、このような医療情報を適切に保護するために有用な管理策を体系化したものです。

２．３　JIS Q 9001

品質に関するマネジメントシステムの要求事項に関する規格で、第 1 版は 1994 年に制定されました。現在使用されているのは、2000 年に改訂された第 2 版です。なお、ISMS 認証基準は、第 2 版と整合性がとられています。

JIS Q 9000 シリーズには、JIS Q 9001 以外に品質マネジメントの基本及び用語をまとめた JIS Q 9000 と、パフォーマンス改善のための指針をまとめた JIS Q 9004 等があります。

２．４　TR Q 0008

2002 年に ISO/IEC Guide73 として制定されたリスクマネジメントの用語を日本語に翻訳した標準情報(TR)です。規格ではありませんが、リスクマネジメントの活動及び用語の使い方の標準として ISMS 認証基準でも採用しています。

> この標準情報は，リスクマネジメントの側面を含む規格の準備，又は改定の際に使用される上位の一般的文書である。
>
> この標準情報の意図は，リスクマネジメント活動の記述及びリスクマネジメント用語の使い方に対する，統一的な取組を促進することである。この標準情報は，リスクマネジメント実施のための手引書としてではなく，ISO 及び IEC のメンバー間の相互理解に貢献することを目的としている。
>
> （TR Q 0008:2003　1.適用範囲　より引用）

＜参考＞

国家規格(National Standards)について審議する日本工業標準調査会では、標準情報(TR)を以下のように説明しています。TR Q 0008 は「タイプ II」です。

TS／TR制度について

本制度は、先端技術分野等の技術進歩の早い分野において、日本工業規格（JIS）として制定するには熟度の低いものについて、迅速かつ適切に標準情報（TS及びTR)として開示することにより、オープンな議論を推進し、コンセンサスの形成を促し、JIS化の促進を図るためのものです。 この制度は、ISO(国際標準化機構）のTS制度及びTR制度と同じ趣旨の制度です。

1. 標準仕様書(TS)及び標準報告書(TR)の分類

① 標準仕様書(TS)　日本工業標準調査会の審議において、市場適合性が確認できない、又は技術的に開発途上にあるなど、JIS制定へのコンセンサスが得られなかったが、将来JIS制定の可能性があると判断され、公表される標準文書。標準仕様書(TS)は、次のとおり細分されます。

a) 標準仕様書(TS／タイプⅠ）

JIS制定への必要なコンセンサスが得られなかったが、将来、JIS制定への可能性がある標準文書。

b) 標準仕様書（TS／タイプⅡ）

技術的に開発途上にあるなど、現時点ではJIS制定が困難であるが、将来、JIS制定への可能性がある標準文書。

なお、標準仕様書（TS)は、発行後3年以内に見直しを行い、JISとするか、更に3年延長するか、又は廃止します。延長は、原則として1回限りとします。

② 標準報告書(TR)

JISとは異なる種類の標準に関連する情報類(標準化関連情報、データ集など）として、これ自体はJISにはならないものの、標準化の推進に資するものとして公表される標準文書。 なお、標準報告書(TR)は、原則として発行後5年をもって廃止します。

2. 標準仕様書(TS)及び標準報告書(TR)は、団体、企業等だれでも提案することができます。

提案する場合は、原案とともに必要な書類を主務大臣に提出する必要があります。詳しくは「標準仕様書（TS）／標準報告書（TR）原案の提案について」をご覧ください。なお、提案者は、提案した標準仕様書(TS)及び標準報告書(TR)に対する意見・質問に対応する責務を負います。

3. 標準仕様書(TS)及び標準報告書(TR)の公表

標準仕様書（TS）及び標準報告書（TR）は、JISC ﾎｰﾑﾍﾟｰｼﾞにおいて閲覧に供します。

（日本工業調査会 Web ページより引用　http://www.jisc.go.jp/jis-act/ts-tr.html　2008.2 現在）

２．５　その他の参考規格

①　TR X 0036-1 ～ -5 (GMITS)

「IT セキュリティマネジメントのガイドライン (Guidelines for the management of IT security)」と称し、ISO/IEC TR 13335 として国際化された標準情報です。このガイドラインでは、IT セキュリティの管理をどのように構築していくかをリスクマネジメントを含めて記述した解説書です。

1996 年から順次制定発行されて、以下の 5 部で構成されています。

- ■ 第 1 部：IT セキュリティの概念およびモデル
- ■ 第 2 部：IT セキュリティのマネジメント及び計画
- ■ 第 3 部：IT セキュリティマネジメントのための手法
- ■ 第 4 部：セーフガードの選択
- ■ 第 5 部：ネットワークセキュリティに関するマネジメントの手引

これらの規格は 2006 年に有効期限が切れ、現在、別の規格として発行または発行が予定されています。一方､本ガイドにとって有益な情報の改訂がまだなされていないこともあり、本ガイドでは旧標準情報からの内容を多く引用しています。

なお、これらの標準情報は改訂によって、次のような規格に一部が引き継がれています。

TR X 0036-1 (ISO/IEC TR 13335-1) ┐
TR X 0036-2 (ISO/IEC TR 13335-2) ┘→ JIS Q 13335-1 (ISO/IEC 13335-1)

TR X 0036-3 (ISO/IEC TR 13335-3) ┐
TR X 0036-4 (ISO/IEC TR 13335-4) ┘→ ISO/IEC 27005 (審議中)

TR X 0036-5 (ISO/IEC TR 13335-5) → ISO/IEC 18028-1

②　JIS Q 13335-1

上記 GMITS の第１部と第２部を統合し国際標準化した規格 ISO/IEC 13335-1(Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management) の国内規格です。用語の定義の多くは、この規格から引用しました。

３．用語及び定義

ISMS 認証基準では、新たに情報セキュリティやリスクマネジメントに関する用語が定義されました。

ISMS 認証基準の用語及び定義の表記順序は、英語表記のアルファベット順に掲載しています。そのため一見すると脈絡無く用語が並んでいるように見えますが、内容により以下の４つに大別して整理すると理解し易いと思います。

表 3-1　用語の分類

基本となる用語の定義	3.1 資産（asset）	
	3.5 情報セキュリティ事象（information security event）	
	3.6 情報セキュリティインシデント（information security incident）	
情報セキュリティに関する用語の定義	3.4 情報セキュリティ（information security）	
	3.3 機密性（confidentiality）	
	3.8 完全性（integrity）	
	3.2 可用性（availability）	
リスクマネジメントに関する用語の定義	3.14 リスクマネジメント（risk management）	
	3.12 リスクアセスメント（risk assessment）	3.11 リスク分析（risk analysis）
		参考　リスク因子（risk source）
		3.13 リスク評価（risk evaluation）
	3.15 リスク対応（risk treatment）	
	3.10 リスクの受容（risk acceptance）	
	3.9 残留リスク（residual risk）	
マネジメントシステムに関する用語の定義	3.7 情報セキュリティマネジメントシステム，ISMS（information security management system）	
	3.16 適用宣言書（statement of applicability）	

３．１　情報セキュリティとは

組織経営に不可欠である情報は、適切に保護されなければなりません。情報が適切に保護されていないと、漏洩したり、内容が不正確であったり、必要な時に使えない等、業務の遂行に支障をきたすといったリスクがあります。「情報セキュリティ」とは、重要な情報をこうしたリスクから守ることです。

ISMS 認証基準では、情報セキュリティを以下のように定義しています。

> 3.4　情報セキュリティ（information security）
> 情報の機密性，完全性及び可用性を維持すること。さらに，真正性，責任追跡性，否認防止及び信頼性のような特性を維持することを含めてもよい（JIS Q 27002:2006）。
> （JIS Q 27001:2006　3 用語及び定義　より引用）

情報セキュリティに関わるリスクを明確にするために、情報セキュリティの主たる 3 要素である「機密性」、「完全性」、「可用性」のそれぞれの観点から分析を行います。その他の 4 つの特性は、通常上記３つの要素から導くことができると考えられます。

> 3.1 資産（asset）
> 組織にとって価値をもつもの（JIS Q 13335-1:2006）。
> （ JIS Q 27001:2006　3 用語及び定義　より引用）

なお、「資産」の詳細については、JIS Q 27002 の箇条 7 に説明されており、情報は資産の一部として扱われることになります。本ガイドでは情報に関わる資産として 4.2.4 (1)②に例示をしていますので、参照して下さい。

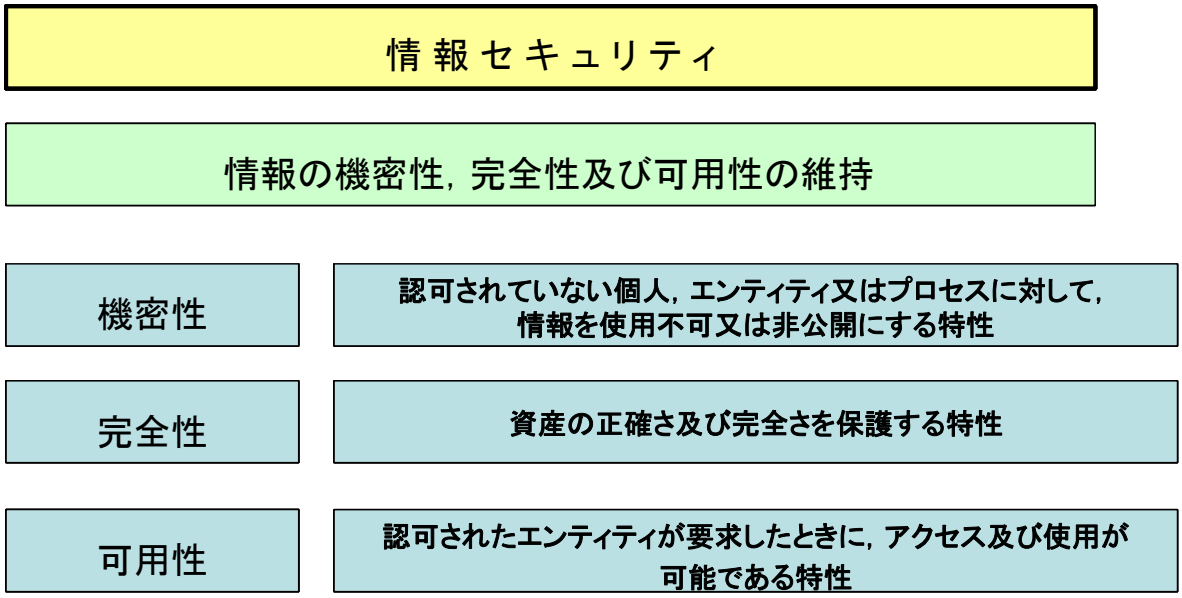


図 3-1　情報セキュリティの主な要素

「機密性」、「完全性」、「可用性」は、1992 年に発行された「OECD 情報セキュリティガイドラインに関する委員会勧告」[1]の附属文書「情報システムのセキュリティガイドライン」[2]（以下、「OECD ガイドライン」という。）において定義されて以来使われてきました。

> 情報システムの機密性、完全性及び可用性を阻害する危害（harm）から情報システムを保護すること
>
> （OECD ガイドライン:1992　より引用）

この 3 つの「～性」は、その頭文字をとって「情報セキュリティの C.I.A」と言われることがあります。

ISMS 認証基準では、機密性、完全性、可用性を以下のように定義しています。

> 3.3　機密性（confidentiality）
> 認可されていない個人，エンティティ又はプロセスに対して，情報を使用不可又は非公開にする特性（JIS Q 13335-1:2006）。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

[1] Recommendation of the Council concerning Guidelines for the Security of Information Systems(adopted by the Council at its 793rd Session of 26-27 November 1992)

[2] Guidelines for the Security of Information Systems,26 November 1992

情報の機密性は、「情報が漏洩しないようにする」ことにより確保されます。

> 3.8　完全性（integrity）
> 資産の正確さ及び完全さを保護する特性（JIS Q 13335-1:2006）。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

完全性には二つの意味があります。一つは情報そのものの完全性を確保することです。これは「情報が改ざんされないようにする」ことに関連します。

もう一つは情報処理の方法の完全性です。これは、「情報システムが勝手に変更されないようにする」ことや「情報の取扱いが手順化されていて、その手順が確実に遵守されるようにする」こと等に関連します。

> 3.2　可用性（availability）
> 認可されたエンティティが要求したときに，アクセス及び使用が可能である特性（JIS Q 13335-1:2006）。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

可用性は、「自然災害やシステムダウンなどにより、情報が使えなくなること」に関連します。

なお、その他の 4 つの特性については、JIS Q 13335-1:2006 に定義があり、以下のようになっています。

> **真正性**（authenticity）
> ある主体又は資源が，主張どおりであることを確実にする特性。真正性は，利用者，プロセス，システム，情報などのエンティティに対して適用する。
>
> **責任追跡性**（accountability）
> あるエンティティの動作が，その動作から動作主のエンティティまで一意に追跡できることを確実にする特性（**JIS X 5004**）。
>
> **否認防止**（non-repudiation）
> ある活動又は事象が起きたことを，後になって否認されないように証明する能力。
>
> **信頼性**（reliability）
> 意図した動作及び結果に一致する特性。
>
> （JIS Q 13335-1　2 用語及び定義　より引用）

３．２　リスクマネジメントとは

ISMS 認証基準では、リスクマネジメントについては以下のように定義しています。

> 3.14　リスクマネジメント（risk management）
> リスクに関して組織を指揮し管理する調整された活動（TR Q 0008:2003)。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

リスクは、「組織の活動の遂行を阻害する事象の発生の可能性」と定義しますが、標準情報（TR Q 0008:2003)「リスクマネジメント－用語－規格において使用するための指針」には以下のように定義しています。

> 3.1.1　リスク（risk）
> 事象（3.1.4）の発生確率（3.1.3）と事象の結果（3.1.2）の組合せ。
> 備考 1.　用語“リスク”は，一般に少なくとも好ましくない結果を得る可能性がある場合にだけ使われる。
> 2.　ある場合には，リスクは期待した成果，又は事象からの偏差の可能性から生じる。
> 3.　安全に関する事項に対しては，ISO/IEC Guide 51:1999 を参照のこと。
>
> （TR Q 0008:2003 3.用語及び定義　より引用）

> 3.4.10 リスクの受容（risk acceptance）
> リスク（3.1.1）を受容する意思決定。
> 備考 1.“受容する（accept)”という動詞は，名詞“受容（acceptance)”のもつ基礎的な辞書の意味を引き継いで選ばれている。
> 2. リスクの受容は，リスク基準に依存する。
>
> （TR Q 0008:2003　3.用語及び定義　より引用）

> 3.4.11 残留リスク（residual risk）
> リスク対応（3.4.1）の後に残っているリスク（3.1.1)。
> 備考　安全に関する適用の場合は，ISO/IEC Guide 51:1999 参照。
>
> （TR Q 0008:2003　3.用語及び定義　より引用）

リスクの特性は、上記リスクの「備考　2.」にあるように、結果そのものの「良い」、「悪

い」により規定されるものではなく、その期待値に対してどのような分布を持つかにより規定されます。また、リスクとはあくまで「可能性」のことを指します。

３．３　マネジメントシステムとは

ISMS 認証基準では、情報セキュリティマネジメントシステム（ISMS）については以下のように定義しています。

> 3.7　情報セキュリティマネジメントシステム，ISMS（information security management system）
> マネジメントシステム全体の中で，事業リスクに対する取組み方に基づいて，情報セキュリティの確立，導入，運用，監視，レビュー，維持及び改善を担う部分。
> 注記　マネジメントシステムには，組織の構造，方針，計画作成活動，責任，実践，手順，プロセス及び経営資源が含まれる。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

ISMS 認証基準では、適用宣言書については以下のように定義しています。

> 3.16　適用宣言書（statement of applicability）
> その組織の ISMS に関連して適用する管理目的及び管理策を記述した文書。
> 注記　管理目的及び管理策は，組織の情報セキュリティに対する，次のものに基づく。
> ― リスクアセスメント及びリスク対応のプロセスの結果及び結論
> ― 法令又は規制の要求事項
> ― 契約上の義務
> ― 事業上の要求事項
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

３．４　情報セキュリティ事象・情報セキュリティインシデントについて

JIS Q 27002:2006 への改正にともなって、「13　情報セキュリティインシデントの管理」がひとつの箇条としてまとめられました。これに伴って、表 3-1 のように関連した用語の定義が追加されました。

3.5 情報セキュリティ事象（information security event）
システム，サービス又はネットワークにおける特定の状態の発生。特定の状態とは，情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性，又はセキュリティに関連するかもしれない未知の状況を示しているものをいう（ISO/IEC TR 18044:2004）。

3.6 情報セキュリティインシデント（information security incident）
望まない単独若しくは一連の情報セキュリティ事象，又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの（ISO/IEC TR 18044:2004）。

（JIS Q 27001:2006　3 用語及び定義　より引用）

詳細は、「JIS Q 27002:2006　13　情報セキュリティインシデントの管理」や「ISO/IEC TR 18044:2004 Information Security Incident Management」を参照して下さい。

参考：「ISO/IEC TR 18044 Information Security Incident Management（情報セキュリティインシデントの管理）」の概要

JTC1/SC27 では、情報セキュリティインシデントの管理に関して ISO/IEC TR 18044 という技術報告書（Technical Report）を発表しています。
この技術報告書は、以下のような点から助言及び指針を与えています。

組織は、情報セキュリティインシデントへの対応手順や迅速に対応できる体制を整備しなければなりません。しかしながら、たとえ体制を確立したとしても、現場の当事者が多くの情報セキュリティ事象の中から情報セキュリティインシデントを検出するのが遅れると、結果的に対応が遅れてしまいます。したがって、情報セキュリティインシデントと認識された以後のことばかりではなく、それ以前の情報セキュリティ事象にも広く注意をする必要があります。つまり、情報セキュリティインシデントとなる可能性や未知の状況を示す「情報セキュリティ事象」が、事業運営を危うくしたり情報セキュリティを脅かしたりする確率を高め、結果として情報セキュリティインシデントに変遷する可能性に留意する必要があります。そのため、情報セキュリティインシデントの管理では、情報セキュリティインシデントとして検出される前の情報セキュリティ事象を対象とする管理策も講じなければなりません。

それらについて以下の流れで示しています。
・情報セキュリティインシデントの検出、報告及び査定

・影響の予防及び低減、並びに、影響からの回復のための適切な管理策の活性化（activation）を含んだ、情報セキュリティインシデントへの対応
・情報セキュリティインシデントからの学習及び予防的管理策の探求、情報セキュリティインシデントマネジメントの総合的な取り組みに対する四六時中の改善

また、これらを確立するために PDCA モデルに似た以下のようなプロセスモデルを適用しています。

・計画準備段階
・利用段階
・レビュー段階
・改善段階

このようなプロセスモデルを適用し、計画準備段階において事前計画に基づく対応手順を充実させた上で、実際の情報セキュリティインシデント発生時に、手順に従って対応することを基本にしています。しかし、その一方で、計画準備段階に用意した手順が情報セキュリティインシデントの実情に沿わないときには、定められた手順以外の対応をするための手続きが必要であることも指摘しています。なぜなら、情報セキュリティインシデントにおいては、予測不可能な状況となることもあり、その場合には、事前計画で想定した範囲内だけで事後対応を実施することは、むしろ想定外の状況に柔軟に対応できなくなる場合があります。そのため、想定外の状況に遭遇した場合には、担当者の判断で、事前に定められた処置とは異なる例外処置をとれるようにすることも必要です。この技術報告書は、そのような例外処置に関する管理策を講じることについても述べています。

４．情報セキュリティマネジメントシステム

４．０　医療情報セキュリティの重要性とセキュリティマネジメントの必要性

（１）何故、医療情報セキュリティが必要なのか

医療分野においては、古くから医療安全のためのアプローチが行われてきました。医療事故防止を組織的に実施するためにリスクマネージャを筆頭とした医療安全対策チームが編成され、ヒヤリ・ハット事例の分析などを積極的に行ってきました。これにより、診療プロセスが継続的に改善され、より安心できる医療が実現されてきています。しかしながら、情報機器の誤った、あるいは不適切な管理・使用による、情報漏えい事故も発生していることが報告されている状況でもあります。また、医療現場の IT 化が推進されるにつれ、情報システムが医療機関の業務運用において重要な位置を占めるようになってきています。情報システムの停止が医療行為に大きな影響を与えるようになり、その対策も必要になってきています。今日、情報セキュリティを維持することは医療機関の管理者にとって重要な経営目標となりつつあります。

情報セキュリティが維持できない場合、以下のようなデメリットが発生します。これらのデメリットに対する対応を行うためにセキュリティマネジメントが重要になっています。

情報セキュリティが維持できない場合のデメリット

・医療サービスの低下と利益の喪失	システム停止による医療行為への影響や診療報酬の喪失
・信用・ブランドイメージの低下	医療機関としての信頼や患者の喪失
・復旧コストの発生	システムを復旧するための時間と労力がコストとして発生
・訴訟・賠償請求	個人情報やその他情報が漏洩した場合にその被害者から訴訟を提起され損害賠償責任を負う可能性
・法的責任	医師法、医療法や個人情報保護法による罰則規定

（２）医療情報セキュリティの目標

情報セキュリティマネジメントを実施する際に重要なのは、「何のために情報セキュリティマネジメントを実施するのか」を明確にすることです。医療情報セキュリティの目標を明確に定義し、その目標達成のためのマネジメントを実践することが重要となります。特に重要と思われる目標の例を以下に示します。

（１）個人情報の保護

診療情報は個人情報のなかでも特に重要な情報であり、診療情報の漏洩が本人の人生を大きく左右することも考えられます。医療機関は取り扱う情報の重要性を認識し、適切に管理しなければなりません。

特に重要な対策（管理策）例としては以下のようなものが挙げられます。

診療情報の保護：

個人情報保護の観点から診療情報の機密性の維持を行うこと

（２）医療事故防止

診療情報の完全性が維持されない場合、誤った情報に基づく診療が実施される恐れがあります。医療機関は、医療事故防止の観点から診療情報の完全性の維持に努めなければなりません。

特に重要な対策（管理策）例としては以下のようなものが挙げられます。

診療情報の完全性の維持：

適切な診療を行う観点から診療情報の完全性の維持を行うこと

（３）病院機能の維持（診療の継続）

医療機関は大きな災害が発生したとき程、その役割が増大します。社会インフラが多大なダメージを受けても速やかに機能回復し、継続して診療を行えるようにする必要があります。また、悪意を持った攻撃に対する適切な防御手段を用意し、サイバーテロなどに対処できるようにしなければなりません。

特に重要な対策（管理策）例としては以下のようなものが挙げられます。

情報システムの可用性の維持：

医療機関としての機能維持のために情報システムの可用性の維持を行うこと

厚生労働省発行の「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(2007.3)」から、災害等の対策としての BCP(事業継続計画)に情報システムを含めて策定することを求めています。

（３）情報セキュリティと情報セキュリティマネジメント

IT の発展速度は極めて速いため、ある時に講じた最高の情報セキュリティ対策が、将来にわたっても最高のものとして永続することは一般的には期待できません。その時々のハードウェア、ソフトウェアの導入は、導入時には適切な対策となっているかもしれませんが、継続性は保証されていません。情報セキュリティ対策は、ある瞬間に考えられるリスクに対応した対策を策定することによって完結する一過性の取り組みではなく、情報セキュリティ基本方針の策定、及びそれに続く日々の継続的な取り組みによって確保される性質のものであることを十分に認識することが大切です。

また、情報セキュリティ基本方針の中には、継続的な情報収集及びセキュリティ確保の体制を構築しておくこと、また「いかに破られないか」のみならず、「破られたときどうするか」についての対策も適切に規定し、当該規定に基づいた対策を十分に構築しておくことが重要です。

さらには、情報セキュリティ基本方針、及び情報セキュリティ基本方針に関連する実施手順等の規定類を定期的に見直すことによって、所有する資産に対して新たな脅威が発生していないか、環境の変化はないかを確認し、継続的に対策を講じていくことが必要です。特に、情報セキュリティの分野では、技術の進歩や不正アクセスの手口の巧妙化に鑑み、早いサイクルで見直しを行っていくことが重要です。

（４）情報セキュリティを確保するために守るべきもの

情報セキュリティを確保するには、医療機関が保有する資産を様々な脅威から守らなければなりません（脅威の詳細については後述）。一般的な医療機関が保有する資産の例としては、以下のものが挙げられます。

資産の種類	例示
情報	コンピュータシステム内の患者情報、診療情報など 紙カルテ、依頼伝票、紹介状などに記載された患者情報など
ソフトウェア資産	業務アプリケーション、システムプログラムなど
物理的資産	コンピュータ装置：コンピュータ、プリンタなど 記憶媒体：MO、磁気テープなど 通信設備：ネットワーク、電話、通信回線など 電気設備：電源ケーブル、発電機、CVCF など
サービス	環境：マシンルーム、建物全体、耐震災設備など
人（知識）	知識としての診療情報、業務ノウハウ、パスワードなど
	保有する資格、技能、経験
無形資産	例えば、組織の評判、イメージ

これら資産を管理するために資産分類を実施し、資産の整理を行った上で管理を実施する必要があります。資産分類の例としては JIS Q 27002:2006「７．資産の管理」が参考になりますが、上記の表ではこの分類に加え、人（知識）を入れています。資産の性格上、人の知識を「情報」のカテゴリに入れることも可能ですが、他の情報と管理手法が異なるためここではあえて別の分類にしています。

（５）医療情報セキュリティにおける脅威およびぜい弱性

（１）脅威とは

リスクが発生する要因のことを脅威といいます。脅威とは、より厳密に言えば、「資産や組織に損失や損害をもたらす不測の事態の潜在的な要因」のことです。

脅威は以下のように分類されます。

脅威			
偶発的脅威		意図的脅威	環境的脅威
過失	故障	故意	災害
データ入力誤り 運用誤り 誤接続 その他	H/S 障害 S/W 障害 回線障害 その他	情報の盗用、改ざん なりすまし、不法侵入 ウィルス、サイバーテロ 物理的破壊、その他	地震 火災 水害 その他

これらの脅威はあくまで「不測の事態の潜在的な要因」であり、脅威があるだけでは問題とはなりません。これら脅威を顕在化し、具体的な損害を与える要因があって初めて脅威は問題となります。

（２）ぜい弱性とは

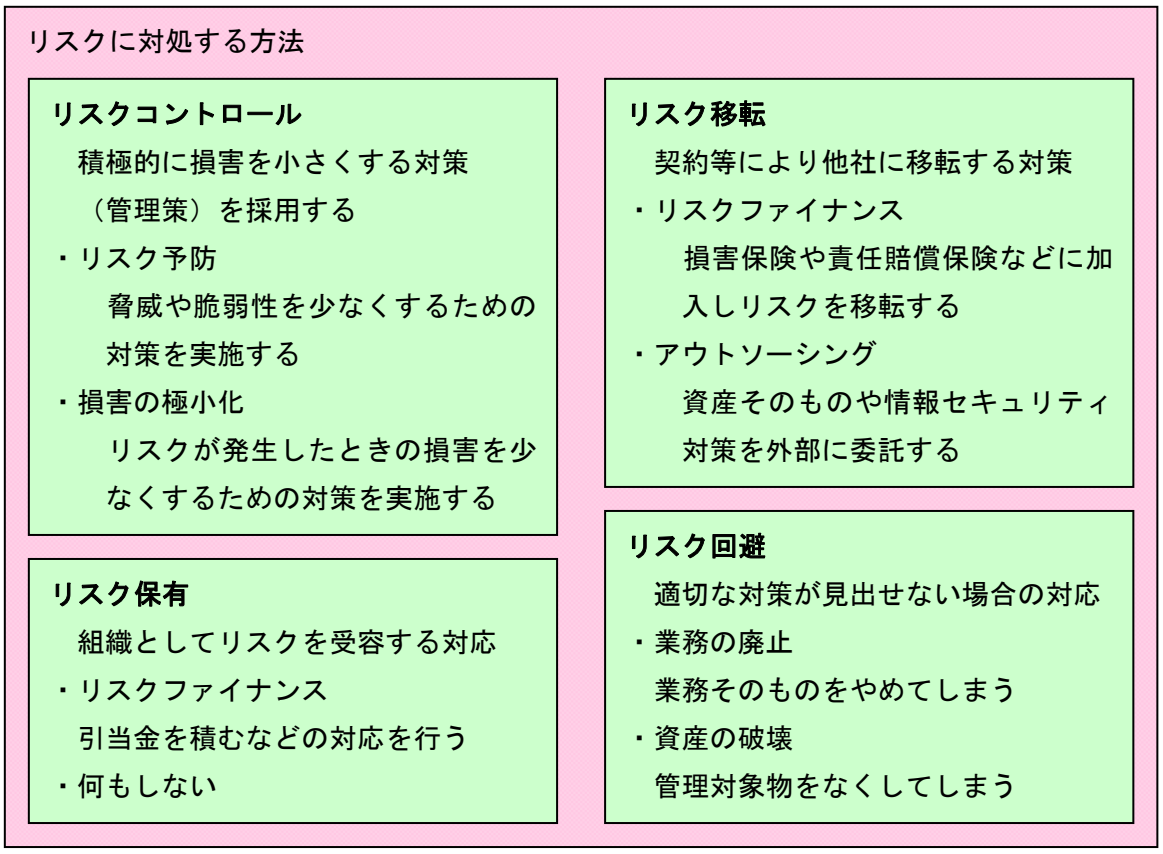
脅威を顕在化する資産が保有する弱点のことを「ぜい弱性」といいます。

ぜい弱性の例	
環境	ドアや窓、電源供給、災害を受けやすい立地など
ハードウェア	駆動部分の経年劣化、バックアップ回路の不備など
ソフトウェア	仕様書の欠如、アクセス制御の不備、プログラムのバグなど
ネットワーク	非暗号化、通信経路の保護の不備、バックアップ回線の不備など
組織	教育プログラムの不備、部外者の管理の不徹底など
個人	スキル不足、低いモラル、誤った理解など
マネジメント	予算不足、情報セキュリティマネジメント意識の欠如など

ぜい弱性はその存在自体が障害となるわけではありません。脅威とぜい弱性が組み合わせられることでリスクの顕在化につながります。

（６）医療情報セキュリティとリスクマネジメント

リスクに対処する方法はいくつかあるが以下のように分類できます。



通常のリスクマネジメントにおいては、これらのどれか一つを選択するということではなく、リスクの重要度や対策の容易性などから総合的に判断し、これらの対策を組み合わせて実施します。この中で、一般的に情報セキュリティ対策として認識されているのは「リスクコントロール」の中の「リスク予防」です。リスク予防はリスクが発生しないようにする予防的な対策であるため、金銭的に補償することが難しいリスクに対して特に有効です。たとえば、クレジットカードの偽造などには保険で対応することは難しくないが、個人情報の大量漏洩（特に医療情報）に対して保険だけでカバーすることは困難です。仮に保険に入るとしても、保険会社は何も予防的対策を施していない医療機関とは契約しないか、もしくは非常に高い料率での契約となるでしょう。医療機関の管理者にとっては費用対効果を念頭に置いた上で最も有効な対策の組合せを検討することも重要なリスクマネジメントの要素です。

（7）4.0章のまとめ

医療情報に対するセキュリティの重要性と情報セキュリティ確保のために情報セキュリティマネジメントシステム(ISMS)が重要であることを述べました。これらを理解した上で、適切な情報セキュリティマネジメントを実施するための方法論を導入することは有用です。医療分野における ISO では ISO/TC 215 において ISO/IEC 27002 の医療版として医療における特殊性を考慮した規格の策定が進んでいます。これら国際標準の方法論を活用し、適切なマネジメントを行っていくことが第三者から正当に評価を受けるために重要といえます。

４．１　ISMS の確立と運用管理（医療機関における情報セキュリティマネジメントシステム（ISMS）の実践）

前章までで ISMS の一般的な解説を行ってきました。本節では医療機関において ISMS を構築するための手順とポイントについて解説していきます。

（１）医療の安全管理の流れと ISMS 構築手順の関係

ヒヤリ・ハットに代表される医療における安全管理も ISMS と同様に PDCA サイクルによって仕組みが出来上がり、それを継続的に改善することでより安全な仕組みになっていきます。しかし、両者は「P（Plan）」の部分で少し違いがあります。図 4-1 に示す医療の安全管理の流れを確認しながら違いを見てみます。

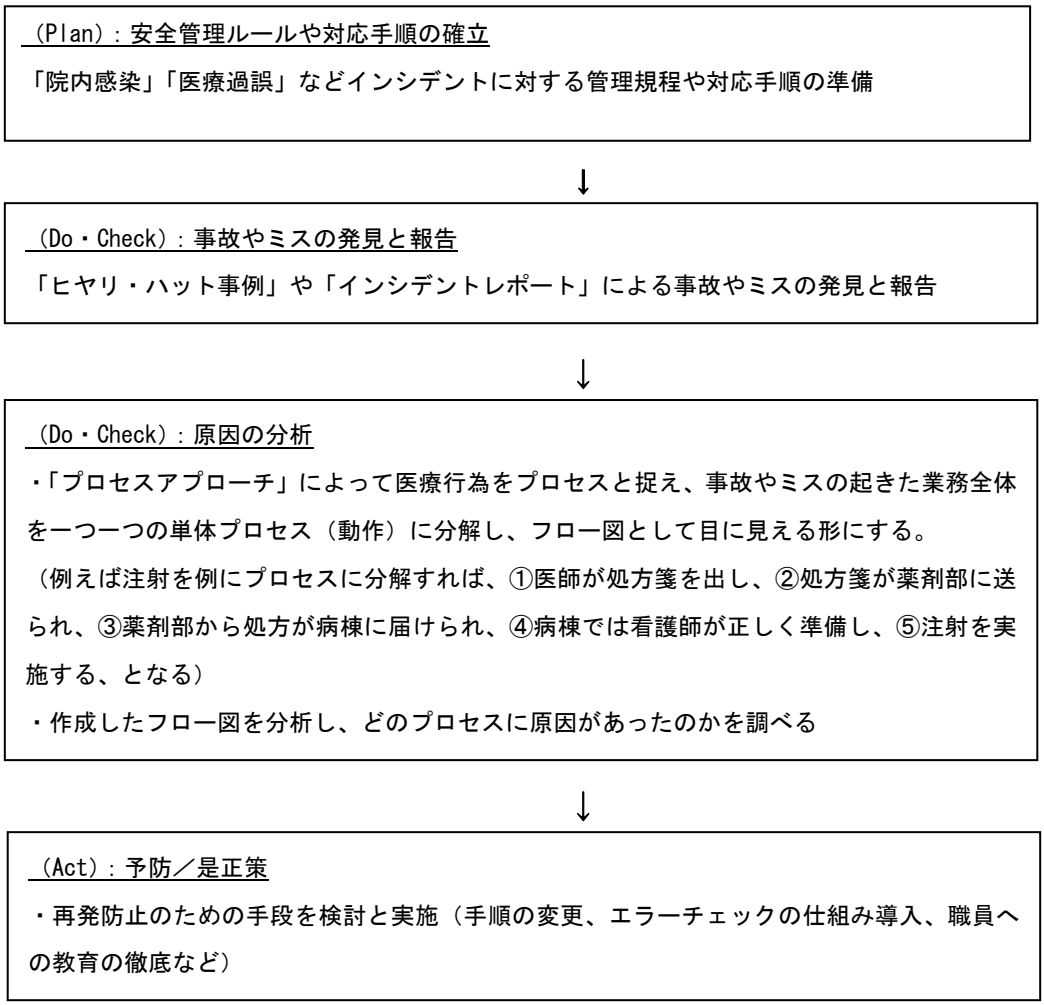


図 4-1　医療の安全管理の流れ

医療における安全管理ではＰで管理規程や対応手順を準備し、日々の運用ではＤ→Ｃ→Ａを繰り返すことが中心になります。これは医療分野では診察、診断、治療、看護などの管理規程や対応手順は過去からの蓄積によってすでに確立されており、事故やミスを発見したときにその手順を分析し、問題箇所の是正と再発防止を周知徹底すればリスクが減り、安全が高まる仕組みが出来上がっているためです。

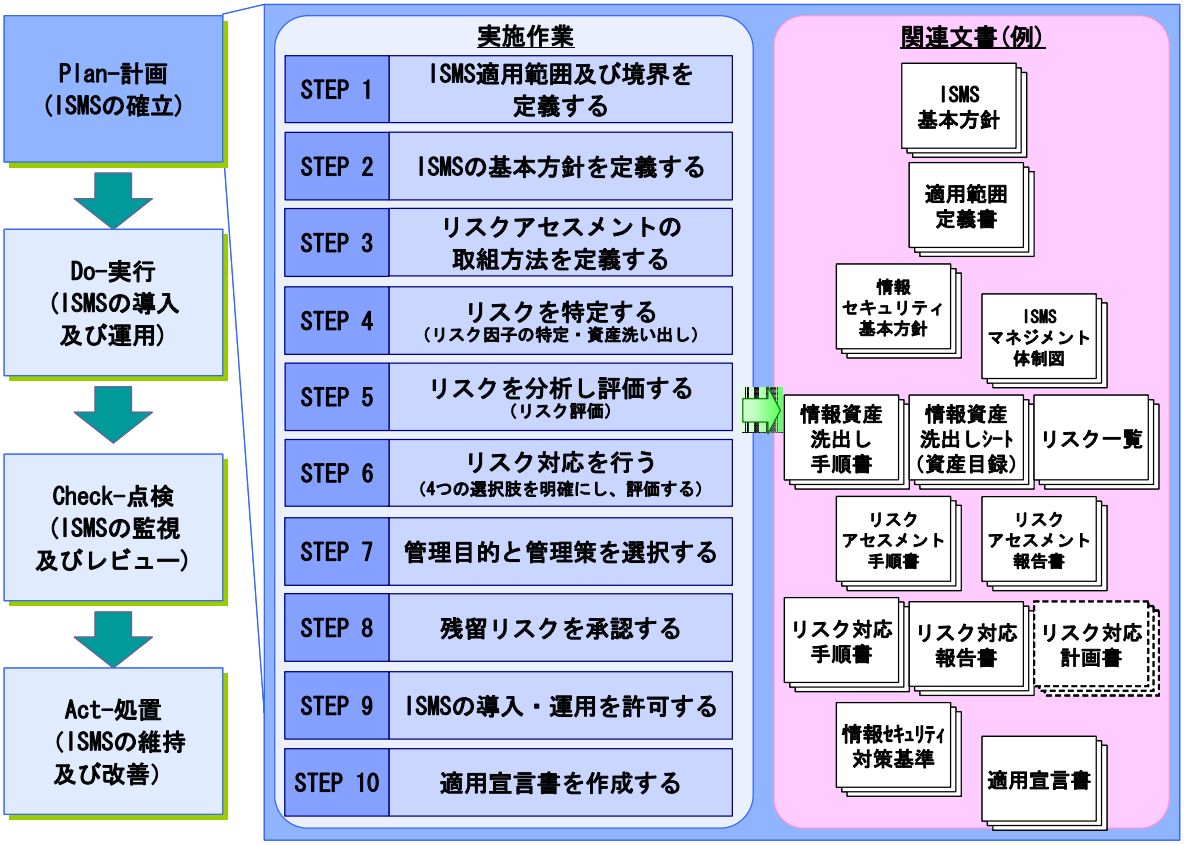
これに対し、情報セキュリティでは IT 技術の著しい発展により、過去の経験の蓄積だけでは想定できない新たなセキュリティ上の問題点（脅威）や弱点（ぜい弱性）が常に存在します。そのため ISMS 構築ではＰでセキュリティ上の問題点（脅威）や弱点（ぜい弱性）が発生する範囲を定め、リスク分析や対策検討を行います。その結果を基に運用管理規程や対応手順を準備し、Ｄ以降を実践します。

しかしＤ→Ｃ→Ａを繰り返すだけでは最新の技術を駆使したセキュリティインシデントには対応できないため、定期的にリスク分析や対策の再検討を行いＰの有効性を確認します。

従い、ISMS 構築では医療の安全管理の仕組みと比べて、Ｐの部分がより重要であり、Ｐの実施具合によって、Ｄ→Ｃ→Ａが有効に機能するかどうかが決まってきます。

４．２　ISMS の確立（Plan-計画）

ISMS 認証基準の「4.2　ISMS の確立及び運営管理」では、Plan-計画（ISMS の確立）の手順を図 4-2 に示す 10 のステップ（STEP 1～STEP 10）で規定しています。



注）文書名は全て例示

図 4-2　Plan-計画（ISMS の確立）の手順

以下、１０のステップについて説明していきます。

４．２．１　STEP1 ISMS 適用範囲及び境界を定義する

ISMS の構築を検討する際、まず始めに適用範囲を検討します。

> a) 事業・組織・所在地・資産・技術の特徴の見地から，ISMS の適用範囲及び境界を定義する。この定義には，適用範囲からの除外について，その詳細及びそれが正当である理由も含めるものとする（1.2 参照）。
>
> （JIS Q 27001:2006　4.2.1 ISMS の確立　より引用）

組織として真に効果的なマネジメントシステムを構築するためには、重要な資産の取り扱いが適正に保たれるために必要な範囲を 1 つの組織体として、ISMS の適用範囲を決定します。

医療分野においては医療施設（病院、診療所、介護センターなど）を 1 つのマネジメントシステムとして適用範囲とすることも可能ですし、1 部門（外来部門、病棟診療部門、薬局、検査センターなど）を適用範囲にすることもできます。

適用範囲を決定する上で重要なことは、1 つのマネジメントとして網羅的であること、及び適用範囲の境界線が明確で、合理的に説明可能であることです。

ISMS 認証基準では、適用範囲を決定するにあたり、以下のようないくつかの観点から検討し、合理的に決定することを要求しています。

- 事業
- 組織
- 所在地
- 資産
- 技術

適用範囲の定義の内容により､今後実施する ISMS 構築の作業負荷が大きく影響されます。

また、資産の洗い出しやリスクアセスメントなどの作業のみならず、管理策の適用や運用管理など適用対象の情報セキュリティ水準を維持する活動全般に影響します。

適用する範囲を決定した後で､その範囲を定義した文書を作成します｡範囲とその決定経緯を明確にし､文書に残しておくことで範囲の変更や範囲に含めるか否かの判断基準が明確になります。

（1）適用範囲を定義する文書

適用範囲を定義する文書に含むことが望ましい事項として、以下のような項目があげられます。

- ISMS の適用範囲及び内容を確立するために用いたプロセス
- 戦略上及び組織上の情況
- 組織で採用した情報セキュリティのリスクマネジメントのアプローチ
- 情報セキュリティのリスク評価の基準及び要求される保証の程度
- ISMS の適用範囲の中にある資産の特定

これらの事項は、必ずしもその全てが文書化される必要はありません。適用範囲を定義する際に考慮すべきポイントとして理解して下さい。適用範囲の定義に関する文書は、決定後も ISMS の構築作業の過程において常に見直されるべきものです。

（２）適用範囲の定義の作業

ISMS 認証基準に求められる適用範囲の定義に関する事項をまとめると図 4-3 の様になります。

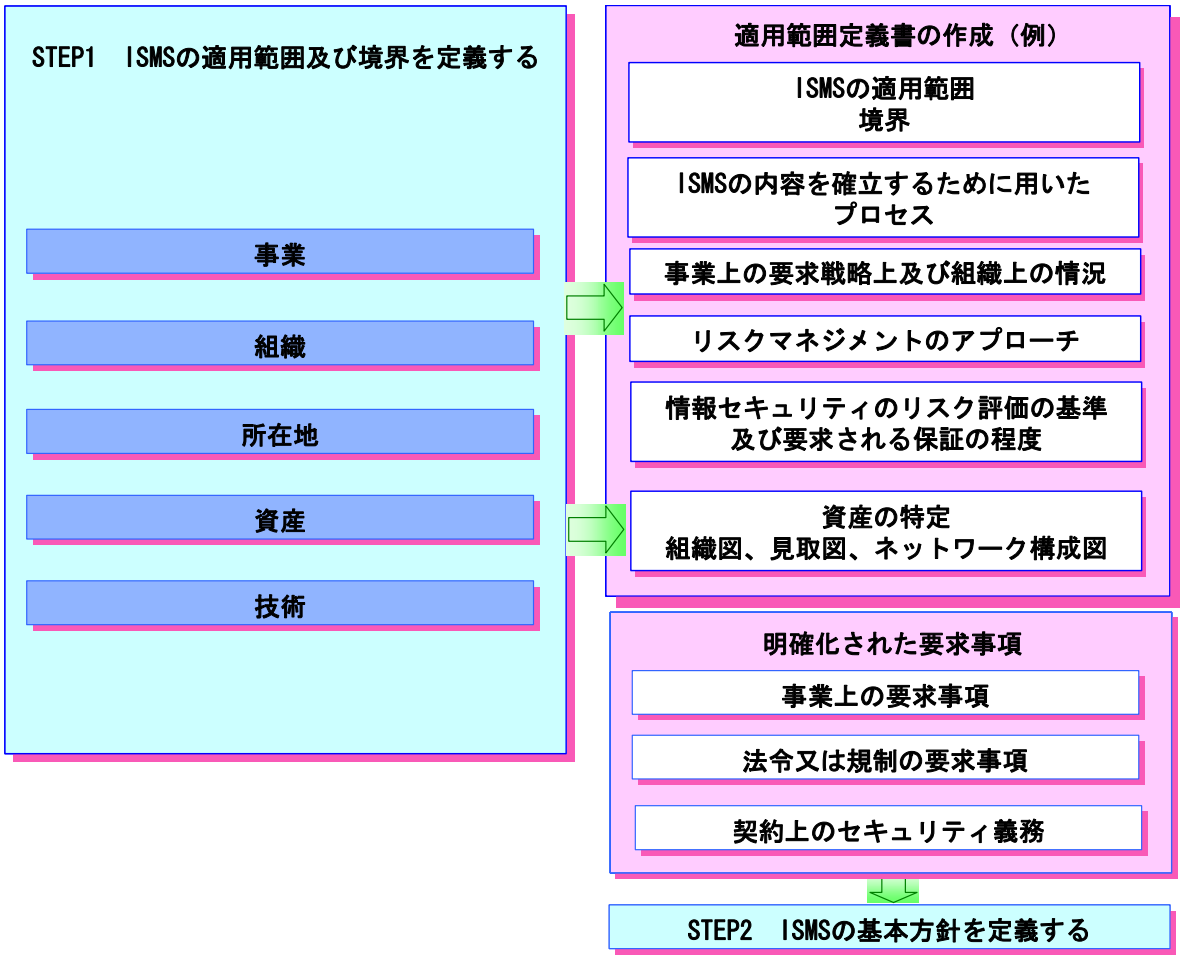


図 4-3　ISMS の適用範囲の定義

適用範囲を定義し、該当するマネジメントシステムを検討することによって、同時に情報セキュリティ上の要求事項も明確になります。特に、次の「ISMS の基本方針の定義」ステップで実施する作業に活用するために、以下の 3 つの要求事項については、特に明確化することに留意して下さい。

- 事業上の要求事項
- 法令又は規制の要求事項
- 契約上のセキュリティ義務

医療機関においては、診療情報として入力した情報を使って診療報酬請求や検体検査（外部検査機関への委託）を行ったり、研修医などその医療法人に属していない第三者がその情報に触れる機会もあるため、適用範囲について注意する必要があります。

例えばオーダリングや医事会計システムは患者基本情報の共有やオーダ実施(オーダリング）→診療請求（医事会計）と連動しており、部門を適用範囲とする場合にはどの部門でどの情報が入力・参照・出力されているかしっかり把握することが大切です。

４．２．２　STEP2 ISMS の基本方針を定義する

ISMS の基本方針は、組織の情報セキュリティマネジメントに対する基本的な考え方を示したものです。同時に、組織として情報セキュリティに関する要求事項に対して責任を負うという意思表示の位置付けとして重要な文書です。その内容は、医療法人、事業所としての使命、目的を表明した経営方針（ビジョン）や行動規範（価値観）と整合性がとられている必要があります。従って、この ISMS 基本方針には従業員の行動を規範するために情報セキュリティに関する全般的な方向性及び行動指針に関する内容が明記される必要があります。換言すると、ISMS 基本方針は、情報セキュリティ基本方針を包含する上位概念であるということがいえます。ただし、これらの方針（ISMS 基本方針、情報セキュリティ基本方針）を物理的にひとつの文書に記載することも可能です。

ISMS 基本方針の策定手順とポイントは表 4-1 のようになります。

表 4-1　ISMS 基本方針の策定手順のポイント

	ポイント	要求事項
(1)	ISMS 基本方針の確立	1) 情報セキュリティに関係する活動の方向性の全般的認識及び原則を確立する。
(2)	ISMS 構築のための組織体制	2) 事業上及び法令又は規制の要求事項、並びに契約上のセキュリティ義務を考慮する。 3) 組織の戦略的なリスクマネジメントの状況と調和をとる。 4) リスクを評価するための基軸を確立する。
(3)	経営陣の承認	5) 経営陣による承認を得る。

次頁以降、(1)～(3)について説明します。

（１）ISMS 基本方針の確立

JIS Q 27002:2006 の「5.1.1　情報セキュリティ基本方針文書」には、基本方針に含まれる事が望ましい内容が以下の様に規定されていますので参考にして下さい。

実施の手引

情報セキュリティ基本方針文書では，経営陣の責任を明記し，情報セキュリティの管理に対する組織の取組み方を示すことが望ましい。この情報セキュリティ基本方針文書には，次の事項に関する記述を含むことが望ましい。

a）情報セキュリティの定義，その目的及び適用範囲，並びに情報共有を可能にする基盤としてのセキュリティの重要性（0.2 参照）

b）事業戦略及び事業目的に沿った情報セキュリティの目標及び原則を支持する経営陣の意向の記述

c）リスクアセスメント及びリスクマネジメントの構造を含む，管理目的及び管理策を設定するための枠組み

d）組織にとって特に重要な，セキュリティの個別方針，原則，標準類及び順守の要求事項の簡潔な説明。これらには，次のようなものがある。

1）法令，規制及び契約上の要求事項の順守

2）セキュリティ教育，訓練及び意識向上に関する要求事項

3）事業継続管理

4）情報セキュリティ基本方針違反に対する処置

e）情報セキュリティインシデントを報告することも含め，情報セキュリティマネジメントに関する一般的な責任及び特定の責任の定義

f）情報セキュリティ基本方針を支持する文書（例えば，特定の情報システムのためのより詳細なセキュリティ方針及び手順，又は利用者が順守することが望ましいセキュリティ規則）への参照

この情報セキュリティ基本方針は，想定する読者にとって，適切で，利用可能で，かつ，理解しやすい形で，組織全体にわたって利用者に知らせることが望ましい。

（JIS Q 27002：2006　5.1.1 情報セキュリティ基本方針文書　より引用）

これらの事項も例示であり、必ずしもその全てが策定する基本方針に含まれる必要はありません。前のステップで定義した適用範囲により内容が変わることも想定されます。

JIS Q 27002:2006 で規定された内容は、基本方針の内容を検討する際に考慮すべきポイントとして理解して下さい。

一般的には ISMS 基本方針は事業の代表者（社長、情報統括役員など）が策定して従業員に周知徹底させますが、医療機関では院長（診療所であれば所長など）が策定し、従業員に周知徹底させることになります。

院内の基本方針は、書面等で文書化するのはもちろん、医療機関を受診する患者にも医療機関の受付や診察室に掲示するなどしてその内容を知れるようにしておくことが望ましいことです。

（２）ISMS 構築のための組織体制

「2) 事業上及び法令又は規制の要求事項、並びに契約上のセキュリティ義務を考慮する。」また「3) 組織の戦略的なリスクマネジメントの状況と調和をとる。」、「4)リスクを評価するための基軸を確立する。」とは ISMS の構築を担当する組織に求められる機能に関する要求事項です。

ISMS を構築する組織の人選においては、様々な情報の取り扱いに関する問題を討議するのに必要かつ十分な範囲から人を召集すると同時に、実際の ISMS 運用の体制についても考慮し、関連部門からも広くメンバーを募るべきです。

ISMS で取扱う情報セキュリティとは、単に「情報リスク」、「IT リスク」を考慮することにとどまりません。また、マネジメントシステムの局面も、日常の管理に属する部分の他、リスクが顕在化した後の被害を最小限にとどめるための対応なども要求されています。このような網羅的な「管理」を実現するためには、認証取得範囲に含まれる現場組織だけではなく、医事・会計部門、資材部門など医療機関組織全体を横断する人材の登用が求められます。

図 4-4 は、「ISMS ユーザーズガイド」に紹介された ISMS 構築のための組織体制の一例です。この例を基に、主要な組織の役割と責任を紹介します。

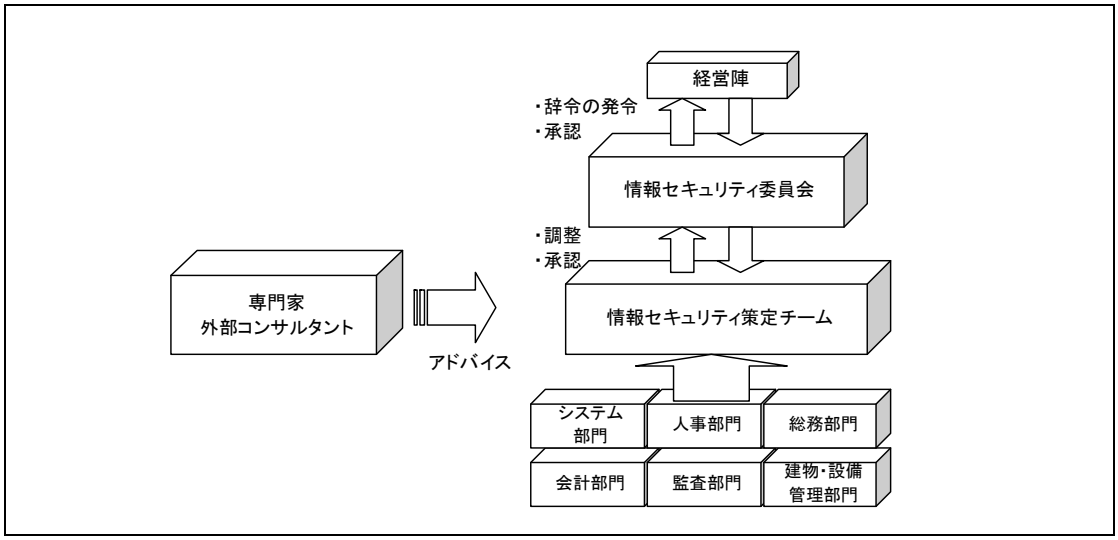


図 4-4　ISMS 構築のための組織体制

表 4-2　医療向け ISMS 構築のための組織体制例

経営陣	院長、理事会（理事長、専務理事・常務理事等）
情報セキュリティ委員会	医療安全管理委員会と兼務でも可 委員長　：副院長 副委員長：医療安全管理者、電算室長（または情報企画部門長） 委員　　：診療部長又は医長、薬剤部長又は薬剤科長、看護部長（又は総看護師長）、事務部長又は事務長、医療安全管理者、電算室長（又は情報企画部門長）
情報セキュリティ策定チーム	電算室情報管理部員、医療安全管理員、経営企画室員
部門：	診療部門、看護部門、臨床検査部門、病理診断部門、放射線部門、薬剤部門、地域連携室、輸血血液部門、手術・麻酔部門、救急部門、栄養部門、リハビリテーション部門、訪問サービス部門、医事・会計部門、人事部門、購買（用度）部門

表 4-2 の組織体制例は、ベッド数 500 床以上の大規模病院をベースにしています。中小規模の医療機関については各部門から構成しなくても、横断的に管理している組織・職員の方などで構成するなど、柔軟に対応することが可能と思われます。

①　情報セキュリティ委員会の役割

情報セキュリティ委員会を中心とした体制で策定される ISMS 関連文書は、委員会だけでなく組織の経営陣により承認された規程として必要に応じて関係者に周知し、定期的に見直

しを行います。

この委員会は、組織の保有する資産の取り扱いに責任を持ち、情報セキュリティの方向性を提言できるだけの情報セキュリティに関する理解と実行力をもった組織であるべきです。

情報セキュリティ委員会は、組織において ISMS の中心的役割を負います。以下は情報セキュリティ委員会の役割の例示です。

- **リスクマネジメントのための環境整備について検討機関となる**
- **ISMS 関連文書の策定時には内容について実質的な決定機関となる**
- **導入段階の ISMS を推進する各種施策や改訂を検討する**
- **運用段階でセキュリティ問題等が発生した場合の検討機関となる**
- **ISMS 運営の評価結果に基づいた改善について検討機関となる**

② 情報セキュリティ策定チームの役割

ISMS の構築実務を担当する策定チームは、適用範囲内の重要な資産について広く現状を把握し、その取り扱いを検討するのに十分な知見を持つメンバーで構成されるべきです。例えば、資産の取り扱い方法の決定に当り、適用範囲内の部署間での見解の相違や、利害関係の調整が必要になる場合があり、策定チームはそのような摩擦の調整役として、部門間の枠をこえて当事者に対してうまく働きかけることが求められます。この場合は、高いセキュリティ知識も当然必要ですが、調整能力や経験に基づくコミュニケーションのスキルも重要になります。

③ 専門家・外部コンサルタント

ISMS の構築作業は、組織が自前で（できれば専任の）要員を確保した上で進めるべきです。しかし、「情報セキュリティ」の対象とする範囲は「IT 技術」、「経営的な判断」や「ビジネスへの理解」など、求められる知識や経験は多岐にわたり、これらの領域をバランスよく俯瞰的に見通す力量が求められます。

組織の主要な業務はその業務に携わっている人が一番知っているものですが、時としてミクロな視点での判断に終始してしまうことがあります。基準に言及されている「外部の専門家・コンサルタントの登用」は、この判断にマクロな視点を与え、また最新の情報を提供してくれる窓口の機能が期待されます。情報セキュリティ委員会へのオブザーバ参加、規定文書のレビューや監査計画策定など、必要な局面で彼らの持つ専門知識を効果的に活用することも良いと思います。しかし、外部の専門家やコンサルタントはあくまでも ISMS の構築支援を行うものであり、当事者ではないので、意思決定を含めた丸投げは避けなければなりません。

また別の観点として、これらの人材は診療情報をはじめとする機密性の高い情報にふれることになるため、人を介した外部への情報漏洩も念頭におき、機密保持契約の締結や訴訟等での責任範囲を明確にする等、検討されることをお奨めします。

（３）経営陣の承認

経営陣には、「情報セキュリティ基本方針」を含む ISMS 基本方針、つまり情報セキュリティに対する組織のビジョンを示し、ISMS の活動に対する支援についてコミットメントすることが求められています。コミットするということは、単に出来上がった「情報セキュリティ基本方針書」に承認印を押す事でありません。詳細は、本ガイドの「5.1 経営陣のコミットメント」を参照して下さい。

「5)経営陣による承認を得る。」という要求事項では、ISMS の構築に対する経営陣のコミットメントの証拠として、情報セキュリティ基本方針の確立をあげています。また、ISMS について書かれた多くの書籍も「情報セキュリティ基本方針は経営陣が承認しなければならない」と明記しています。

情報セキュリティに対する組織の取り組み姿勢の定着に経営陣が積極的に関与し、その責任の下に継続的な改善を行うことにより、情報セキュリティは組織文化として定着します。

情報セキュリティについての意識が浸透している組織では、突発的な事態に対して要員が経営陣の意図する行動を自然に取ることが期待されます。これは、めまぐるしく変化する環境においては非常に重要なポイントです。

事業環境の変化の激しい組織における型にはまった手順書は、更新に時間がかかり、常に実業務との整合性を確保することに多大な労力を要することがあります。

そのような場合にも、情報セキュリティの意識を組織文化として浸透させる活動を実施すれば、規模が大きく業種や業態が多岐にわたる組織でも要員が等しく安全な行動をとるようになります。

４．２．３　STEP3 リスクアセスメントの取組み方法を定義する

前述までで、「ISMS を適用する範囲の定義」と「ISMS を確立するための基本方針の定義」を説明しました。STEP3 では ISMS 構築に必要なリスクアセスメントを実施する前の準備として、リスクアセスメント手順や判断基準を明確にする、ということを説明します。その上で「STEP4　リスクの特定」で資産とそのリスクを洗い出し、「STEP5　リスクを分析し評価する」で洗い出したリスクの大きさを分析し、「STEP6　リスク対応」で各リスクへの取るべ

き対策を決定する、という流れで進みます。内容は医療機関向けに簡単にわかり易く説明しています。

（１）リスクアセスメントとその必要性

リスクアセスメントとは、識別された資産に対するリスクを識別し、それらの大きさを手順に従い決定することです。

> 3.12 リスクアセスメント（risk assessment）
> リスク分析からリスク評価までのすべてのプロセス（TR Q 0008:2003）。
> （JIS Q 27001：2006　3 用語及び定義　より引用）

リスクアセスメントでは組織が保有する資産を対象に以下の事項を把握します。

- どのような脅威が存在するのか
- その脅威はどの程度発生する可能性があると考えるか
- 脅威が顕在化したときにどの程度の影響を受けるか

本ガイド「4.1（１）　医療の安全管理の流れと ISMS 構築手順の関係」で医療の安全管理の仕組みと照らし合わせたように ISMS の構築において、リスクを洗い出しその被害や影響の度合いを分析・評価して、しかるべき対策を立てることは医療の安全確保を行う場合と同様であり、必要不可欠です。

加えて情報技術(IT)の分野では医療安全管理では想定されない「経験したことのない、新たな起こりえるリスク」が常に発生しており、これらについても検討し、対策を取ることが必要です。ISMS は資産に対する未経験・新しいリスクに対するリスクアセスメントの手法を取っていますので活用してください。

（２）リスクアセスメントについての体系的な取組み方法の確立

ISMS 認証基準では、リスクアセスメント手順や判断基準を明確にすることを、「組織の取組み方」として以下のように規定しています。

> c) リスクアセスメントに対する組織の取組み方を，次を満たすように定義する。
> 1) ISMS，特定された事業上の情報セキュリティの要求事項，並びに特定された法令及び規制の要求事項に適したリスクアセスメントの方法を特定する。

> 2) リスク受容基準を設定し，また，リスクの受容可能レベルを特定する［5.1 f）参照］。
>
> 選択するリスクアセスメントの方法は，それを用いたリスクアセスメントが，比較可能で，かつ，再現可能な結果を生み出すことを確実にしなければならない。
>
> （JIS Q 27001:2006　4.2.1 ISMS の確立　より引用）

組織に偏在する多岐にわたる資産のリスクアセスメントを複数の担当者で実施する上では特に必要な活動です。

リスクアセスメントの体系的な取組み方法の確立では

① 適切な分析手法の選択
② アセスメントの手順を文書化する
③ リスク対応の方針及び目標を設定する
④ 受容可能なリスクの水準を特定する

を行います。

（３）適切な分析手法の選択

リスクアセスメントには様々な手法があります。個々の手法には特徴があり、メリット、デメリットがあります。よって、手法の種類とそれらの長所・短所を知り、その上で組織の特徴に合わせてリスクアセスメント手法を選択する必要があります。

図 4-5 は GMITS「IT セキュリティマネジメントのための手法」に記載されているもので、セキュリティマネジメントを説明したものです。

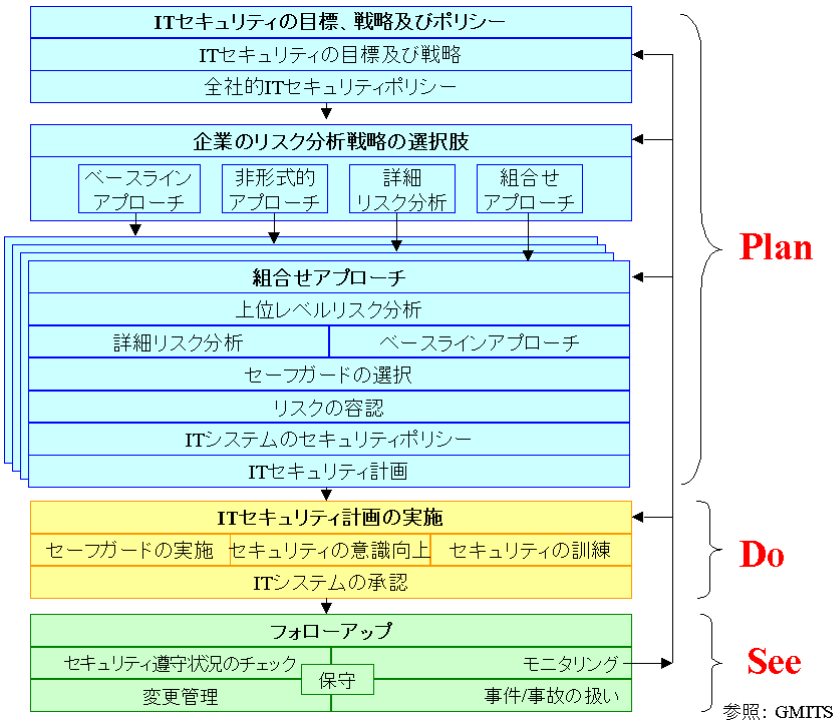


図 4-5　セキュリティマネジメント

ここでは、リスクアセスメントの方法として４つのアプローチが挙げられています。

① ベースラインアプローチ（Baseline　Approach）

一般的な情報セキュリティに関する基準や、業種・業界で採用されている標準やガイドラインなどを参照し、リスク評価することなくセキュリティ対策を実施します。

【特徴】

簡便であるため、リスクアセスメントにかかる時間と費用を削減できるが、組織によってはガイドラインとのバランスが合わないこともあります。

② 詳細リスク分析（Detail　Risk　Analysis）

資産の機密性、完全性又は可用性の喪失による潜在的な影響と、脅威及びぜい弱性の観点から起こりうるセキュリティ障害などを現在実施されている管理策を考慮した現実的な発生可能性からリスクを評価します。

【特徴】

厳密なリスク評価が行えるため、リスクに応じた適切な管理策を効率的に選択できるが、リスクアセスメントには時間と費用がかかります。

③ 組合せアプローチ（Combined Approach）

一般には、ベースラインアプローチと詳細リスク分析を組合せる手法です。

【特徴】

それぞれの手法の長所と短所を相互に補完するアプローチですが、重要な資産の特定に失敗すると組合せアプローチのメリットを生かせなくなります。

④ 非形式的アプローチ（Informal Approach）

組織や担当者の経験や判断によってリスクを評価する手法です。

【特徴】

改めて技術を習得することなくリスクの評価ができる反面、方法が構造化されていないために、漏れや見落としの可能性があります。

医療機関におけるリスクアセスメント手法の選択のポイントとしては、自分たちが属している医療機関の施設や規模に応じて手法を使い分けることがあげられます。例えば、病院であれば外来診療、検査、病棟、リハビリテーションなど多種多様な施設があり、それぞれで情報処理設備が置かれ、医療機器や他のシステムと情報がやり取りされています。その場合は、まずベースラインアプローチで考えられるリスクをチェックリスト形式で洗い出し、必要最低限の対策を取ることも考えられます。また、小規模の病院や診療所などでは設備や情報の範囲も限られているので、詳細リスク分析でより確実なリスクアセスメントすることも可能です。

・ベースラインアプローチ

ベースラインアプローチとは、後述する詳細リスク分析とは異なり、資産ごとにリスクそのものを評価しません。

一般の情報セキュリティに関する基準や、業種・業界で採用されている標準やガイドラインなどを参照し、組織全体で共通のセキュリティ対策を実施します。実現可能な水準の管理策を採用し、組織全体でセキュリティ対策に抜け漏れが無い様に補強していくアプローチです。

ベースラインアプローチは、大きく分けると以下の 2 つの手順で実施されます。

- **ベースラインの決定**
- **ギャップ分析の実施**

ベースラインアプローチでは、組織の達成する情報セキュリティ管理について独自の「対策の標準」を作成します。一般に、この対策の標準のことを「ベースライン」と呼びます。

しかし、ISMS 認証基準は、情報セキュリティマネジメントシステムに関する規格として一定の管理の枠組みが簡潔に規定されています。

実際に採用すべき管理策について余り詳細な記述が無く、採用する管理策についてもう少し詳細な情報がほしいと感じる時には先ず JIS Q 27002:2006 及び ISO 27799 を参照して下さい。特に新たに採用する管理策については、JIS Q 27002:2006 を精査して下さい。

本ガイドの ANNEX A.に掲載している「参考文献」の一覧にも、ベースラインに採用すべきコントロールの例として参照可能な法律、ガイドライン、報告書、文献などが収集され、活用可能な内容となっています。

また、上記以外にも有用な情報源が入手できる機会があると思います。今後策定されるであろう情報セキュリティに関する基準、制度や、外部コンサルタントから提供されるノウハウなどです。実際にどのようなコントロールを導入するのか、「出来る、出来ない」の判断をする前に広く管理策についての情報を収集し、組織が要求する情報セキュリティの管理水準が、達成可能なベースラインであるかを検討して下さい。

次に、ギャップ分析について説明します。

ギャップ分析実施の目的は、組織の定める基準への準拠状況の把握にあります。

基準で要求される管理のレベルと事業者の管理レベルの現状を比較し「大きな差が認められる個所」、「明らかに管理策の適用を必要としている個所」、「過度に管理策が適用されている個所」等を確認します。

図 4-6 は、それぞれの資産を対象に、現状の対策の度合いと組織によって定められる「要求される保証の度合い」との乖離を示しています。図 4-6 の要求される保証の度合いはひとつの平面として表現されていますが、本来、要求される保証の度合いは一律ではなく、資産の属性や性質、組織における重要度により資産ごとに決定されます。

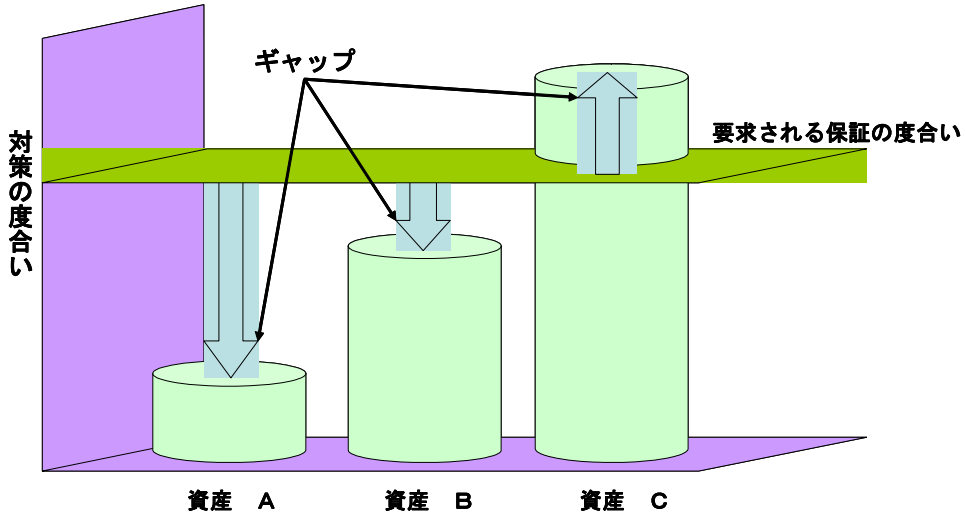


図 4-6　要求される保証の度合い

・詳細リスク分析

詳細リスク分析では、資産ごとの関連するリスクの識別を個別に実施します。（図 4-7 参照）。

リスクが顕在化する頻度は、脅威が発生する（顕在化する）可能性、管理上の弱点につけ込まれる可能性（ぜい弱性）の他に、資産が攻撃者から見てどれほど魅力的なものであるのか等にも依存します。

まずリスク分析の対象範囲の定義付けをしなければなりません。プロセスが密接に絡み合っているにも関わらず、安易に範囲を狭め、慎重な定義付けを怠ると、後に不必要な作業が増えたり、抜けが見られたりすることに繋がるからです。

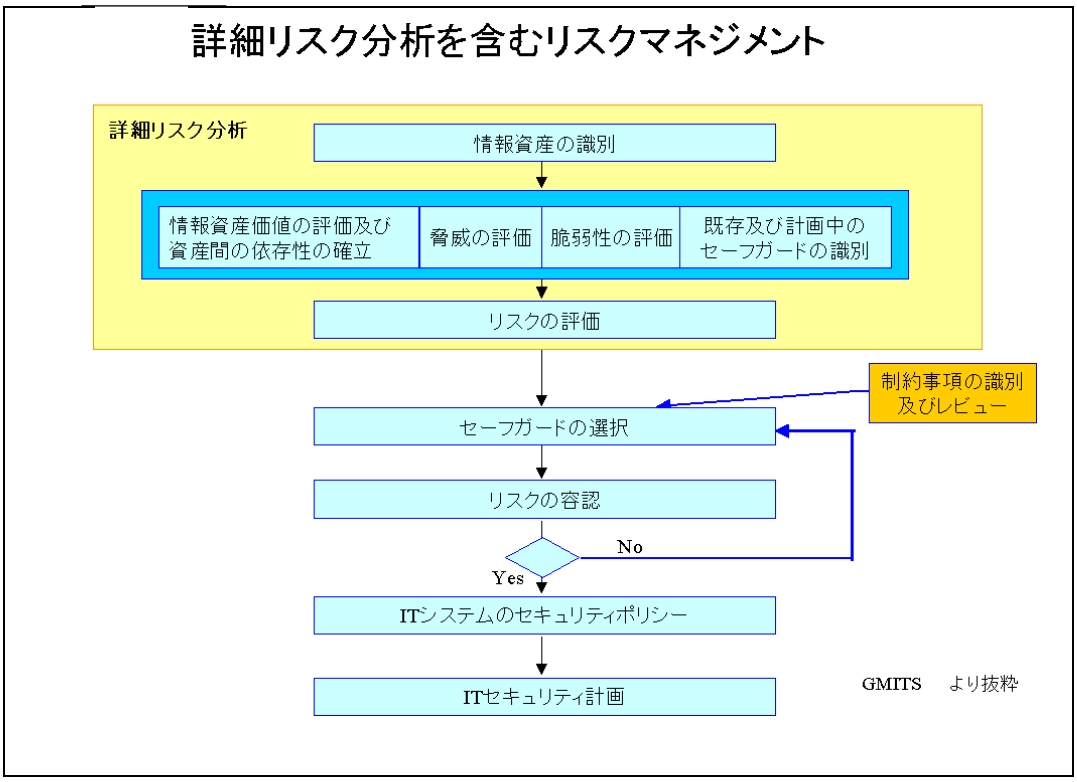


図 4-7　詳細リスク分析を含むリスクマネジメント

・組合せアプローチ

一般には、ベースラインアプローチと詳細リスク分析を併用する組合せアプローチを採用することが効率的であると紹介されています。

どのような場合にどのアプローチを採用するかは一概には決定できません。適切なアプローチの採用のための判断材料は、資産に求められるセキュリティ要求事項（前述の事業上の要求事項、法令又は規制の要求事項、契約上のセキュリティ義務など）に依存します。組合せアプローチには、それぞれの資産を取り巻くリスク環境を確認し、適切なリスク分析のアプローチを採用し、それぞれのアプローチの弱点を相互に補完し合うことにより、ISMS 適用範囲全体のリスク分析を効率的に実施する目的があります。「ベースラインアプローチ」のみでは、高い水準でセキュリティ対策が実装されるべきリスクの高いシステムについて対応策が不充分になる可能性があること、また、「詳細リスク分析」をすべてのシステムに適応することは効率的な観点から現実的でないことが大きな理由です。

図 4-8 は、前述の GMITS で定義されている組合せアプローチの例です。

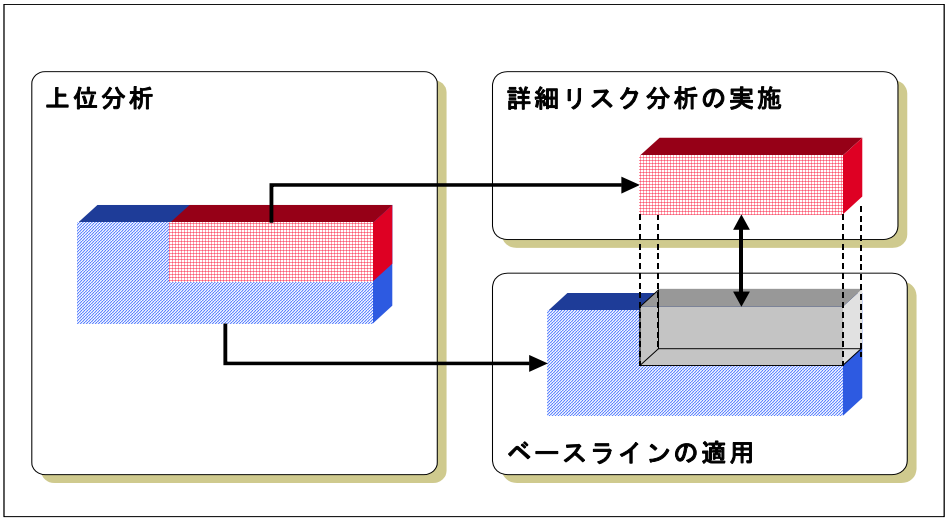


図 4-8　組合せアプローチ

・非形式的アプローチ

非形式的アプローチは、ここまで説明をしてきたリスク分析と異なり体系的なアプローチをとりません。この手法は主に現場担当者の長年にわたり培われた経験、知見に基づいてリスク因子の特定や対策の選択を実施します。

このアプローチは、分析を実施する際に手法について新たに学習すべき事項も少なく迅速

に作業に着手できます。また、詳細な分析を実施する場合に比べ投入する人的資源や時間が少なくて済みます。

一般にリスクの分析や評価の作業において、客観性がもっとも重視される事項です。このアプローチは担当者の特定の考え方に結果が影響される可能性があることは明らかです。しかし、体系的なリスク分析が実施できない場合などに対象を限定し、次項で説明する点に留意し、他のアプローチと組み合わせて実施することは有用です。

（４）リスクアセスメントの手順を文書化する

リスクアセスメントには、作業を実施するために必要な手順が文書化されている必要があります。

- **リスクアセスメントの定義**
- **リスクアセスメントの目的**
- **リスクアセスメントの方法**

また、上記の「リスクアセスメントの方法」には、以下の様な判断の基準等が含まれます。

- **資産の価値判断の基準**
- **脅威の評価基準**
- **ぜい弱性の評価基準**
- **リスク値の算出方法**
- **リスクアセスメントを行う頻度**

これらの文書策定は、リスクアセスメントが比較可能で、かつ、再現可能な結果を生み出すために確実に行なう必要があります。このことは、仮にリスクアセスメントの方法を変更した場合でも、その変更を管理し、必要に応じてリスクアセスメントの結果の比較が可能な状態にしておくことを含みます。

（５）リスク対応の方針及び目標を設定する

組織は、リスクアセスメントを実施し算出されたリスク値に基づいてリスク対応を実施します。

このステップでは、算出されたリスク値に基づきリスクマネジメントの枠組みの中でどの

ような対応を取るのかの選択肢を明らかにします。

リスク対応の選択肢については、前述の TR Q 0008 に以下の 4 つが紹介されています。

- **リスクの回避**
- **リスクの最適化**
- **リスクの移転**
- **リスクの保有**

（注記）「リスクの最適化」、「リスクの保有」、「リスクの移転」は、JIS Q 27001:2006 では、「適切な管理策の適用」、「組織の方針及びリスク受容基準を明確に満たすリスクの、意識的、かつ客観的な受容」、「関連する事業上のリスクの、他者（例えば、保険業者、供給者）への移転」（4.2.1 f）参照）といいます。

「リスク対応」の内容については、本ガイドの「4.2.6　STEP6　リスク対応を行う」で説明しています。

ここで決定したリスク対応の選択肢も、文書化し ISMS 文書に含めることが要求されています。

（６）受容可能なリスクの水準を特定する

ここでいう「受容可能なリスク」とは、組織として保有すること（「リスク保有」）が可能なリスクです。特に「受容」という言葉には、組織においてリスクを保有する積極的な「意思」が発生します。

> 3.10　リスクの受容（risk acceptance）
> リスクを受容する意思決定（TR Q 0008:2003）。
>
> （ISO/IEC 27001:2006　3 用語及び定義　より引用）

本来、リスクの受容可能な水準は、リスクアセスメントを実施しその結果に基づいて決定します。

ISMS 認証基準に規定されているこのステップでは、（２）で文書化したリスクアセスメントの手順に従って算出したリスク値を用いてリスク評価を実施するかを明らかにし、リスク受容の意思決定手順の確認を行います。

４．２．４　STEP4 リスクを特定する

リスクアセスメントは、まず「リスクを特定する」ことから始めます。単にリスクを特定するといっても、リスクそのものは手に取って認識することは出来ません。

本来、リスクは様々なリスク因子の因果関係により成り立っています。図 4-9 は、GMITS においてリスクとリスク因子の関係を示したもので、リスク値がそれを取り巻く「資産価値」、「脅威」、「ぜい弱性」により決定されることが表現されています。

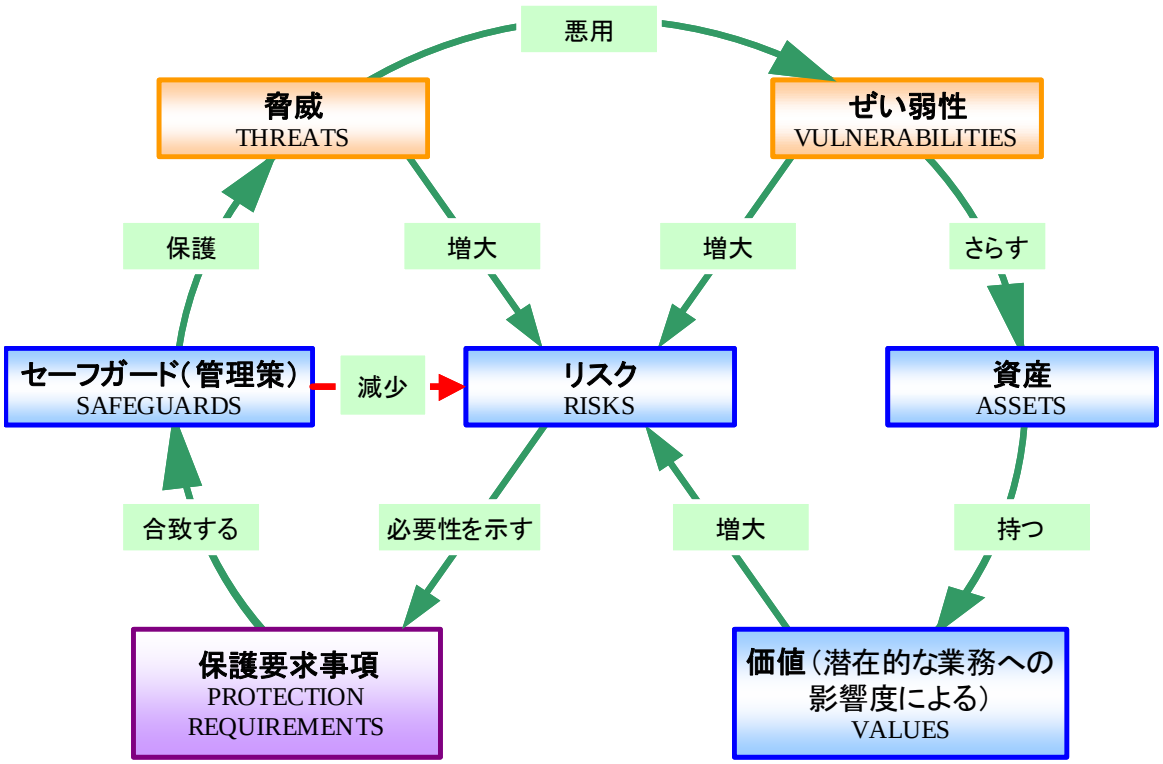


図 4-9　リスクとリスク因子の因果関係

リスクの特定では、具体的には以下の 2 つの作業が実施されます。

（１）資産の洗い出し

（２）脅威・ぜい弱性の明確化

以下、それぞれの内容について例示を用いて紹介します。

（１）資産の洗い出し

ここでは、組織の ISMS 適用範囲における資産の保有状況を確認します。ISMS の管理対象の詳細を把握し、適切な管理策を選択するためには、各々の資産の属性や価値を明確にすることが理想です。また ISMS 認証基準では、資産の洗い出しにおいて、それぞれの「資産の管理責任者」を特定することが求められています。

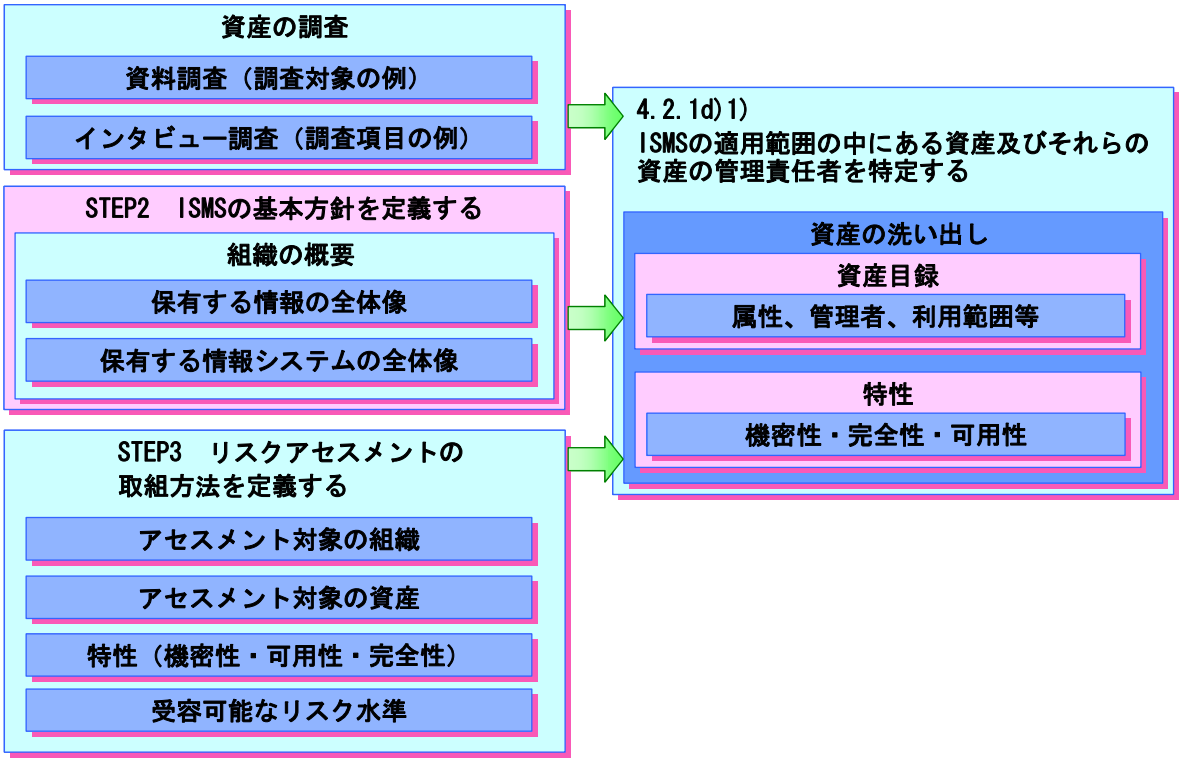


図 4-10　資産の洗い出し

①　資産目録の作成

「資産目録」を作成することは、JIS Q 27002:2006 では、「7.1.1 資産目録」という項目で推奨しています。

実施の手引 組織は，すべての資産を識別し，それら資産の重要度を記録することが望ましい。資産目録には，資産の種類，形式，所在，バックアップ情報，ライセンス情報及び業務上の価値を含め，災害から復旧するために必要なすべての情報を記載することが望ましい。目録は，他の目録と不必要に重複しないことが望ましく，その記載内容が他の目録と整合していることを確実にすることが望ましい。 さらに，各々の資産の管理責任者（7.1.2 参照）及び情報の分類（7.2 参照）について合意し文書化す

> ることが望ましい。資産の重要度に応じた保護のレベルは，資産の重要度，業務上の価値及びセキュリティ上の分類に基づいて決めることが望ましい（資産の重要度を表すための評価手法については，TR X 0036-3 参照）。
>
> （JIS Q 27002:2006　7.1.1 資産目録　より引用）

洗い出しの結果、資産目録に書き込む情報として以下の内容を参考に検討して下さい。

- **資産の管理責任者（資産の所有者・管理者名）**
- **資産の形態**
- **保管形態**
- **保管場所**
- **保管期間**
- **廃棄方法**
- **用途**
- **利用者の範囲（＋業務プロセス）**
- **他のプロセスとの依存性**

資産を個別に識別しその性質を理解することは､後の作業に関わる脅威やぜい弱性の識別と資産価値の判定の手助けとなります。

②　資産の例示

JIS Q 27002:2006 の「7.1.1　資産目録」には、資産の例示があります。JIS Q 27002:2006 では、資産の種類は「情報」「ソフトウェア資産」「物理的資産」「サービス」「人」「無形資産」の６つですが、この中で「人」という分類に注目してください。病院・診療所などの医療施設では、人の命に係わる重要な情報をもつ医師、看護師、技師などのコメディカルが多数勤務を行う特殊なところですので､これらに係わる人に関するリスクについても考慮し必要に応じて対策を検討して下さい。

表 4-3　資産の例示

資産の種類	例示
情報	データベース及びデータファイル、契約書及び同意書、システムに関する文書、調査情報、利用者マニュアル、訓練資料、運用手順又はサポート手順、事業継続計画、代替手段の取決め、監査証跡、保存情報
ソフトウェア資産	業務用ソフトウェア、システムソフトウェア、開発用ツール、ユーティリティソフトウェア
物理的資産	コンピュータ装置、通信装置、取外し可能な媒体、その他の装置
サービス	計算処理サービス、通信サービス、一般ユーティリティ（例えば、暖房、照明、電源、空調）
人（知識）	医師、看護師、コメディカルなど（患者情報や診療情報をはじめとする情報と、それにアクセスする方法を知っている人）
	保有する資格、技能、経験
無形資産	例えば、組織の評判、イメージ

この例では、電子的なデータはもちろんそれらを処理するコンピュータ本体、記録媒体やファームウェアなども含まれています。また、紙媒体の情報や会話、物理的な施設・設備といったものも該当します。

③　資産のグループ化

ISMS 適用範囲に存在する資産の洗い出し作業の負荷が非常に大きいことは容易に想像できます。

リスク分析の作業を進めるにあたり、「資産のグループ化」は作業負荷軽減と今後の分析作業の効率化に有効な考え方です。

例えば、資産価値や属性（保管形態や保管期間、用途等）が一致するものを一つのグループとする等です。重要性や属性が同じで、結果的に適用されるセキュリティ対策が同じであれば、同じグループとしてまとめて管理することが効率的です。

そもそも資産の洗い出しをする目的は、ISMS の適用対象全体で適切なセキュリティ対策を決定することです。組織の全ての資産を網羅し、一つひとつの資産の属性を明記した詳細な資産台帳を作成することが必ずしも重要ではありません。

④　情報区分（影響度の基準）

資産目録の作成後、資産価値を評価します。資産価値は、組織の事業上重要なプロセスに

対する影響度ととらえることが可能です。

組織のニーズに基づく資産の識別と評価は、リスクアセスメントにおける重要な要因となります。従って、主要な資産の価値の評価は、組織の業務をよく理解した情報の管理責任者（「情報オーナ」などという場合もある。）によって行われなければなりません。

組織は、資産の価値を判定する際に C.I.A.の 3 要素に関する組織独自の判断基準を開発しなければなりません。表 4-4～表 4-6 に、機密性、完全性及び可用性の基準の例を示します。

表 4-4　機密性の基準の例

資産価値（機密性）	クラス	説明
1	公開	第三者に開示･提供可能 内容が漏洩した場合でも、医療業務への影響はほとんど無い
2	院外秘	組織内では開示･提供可能（第三者には不可） 内容が漏洩した場合、医療業務への影響は少ない
3	秘密	特定の関係者または部署のみに開示･提供可能 内容が漏洩した場合、医療業務への影響は大きい
4	極秘	所定の関係者のみに開示･提供可能 内容が漏洩した場合、医療業務への影響は深刻かつ重大である

表 4-5　完全性の基準の例

資産価値（完全性）	クラス	説明
1	不要	参照程度でしか利用されていないので問題がない。
2	要	改ざんされると問題があるが、医療業務への影響はない
3	重要	完全性が維持できないと医療業務への影響は深刻かつ重大である

表 4-6　可用性の基準の例

資産価値（可用性）	クラス	説明
1	低	情報が利用できなくても医療業務に支障がない
2	中	情報が利用できないと医療業務への支障はあるが、代替手段で業務ができる。または、情報が利用できるまでの遅延が許される。
3	高	必要時に確実に情報が利用できないと医療業務への影響は深刻かつ重大である

個別の資産の価値は、表 4-3 の例示のように予め規定された情報区分に基づき、主に情報の管理責任者の主観で判定されます。

（２）脅威・ぜい弱性の明確化

ISMS 認証基準では、リスク因子を個別の資産がさらされるであろう「脅威」と管理上の問題点などによる「ぜい弱性」の組合せと規定しています。また、リスク因子とはリスクが顕在化する要因です。

> 3.1.5　リスク因子(source)
> 結果（3.1.2）をもたらす可能性が潜在する物事や行動。
>
> （TR Q 0008:2003　3.用語及び定義　より引用）

①　脅威の識別

「脅威」とは、情報システムや組織に損失や損害をもたらすセキュリティ事故の潜在的な原因です。脅威は後述する「ぜい弱性」により誘引され、顕在化することにより組織及び組織の業務に影響を与えます。脅威の大きさは、その要因や対象となる資産ごとに、その発生の可能性を評価して決定します。

GMITS では表 4-7 の様に大別して説明しています。

表 4-7　脅威の分類例

人為的脅威		環境的脅威
意図的（計画的）脅威	偶発的脅威	環境的脅威
deliberate ⇒ D	accidental ⇒ A	environmental ⇒ E

情報の管理責任者は、前述した資産の価値の決定同様、情報利用者や他部門の関係者、外部の専門家から提供される脅威に関する情報を元に、自らが管理する資産がさらされる脅威を識別し、表 4-8 の例示のような一覧表を作成します。

表 4-8　脅威の例示とその分類例

脅威	分類 (D,A,E)
地震	E
停電	D,　A　,E
静電気	E
オペレータの操作ミス	D,　A
人的リソース（スタッフ）不足	A
ID の偽り	D
悪意のあるソフトウェア	D,　A
……	……

脅威の洗い出しは、表 4-8 の例などを参考に実施します。

例えば、意図的（計画的）脅威は、攻撃者の動機、攻撃に必要とされるスキル、利用できるリソースを考慮に入れ、資産の特性、魅力、ぜい弱性から、どのような要因が脅威であるかを識別します。

偶発的な脅威は、立地条件、極端な気候条件の可能性及び要員によるミスや誤動作などから影響を及ぼす可能性を識別します。

次に、脅威の発生頻度を評価します。

頻度についても、脅威の識別と同様に自身の業務と関連する他部門と協力して整理します。作成した脅威一覧に基づき、業務上の経験や過去に収集した統計的なデータに基づいて検討します。

評価にどの程度の正確性を要求されるかにもよりますが、「低い」、「中程度」、「高い」の 3 つの区分とする場合が多い様です。表 4-9 に、3 つに区分した場合の判断基準を例示します。

表 4-9　脅威の判断基準

脅威		
発生可能性	区分	説明
1	低い	発生する可能性は低い。発生頻度は 1 年に 1 回あるかないかである。
2	中程度	発生する可能性は中程度である。発生頻度は半年以内に 1 回あるかないかである。
3	高い	発生する可能性は高い。発生頻度は 1 ヶ月に 1 回以上である。

② ぜい弱性の識別

ぜい弱性とは、脅威発生を誘引する資産固有の弱点やセキュリティホールのことです。ぜい弱性は、それだけでは何ら障害とはなりませんが、脅威を顕在化させ、損害や障害を導く可能性があります。逆にいえば、脅威が存在しないぜい弱性は、あまり気を配らなくても良いということになります。

ぜい弱性の分類の例を表 4-10 に示します。ぜい弱性をリスト化する際には、表 4-10 のように脅威と関連づけて整理する必要があります。

表 4-10　ぜい弱性の識別

ぜい弱性の分類	ぜい弱性の例	関連する脅威の例
環境、施設	ドア、窓などの物理的保護の欠如	盗難
	不安定な電源設備	停電、誤作動
	災害を受けやすい立地条件	洪水、地震、災害
ハードウェア	温湿度変化に影響を受けやすい	故障、誤作動
	記憶媒体のメンテナンス不足	故障、情報漏洩
ソフトウェア	仕様書の不備	ソフトウェア障害、誤作動
	アクセスコントロールの欠如	なりすまし、改ざん、情報漏洩
	不適切なパスワード	不正アクセス、改ざん、情報漏洩
	監査証跡（ログ管理）の欠如	不正アクセス
	バックアップコピーの欠如	復旧不能
……	……	……

ぜい弱性は、資産の性質や属性と関連付けて検討すると識別が容易です。

例えばノート PC を例にとれば、その性質として、「持ち運びやすい」、「衝撃に弱い」、「公共の場で用いられる」などが挙げられます。と同時にその性質は、「盗難や置き忘れ」、「故障」、「情報漏洩」という脅威に対するぜい弱性を示しています。

このことは、その資産の利用環境や保管場所、プロセスの進行状況（ステージ）、形態、時間など、その環境によっては全く異なるぜい弱性が存在することを示しています。同じ資産（例えばノート PC）であっても、その利用形態や性質などから「ノート PC（院内利用）」、「ノート PC（院外利用）」などと分けて識別して管理すべき場合もあることに留意しなければなりません。

ぜい弱性の評価は、その資産の持つ弱点がどの程度であるかを評価することになります。何も対応策を施しておらずその弱点が剥き出しであるような場合は、ぜい弱性は高いと判断できます。組織によりどの程度分類するかは異なりますが、脅威同様、ぜい弱性に関しても、

「低い」、「中程度」、「高い」などで区分します。

４．２．５　STEP5 リスクを分析し評価する

リスクアセスメントは、アセスメント手順を決定し、資産目録を作成し、資産の重要性の分類及び脅威・ぜい弱性の評価基準を明確にすることにより実施が可能になります。

資産の重要性は、前述の C.I.A.毎に分けて情報の管理責任者が評価します。

脅威・ぜい弱性の評価は、作業を専門家に依頼して実施した方が客観性や効率性の確保の面から良い場合もあります。また、情報セキュリティ監査制度を利用し、外部の専門家がぜい弱性評価の支援することも考えられます。

（１）リスク値の算出

リスク値は、前の作業で明確になった「資産の価値」、「脅威の大きさ」、「ぜい弱性の度合い」を用いて、例えば、簡易的に以下のような式で算出します。

リスク値 ＝ 「資産の価値」 × 「脅威」 × 「ぜい弱性」

（例）

特性	資産の価値
C:機密性	4
I:完全性	2
A:可用性	1
脅威	3（情報が関係者外に漏洩した場合、信用の失墜に繋がる）
ぜい弱性	3（すべての作業担当者に特権が付与されていたので）

この場合のリスク値は、以下の様になります。

機密性に関わるリスク値：4×3×3＝36

完全性に関わるリスク値：2×3×3＝18

可用性に関わるリスク値：1×3×3＝9

図 4-11　リスク値の計算例

また、リスク値を算出し表 4-11 の例のようなマトリクス「リスク値早見表」を作成すると、以降の作業を効率的に進める助けになります。

表 4-11　リスク値早見表例

	脅威								
	1			2			3		
	ぜい弱性								
資産の価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

例えば、受容可能なリスク値は表 4-12 の例の様な一覧表になることが考えられます。

表 4-12　リスク受容一覧の例(1)

	脅威								
	1			2			3		
	ぜい弱性								
資産の価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

リスクを受容できる範囲

リスクに対して何らかの対策を講じる範囲

表 4-12 のリスク受容一覧の例(1)は、本ガイドの 4.2.3(6)で特定した「受容可能なリスク水準」を[9]とした場合です。リスク評価作業の際に作成したリスク値のマトリクス（「リスク値早見表」）で、リスク値が「9」未満のものについては、現状の管理を受容し、受容したリスクについては「残留リスク」として管理します。

表 4-13　リスク受容一覧の例(2)

	脅威								
	1			2			3		
	ぜい弱性								
資産の価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

リスクを受容できる範囲

リスクに対して何らかの対策を講じる範囲

また、表 4-13 のリスク受容一覧の例(2)では、資産の価値が最大の「4」であれば無条件に対策をとるべきであるということで、リスク値の許容水準は「4」未満となります。

このリスク受容一覧は、あくまでリスク評価実施時のリスク環境を表わすもので、資産の価値や脅威、ぜい弱性等の環境に変化が生じた場合は、適宜リスク値の見直しを実施しなければなりません。

（２）作業上の留意点

リスクアセスメントは、体系だった手順の策定と、それに従った実施が求められます。

例えば、経済産業省リスク管理・内部統制に関する研究会の「リスク新時代の内部統制～リスクマネジメントと一体となって機能する内部統制の指針～」ではリスクの算定について以下の通り説明しています。

> 特定されたリスクは、それぞれのリスクが顕在化した場合の企業への影響度と発生可能性に基づき、企業にとっての重要度を算定されなければならない。必ずしも全てのリスクについて定量的に算定することができるわけではないが、リスクの算定は、関係者が納得できる合理的な指標を用いて、統一的な視点で相対的な比較が可能となるよう行われることが望ましい。例えば、リスクの影響度とその発生可能性をそれぞれ「大」、「中」、「小」に区分し、影響度と発生可能性の組合せにより評価すること等が考えられる。
>
> ＜中略＞

また、リスクを定性的にしか把握できない場合には、経験等に基づく推測により、その影響度と発生可能性をそれぞれ「大」、「中」、「小」とランク付けし、評価すること等が考えられる。

（リスク新時代の内部統制～リスクマネジメントと一体となって機能する内部統制の指針～
第二部　ＩＩ.1.リスクマネジメントのあり方(3) リスクの算定
平成 15 年 6 月　経済産業省リスク管理・内部統制に関する研究会　より引用）

つまり前述の計算方法を採用した場合にも、リスク値が変わる可能性があります。

リスク値 ＝ 「資産の価値」 × 「脅威」 × 「ぜい弱性」

という計算式には厳密な理論性はありません。似た属性を持つ同種の資産であっても、個別の資産についての価値や脅威、ぜい弱性の評価結果や、評価者の判断でリスク値に差が出てしまうことはあり得ます。

また、資産の価値や、脅威、ぜい弱性の値を足し算してリスク値を算出しても評価は可能です。

ISMS 認証基準では、リスク値を算出することが要求事項に規定されています。しかし極論すれば、点数だけに頼ってリスク値を決定せず、人間の判断を優先して対策の必要性の有無を決定するというリスクアセスメントの枠組みの採用も、選択肢のひとつとなると思います。

例えば前述の、評価者の判断のばらつきについても、分析の初期の段階から十分な例を用意し、評価者に十分な説明を実施すれば、結果をある程度平準化することは可能になります。

更に、日常当該資産を利用している（もしくは主に管理している）情報の管理責任者の認識をリスク値の評価の参考として収集し確認することも、現状の対策の程度が十分であったかを検証する指標となります。

４．２．６　STEP6 リスク対応を行う

3.15　リスク対応（risk treatment）
リスクを変更させるための方策を，選択及び実施するプロセス（TR Q 0008:2003）。
注記　この規格では，“管理策”という用語を“方策”の類義語として使用する。

（JIS　Q　27001:2006　3 用語及び定義　より引用）

リスク対応とは、「リスクを変更させるための方策を選択及び実施するプロセス」と説明されています。リスクを変更させるための方策として、次の 4 つの選択肢があります。

- **適切な管理策を採用する**
- **組織の方針及びリスク受容基準を明確に満たすリスクを、意識的、かつ、客観的に受容する**
- **リスクを回避する**
- **リスクを移転する**

リスクアセスメントで明確にされた管理対象とするリスクに対し､上記 4 つの選択肢からどれを選択するかについて評価します。

（1）適切な管理策を採用する

「適切な管理策を採用し、リスクを低減する」方法は、リスク対応の実施の際に最も多く採用されます。

例えば、ISMS 認証基準の附属書 A に記載されている 133 項目の管理策の適用や要求事項に明記されていない対策の追加実施等はこれに相当します。

リスク低減について概念的に示したものを図 4-12 に示します。この場合、リスク低減は「リスクの発生の可能性を低減する」ことと「リスクが顕在化した場合の影響度を低減する」ことにより実現されることが分かります。

図 4-12 で、

R はリスク：Risk
C はリスクを低減させるための対策：Control
E は対策を講じた後のリスク：Exposure

を示しています。

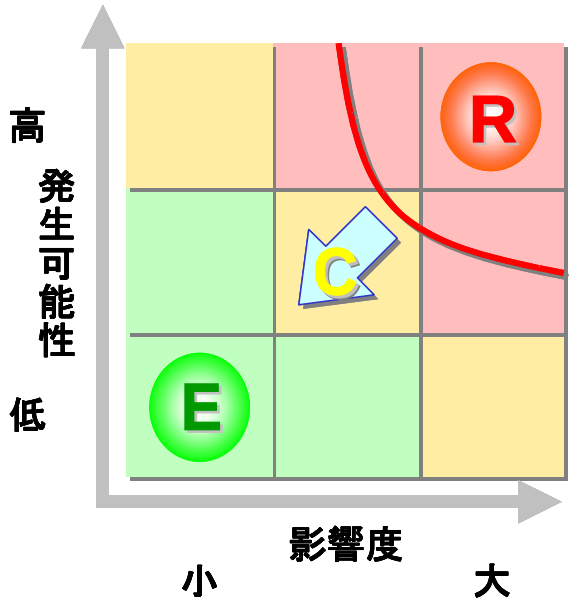


図 4-12　リスク低減の概念

リスク発生可能性の低減の例として、「入退室をより厳重に管理する」などの対策が考えられます。

影響度の低減では、「バックアップ頻度を増やし、修復可能なデータを増やす」などの対策が考えられます。

現実には、対策の実施によるリスクの完全な除去は不可能です。多くの場合、利便性の確保や、対策にかかる費用と効果の比較により、顕在化したときのリスクを受容可能な水準にとどめるのに十分な費用を投入して対策を実施し、残留リスクを次項「リスクを意識的、かつ、客観的に受容する」の対象として管理します。

（2）リスクを意識的、かつ、客観的に受容する

「リスクを意識的、かつ、客観的に受容する」とは、リスクが組織の方針及びリスクの受容のための評価基準を明らかに満たす場合に用いる選択肢です。

保有するリスクは、以下の 2 つに大別できます。

- **識別され受容されるリスク**
- **識別されず組織に内在するリスク**

保有するリスクの内、リスクが組織の基本方針及びリスクの受容のための評価基準を明らかに満たす場合には、意識的かつ客観的に当該リスクを受容することになります。

（3）リスクを回避する

「リスクを回避する」とは、リスク対応を検討した上で、コストの割に利益が得られない場合や、適切な対応策が見出されない場合、リスクを回避するために、業務を廃止したり、資産を破棄するといった方法をとることです。

例えば、個人情報は漏洩するリスクや開示要求に応じて適切に開示できないというリスクが想定されます。これらのリスクに対し、それらの個人情報が、担当者個人単位で保有するデータに依存しているのであれば、業務上の必要性が乏しくなった個人情報などを洗い出し、担当者が保有していたデータを廃棄するというリスク対応が考えられます。

また、売上に寄与していないメーリングリストは、不注意で個人情報が漏洩したり、ウィルス蔓延に利用されるリスクがあるため、メーリングリストを廃止するというリスク対応が考えられます。

これらの考え方はリスクを回避するということになります。

（4）リスクを移転する

リスクを移転するとは、契約等によりリスクを他者（他の機関、会社）に移転することです。

リスクを移転する方法は大別すると 2 種類あります。一つは資産や情報セキュリティ対策を外部に委託する方法（アウトソーシング）で、もう一つはリスクファイナンスの一種として保険等を利用する方法です。

例えば、前者の例として資産を外部のデータセンターに預けるというコロケーションサービスの利用や、運用を委託するという方法があります。医療機関は、このようなアウトソーシング等にリスクを移転する場合、「移転したリスク」、「移転しなかったリスク」、「移転したことにより新たに発生するリスク」の 3 つを明確にすることが重要となります。また、移転したリスクを明確にするために、セキュリティ対策について契約書等に織り込むことが重要となります。

ISMS 認証基準の附属書 A には以下のような管理策が記載されており、リスクを移転することにより新たに発生するリスクを低減するための管理策といえます。

A.10.2 第三者が提供するサービスの管理 目的：第三者の提供するサービスに関する合意に沿った，情報セキュリティ及びサービスの適切なレベルを実現し，維持するため。		
管理策		
A.10.2.1	第三者が提供するサービス	管理策 第三者が提供するサービスに関する合意に含まれる，セキュリティ管理策，サービスの定義，及び提供サービスレベルが，第三者によって実施，運用，及び維持されることを確実にしなければならない。

（JIS Q 27001:2006　A.10.2 第三者が提供するサービスの管理　より引用）

リスクマネジメント上は、ISMS 認証基準の管理策を適用できない場合や、適用してもリスク値が受容水準以上の場合、リスク移転を検討します。

リスクファイナンスとしてリスクの移転の典型的な例は保険の採用です。例えば、地震等の不可避な脅威について、事業に与える影響は大きいが、比較的発生する可能性が低いので保険の利用を検討する等ということが相当します。

今日では、情報システム障害に対応するための保険が販売されています。例えば、顕在化したリスクの影響から復旧するために必要な費用や機器の買い替え費用が保険により支払われるというものです。

保険の場合、保証されるのは損害に対する金銭的な保証の一部に過ぎません。そのため、保険のみを利用したリスク対策には限界があります。（例えば、情報漏えいをおこし、医療機関のイメージが低下しても保険により損害を補填することは困難です）。つまり、保険によるリスク対応は万能ではありません。あくまでも、管理策を実施しても補填できないリスクがある場合に予備的に利用するのが本来の目的と思われます。

また、保険は、免責事項などが細かく決められていますので、契約を結ぶ前に細かく確認することが重要です。

４．２．７　STEP7 管理目的と管理策を選択する

ISMS 認証基準の附属書 A「管理目的及び管理策」より、リスク対応に関する管理目的及び管理策を選択します。適切な管理目的又は管理策が附属書 A に記載されていない場合は、独自に追加の管理策を採用することができます。

また、この選択については、リスクアセスメント及びリスク対応プロセスの結果に基づいてその妥当性を示すことが重要です。

また、附属書 A「管理目的及び管理策」に記載されている管理策の幾つかは、すべての情報システム又は環境に適用できるとは限らないこと、及び組織によっては実施できない場合

もあることを認識しておく必要があります。JIS Q 27002:2006 「4.2 セキュリティリスク対応」では例示として、「例えば，10.1.3 では，不正行為及び過失を防止するための職務の分割について規定している。比較的小規模の組織にとって、すべての職務を分割することは不可能であり、同じ管理目的を達成する他の方法が必要となる場合がある」と記載されています。しかし、このような場合でも、組織は管理目的を達成するにあたり、リスクが受容可能な範囲に低減できる代替措置を講じられるのであれば､附属書 A に記載されている管理策以外の管理策を選択し、確実に実装していく必要があります。

４．２．８　STEP8 残留リスクを承認する

残留リスク（リスク対応の後に残っているリスク）が受容リスク水準以下であるか、又は受容リスク水準以下になる計画であることを経営陣が確認し、承認します。

４．２．９　STEP9 ISMS の導入・運用を許可する

経営陣が ISMS を導入し、運用することに対して確認し、承認します。

４．２．１０　STEP10 適用宣言書を作成する

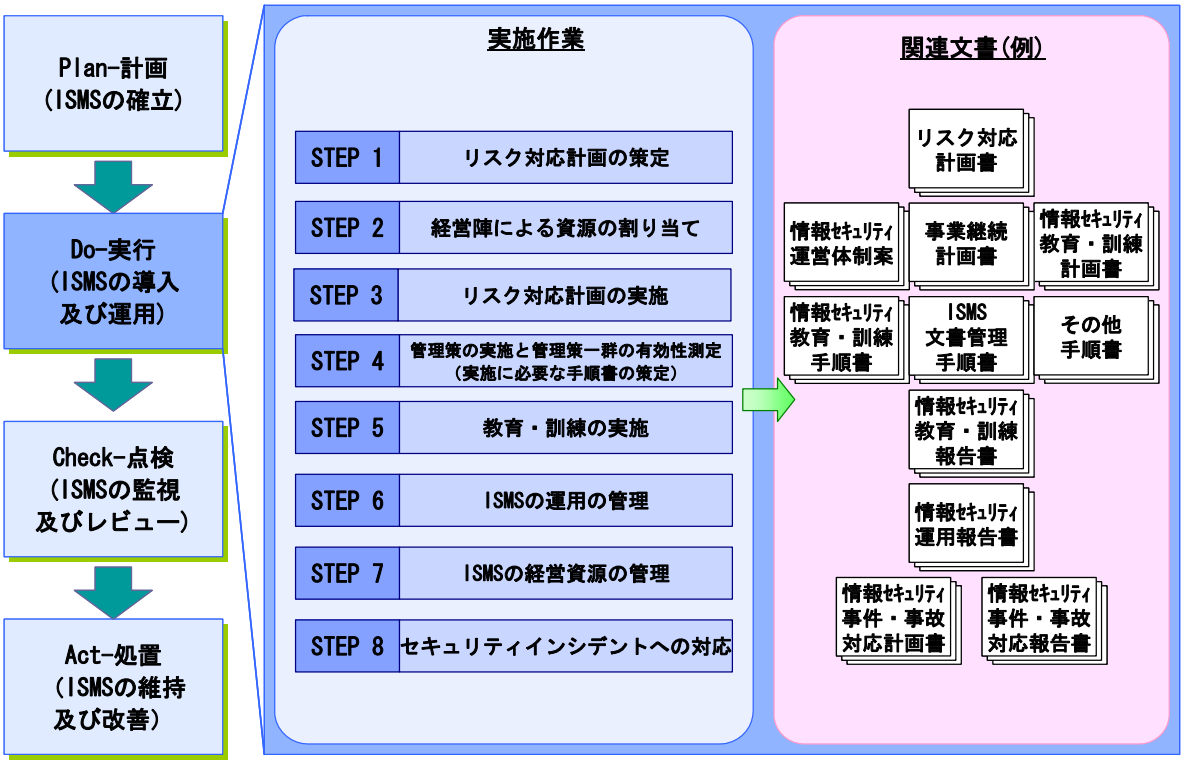
STEP7 で選択した管理目的及び管理策、並びにこれらを選択した理由を文書化し、適用宣言書を作成します。

また、附属書 A に記載された管理目的及び管理策の中から適用除外としたものは、除外した管理策及びその理由について記録を残すことが要求されています。

以上、「ISMS の確立」の１０の STEP を解説しましたが、対応結果を記録文書として残し病院長または理事会の承認を行うことは､患者や地域社会への情報セキュリティに対する取組む姿勢を示すことになります。また万が一の情報セキュリティ事故、インシデントが発生し訴訟問題などになった場合でもこれらの活動と記録文書はとても大切な証拠となります。是非、参考にして実施してください。

４．３　ISMS の導入及び運用（Do-実行）

ISMS 認証基準の「4.2　ISMS の確立及び運営管理」では、ISMS の導入及び運用の手順を図 4-13 の 8 つのステップで規定しています。



注）文書名は全て例示

図 4-13　ISMS 導入及び運用の手順

組織は，次の事項を実行しなければならない。

a) リスク対応計画を策定する。この計画では，情報セキュリティリスクを運営管理するための，経営陣の適切な活動，経営資源，責任体制及び優先順位を特定する。

b) 特定した管理目的を達成するためにリスク対応計画を実施する。この計画には，必要資金の手当て並びに役割及び責任の割当てへの考慮を含む。

c) 4.2.1 g) によって選択した管理策を，その管理目的を満たすために実施する。

d) 選択した管理策又は一群の管理策の有効性をどのように測定するかを定義し，また，比較可能で再現可能な結果を生み出すための管理策の有効性のアセスメントを行うために，それらの測定をどのように利用するかを規定する［4.2.3 c) 参照］。

注記　管理策の有効性の測定は，管理策が，計画した管理目的をよく達成していることを，管理者及び要員が判断することを可能にする。

e) 教育・訓練及び意識向上のためのプログラムを実施する（5.2.2 参照）。

f) ISMS の運用を管理する。 g) ISMS のための経営資源を管理する（5.2 参照）。 h) 迅速にセキュリティ事象を検知でき，かつ，セキュリティインシデントに対応できるための手順及びその他の管理策を実施する［4.2.3 a）参照］。 （JIS Q 27001:2006　4.2.2 ISMS の導入及び運用　より引用）

４．３．１　STEP1 リスク対応計画の策定

リスク対応計画とは、リスクアセスメントの結果に基づき、受容できないリスクを低減するためにとるべき活動と、選択した管理目的及び管理策の実装に関する実行計画を明らかにすることです。

リスクマネジメントに必要な経営資源の割り当てや実際の作業は、このリスク対応計画に基づいて実施されます。

経営陣は、この計画が策定されることを確実にする責任があります。詳細は、次章「5. 経営陣の責任」でふれますが、ISMS 認証基準ではリスク対応計画に経営陣の適切な活動、責任及び優先順位を明確にすることが要求されています。

リスク対応計画に不備があれば、十分な管理目的及び管理策が実装できないことにも繋がりますので、様々な条件を考慮に入れて計画を策定する必要があります。

リスク対応計画では、単にリスクを低減するための管理目的及び管理策を策定するだけではなく、導入した管理目的及び管理策が適切かつ効果的に動作していることを確認するための管理目的及び管理策や、異常を検出するための管理目的及び管理策等を導入する計画も合わせて策定する必要があります。

例えば、管理策としてアンチウィルスソフト、ファイアウォール、アクセス制御などのセキュリティ製品を導入する場合について考えてみます。これらの製品を導入する際には、セキュリティを強化するための設定に留まらず、それらの状態を示す情報や、処理した結果のログなどを抽出して解析することにより、異常検出を考慮した設定を実装することなども計画に盛り込むことが必要です。

また、解析に必要な装置などが高価な場合、その導入による効果を確実にするための管理策も視野に入れて検討することが重要です。

リスク対応計画により、組織が識別したリスクに対する管理策の実施状況と、対策は実施したが残留リスクが受容可能な水準以下に低減されていないリスクへの追加的対策の進捗状況を容易に把握することが可能となります。

リスク対応計画に含むことが望ましい内容として以下の 4 点があります。

- **日程表**
- **優先順位**
- **詳細な作業計画**
- **管理策を実施する責任**

４．３．２　STEP2 経営陣による資源の割り当て

本ガイドの「5. 経営陣の責任」を参照して下さい。

４．３．３　STEP3　リスク対応計画の実施

特定した管理目的を達成するためにリスク対応計画を実施します。ここでは、STEP1 及び STEP2 で定めたプロセスに従い、必要資金の手当て並びに役割及び責任の割当て等を考慮に入れ、確実に管理目的を達成するために当該責任者を中心にリスク対応計画を実施します。

４．３．４　STEP4 管理策の実施と有効性測定

リスク対応計画に従い、優先順位の高い管理策から実施していきます。

その際には、管理策の運用に関する手順や、セキュリティインシデントに対応する手順などを文書化し、関係者に周知する必要があります。

さらに新たな要求事項として、「管理策の有効性の測定」が加わりました。詳細は本ガイド」の「9. 有効性の測定」を参照してください。

４．３．５　STEP5 教育・訓練の実施

本ガイドの「5.2.2 教育・訓練、認識及び力量」を参照して下さい。

４．３．６　STEP6 ISMS の運用の管理

導入した管理策が適切に運用されることを管理するための手順書を策定します。また、策

定する各々の手順書には、運用管理者、利用者などの関係者の責任が明記されている必要があります。

手順書に含まれる例を以下に示します。

- **バックアップに関する手順**
- **変更に関する手順**
- **復旧に関する手順**
- **正常動作確認のための手順**
- **緊急時の対応に関する手順**

４．３．７　STEP7 ISMS の経営資源の管理

本ガイドの「5.2 経営資源の運用管理」を参照して下さい。

４．３．８　STEP8 セキュリティインシデントへの対応

顕在化したセキュリティインシデントに対する被害を最小限に抑えるために、先ずそれらを適切に検出し、迅速な処置をとることが重要です。

セキュリティインシデントに対応するための手順書の策定と、その内容の定期的な検証は重要な作業です。特に、初期段階における対応の責任者の設定及び必要な関係者を対象とした連絡・報告の体制、適切な処置の実施に関する一連の手順の策定は重要です。

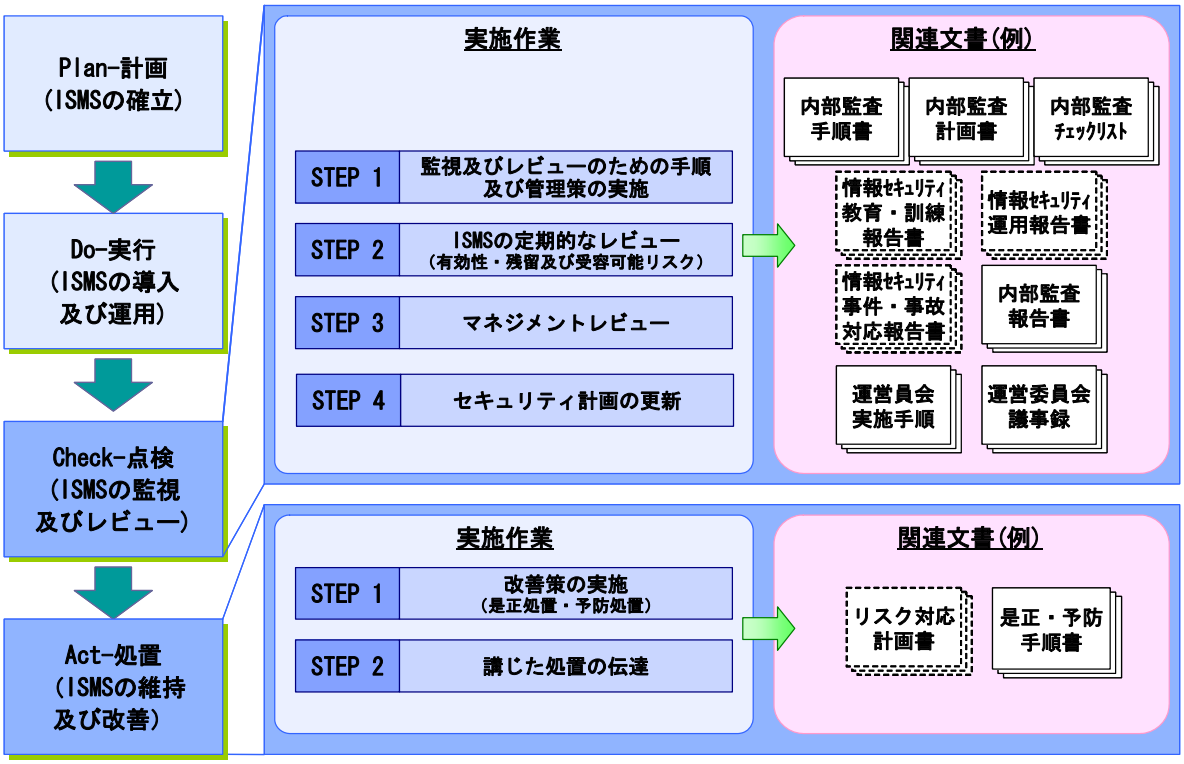
また、検出されたセキュリティインシデントを報告し、適切な処置として組織全体に反映することは、今後の再発防止のために重要です。セキュリティインシデントを報告する報告書には、以下の次項を含めることに留意して下さい。

- **セキュリティインシデントの記録**
- **管理策の不具合**
- **処置の内容**
- **必要な追加の管理策など**

報告をマネジメントレビューのインプットとすることは、情報セキュリティを継続的に向上させるうえで重要です。

４．４　ISMS の監視及びレビュー（Check-点検）・ISMS の維持及び改善（Act-処置）

ISMS 認証基準の「4.2 ISMS の確立及び運営管理」では、ISMS の監視及びレビュー、ISMS の維持及び改善の手順をそれぞれ図 4-14 の様に規定しています。



注）文書名は全て例示

図 4-14　ISMS の監視、レビュー、維持及び改善の手順

組織は，次の事項を実行しなければならない。

a) 監視及びレビューの手順並びにその他の管理策を，次のために実施する。

1) 処理結果の中の誤りを迅速に検知する。

2) 未遂であるか既遂であるかを問わず，セキュリティの違反及びインシデントを迅速に特定する。

3) 人力にゆだねて又は情報技術を導入して実施しているセキュリティ活動が期待どおりかどうかを経営陣が判断することを可能にする。

4) セキュリティ事象の検知を補助し，その結果の表示を利用してセキュリティインシデントを防止する。

5) セキュリティ違反を解決するためにとった処置が有効であるかどうかを判断する。

b) ISMS の有効性について定期的にレビューする。これには，ISMS 基本方針及び目的を満たしていることのレビューとセキュリティ管理策のレビューとがある。このレビューでは，セキュリティ監査の結果，インシデント，有効性測定の結果，提案，及びすべての利害関係者からのフィードバックを考慮

する。

c) セキュリティ要求事項を満たしていることを検証するために，管理策の有効性を測定する。

d) リスクアセスメントをあらかじめ定めた間隔でレビューする。残留リスク及び特定したリスク受容可能レベルをレビューする。これらのレビューでは，次に起きた変化を考慮する。

1) 組織

2) 技術

3) 事業の目的及びプロセス

4) 特定した脅威

5) 導入した管理策の有効性

6) 外部事情（例えば，法令又は規制の状況，契約上の義務，社会的風潮）

e) あらかじめ定めた間隔で ISMS 内部監査を実施する。

注記　第一者監査と呼ばれる内部監査は，内部目的のために，その組織自身又はその組織に代わる者が実施するものである。

f) 適用範囲が引き続き適切であること，及び ISMS のプロセスにおける改善策を特定（7.1 参照）することを確実にするために，ISMS のマネジメントレビューを定期的に実施する。

g) 監視及びレビューの活動から見出された事項を考慮に入れるために，セキュリティ計画を更新する。

h) ISMS の有効性又はパフォーマンスに影響を及ぼす可能性のある活動及び事象を記録する（4.3.3 参照）。

（JIS Q 27001:2006　4.2.3 ISMS の監視及びレビュー　より引用）

組織は，常に次の事項を実行しなければならない。

a) 特定した改善策を ISMS に導入する。

b) 8.2 及び 8.3 に従った適切な是正処置及び予防処置をとる。自他の組織のセキュリティの経験から学んだものを適用する。

c) すべての利害関係者に，状況に合った適切な詳しさで，処置及び改善策を伝える。該当するときは，処置及び改善策の進め方について合意を得る。

d) 改善策が意図した目的を達成することを確実にする。

（JIS Q 27001:2006　4.2.4 ISMS の維持及び改善　より引用）

Check（点検）のフェーズでは、主にマネジメントレビューに必要なインプット情報の収集について規定されています。経営陣はマネジメントレビューを実施し、PDCA サイクルの前半部分「Plan（計画）～Do（実行）」で決定した手順に従いプロセスが実施されているか、また計画の段階で期待されている成果が上がっているか検証します。これは ISMS の維持や継続的な改善活動に必要不可欠な作業です。

マネジメントレビューのインプット情報として､監視の対象とすべき事項には以下のような例があります。

■処理の誤りや、セキュリティインシデントの記録
■セキュリティ活動の実施状況と管理策有効性の測定結果
■提案
■利害関係者からのフィードバック
■環境（社会的、技術的環境や法的規制、事業上の環境など）の変化
■内部監査からのフィードバック

ここに出てくる「提案」とは、JIS Q 27001:2006 の「7.2 レビューへのインプット）の
　i）改善のための提案
に該当します。

この i)が何を指すのか、JIS Q 27001:2006 では規定されていませんが、JIS Q 9001:2000 ではこれに相当するものが、「5.6.2 マネジメントレビューへのインプット」の中の
　g）改善のための提案
であり、さらにこの g）は「5.5.2 管理責任者」にある、以下の規定があることと関連して解釈されています。

> トップマネジメントは，管理層の中から管理責任者を任命すること。管理責任者は与えられている他の責任とかかわりなく次に示す責任及び権限をもつこと。
> b）品質マネジメントシステムの実施状況及び改善の必要性の有無についてトップマネジメントに報告する。
>
> （JIS Q 9001:2000　5.5.2 管理責任者　より引用）

つまり、g）の指す「提案」とは、組織内部からの提案を想定している、ということになりますので、JIS Q 27001:2006 でもそれに従い、「組織内部からの提案」と想定されます。

経営陣は､マネジメントレビューの結果として以下の事項について判断しなければいけません。

■ ISMS の有効性
■ 経営資源の割り当て
■ 残留リスク及び受容可能なリスクの水準

■ セキュリティ計画の見直し

ここで出てくるセキュリティ計画とは、リスク対応計画や是正計画、資源計画、教育計画などを含む、ISMS 構築に関連する様々な計画の総称として捉えることができます。

これらの活動については、ISMS 認証基準の「5　経営陣の責任」、「6　ISMS 内部監査」「7 ISMS のマネジメントレビュー」、「8　ISMS の改善」の章に詳細に規定されています。具体的内容については、本ガイドの「5.　経営陣の責任」以降の説明を参照して下さい。

４．５　文書化に関する要求事項

ISMS 認証基準は、ISMS の文書化について、下記を要求しています。

> 文書には，経営陣の決定に関する記録も含めなければならない。文書は，とった処置から，経営陣の決定及び方針へたどれること，並びに記録した結果が再現可能であることを確実にしなければならない。
>
> 選択した管理策からリスクアセスメント及びリスク対応のプロセスまで，更には ISMS 基本方針及び目的までにつながる関係を説明できることが重要である。
>
> （JIS Q 27001:2006　4.3 文書化に関する要求事項　4.3.1 一般　より引用）

ISMS の活動では、経営陣が決定した ISMS 基本方針及び目的に基づいて、リスクアセスメント及びリスク対応のプロセスを実施し、その結果によって管理策を選択します。

ISMS 認証基準では、管理策をリスクアセスメント及びリスク対応のプロセスの結果に基づき選択し、さらに、それらのプロセスが ISMS 基本方針及び目的に基づいて実施されていることを関連付けられるような文書の作成を求めています。

また、リスクアセスメントや有効性の測定の方法は、それを実施する人によって異なる方法となってしまっては結果を比較できず、情報セキュリティを効果的に管理することができません。

したがって、記録された結果が再現可能なことを確実にするために、文書化は重要になります。

また、定めた管理策について実施者がそのとおりに実施するように、手順を確立し明文化することが求められています。

> ISMS 文書には，次を含めなければならない。
>
> a) 文書化した ISMS 基本方針［4.2.1 b)参照］及び目的
>
> b) ISMS の適用範囲［4.2.1 a)参照］
>
> c) ISMS を支えている手順及び管理策
>
> d) リスクアセスメントの方法［4.2.1 c)参照］の記述
>
> e) リスクアセスメント報告［4.2.1 c)～4.2.1 g)参照］
>
> f) リスク対応計画［4.2.2 b)参照］
>
> g) 情報セキュリティのプロセスを有効に計画，運用及び管理することを確実にするために，組織が必要と

する文書化した手順。管理策の有効性をどう測定するか［4.2.2 d)参照］を記述するために，組織が必要とする文書化した手順。

h) この規格が要求する記録（4.3.3 参照）

i) 適用宣言書

注記 1 この規格で“文書化した手順”という用語を使う場合には，その手順を確立し，文書化し，実施し，かつ，維持していることを意味する。

注記 2 ISMS の文書化の程度は，次の理由から組織によって異なることがある。

－ 組織の規模及び活動の種類

－適用範囲，並びにセキュリティの要求事項及び運営管理するシステムの複雑さ

注記 3 文書・記録の様式及び媒体の種類は，どのようなものでもよい。

（JIS Q 27001:2006　4.3 文書化に関する要求事項　4.3.1 一般　より引用）

ISMS 認証基準では、「文書化した手順」として、明確に記載している部分が 5 ヶ所あります。

4.3.1g)	情報セキュリティのプロセスを有効に計画，運用及び管理することを確実にするために，組織が必要とする文書化した手順。管理策の有効性をどう測定するか［4.2.2 d）参照］を記述するために，組織が必要とする文書化した手順。
4.3.2	ISMS が要求する文書は，保護し，管理しなければならない。次の事項を行うのに必要な管理活動を定義するために，文書化した手順を確立しなければならない。
6	監査の計画・実施に関する責任及び要求事項，並びに結果報告・記録維持（4.3.3 参照）に関する責任及び要求事項を，文書化した手順の中で定義しなければならない。
8.2	組織は，ISMS の要求事項に対する不適合の原因を除去する処置を，その再発防止のためにとらなければならない。是正処置のために文書化された手順の中で，次のための要求事項を定義しなければならない。
8.3	組織は，ISMS の要求事項に対する不適合の発生を防止するために，起こり得る不適合の原因を除去する処置を決定しなければならない。とられる予防処置は，起こり得る問題の影響に見合ったものでなければならない。予防処置のために文書化された手順の中で，次のための要求事項を定義しなければならない。

（JIS Q 27001:2006　上記各項　より引用）

４．６　文書管理

ISMS 文書は、版管理され適切な文書を必要とする人が必要なときに使用可能な状態で管理されている必要があります。ISMS 文書の管理について、以下の点を盛り込んだ管理手順を確立し、文書管理する必要があります。

> ISMS が要求する文書は，保護し，管理しなければならない。次の事項を行うのに必要な管理活動を定義するために，文書化した手順を確立しなければならない。
>
> a) 適切かどうかの観点から，文書を発行前に承認する。
>
> b) 文書をレビューする。また，必要に応じて更新し，再承認する。
>
> c) 文書の改変を特定すること及び現在の改版状況を特定することを確実にする。
>
> d) 使用する必要があるとき，適用する文書の関連する版が使用可能であることを確実にする。
>
> e) 文書は読みやすく，かつ，容易に識別可能であることを確実にする。
>
> f) 文書を，それを必要とする者には利用可能にすることを確実にする。また，文書を，その分類区分に適用される手順に従って受け渡すこと，保管すること，及び最終的には処分することを確実にする。
>
> g) 外部で作成された文書であることの識別を確実にする。
>
> h) 文書配付の管理を確実にする。
>
> i) 廃止文書の誤使用を防止する。
>
> j) 廃止文書を何らかの目的で保持する場合には，適切な識別を施す。
>
> （JIS Q 27001:2006　4.3.2 文書管理　より引用）

４．７　記録の管理

記録は、組織の ISMS が要求事項へ適合していること及び運用の効果を示す証拠として作成、維持、管理します。

PDCA プロセス全般における活動の記録、管理策の実施状況の記録、及び ISMS に関連する全てのセキュリティインシデントの発生に関する記録を維持することが要求されます。

記録の管理として、以下の事項の実施が求められます。

- **識別、保管、保護、検索、保管期間及び廃棄に関して必要な管理を文書化すること**
- **運営管理プロセスで記録の必要性及び記録の範囲を定めること**
- **法律等によって保管期間が定められている場合には、法的要求事項に適合した保存期間を決定すること**

ISMS 認証基準の附属書 A「A.15　順守」に、以下のような管理策があることにも留意する必要があります。

A.15.1.3	組織の記録の保護	重要な記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊及び改ざんから保護しなければならない。

（JIS Q 27001:2006　附属書 A（規定）A.15.1　法的要求事項の順守　より引用）

４まとめ

本章では医療機関における情報セキュリティマネジメント（ISMS）の実践として PDCA サイクルの P（計画：ISMS の確立）の部分を中心に医療機関向けの事例とともに解説してきました。何事も始めが肝心であり、また計画・準備をしっかり行えばそれだけ実効性の高い ISMS の構築が可能となります。

さらに確立したあとで、それらを実施（Do）し、有効性を確認（Check）しながら、常に見直しと改善（Act）を繰り返すことも重要です。医療でも治療計画、看護計画を立てたあとで、計画の実施段階では日々の観察をすることで患者の状態の変化を発見し、それに合わせて治療や看護方法を変えるのと同様、日々の情報処理の状況、IT 環境の変化に合わせて、構築した ISMS の見直しと継続的な改善をしてください。

５．経営陣の責任

本ガイドの「4 情報セキュリティマネジメントシステム」では、ISMS を確立、導入、運用、監視、レビュー、維持及び改善するために重要な要求事項について説明しました。ISMS 認証基準の「5　経営陣の責任」では、その活動における経営陣の役割をより詳細に規定していますので、本章では視点を変えて、改めて説明します。

医療法人等の医療機関における経営陣として、医療法人全体の運営について責任をもつ理事長が考えられます。また、ISMS の対象を医療法人におけるある病院だけを考える場合には病院長、ある部門だけを考える場合には、外科部長、看護部長などが考えられます。

ISMS の活動のあらゆる段階において、様々な活動が確実に実施されていることについて、経営陣の果たすべき役割は非常に重要です。ISMS の対象を医療機関全体ではなく、ある医院、又は部門とし、マネジメントの対象を限定する場合も多いと思われますが、その時でも、医療機関全体としてのマネジメントを意識することが重要です。

典型的な組織のマネジメントは、図 5-1 のように階層構造を持ち、下位組織階層のマネジメントシステムは上位組織階層のマネジメントシステムと協調して活動します。

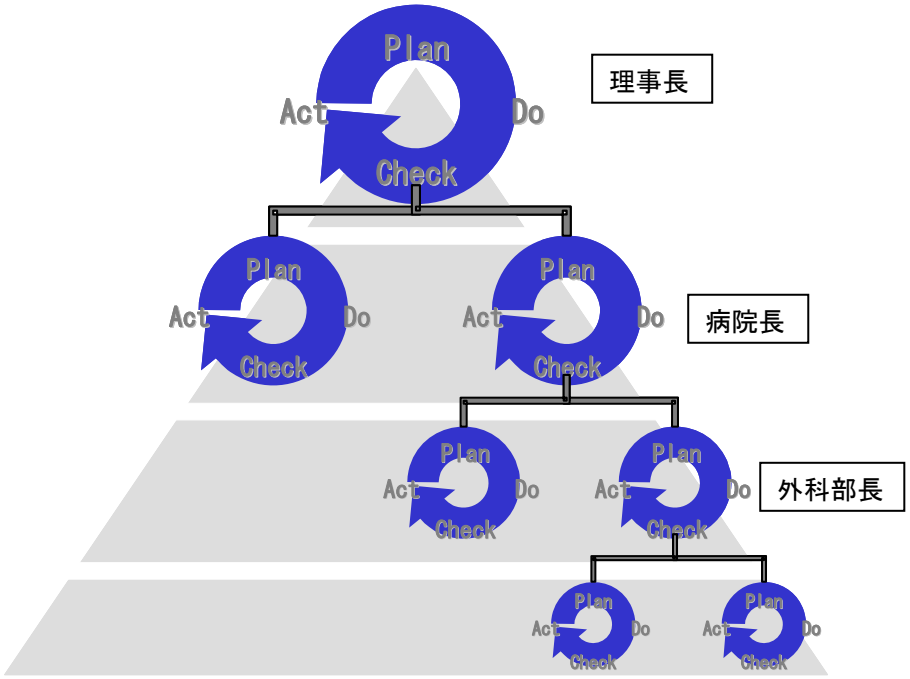


図 5-1　医療法人を例にしたマネジメントシステム

ISMS の構築の初期段階においては、適用範囲を例えば、特定の病院や部門などに限定し、特にリスクの大きい領域への対策を優先することに注力することもあります。しかし、経営陣はその場合においても前述のマネジメントシステム間の連携を認識し、最終的に想定したゴールに導く責任を負います。

５．１　経営陣のコミットメント

経営陣の果たすべく重要な役割のひとつにコミットメントがあります。ISMS の確立、導入、運用及び維持等に関与し、組織として情報セキュリティの実施責任を利害関係者に宣言する「コミットメント」は、執行権限を有する経営陣にのみ実施する事が許されるからです。

ISMS 認証基準では、経営陣のコミットメントを次のように規定しています。

> 経営陣は，ISMS の確立，導入，運用，監視，レビュー，維持，及び改善に対する自らのコミットメントの証拠を，次によって提供しなければならない。
>
> a) ISMS 基本方針を確立する。
>
> b) ISMS の目的及び計画の確立を確実にする。
>
> c) 情報セキュリティのための役割及び責任を確立する。
>
> d) 組織に，次を伝える。
>
> －情報セキュリティ目的を満たすことの重要性
>
> －情報セキュリティ基本方針に適合することの重要性
>
> －法のもとでの責任
>
> －継続的改善の必要性
>
> e) ISMS の確立，導入，運用，監視，レビュー，維持及び改善のために十分な経営資源を提供する（5.2.1 参照）。
>
> f) リスク受容基準及びリスクの受容可能レベルを決定する。
>
> g) ISMS 内部監査の実施を確実にする（箇条 6 参照）。
>
> h) ISMS のマネジメントレビューを実施する（箇条 7 参照）。
>
> （JIS Q 27001:2006　5.1 経営陣のコミットメント　より引用）

経営陣は、どの程度の水準でリスクを受容するのかを判断します。これは、経営陣が ISMS の確立、導入、運用及び維持等に最終的な責任を負っているからです。しかし、経営陣は、組織のマネジメントシステムに責任を持ちますが、全ての活動に関与することは不可能です。

そこで、経営陣は、まず ISMS の方向性を示す ISMS 基本方針を確立します。ISMS 基本方針については、「4.2.2　STEP2　ISMS の基本方針を定義する」で説明されていますので参考にして下さい。

次に、ISMS の目的を設定し、ISMS の実践のための計画が策定されることを明確に指示し、確実に実施されることに責任を負います。

また、ISMS の実効性を担保するために、医療機関における情報セキュリティ上の役割及び責任を定め、ISMS の確立、導入、運用及び維持等に十分な経営資源を提供しなければなりません。このことについては、後述の「5.2　経営資源の運用管理」で説明します。

最終的に経営陣は、構築した ISMS が意図した通り有効に機能していることを自身が ISMS 内部監査等を通じて把握し、改善のための意思決定等を行うためにマネジメントレビューを実施することが重要となります。このことについては、「6. ISMS 内部監査」及び「7.マネジメントレビュー」で説明します。

５．２　経営資源の運用管理

５.２.１　経営資源の提供

経営陣の重要な役割の一つとして、「人」、「物」、「金」といった経営資源の提供があります。経営陣は、ISMS の必要性を理解し、そのために必要な経営資源の提供を行わなければなりません。ISMS 認証基準では、経営資源の提供を次のように規定しています。

> 組織は，次の事項を行うのに必要な経営資源を決定し，提供しなければならない。
>
> a) ISMS を確立，導入，運用，監視，レビュー，維持及び改善する。
>
> b) 事業上の要求事項を満たすことに，情報セキュリティの手順が寄与することを確実にする。
>
> c) 法令及び規制の要求事項並びに契約上のセキュリティ義務を明確にし，これを扱う。
>
> d) 導入したすべての管理策を正確に適用することによって，十分なセキュリティを維持する。
>
> e) 必要に応じてレビューし，レビューの結果に対して適切に対応する。
>
> f) 必要な場合には，ISMS の有効性を改善する。
>
> （JIS Q 27001:2006　5.2 経営資源の運用管理　より引用）

経営陣の掛け声だけでは、ISMS の確立、導入、運用及び維持等は難しいと思われます。ISMS の構築に必要な一連のプロセスには経営資源の割り当てが必要となります。

５．２．２ 教育・訓練、認識及び力量

経営資源の中でも「人」の問題は特に重要です。

ISMS 認証基準では、「人」に関連する教育・訓練、認識および力量を次の 4 つの事項を挙げて説明しています。

> 組織は，ISMS に定義された責任を割り当てた要員すべてが，要求された職務を実施する力量をもつことを，次の事項によって確実にしなければならない。
>
> a) ISMS に影響がある業務に従事する要員に必要な力量を決定する。
>
> b) 必要な力量がもてるように教育・訓練するか，又は他の処置（例えば，適格な要員の雇用）をとる。
>
> c) とった処置の有効性を評価する。
>
> d) 教育，訓練，技能，経験及び資格についての記録を維持する(4.3.3 参照)。
>
> 組織は，また，関連する要員すべてが，自らの情報セキュリティについての活動がもつ意味と重要性とを認識し，ISMS の目的の達成に向けて，自分はどのように貢献できるか認識することを確実にしなければならない。
>
> （JIS Q 27001:2006　5.2 経営資源の運用管理　より引用）

ISMS の確立、導入、運用及び維持等を行っているのは、人であるということを忘れてはなりません。組織の各個人が情報セキュリティに関連する責任を果たし、期待される役割を実行するためには、本人の力量が伴わなければならないことは明らかです。

経営陣には、明確にされた役割を割り当てられた要員全てが、要求される業務を実施する力量を持つことを確実にするために、教育・訓練を実施させる責任があります。また、実施する教育・訓練の内容は、全ての要員が自らの情報セキュリティについての活動の意味とその重要性を認識し、ISMS の目的の達成に向けてどのように貢献できるかを認識できるようなものが理想です。

実施した教育・訓練については、その有効性を評価し、力量を持った要員の確保に役立てることが重要です。必要とされる力量は、それぞれの業務により異なることになります。ISMS の確立、導入、運用及び維持等のために必要となる力量としては、表 5-1 のような分野が考えられます。

表 5-1　力量の分野

マネジメントに関連する力量	マネジメント論全般、リーダシップなど
監査に関連する力量	監査理論全般、監査の実務
セキュリティ技術に関連する力量	ネットワークセキュリティ、サーバアプリケーションセキュリティ、OS セキュリティ、ファイアウォール、侵入検知システム、ウィルス、セキュアプログラミング、暗号などに関する理論や実践

これらの力量を適切に定義し、その達成度を確認することが重要となります。

また、この力量の有無を検討する一つの目安として、資格制度を利用することも有益と思われます。それぞれの力量と関連する資格の例としては表 5-2 のような資格、試験合格者が考えられます。

表 5-2　力量と関連する資格

内部監査	公認内部監査人(CIA)[3]、公認会計士、公認システム監査人[4]、システム監査技術者[5]、公認情報システム監査人(CISA)[6]、ISMS 主任審査員、ISMS 審査員、公認情報セキュリティ監査人（CAIS）[7]
セキュリティ技術	情報セキュリティアドミニストレータ、上級システムアドミニストレータ、テクニカルエンジニア（情報セキュリティ）[8]、公認情報セキュリティ管理者(CISM)[9]、公認情報システムセキュリティ専門家(CISSP)、公認システムセキュリティ熟練者(SSCP)[10]

[3] 公認内部監査人（Certified internal Auditor）は内部監査人協会（The Institute of Internal Auditors,Inc.(IIA) http://www.theiia.org）が認定する内部監査人の資格。内部監査人協会は 1941 年に米国で設立され、2006 年現在、全世界で 122,000 名が内部監査人協会に所属している。

[4] 公認システム監査人は特定非営利活動法人日本システム監査人協会（http://www.saaj.or.jp）が認定するシステム監査人の資格。

[5]独立行政法人情報処理推進機構により行われている、システム監査技術を有していることを認定するための国家試験。

[6] 公認情報システム監査人は、情報システムコントロール協会（Information Systems Audit and Control Association　http://www.isaca.org）により認定されるシステム監査人の資格。情報システムコントロール協会は 1967 年に米国で設立され、2006 年現在全世界で約 50,000 名が協会に所属している。

[7] 公認情報セキュリティ監査人は、特定非営利法人日本セキュリティ監査協会により認定される情報セキュリティ監査人の資格

[8]情報セキュリティアドミニストレータ、上級システムアドミニストレータ、テクニカルエンジニア（情報セキュリティ）は独立行政法人情報処理推進機構により行われている、情報セキュリティ管理、システム管理、情報セキュリティについての一定の専門的知識・能力を有していることを検定するための国家試験。

[9] 公認情報セキュリティ管理者（Certified information security manager）は、情報システムコントロール協会（Information Systems Audit and Control Association　http://www.isaca.org）により認定されるセキュリティ管理者としての専門的能力を有していることを証明する資格。

[10] 公認情報システムセキュリティ専門家（Certified information system security professional）、公認システムセキュリティ熟練者（System security certified practitioner）は(ISC)^2（International Information Systems Security

また、情報セキュリティについての業務毎に必要とされる力量を決定する際に、経済産業省が発表している情報セキュリティ教育についての報告書[11]や、独立行政法人情報処理振興事業協会（IPA）が発表しているセキュリティスキル標準[12]、スキルマップ[13]についての報告書[14]などを参考にされるとよいと思われます。

また、医療情報の管理については、診療情報管理士をはじめ、様々な有用と思われる資格があります。患者の権利利益の保護のため、また、個人情報保護法の成立により、患者の診療情報の適正な管理が今後ますます重要となります。

Certification Consortium http://www.isc2.org）により認定される情報セキュリティについての専門的能力を有していることを保証する資格。

[11] http://www.meti.go.jp/policy/netsecurity/edu_report.html

[12] http://www.jitec.jp/1_17skill/skill_00.html

[13] http://www.ipa.go.jp/security/manager/edu/training/expert.html

[14] http://www.ipa.go.jp/security/fy14/reports/professional/sec-pro-outline.pdf

６．ISMS 内部監査

マネジメントレビューのインプットの重要なものとして、内部監査の結果があります。ISMS 認証基準では、内部監査についてより詳細に規定しています。

内部監査は、ISMS の管理目的、管理策、プロセス及び手順が次の事項を満たしているか否かを判断するために実施されます。

組織は，その ISMS の管理目的，管理策，プロセス及び手順について，次の事項を判断にするために，あらかじめ定めた間隔で ISMS 内部監査を実施しなければならない。

a) この規格及び関連する法令又は規制の要求事項に適合しているかどうか。

b) 特定された情報セキュリティ要求事項に適合しているかどうか。

c) 有効に実施され，維持されているかどうか。

d) 期待したように実施されているかどうか。

組織は，監査の対象となるプロセス及び領域の状況及び重要性，並びに前回までの監査結果を考慮して，監査プログラムを策定しなければならない。監査の基準，範囲，頻度及び方法を定義しなければならない。

監査員の選定及び監査の実施においては，監査プロセスの客観性及び公平性を確実にしなければならない。

監査員は，自らの仕事を監査してはならない。

監査の計画・実施に関する責任及び要求事項，並びに結果報告・記録維持（4.3.3 参照）に関する責任及び要求事項を，文書化した手順の中で定義しなければならない。

監査された領域に責任をもつ管理者は，発見された不適合及びその原因を除去するために遅滞なく処置がとられることを確実にしなければならない。フォローアップには，とった処置の検証及び検証結果の報告を含めなければならない（箇条 8 参照）。

注記 JIS Q 19011:2003 は，ISMS 内部監査の実施のための有益な手引となる場合がある。

（JIS Q 27001:2006　6 ISMS 内部監査　より引用）

ISMS の認証を取得するためには、ISMS 認証基準に準拠していることが求められますが、それと同時に法令を順守することも当然に求められます。

ISMS に関連する法律としては、個人情報保護法（地方公共団体の医療機関の場合はそれぞれの地域の個人情報保護条例）、建築基準法、消防法、医師法、看護師法などがあります。

また、医療機関に関連する各種規制事項、取引先との契約事項などにも適合している必要があります。

ISMS 内部監査では、ISMS が有効に実施され、維持されていること、期待通りに実施されていることを確認することが求められています。

ISMS 内部監査は計画的に実施される必要があり、監査員は、監査の対象となる管理目的、管理策、プロセス及び手順の状況と重要性、並びにこれまでの監査結果を考慮して監査プロ

グラムを策定します。監査の実施にあたり、監査のための評価基準、対象範囲、頻度及び方法を定義しなければなりません。

監査員の選定においては、監査プロセスの客観性及び公平性を確保しなければなりません。

監査員の選定について重要な点は、監査員にはセキュリティの運用者、管理者とは異なる力量が求められると言うことです。例えば、監査員には以下に示すように監査に関連する一連のプロセスを実施する力量が求められます。

- **監査の計画及び実施**
- **結果の報告**
- **是正及び予防処置の提案　等**

また、組織は上記のような監査員に関する責任並びに監査に関連する一連のプロセスを、文書化された手順の中で規定することが求められます。

要求する力量をもった監査員を組織内に確保することが困難な場合には、外部の監査員の利用も考えられます。なお、客観性を確保するためにも、自らの業務を監査することはできません。

監査を受けたプロセス等に責任をもつ管理者は、発見された不適合及びその原因を除去するための処置が遅滞無く確実に講じられるようにしなければなりません。これは、不適合となっている部分をすぐに改善しなければならないという事ではありません。また、実施した改善活動には、講じた処置の検証及び検証結果の報告を含めなければなりません。

ISMS についての内部監査は、ガバナンスの視点から考えると、医療機関全体の経営監査の内部監査の一部として、あるいは連携して実施することが効果的です。また、監査の実施にあたっては、「品質及び／又は環境マネジメントシステム監査のための指針」である JIS Q 19011：2003 を参考にすると良いでしょう。

また、情報セキュリティ監査制度、システム監査制度を利用し、専門家に内部監査の実施を依頼することも考えられます。

医療機関においては、今まであまり経営全体としての内部監査が行われていなかったかもしれません。しかしながら、厚生労働省発行の「医療情報システムの安全管理に関するガイドライン第１版(2005.3)」から、監査することが記載されています。この領域に対して監査を実施することを起点にして、内部監査の組織を構築・整備していくことも可能でしょう。ISMS の運用を実施していく中で、内部監査についても継続的な改善を行い、最終的には、医療機関全体の経営監査の一環としての ISMS の内部監査が実施できればよいのではないでしょうか。

７．ISMS のマネジメントレビュー

７．１　一般

病院長、理事長、又はそれらの者から情報セキュリティマネジメントの運用責任を委任された者（以下、医療機関の経営陣）の責任として、マネジメントレビューの実施が重要であることは 5.1 項で触れましたが、このマネジメントレビューは、ISMS を維持し、今後の活動を効果的に実施するために必要な活動です。これは、PDCA サイクルにおける「Check-点検」のプロセスの一部と言えます。ISMS が意図した通り有効に機能していることを医療機関の経営陣自身が把握し、改善のための意思決定等を行います。

マネジメントレビューとは、医療機関の経営陣が ISMS の効果を把握し、改善のための意思決定をする一連のプロセスです。ISMS のマネジメントレビューは、1 年以内の予め定められた間隔で実施しなければなりません。

マネジメントレビューでは、ISMS に対する改善の機会の評価、情報セキュリティ基本方針及び目的を含む ISMS の変更の必要性に関する評価も実施することになります。また、マネジメントレビューの結果は、記録として維持されていることが必要です。

７．２　マネジメントレビューへのインプット

マネジメントレビューのためのインプット情報として、ISMS 認証基準では次のものを挙げています。

> 7.2 レビューへのインプット
> 次の情報を，マネジメントレビューに対して提供しなければならない。
> a) ISMS 監査及びレビューの結果
> b) 利害関係者からのフィードバック
> c) ISMS のパフォーマンス及び有効性を改善するために組織の中で利用可能な技術，製品又は手順
> d) 予防処置及び是正処置の状況
> e) 前回までのリスクアセスメントが十分に取り上げていなかったぜい弱性又は脅威
> f) 有効性測定の結果
> g) 前回までのマネジメントレビューの結果に対するフォローアップ
> h) ISMS に影響を及ぼす可能性がある，あらゆる変化
> i) 改善のための提案
>
> （JIS Q 27001:2006　7.2 レビューへのインプット　より引用）

マネジメントレビューへのインプットとして具体的には次のようなものが挙げられます。

- **内部監査や外部監査の結果（例えば、審査登録機関による不適合の指摘や観察事項など）**
- **患者、取引先、職員などの利害関係者、及び行政機関からのフィードバック**
- **新たに利用可能となった技術、ベンダー等が発表した新製品・新サービスに関する情報**
- **実施した予防処置及び是正処置の実施状況及びその効果**
- **過去において、予算上、環境上、法令上の制約等で取り扱わなかった、ぜい弱性又は脅威などに対するリスクアセスメントの見直しの必要性の判断**
- **管理策または一群の管理策に対して、有効性を測定するための測定表などを用いて測定したことによって把握できた内容（本ガイドの 9.3.1 を参照）**
- **過去のマネジメントレビューの結果に適切に対応したかどうかについてのフォローアップの状況等についての報告**
- **経営環境の変化（法改正等）、組織の変化などを含む ISMS に影響を及ぼす可能性のある全ての組織内外の変化**
- **情報セキュリティに関連するヒヤリ・ハット事例（ISMS の対象となる医療機関、その他の医療機関のもの）**

特に、ヒヤリ・ハットによる現場レベルの改善が多くの医療機関において行われています。リスクマネージャは、医療機関の経営陣にヒヤリ・ハットを集積・分析し、改善策を実施し、その有効性・妥当性を報告していることも多いでしょう。ヒヤリ・ハットの事例は医療過誤に関するものがそのほとんどと思われますが、これらの事例に加え情報セキュリティに関連するリスクを洗い出し、マネジメントレビューにつなげていくことを ISMS では要求しています。

また、病院機能評価を行っている医療機関では、評価項目（チェック項目）に情報管理という項目があります。ISMS のマネジメントレビューを実施していることをもって、情報管理が適切になされていると説明ができるものと考えられます。

７．３　マネジメントレビューからのアウトプット

医療機関の経営陣は、インプットされた情報に基づいて経営的な判断、つまり経営の意思決定を行わなければなりません。その際の意思決定のポイントつまりマネジメントレビューからのアウトプットとして、ISMS 認証基準では次の 3 つの事項を挙げています。

> 7.3 レビューからのアウトプット
>
> マネジメントレビューからのアウトプットには，次に関係する決定及び処置を含めなければならない。
>
> a) ISMS の有効性の改善
>
> b) リスクアセスメント及びリスク対応計画の更新
>
> c) ISMS に影響を与える可能性がある内外の事象に対応するために，必要に応じた，情報セキュリティを実現する手順及び管理策の修正。
>
> d) 必要となる経営資源
>
> e) 管理策の有効性測定方法の改善
>
> （JIS Q 27001:2006　7.3 レビューからのアウトプット　より引用）

上記 a)について、医療機関の経営陣は、マネジメントレビューのアウトプットとして、現状の ISMS をより効果的なものにするための改善を示さなければなりません。

上記 c)について、ISMS の内部、外部環境が変化している場合は、環境変化に対応して情報セキュリティを実現する手順を修正しなければなりません。この内部、外部の環境には次のようなものが含まれます。

> c) ISMS に影響を与える可能性がある内外の事象に対応するために，必要に応じた，情報セキュリティを実現する手順及び管理策の修正。そのような事象には，次について起きた変化が含まれる。
>
> 1) 事業上の要求事項
> 2) セキュリティ要求事項
> 3) 現在の事業上の要求事項を実現する業務プロセス
> 4) 法令又は規制の要求事項
> 5) 契約上の義務
> 6) リスクのレベル及び／又はリスク受容基準
>
> （JIS Q 27001:2006　7.3 レビューからのアウトプット　より引用）

医療機関においては、電子カルテシステムの導入が進められているところも多いでしょう。このような場合、新しいシステムの導入に伴い、情報システムや業務プロセスが変更され、医療機関におけるリスクが変化します。したがって、このような 1）事業ドメインの重要性に変化が生じた場合及び 3）業務プロセスに変更が行われた場合は、現在実施されている情報セキュリティ対策が引き続き適切であることを確認しなければなりません。

4）新たな法令の施行、既存の法令の改正、規制の新設、改正が行われている場合、現在のプロセスが引き続き法令等に準拠していることを確認することは重要です。特に最近は、IT 関連の法令、個人情報保護法の施行及びガイドラインの公表など、改正が頻繁に行なわれており、注意が必要です。

5）他者との関係を持つ業務では、その相手方と締結した契約上の義務についても順守しなければなりません。これについては相手方が個別に求めてくるものですので、その内容を個々に確認することが必要です。また、求められる実施事項が具体的になっていない場合には、相手方に対して何を持って義務を果たしたことになるのかなどを確認しておくことが必要です。

2）や 6）に関しても注意が必要です。情報技術の進歩は著しく、それに伴って新たな脅威（例えば、新しい攻撃手法の出現）が生じたり、新たなぜい弱性（例えば、新たなオペレーティングシステムやアプリケーションシステムのぜい弱性）が発見されたりします。また、既存の対応策に関するぜい弱性が変化し、リスクの度合いが変化することもあります。このような環境変化に対応して情報セキュリティを実現する手順を修正することが重要です。とりわけ、医療機関においては、個人情報の漏えいや情報システムの停止につながる悪意のあるソフトウェア（たとえば、コンピュータウィルスやワームなど）から、システムを守らなくてはなりません。情報システムに対する脅威情報やぜい弱性情報の収集分析、及び新しい脅威やぜい弱性に適時の対応が重要となります。

医療機関の経営陣は、マネジメントレビューを通じて必要と認識された、ISMS の改善のために必要となる経営資源の提供についても確約する必要があります。改善に必要な経営資源の提供が確約されなければ、改善の実施は達成されないからです。医療機関の組織形態により、会計年度途中での新たな投資が困難な場合が想定されます。たとえば既存の電子カルテシステムに対して、重要なぜい弱性が発見され、緊急の対応を行う必要に迫られる場合も想定されます。現在はなくても今後、その可能性が高まることは十分に予想されます。したがって、情報システム等に対する予算については、ある程度、弾力的に運用できるようにすることが望ましいといえます。

８．ISMS の改善

８．１　継続的改善

情報セキュリティの継続的な改善に病院長、理事長、又はそれらの者から情報セキュリティマネジメントの運用責任を委任された者（以下、医療機関の経営陣）が責任を持つことにより、セキュリティ対策が確実に実施され組織の ISMS の水準も継続して向上することが期待できます。

情報セキュリティ基本方針及び目的、監査結果、監視した事象の分析、是正処置、予防処置及びマネジメントレビューのアウトプットを通じて、ISMS の有効性を継続的に改善することが重要です。

改善には是正処置、予防処置の 2 つがあり、以下ではこれらについて説明します。

８．１．１　是正処置

監査やマネジメントレビューの結果等により ISMS の導入及び運用に関連する不適合が発見された場合､不適合の原因を除去するための処置及び再発防止のための処置を講じなければなりません。これを「是正処置」といいます。

この是正処置には、ISMS 認証基準で規定している次の事項を含む手順を文書化することが必要です。

> 組織は，ISMS の要求事項に対する不適合の原因を除去する処置を，その再発防止のためにとらなければならない。是正処置のために文書化された手順の中で，次のための要求事項を定義しなければならない。
>
> a) 不適合の特定
>
> b) 不適合の原因の決定
>
> c) 不適合の再発防止を確実にするための処置の必要性の評価
>
> d) 必要な是正処置の決定及び実施
>
> e) とった処置の結果の記録（4.3.3 参照）
>
> f) とった是正処置のレビュー
>
> （JIS Q 27001:2006　8.2 是正処置　より引用）

医療機関において、個人情報の漏えい、情報や情報システムの取扱いのミスによる問題は大きな社会問題にまで広がる恐れがあります。万が一、事故を起こしてしまった場合は、事

故究明の際、情報システムに対する脅威やぜい弱性を再評価し、再発防止を確実にしていくことが重要になってきます。

８．１．２　予防処置

起こり得る不適合を早期に発見し、処置を講じることを「予防処置」といいます。ISMS 認証基準 4.2.3 d)で示したリスクの変化に着目して、組織は予防処置についての要求事項を特定する仕組みを持つ必要があります。そのため、マネジメントレビューを通じてリスクアセスメントの結果に基づく優先順位で、予防処置が取られるよう留意することが求められます。

この予防処置には、ISMS 認証基準で規定している次の事項を含む手順を文書化することが必要です。

> 組織は，ISMS の要求事項に対する不適合の発生を防止するために，起こり得る不適合の原因を除去する処置を決定しなければならない。とられる予防処置は，起こり得る問題の影響に見合ったものでなければならない。予防処置のために文書化された手順の中で，次のための要求事項を定義しなければならない。
>
> a) 起こり得る不適合及びその原因の特定
>
> b) 不適合の発生を予防するための処置の必要性の評価
>
> c) 必要な予防処置の決定及び実施
>
> d) とった処置の結果の記録（4.3.3 参照）
>
> e) とった予防処置のレビュー
>
> 組織は，変化したリスクを特定し，大きく変化したリスクに注意を向けて，予防処置についての要求事項を特定しなければならない。
>
> 予防処置の優先順位は，リスクアセスメントの結果に基づいて決定しなければならない。
>
> 注記　不適合を予防するための処置は，多くの場合，是正処置よりも費用対効果が大きい。
>
> （JIS Q 27001:2006　8.3 予防処置　より引用）

これまでも述べたように多くの医療機関において、日常診療の現場で、“ヒヤリ”としたり、“ハッ”とした経験を有する事例を収集して、ヒヤリ・ハット事例として分析し、改善、とりわけ予防処置として対応されていることでしょう。これらの事例（インシデント）のなかに情報セキュリティに関連するものも含め、分析、改善に努めていくことは、今後、電子カルテシステムなどを導入し、効果的に利用する際、不可欠になってきます。リスクマネージャ等は、これらのことを考慮して対応していくことが予防処置でも重要です。

明確なことは、不適合が起こってから改善する「是正処置」より、起こらないように未然に防止する「予防処置」を講じる方が望ましいのは言うまでもありません。多くの場合、是

正処置よりも予防処置の方が費用対効果も高いと言われています。

予防処置には、起こり得る不適合や原因の早期発見が重要です。組織の ISMS 構築にあたり、変化したリスクを特定し、大きく変化したリスクに注意を向けて要求事項を特定する機能がマネジメントプロセスに組み込まれており、マネジメントレビューを通じてリスクアセスメントの結果に基づいた優先順位で予防処置が取られるよう留意することが求められます。

９．有効性の測定

本章では、ISMS の有効性の測定について検討していきます。ISMS の有効性を測定することは、構築した ISMS を形骸化させることなく、継続的な改善を実施する上で有用です。

９．１　有効性測定の目的

ISMS 認証基準では、ISMS 全体及び個々の管理策について、有効性を測定することを明確化しています。有効性の測定結果を、ISMS の継続的な改善の機会と捉え、適切な行動をとることを促し、組織固有のセキュリティ目的及び事業（業務）目的を達成する管理策を確実にすることは重要な意味を持ちます。このことは、有効性測定を図 9-1 を基に考えるとより明確になります。

マネジメントシステムにおいては、個々のプロセスが要求される事項や期待を満たしていることを確実にするために、必要な PDCA を構築し、アウトプットの妥当性や有効性を測定し、測定結果をプロセスの管理責任者にフィードバックさせる機能を有することが求められています。

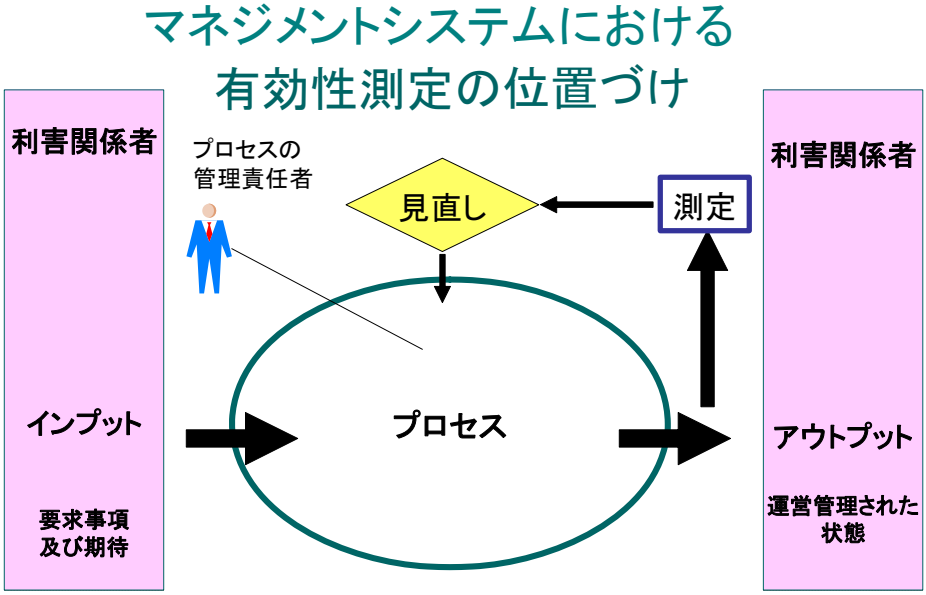


図 9-1　マネジメントシステムにおけるプロセスの有効性測定の位置づけ

上図では、要求事項、期待を含むインプットに対し、それらに応答するためのプロセス及びプロセスからのアウトプットの有効性測定を行い、適時、プロセスの管理責任者にフィードバックをしていることを示しています。

この図のプロセスを一連の ISMS の活動としたとき、図中の「測定」は ISMS 全体の有効性について測定することになります。

他方、一連の ISMS の活動は、複数のプロセスから構成されていると捉えることも可能です。従って、下図のように、複数のプロセスの有効性の測定結果から、全体として、ISMS の有効性を図ることも可能です。

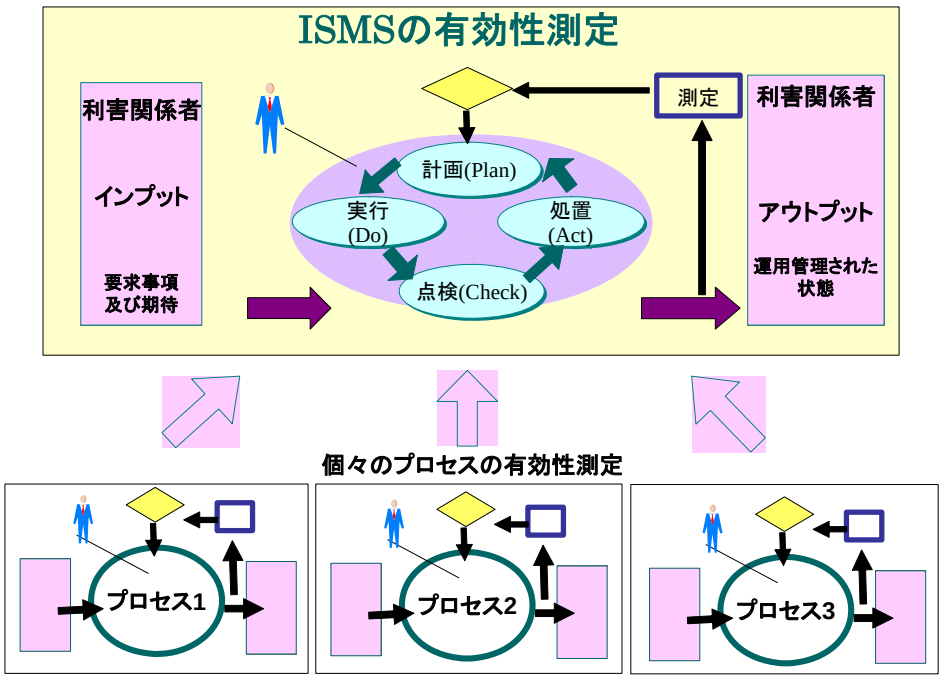


図 9-2　ISMS の有効性測定

個々のプロセスの有効性を測定する場合などは、そのプロセスに導入した管理策または一群の管理策の有効性を測定し、プロセス全体の有効性を把握するのに役立ちます。特に、一連のプロセスが複雑な場合、測定可能な個々のプロセスに分けて、各々の結果からプロセス全体の有効性を把握することは効果的な手法です。

ISMS 認証基準では、有効性の測定について ISMS 全体と管理策の有効性の 2 つのレベルについて規定しています。

ISMS 全体の有効性としては、以下のように規定しています。

8　ISMS の改善
8.1　継続的改善
組織は，情報セキュリティの基本方針及び目的，監査結果，監視した事象の分析，是正及び予防の処置，並びにマネジメントレビューを利用して，ISMS の有効性を継続的に改善しなければならない。

（JIS Q 27001:2006　8.1 継続的改善　より引用）

また、管理策の有効性については以下のように規定しています。

> 4.2.2 ISMS の導入及び運用
> d) 選択した管理策又は一群の管理策の有効性をどのように測定するかを定義し，また，比較可能で再現可能な結果を生み出すための管理策の有効性のアセスメントを行うために，それらの測定をどのように利用するかを規定する(4.2.3c)参照)。
>
> (JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用)

ISMS 全体及び管理策の有効性を混在させた形では、以下のように規定しています。

> 4.2.3 ISMS の監視及びレビュー
> b) ISMS の有効性について定期的にレビューする。これには，ISMS 基本方針及び目的を満たしていることのレビューとセキュリティ管理策のレビューとがある。このレビューでは，セキュリティ監査の結果，インシデント，有効性測定の結果，提案，及びすべての利害関係者からのフィードバックを考慮する。
>
> (JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用)

これらの目的については、以下のように考えることができます。

- ISMS 全体の有効性の測定は、構築した ISMS が ISMS 基本方針及び目的を満たしていることを確実にするために実施する。
  - ISMS 全体の有効性の測定は、セキュリティリ監査の結果、インシデント、有効性測定の結果、提案、及び利害関係者からのフィードバックを考慮する。
- 管理策又は一群の管理策の有効性の測定結果は、最終的には ISMS の有効性の測定のためであり、ISMS 全体の継続的な改善のために活用する。

（注記１）有効性測定に関しては、ISMS 認証基準では「管理策又は一群の管理策の有効性測定」が要求事項となっています。(JIS Q 27001:2006 4.2.2 d) 参照)
（注記２）ISMS 全体については、ISMS 認証基準では「ISMS 全体の有効性のレビュー」が要求事項となっており、「ISMS 全体の有効性測定」は要求事項となっていませんが、適用可能ならば測定することが提案されています。(JIS Q 27001:2006 0.2.2 プロセスアプローチ点検より参照)

９．２　有効性測定のプロセス

ここでは、有効性を測定することについて、説明します。
有効性の測定もひとつのプロセスと考えることができますから、プロセスアプローチの考

え方を適用すると図 9-3 のようになります。

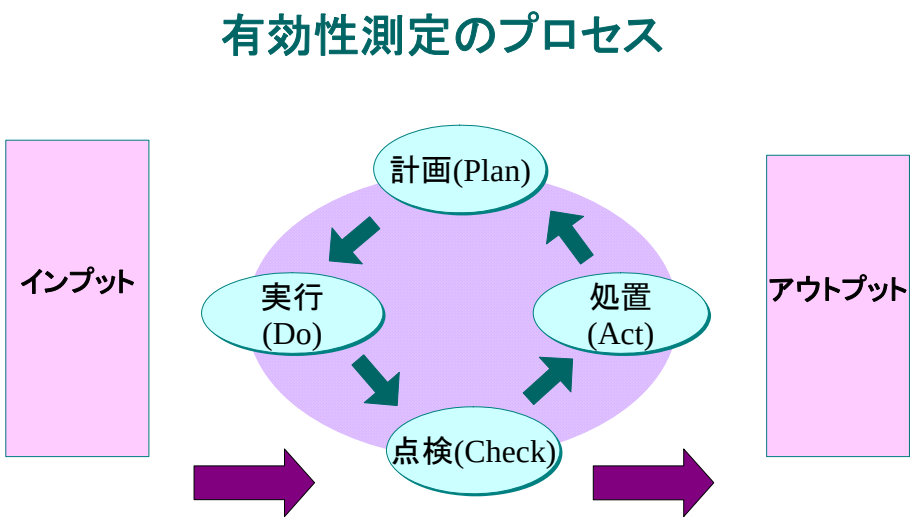


図 9-3　有効性測定のプロセス

図中の PDCA は、どのように有効性を測定するかを計画し、実行し、その結果について点検し必要に応じ、測定方法を見直すことを示しています。図中のインプットは、有効性測定をする上で考慮しなければならない事項であり、アウトプットは測定結果として捉えることができます。

９．３　有効性測定の PDCA

９．３．１ 計画（Plan）

（１）ISMS 全体の有効性測定（ISMS 認証基準では有効性のレビュー）に関する計画

まず ISMS 全体の有効性測定のインプットとして、ISMS 認証基準では以下のように規定しています。

4.2.3 ISMS の監視及びレビュー b) ISMS の有効性について定期的にレビューする。これには，ISMS 基本方針及び目的を満たしていることのレビューとセキュリティ管理策のレビューとがある。このレビューでは，セキュリティ監査の結果，インシデント，有効性測定の結果，提案，及びすべての利害関係者からのフィードバックを考慮する。 （JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

インプットとしては、

・ISMS 基本方針及び目的
・セキュリティ監査の結果
・インシデント
・有効性測定の結果
・提案
・利害関係者からのフィードバック

などが挙げられています。
また、これ以外にも管理策の有効性を測定する上で、

・管理策の配下にある資産やそれらを取巻く環境
・リスクアセスメントの結果等

なども有効性を測定する上のインプットとして役立ちます。

特に直感的に管理策の有効性を測定する上で役立つインプットとしては､インシデントや管理策の配下の資産の状態などが考えられます｡影響が大きいインシデントが複数回起きた、又､管理策配下の資産が既に消去されているなどの場合､管理策はもはや有効でないと即座に導くことが可能です。このことは、有効性の測定プロセスにはインシデント管理、資産管理等との密接な連携を取り合う仕組みが必要であることを示唆しています。

上記のインプットの内の「有効性測定の結果」とは、管理策または、一群の管理策に対して､有効性を測定するための測定表などを用いて測定したことによって把握できた内容のことです。それらの結果を基に、最終的な判定を下すこともあります。このことについては、「管理策の有効性測定」の項で説明します。

アウトプットとしては、

・有効性測定の判定結果

と考えることができます。

この際、情報セキュリティの目的、すなわち情報の C(機密性)、I(完全性)、A（可用性）の維持という視点から、また必要に応じて真正性、責任追跡性、否認防止及び信頼性のような特性の維持のために、実行している管理策が有効であるのかを判定する必要があります。情報セキュリティでは､よく機密性と可用性の維持をバランスよく､とっていくことが困難であるといわれています｡機密性を高めれば利便性が欠如し､可用性を高めればおのずと機密性は損なわれるという情報セキュリティの特性の中で､各プロセスのリスクに応じるために実施、運用している管理策の有効性を測定し、管理策をチューンアップしていくことは、重要なプロセスです。

また､管理策は維持させたい情報セキュリティの特性､すなわち C(機密性)､I(完全性)､A（可用性）毎に異なる場合があります。例えば、機密性であれば暗号化、可用性であれば

システムの多重化という具合に管理策を考えることが通常です。その際、個別に暗号化のみの有効性や二重化のみの有効性を測定しても、プロセスがもつ両方の管理策がはたして有効なものなのかを測定していなければ、バランスがとれた管理策の実施には繋がりません。プロセス全般のリスクを考慮した上で、管理策または一群の管理策の有効性を測定することが効果的です。

フィードバックとしては、
上記のようにプロセス全体を考慮して、管理策または一群の管理策の有効性について判定を導き出すことは当然重要ですが、これらの判定結果をどのように活用するかを考慮することも重要です。有効性測定結果のフィードバック先としては、以下のように考えることが可能です。

管理策または一群の管理策の有効性について測定した場合のフィードバック先

- ISMS 全体の有効性測定へのインプット
  ISMS 全体の有効性測定の一要素として活用する。
- リスクアセスメントプロセス
  プロセスの管理責任者やシステム管理者等に報告し、リスクアセスメント結果の妥当性確認や必要に応じて再リスクアセスメントを実施し、追加の管理策の必要性等を検討する。
- モニタリングプロセス
  測定する上で必要なモニタリングについて再検討する
- インシデント管理
  測定結果を基に、インシデント対応をするための基準等を再検討する
- 有効性測定プロセス
  測定結果を基に、測定方法自体や測定頻度などについて再検討する等

① リスクアセスメントプロセスへのフィードバック

上記のリスクアセスメントへのフィードバックに関して、ISMS 認証基準ではリスクアセスメント全体、及び残留リスク、特定したリスク受容可能レベルをあらかじめ定めた間隔でレビューすることを要求しています。リスクアセスメントのレビューでは、次に起きた変化を考慮することを要求しています。

4.2.3 ISMS の監視及びレビュー
d) リスクアセスメントをあらかじめ定めた間隔でレビューする。残留リスク及び特定したリスク受容可能レベルをレビューする。これらのレビューでは，次に起きた変化を考慮する。
1)組織
2)技術
3)事業の目的及びプロセス
4)特定した脅威
5)導入した管理策の有効性
6)外部事情（例えば，法令又は規制の状況，契約上の義務，社会的風潮）

（JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

従って、導入した管理策の有効性の測定結果をリスクアセスメントにフィードバックし、必要に応じて再度､リスクアセスメントを実施する改善等に向けたアクションを取ることになります。

ISMS の有効性について測定した場合のフィードバック先

② マネジメントレビューへのフィードバック

マネジメントレビューのインプットとして活用し、ISMS の継続的な改善を検討する

ISMS 認証基準では、管理策の有効性に関する「ISMS のマネジメントレビュー」を以下の様に規定しています。

7.2 レビューへのインプット
f) 有効性測定の結果
7.3 レビューからのアウトプット
a) ISMS の有効性の改善。
e) 管理策の有効性測定方法の改善

（JIS Q 27001:2006　7 ISMS のマネジメントレビュー　より引用）

a) マネジメントレビューへのインプット

ISMS 認証基準では、以下の通り有効性測定の結果をマネジメントレビューへインプットすることを要求しています。

- 管理策の有効性測定結果から把握できた内容を、マネジメントレビューのインプットとする。
  - ✓ 各管理策の有効性測定結果
  - ✓ 各管理策の有効性評価結果
  - ✓ 有効性測定及び評価結果のまとめ

b) マネジメントレビューからのアウトプット

ISMS 認証基準では、以下の通りマネジメントレビューの結果、次の ISMS 有効性に関する決定や処置をアウトプットすることを要求しています。

- ISMS 全体について ISMS 基本方針や目的が達成されていない内容に関しての改善処置
- 各管理策の評価結果、有効でなかった管理策に対する改善処置
- 管理策の有効性測定結果により、有効でなかった管理策を発見できなかった等、管理策有効性測定に関して測定方法に要する改善処置

（２）管理策の有効性測定に関する計画

管理策の有効性を測定するためには､まずどのように測定するかを定義しておく必要があります。

ISMS 認証基準では、管理策の有効性測定の定義を以下の様に規定しています。

> 4.2.2 ISMS の導入及び運用
> d) 選択した管理策又は一群の管理策の有効性をどのように測定するかを定義し，また，比較可能で再現可能な結果を生み出すための管理策の有効性のアセスメントを行うために，それらの測定をどのように利用するかを規定する[4.2.3c)参照]。
>
> （JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

管理策の有効性測定を定義付ける場合､以下のような項目を考慮すると比較可能で再現可能な測定に役立つでしょう。

- 管理策の目的
  組織にとって当該管理策の目的は何なのかを明確化する。管理策を実施した結果、この目的を達成したかどうかが管理策が有効かどうかのポイントとなる。
- 測定する単位
  選択した管理策又は関連する管理策をグループ化した一群の管理策の単位で、測定を実施するのかを定義する。
- 有効性測定の方法
  有効性を測定するために必要な項目を定義する。
  また、その方法は比較可能で再現可能な結果を生み出す必要がある。
- 有効性を評価（判定）する方法
  測定された結果を基に、有効性を評価するための方法を定義する。
  また、その方法は比較可能で再現可能な結果を生み出す必要がある。
- 評価結果のフィードバック先
  評価結果のフィードバック先を定義する。

評価結果は、管理策の有効性のレビュー及び ISMS 有効性のレビューで活用され、管理策や ISMS 全体が有効と認められない場合は、改善実施のために活用する。

① 有効性測定の方法に関するポイント

管理策の有効性測定を定義する場合、次の 2 つの視点を考慮すると、測定に対しレビューや判定を行なう上で有用であると考えられます。

管理策の有効性を測定するためには、まず何を測定するかを定義する必要があります。管理策有効性レビュー及び ISMS 有効性レビューのための活用を考慮して、例えば次の 2 つの項目の測定が考えられます。

a) 実施度

実施度は管理策を実装し運用した結果、計画した管理策に対してどの程度実施されたかを測定したものを言います。この測定値は、管理策の実装・運用の妥当性をチェックしたり、そのような実装・運用で不足しているものを特定するために使用します。

b) 達成度

達成度は計画した管理策を実施した結果、それに対して計画した管理目的が達成された程度（目的の達成度）を言います。この測定値は、セキュリティ管理策の実装・運用が、当初の当該管理策の目的や目標を達成するために有効に役割を果たしかどうか評価し、有効でない場合は管理策の実装・運用の仕方を改善するために使用します。

上記のように管理策の a)実施度、b)達成度を測定することにより、管理策の有効性を評価し、管理策の改善に向けた対応を実施することが可能となります。

② 有効性測定の実施例

前述の考慮事項を含む、有効性測定の実施のために有効だと思われる実施例を下表に示します。本表では、表中のステップ①からステップ⑩までの要領で、有効性測定を実施することを示しています。

目的	A.nn.n［管理目的タイトル記入］ 管理目的をそのまま転記する
管理策又は一群の管理策	A.nn.n.n［管理策タイトル記入］ 管理策をそのまま転記する
記述項目	記述内容
①管理策の目的、目標	当該組織における本管理策の目的は何なのかを具体的に記す。 その管理策を実施する事によって、具体的に何を実現しようとしているのか、

	或いはリスクをどう低減しようとしているのかを記す。 （注）この内容は、“目的の達成度”の測定に直接関連するので、充分考えて設定する必要がある。
②リスク	管理策に関連して想定されるリスクを挙げる。 （注）管理策に関連してリスクが直接的に想定できない場合は、“①管理策の目的、目標”から考える。
③測定の前提条件	実施度及び達成度を測定する前に、管理策を実施する前提として必要な事項を記す。 （注）“管理策が実施されている”と言う状況の明確な定義が必要であり、そう言う状況にある“対象”が識別されていることが必要である。すなわち、管理策の実施時にはその管理策の対象が識別されていなければならない（原則として測定式の分母として設定する）。
④測定項目	（１）実施度 ③の前提条件で定義した管理策を適用すべき対象に対して管理策が実施されている程度（実施度）を測定する。 （注）実施度を測定するための項目の設定には、各組織のセキュリティ標準書や手順書を参考にすることが出来る。これらが充分に整備されていない場合は、JIS Q 27002 の実施の手引に書かれている作業／行為／対策が、この実施度を設定する際に参考になる。 （２）達成度 ①で設定した管理策の目的／目標を達成したかどうかの程度（達成度）を測定する。 （注）例えば ・管理策の目的/目標に関係するインシデント発生 ・リスクアセスメント時に用いたリスクに関係するレベルの測定
⑤測定値（基礎データ）	（１）実施度を示す測定値（基礎データ） （２）達成度を示す測定値（基礎データ）
⑥測定責任組織（部門）	その管理策に関して実施責任を持っている部署 （１）実施度を示す測定値の測定組織 （２）達成度を示す測定値の測定組織 （３）実施度及び達成度より管理策の有効性を評価する組織
⑦測定の頻度	その管理策に関して測定する頻度 （１）実施度を示す測定値の測定頻度 （２）達成度を示す測定値の測定頻度
⑧有効性を評価するための算定式	④測定項目に基く算定式 （１）⑤実施度測定値（基礎データ）と③測定の前提で考慮した測定対象　等に基き、実施度を示す算定式を記す。 （２）⑤達成度測定値（基礎データ）と③測定の前提で考慮した測定対象　等に基き、達成度を示す算定式を記す。
⑨有効性指標による評価	管理策の有効性の評価（有効性指標）に関して記す。 実施度であるから管理策で規定した個々の対応策の実施（実装及び運用）は100%であるべきだが、実際はこの測定値は次のような特性を持つ。 目的・目標の設定により、測定の前提条件となる対象が異なり算定値が変わる。 測定の精度により算定値が変わる。管理策の目的・目標、成熟度により、測定に実装・運用する技術、費用等が異なり測定の精度が変わる。 対応策の不備・不足により有効性が損なわれる場合がある。又、実施度の未

	達成により、有効性が損なわれる場合がある。 達成度であるから、当該管理策の目的を達成したかどうかで計測するので、必ずしも 100%である必要はない。実際は、この測定値は次のような特性を持つ。 測定の前提条件となる対象の選択により算定値が変わる 実際は網羅的に 100%とはならない。例えば、 インシデント発生率が目標値以下に減少しているか リスクレベルが目標値以下に減少しているか 管理策の有効性の評価は、（１）実施度、及び（２）達成度の結果より、有効性の評価を行う。評価結果、管理策の実装・運用の改善は、次の段階である。例えば、 管理策を 100%実施（実施度）したにもかかわらず、目的を達成（達成度）していなければ、当該管理策として実施した対応策（実装及び運用）は有効でないと評価する。 有効でないと評価された管理策は、改善が必要となる。
⑩関連する他の管理策	例えば、 ・　本管理策が実施されるために必要な他の管理策を記す。 ・　本管理策の共通の管理目的・目標を持つ他の管理策を記す。
備考	例えば、JIS Q 27002:2006 実施の手引に有効な情報があれば参考にすることができる。

９．３．２ 実行（Do）

ISMS 認証基準では、ISMS の監視及びレビュー（Check-点検）のステップにおいて、管理策有効性の測定の実施が要求されています。

> 4.2.3 ISMS の監視及びレビュー
> c) セキュリティ要求事項を満たしていることを検証するために，管理策の有効性を測定する。
>
> （JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

ここでは、前述の有効性測定の定義に従って、管理策の有効性測定を実行します。

そしてこれらの測定結果は、管理策の有効性レビュー及び ISMS の有効性レビューに使用されます。

ISMS 認証基準では、ISMS の有効性レビューについて以下のように規定しています。

4.2.3 ISMS の監視及びレビュー b) ISMS の有効性について定期的にレビューする。これには，ISMS 基本方針及び目的を満たしていることのレビューとセキュリティ管理策のレビューとがある。このレビューでは，セキュリティ監査の結果，インシデント，有効性測定の結果，提案，及びすべての利害関係者からのフィードバックを考慮する。 （JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

ここでは、ISMS の有効性についての定期的なレビューが要求されています。ISMS 有効性レビューには、（１）ISMS 基本方針及び目的を満たしていることのレビューと（２）管理策のレビューとがあります。

（１） ISMS 基本方針及び目的を満たしていることのレビュー

- 導入した ISMS が、設定している ISMS 基本方針の各項目を満たしているかレビューする
- 導入した ISMS が、設定した ISMS の目的を満たしているかレビューする

（２） 管理策の有効性のレビュー

- 管理策または一群の管理策に対して測定された結果に基づき、改善に向けた対応が必要かレビューを実施します。

（注記）

上記レビューには、

- セキュリティ監査の結果
- インシデント
- 有効性測定の結果
- 提案
- すべての利害関係者からのフィードバック　等

を考慮する必要があります。

９．３．３ 点検と処置（Check and Act）

管理策の有効性測定結果により、有効でなかった管理策を発見できなかった等、管理策有効性の測定方法に関しては、有効性測定のプロセスの中で監視し課題を発見して改善処置を取ります。管理策有効性の測定方法に関する課題としては、次のような場合が考えられます。このような場合、管理策有効性測定方法に関して改善処置をする必要があります。

- 有効性を判断するために管理目的を達成しているかどうかを正確に判断できるデータを測定できていない
- 有効性を判断するために管理策が実施できているかどうかを正確に判断できるデータを測定できていない
- 実施が充分出来ていないのに管理目的を達成していることが、有効性測定方法が不十分なことに起因している場合

９．４　有効性測定手順書の概要例

ISMS 認証基準では、管理策の有効性に関する「文書化に関する要求事項」を以下のように規定しています。

> 4.3 文書化に関する要求事項
> 4.3.1 一般
> g)情報セキュリティのプロセスを有効に計画，運用及び管理することを確実にするために，組織が必要とする文書化した手順。管理策の有効性をどう測定するか[4.2.2 d) 参照]を記述するために，組織が必要とする文書化した手順。
>
> （JIS Q 27001:2006　4.3 文書化に関する要求事項　より引用）

これまでの有効性測定に関する内容をまとめて、以下に文書化する上で有用だと思われる項目を例示します。

「管理策有効性測定手順の概要」（例示）

１．管理策有効性測定概要
　　１－１　概要及び目的
　　１－２　適用範囲
　　１－３　改訂履歴
２．測定手法
　　２－１　管理策の目的/目標の設定
　　２－２　実施度と達成度
　　２－２　測定値及び算定式の定義
　　２－３　測定体制
３．有効性の評価
　　３－１　評価の方法
　　３－２　評価結果への対応
　　　３－２－１　有効であると評価された管理策
　　　３－２－２　有効でなく改善が必要と評価された管理策
　　　３－３－３　経過観察が必要と評価された管理策

添付１．管理策有効性測定票（管理策毎又は一群の管理策）

ANNEX A.　参考文献

本章では､医療機関における情報セキュリティ対策と情報セキュリティマネジメントシステム（ISMS）の理解を深めるために適宜、参照していただきたい参考文献、法令等を紹介します。

また、本資料は ISMS ユーザーズガイドの参考文献を基とし、医療機関向けに追加させたものであります。

１　参考文献

参考文献は、次の通りに分類しています。

- 📖 書籍・文献
- 💻 WEB公開情報
- ★　法律あるいは解説

１．１　医療機関に関連する基準・規格・ガイドライン・解説

📖 「JIS T 1001:1992　医用電気機器の安全通則」(2006年11月で廃止)
日本規格協会　和文冊子

📖 「JIS T 1002:1992　医用電気機器の安全性試験方法通則」(2006年11月で廃止)
日本規格協会　和文冊子

📖 「JIS T 0601-1:1999　医用電気機器―第1部：安全に関する一般要求事項」
日本規格協会　和文冊子/和文PDFダウンロード、英文冊子/英文PDFダウンロード

📖 「ISO 13485:2003(Medical devices– Quality management systems –Requirement Requirements for regulatory purpose) 医療用具―品質マネジメントシステム―規制目的のための要求事項」
日本規格協会　英文冊子/英文PDFダウンロード

📖 「ISO 15189:2003(Medical laboratories – Particular requirements for quality and competence)臨床検査室―質と適合能力に対する特定要求事項」英和対訳版
日本規格協会　和文冊子/和文PDFダウンロード、英文冊子/英文PDFダウンロード

📖 「JIS T 14971:2003 (ISO 14971:2000 (Medical devices – Application of risk management medical devices)医療機器―リスクマネジメントの医療機器への適用」
日本規格協会　和文冊子/和文PDFダウンロード、英文冊子/英文PDFダウンロード

📖 「JIS Q 14971:2001 (ISO 14971:1998 (Medical devices ― Risk management ― Part 1: Application of risk analysis)医療用具―リスクマネジメント―第1部：リスク分析の適用」
日本規格協会　和文冊子/和文PDFダウンロード、英文冊子/英文PDFダウンロード

📖 「ISO/IEC Guide 63:1999(Guide to the development and inclusion of safety aspects in International Standards for medical devices)医療用具に関する国際規格の作成及び安全面を包めるための手引」英和対訳版
日本規格協会　和文冊子、英文冊子/英文PDFダウンロード

📖 「保健医療分野のプライバシーマーク制度　参考資料集」
財団法人医療情報システム開発センター　2008.4.25
http://privacy.medis.jp/book.html（入手案内）
－保健医療福祉分野のプライバシーマーク認定指針　（平成１８年１０月）

📖 「保健医療分野のプライバシーマーク関連情報」
財団法人医療情報システム開発センター　2003.07

💻 厚生労働省通知（医政発0912001号、平成15年9月12日）
診療情報の提供等に関する指針の策定について
http://wwwhourei.mhlw.go.jp/hourei/doc/tsuchi/150916-a.pdf
診療情報の提供等に関する指針（別添）
http://wwwhourei.mhlw.go.jp/hourei/doc/tsuchi/150916-b.pdf

📖 「リモートサービスセキュリティガイド」
社団法人日本画像医用システム工業会規格　2004.03

💻 「医療情報システムの安全管理に関するガイドライン　第３版」
厚生労働省　2008.03
http://www.mhlw.go.jp/shingi/2008/03/s0301-2.html

💻 リモートサービスセキュリティガイドライン
保健医療福祉情報システム工業会 及び 社団法人日本画像医療システム工業会
2006.05
http://www.jahis.jp/standard/seitei/st06-001/st06-001.htm
http://www.jira-net.or.jp/commission/system/04_information/files/RSS_GL_JESRA.pdf

💻 個人情報保護に役立つ監査証跡ガイド
財団法人医療情報システム開発センター　2007.03
http://www.medical-it-link.jp/temporary/temp_1_445.pdf

💻 「保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム」の「実装事例報告書」「NWセキュリティチェックシート」等
保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム
http://www.heasnet.jp/index_J.htm

以下、社団法人 情報サービス産業協会（JISA）の個人情報保護およびプライバシーマーク関連リンク集（http://www.jisa.or.jp/pdguide/link06b-j.html）から厚生労働省所轄のものを抜粋　2008.5

- 全日本病院協会(AJHA)**「全日本病院協会における個人情報保護指針」**(PDFファイル)
  http://www.ajha.or.jp/nintei/pdf/05.pdf
- 全日本病院協会(AJHA)**「個人情報保護法に関するＱ＆Ａ」**(PDFファイル)
  http://www.ajha.or.jp/about_us/activity/zen/20050308-8.pdf
- 日本医師会(JMA)**「医療機関における個人情報の保護」**(冊子のみの頒布)
- 日本医師会(JMA)**「診療情報の提供に関する指針」**
  http://www.med.or.jp/nichikara/joho2.html
- 日本医薬品卸業連合会(JPWA)**「個人情報保護法医薬品卸売業関係ガイドライン」**(PDFファイル)
  http://www.jpwa.or.jp/jpwa/kjHogoGuide.pdf
- 日本衛生検査所協会**「衛生検査所における個人情報の適切な取扱いのためのガイドライン」**(PDFファイル)
  http://www.jrcla.or.jp/info/info/privacy2.pdf
- 日本看護協会(JNA)**「看護記録および診療情報の取り扱いに関する指針」**(会員限定で公開)
- 日本製薬団体連合会**「製薬企業における個人情報の適正な取扱いのためのガイドライン」**
  http://www.fpmaj.gr.jp/documents/guide.pdf
- 日本病院会(JHA)**「病院における個人情報保護法への対応の手引き」**(冊子のみの頒布)
- 日本臨床衛生検査技師会(JAMT)　**「個人情報保護ガイドライン」**
  http://www.jamt.or.jp/materials/materials.html
  >検査情報システムの安全管理に関するガイドライン(PDF)
  http://www.jamt.or.jp/information/privacy/p_guideline1.pdf
  >医療安全管理に関するガイドライン(PDF)
  http://www.jamt.or.jp/information/privacy/p_guideline2.pdf
  >検査室における個人情報保護ガイドライン(PDF)
  http://www.jamt.or.jp/information/privacy/p_guideline3.pdf
  >医療機器管理に関するガイドライン(PDF)
  http://www.jamt.or.jp/information/privacy/p_guideline4.pdf

📖 「SPC白書(通称)」

NEMA(米国電気機器製造業者協会、COCIR(欧州放射線医用電子機器産業連合会)、JIRA(日本画像医用システム工業会)の Joint Security and Privacy Committee(略称　SPC)による作成文書です。

① Defending Medical Information Systems Against Malicious Software (2003.12)
医療情報システムにおける有害なソフトウェアに対する防衛
② Break-Glass An Approach to Granting Emergency Access to Healthcare Systems (2004.12)
ブレークグラス：医療システムへの緊急アクセスのためのアプローチ
③ Remote Service Interface - Solution (A) - Version 2: IPSec over the Internet UsingDigital Certificates (2003.12)
リモートサービスインターフェースー解決策(A)－Version 2:電子署名を使ったインターネット上の IPSec
④ Patching Off-the-Shelf Software Used in Medical Information Systems (2004.10)
医療情報システムへの市販ソフトウェアのパッチ
⑤ Management of Machine Authentication Certificates (2007.5)
機器認証証明書のマネジメント
⑥ Information Security Risk Management for Healthcare Systems (2007.10)
医療機器の情報セキュリティリスクマネジメント
(http://www.jira-net.or.jp/commission/system/index.html)

※英文版はいずれも下記ＵＲＬからアクセスできます。
http://www.medicalimaging.org/policy/security.cfm

１．２　医療機関に関連する参考図書

📖 保健医療分野のプライバシーマーク制度の参考図書（入手案内）
財団法人医療情報システム開発センター　2008.4.25
http://privacy.medis.jp/book.html
－ 産業保健版・個人情報の保護と活用の手引きー働く人の健康情報活用法－
－ 患者情報管理体制　実践ガイド
－ 医療・介護　個人情報の保護と活用の手引き
－ 医療・介護・福祉の個人情報保護ガイド（ＣＤ－ＲＯＭ付き）
－ 医療の個人情報保護とセキュリティ
－ 個人情報保護法の解説≪改訂版≫
－ 逐条個人情報保護法

１．３　ISMS 全般

💻 「情報セキュリティ読本」(情報処理振興事業協会 セキュリティセンター(IPA/ISEC))
2007.7　http://www.ipa.go.jp/security/publications/dokuhon/2006/index.html

- 「情報セキュリティ教本」(情報処理振興事業協会 セキュリティセンター(IPA/ISEC))
  2007.4　http://www.ipa.go.jp/security/publications/kyohon/index.html
- 「読者層別： 情報セキュリティ対策 実践情報」(情報処理振興事業協会 セキュリティセンター(IPA/ISEC))
  2005.8　http://www.ipa.go.jp/security/awareness/awareness.html
- 情報セキュリティ監査研究会報告書（経済産業省）
  2003.3.26
  http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Report.pdf
- 「リスク管理・内部統制に関する研究会報告書（リスクマネジメントと一体となって機能する内部統制に係る指針)」(経済産業省　リスク管理・内部統制に関する研究会)
  2003.6　http://www.meti.go.jp/kohosys/press/0004205/

１．４　基準・規格・ガイドライン・解説

- ISMS適合性評価制度の概要（パンフレット）(JIPDEC)
  2008.1　http://www.isms.jipdec.jp/doc/ismspanf.pdf
- ISMS認証基準(Ver.2.0)　(JIPDEC) ※ 2007年11月で廃止。
  2003.4.21　http://www.isms.jipdec.jp/doc/JIP-ISMS100-20.pdf
- ISMSガイド(Ver.1.0)　(JIPDEC)
  2002.4.1　http://www.isms.jipdec.jp/doc/JIP-ISMS110-10.PDF
- ISMSユーザーズガイド (JIPDEC)
  2008.1.31　http://www.isms.jipdec.jp/doc/JIP-ISMS111-21.pdf
- ISMSユーザーズガイド リスクマネジメント編　(JIPDEC)
  2008.1.31　http://www.isms.jipdec.jp/doc/JIP-ISMS113-21.pdf
  http://www.isms.jipdec.jp/doc/JIP-ISMS113-11ap1.pdf（付録）
- 医療機関向けISMSユーザーズガイド (JIPDEC)
  2008.5.31　http://www.isms.jipdec.jp/doc/JIP-ISMS114-21.pdf
- 法規適合性に関するISMSユーザーズガイド (JIPDEC)
  2005.4.18　http://www.isms.jipdec.jp/doc/JIP-ISMS115-10.pdf
- クレジット産業向けISMSユーザーズガイド (JIPDEC)
  2006.3.31　http://www.isms.jipdec.jp/doc/JIP-ISMS116-10.pdf
- 外部委託におけるISMS適合性評価制度の活用方法 (JIPDEC)
  2006.6.30　http://www.isms.jipdec.jp/doc/JIP-ISMS117-10.pdf
- 情報セキュリティ監査基準(Ver1.0)ほか（経済産業省）2003.4
  http://www.meti.go.jp/policy/netsecurity/audit.htm
- 「ASP・SaaSにおける情報セキュリティ対策ガイドライン」(総務省)
  http://www.soumu.go.jp/s-news/2008/pdf/080130_3_bt3.pdf

- 「JIS Q 27001:2006 情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項」(日本規格協会)
- 「JIS Q 27002:2006 情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範」(日本規格協会)
- 「BS 7799-3:2006 Information security management systems-Part 3: guidelines for information security risk management (情報セキュリティマネジメントシステムー第3部：情報セキュリティリスクマネジメントの指針)」(訳；日本規格協会)
- 「JIS Q 13335-1:2006 情報技術―セキュリティ技術―情報通信技術セキュリティマネジメント―第１部：情報通信技術セキュリティマネジメントの概念及びモデル」(日本規格協会)
- 「TR X 0036シリーズ (ISO/IEC TR 13335-1～-5 (Information technology – Guidelines for the management of IT Security)) ITセキュリティマネジメントのガイドライン」
  TR X 0036-1:2001 ITセキュリティの概念及びモデル
  TR X 0036-2:2001 ITセキュリティのマネジメント及び計画
  TR X 0036-3:2001 ITセキュリティマネジメントのための手法
  TR X 0036-4:2001 セーフガードの選択
  TR X 0036-5:2003 ネットワークセキュリティに関するマネジメントの手引
  (日本規格協会)
- BIP 0071 - Guidelines on requirements and preparation for ISMS certification based on ISO/IEC 27001 (BSI)
- BIP 0072 - Are you ready for an ISMS audit based on ISO/IEC 27001? (BSI)
- BIP 0073 - Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001 (BSI)
- BIP 0074 - Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001 (BSI)

- OECD セキュリティガイドライン
  情報システム及びネットワークのセキュリティのためのガイドライン (仮訳)
  (OECD Guidelines for the Security of Information Systems and Networks)
  2002.7.25 http://www.meti.go.jp/policy/netsecurity/oecd020924.htm
- 「TR Q 0008:2003(ISO/IEC Guide 73:2002 Risk management -- Vocabulary -- Guidelines for use in standards) リスクマネジメント―用語―規格において使用するための指針」(日本規格協会)
- 「JIS Q 2001:2001 (Guidelines for development and implementation of risk management system) リスクマネジメントシステム構築のための指針」(日本規格協会)

- 「JIS Q 19011:2003 (Guidelines for quality and/or environmental management systems auditing)　品質及び／又は環境マネジメントシステム監査のための指針」
  (日本規格協会)
- 「ISO/IEC TR 18044:2004 (Information technology -- Security techniques -- Information security incident management)」
  JEITA ITR-1001A 情報システムの設備ガイド　(社)電子情報技術産業協会　2003.3
  http://it.jeita.or.jp/document/setsubi/ITR1001-1002/1001B.html (入手案内)
- JEITA IT-1002 情報システムの設備環境基準　(社)電子情報技術産業協会　2003.03
  http://it.jeita.or.jp/document/setsubi/ITR1001-1002/1002.html (入手案内)
- 無線LANのセキュリティに関するガイドライン改訂版 (社)電子情報技術産業協会
  2004.4　http://it.jeita.or.jp/perinfo/committee/pc/wirelessLAN2/index.html
- 情報セキュリティに関するRFC (IPA/ISEC)
  http://www.ipa.go.jp/security/rfc/RFC.html

１．５　ISMS構築事例

- ISMS構築事例集～情報セキュリティへの取り組み事例～ (JIPDEC)
  2003.7.24 公開開始　http://www.isms.jipdec.jp/doc/const/001top.PDF

１．６　ISMS関連指針

- 政府機関の情報セキュリティ対策における統一基準の策定と運用等に関する指針
  (平成１７年９月１５日 情報セキュリティ政策会議決定)
  http://www.nisc.go.jp/active/general/pdf/2siryou04-2d.pdf
- 政府機関の情報セキュリティ対策のための統一基準 (第２版)
  http://www.nisc.go.jp/active/general/pdf/k303-071.pdf
- 重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 (平成18年2月2日情報セキュリティ政策会議決定)
  http://www.nisc.go.jp/active/infra/pdf/infra_pl07.pdf

- 財団法人　金融情報システムセンター(FISC)
  「金融機関等におけるコンティンジェンシープラン策定のための手引書 (第３版)」
  2006/3
  「金融機関等コンピュータシステムの安全対策基準解説書 (第７版)」2006/3
  http://www.fisc.or.jp/publication/ (入手案内)

１．７　情報セキュリティ対策

- 情報セキュリティ対策の資料(IPA/ISEC)

  http://www.ipa.go.jp/security/
  - ・情報システム部門責任者向けのページ
    http://www.ipa.go.jp/security/awareness/management/management.html
  - ・システム管理者向けのページ
    http://www.ipa.go.jp/security/awareness/administrator/administrator.html
  - ・エンドユーザ・ホームユーザ向けのページ
    http://www.ipa.go.jp/security/awareness/end-users/end-users.html
  - ・SOHO（小規模サイト）向けのページ
    http://www.ipa.go.jp/security/awareness/soho/soho.html
  - ・ネットワークサービス事業者向けのページ
    http://www.ipa.go.jp/security/awareness/isp/isp.html
  - ・ソフトウェア開発者向けのページ
    http://www.ipa.go.jp/security/awareness/vendor/software.html

１．８　不正アクセス対策

- コンピュータ不正アクセス対策（IPA/ISEC）

  http://www.ipa.go.jp/security/fusei/ciadr.html
- 情報セキュリティに関する政策、緊急情報（経済産業省）

  http://www.meti.go.jp/policy/netsecurity/
- サイバー犯罪対策（警察庁）

  http://www.npa.go.jp/cyber/
- 国民のための情報セキュリティサイト（総務省）

  http://www.soumu.go.jp/joho_tsusin/security/

１．９　コンピュータウイルス対策

- ウイルス対策のWEBページ（IPA/ISEC）

  http://www.ipa.go.jp/security/isg/virus.html

１．１０　知的財産権、著作権保護

- 経済産業省　－　知的財産政策

  http://www.meti.go.jp/policy/intellectual_property/index.html
- 文化庁　－　著作権

  http://www.bunka.go.jp/chosakuken/index.html
- 社団法人コンピュータソフトウェア著作権協会(ACCS)

  http://www2.accsjp.or.jp/
- 社団法人著作権情報センター(CRIC)

  http://www.cric.or.jp

１．１１　個人情報保護

★　個人情報の保護に関する法律
http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/index.html

★　行政機関・独立行政法人等の個人情報保護法
http://www.soumu.go.jp/gyoukan/kanri/kenkyu.htm

📖「JIS Q 15001:2006 (Personal information protection management systems – Requirements 個人情報保護マネジメントシステム―要求事項)」(日本規格協会)

💻　個人情報の保護（内閣府国民生活局）
http://www5.cao.go.jp/seikatsu/kojin/

💻　情報政策（個人情報保護）　経済産業省
http://www.meti.go.jp/policy/it_policy/privacy/index.html

💻　プライバシーマーク事務局 WEBページ（JIPDEC）
http://privacymark.jp/

【その他】

１．１２　法律関係

💻　法令データ提供システム（総務省行政管理局）
http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi

💻　最近の法律・条約（内閣法制局）
http://www.clb.go.jp/contents/index.html

１．１３　情報セキュリティの調査報告

💻　わが国における情報セキュリティの実態（JIPDEC）
http://www.jipdec.jp/security/security05/

💻　情報通信政策（総務省）
http://www.soumu.go.jp/joho_tsusin/joho_tsusin.html

💻　情報通信白書（総務省）
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm

💻　セキュリティ被害調査ほか（日本ネットワークセキュリティ協会　NPO）(2002.6.13)
http://www.jnsa.org/result/

💻　リスクマネジメントシステムのあり方に関する調査・研究（JIPDEC）(2003.3)
http://www.jipdec.jp/security/JRMS.htm

２　法令等

２．１　情報保護に関する法令

法令の名称	主な参考条項
日本国憲法	第21条
個人情報の保護に関する法律	全般
行政機関の保有する個人情報の保護に関する法律	全般
独立行政法人の保有する個人情報の保護に関する法律	全般
情報公開・個人情報保護審査会設置法	全般
行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律	全般
貸金業の規制等に関する法律	第30条第2項　個人信用情報の目的外使用の禁止
割賦販売法	第39条　信用情報の適正な使用等
不正競争防止法	全般

２．２　コンピュータ犯罪に関する法令

法令の名称	主な参考条項
刑法	第7条の2　　電磁的記録の定義 第157条第1項　電磁的公正証書原本不実記録罪 第158条第1項　不実記録電磁的公正証書原本供用罪 第161条の2　電磁的記録不正作出・不正作出電磁的記録供用罪 第234条の2　電子計算機損壊等業務妨害罪 第246条の2　電子計算機使用詐欺罪 第258条　　公用電磁記録毀棄罪 第259条　　私用電磁記録毀棄罪
不正アクセス行為の禁止等に関する法律	全般
労働基準法	第91条　制裁規定の制限
労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律	第24条の4　秘密を守る義務
児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律	全般

２．３　設備に関する法令

法令の名称	主な参考条項
建築基準法	第1条　目的 第2条　用語の定義 第6条　建築物の建築等に関する申請及び確認 第7条　建築物に関する完了検査 第20条　構造耐力
建築基準法施行令	第1条　用語の定義 第82条　応力度等 第82条の2　層間変形角 第82条の3　剛性率・偏心率等 第82条の4　保有水平耐力 第88条　地震力 第107条　耐火構造 第107条の2　準耐火構造 第108条　防火構造 第108条の2　準防火構造 第109条　防火戸その他の防火設備 第110条　防火戸の構造 第112条　防火区画 第117条　廊下、避難階段及び出入口の適用の範囲 第119条　廊下の幅 第120条　直通階段の設置 第121条　二以上の直通階段を設ける場合 第122条　避難階段の設置 第125条　屋外への出口 第126条の2　排煙設備の設置 第126条の3　排煙設備の構造 第129条　特殊建築物等の内装 第5章　避難施設等
消防法	第2条　用語例 第8条　防火管理 第9条　危険物等の貯蔵等の基準 第10条　危険物の貯蔵等の取締り 第17条　消防用設備等の設置、維持義務等 第17条の3　消防用設備等の点検及び報告

法令の名称	主な参考条項
消防法施行令	第3条　防火管理者の資格 第4条　防火管理者の責務 第7条　消防用設備等の種類 第10条　消火器具に関する基準 第11条　屋内消火栓設備に関する基準 第12条　スプリンクラー設備に関する基準 第13条　水噴霧消火設備等を設置すべき防火対象物 第14条　水噴霧消火設備に関する基準 第15条　泡消火設備に関する基準 第16条　二酸化炭素消火設備に関する基準 第17条　ハロゲン化物消火設備に関する基準 第18条　粉末消火設備に関する基準 第21条　自動火災報知設備に関する基準 第23条　消防機関へ通報する火災報知設備に関する基準 第24条　非常警報器具又は非常警報設備に関する基準 第25条　避難器具に関する基準 第26条　誘導灯及び誘導標識に関する基準 第28条　排煙設備に関する基準
消防法施行規則	第3条　　消防計画 第4条　　防火管理者の選任又は解任の届出 第4条の4　防炎表示等 第23条　　自動火災報知設備の感知器等 第24条　　自動火災報知設備に関する基準の細目 第30条　　排煙設備に関する基準の細目 第31条の4　消防用設備等の点検及び報告
高圧ガス保安法	第35条　　保安検査 第35条の2　定期自主検査
冷凍保安規則	第7条　定置式製造設備に係る技術上の基準 第8条　移動式製造設備に係る技術上の基準
大規模地震対策特別措置法	全般
建築物の耐震改修の促進に関する法律	全般
危険物の規制に関する政令	第8条の5　定期的に点検しなければならない製造所等の指定
電気通信事業法	第4節　電気通信設備
電気事業法	第42条　保安規程
電気設備技術基準	第15条　地絡に対する保護対策

法令の名称	主な参考条項
エネルギーの使用の合理化に関する法律	全般

２．４　社会的情報インフラに関する法令

法令の名称	主な参考条項
高度情報通信ネットワーク社会形成基本法	第22条　高度情報通信ネットワークの安全性の確保等
電子署名及び認証業務に関する法律	全般
電気通信事業法	第4条　秘密の保護 第35条　業務の停止等の報告 第41条　電気通信設備の維持
有線電気通信法	第9条　有線電気通信の秘密の保護
電波法	第59条　秘密の保護
特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律	第3条　損害賠償責任の制限 第4条　発信者情報の開示請求等

２．５　知的財産権に関する法令

法令の名称	主な参考条項
著作権法	第2条　定義 第10条　著作物の例示 第12条の2　データベースの著作物 第20条　同一性保持権 第47条の2　プログラムの著作物の複製物の所有者による複製等 第76条の2　創作年月日の登録 第113条　侵害とみなす行為
特許法	全般
知的財産基本法	第6条　地方公共団体の責務 第7条　大学等の責務 第8条　事業者の責務

２．６　情報保護に関する法令、その他の規範

法令の名称	主な参考条項
刑法	第134条（秘密漏示）
国家公務員法	第100条（秘密を守る義務）
地方公務員法	第34条

法令の名称	主な参考条項
労働安全衛生法	第104条
じん肺法	第35条の3
医療法	第1条の4 （医師等の責務）、第72条 （秘密漏示）
保健師助産師看護師法	第42条
診療放射線技師法	第29条 （秘密を守る義務）
臨床検査技師、衛生検査技師等に関する法律	第19条 （秘密を守る義務）
理学療法士及び作業療法士法	第16条 （秘密を守る義務）
歯科技工士法	第20条の2
社会福祉士及び介護福祉士法	第46条 （秘密保持義務）
児童虐待の防止等に関する法律	第6条、第7条 （児童虐待に関わる通告）
社会保険診療報酬支払基金法	第14条の5
医師の倫理（日本医師会）	

２．７　医療関連の法規定

法令の名称	主な参考条項
医療提供に関する法規	医療法
医療資格に関する法規	医師法
	保健師助産師看護師法
	薬剤師法
	診療放射線技師法
	臨床検査技師、衛生検査技師等に関する法律
	理学療法士及び作業療法士法
	歯科技工士法
	社会福祉士及び介護福祉士法
社会保障や福祉に関係する法規	生活保護法
	児童福祉法
	身体障害者福祉法
	精神薄弱者福祉法
	母子福祉法
	老人福祉法
介護に関連する法規	介護保険法

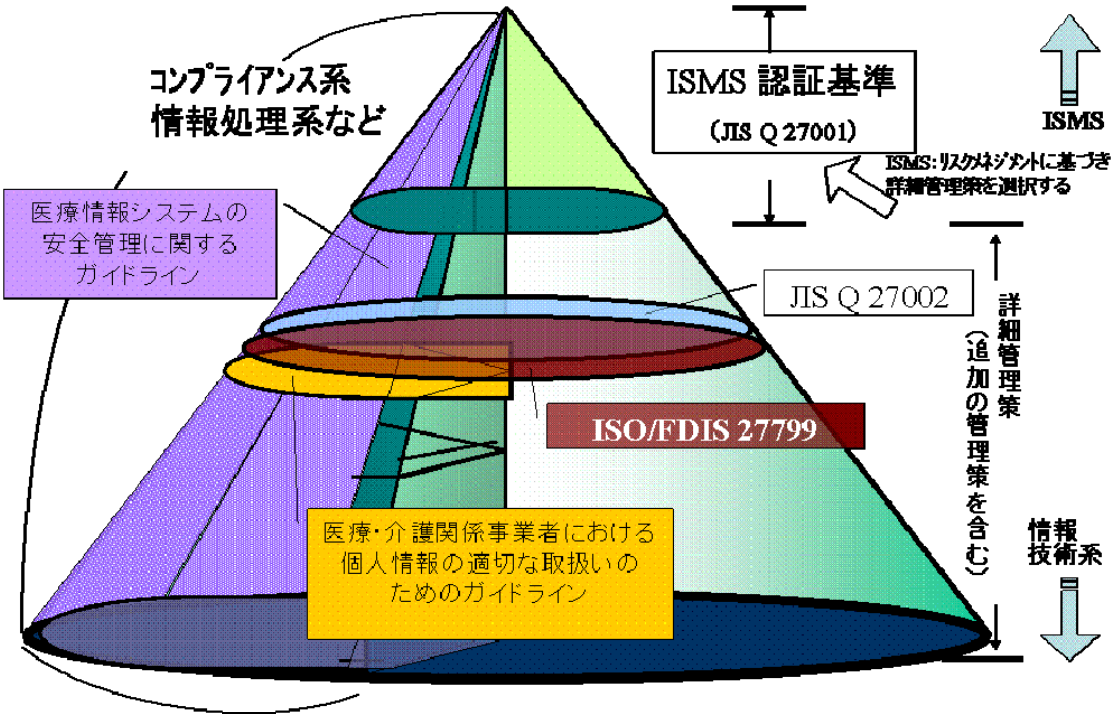
法令の名称	主な参考条項
医療費支払い保険制度に関係する法規	健康保険法
	国民健康保険法
	老人保健法
	船員保険法
	日雇労働者健康保険法
	労働者災害保障保険法
	自動車損害賠償保険法
	厚生年金法
	国民年金法
	雇用保険法
	社会保険診療報酬支払基金法
その他、病院の医療活動に関係する法規	環境衛生関係の法規
	放射線同位元素などによる放射線障害の防止に関する法規
	死体解剖保存法
	角膜移植に関する法規
	医学および歯学の教育のための献体に関する法規
	救急病院などを定める省令
	死産届書・死産証明および死胎検索書の関する省令
感染症に関する法規	感染症の予防および感染症の患者に対する医療に関する法律
	結核予防法
	検疫法
	予防接種法
	トラホーム予防法
	寄生虫予防法
	狂犬病予防法
	母体保護法
	精神保健福祉法
	母子保健法
	学校保健法

法令の名称	主な参考条項
薬剤に関する法規	薬事法
	麻薬および向精神薬取締法
	覚せい剤取締法
	毒物および劇物取締法
	あへん法
	医薬品副作用被害救済・研究振興
災害時に適用される法規	災害対策基本法
	災害救助法
	日本赤十字社法
職員の労働に関する法規	労働基準法
	労働安全衛生法
	作業環境測定法

２．８　その他

法令の名称	主な参考条項
電子消費者契約及び電子承諾通知に関する民法の特例に関する法律	第3条　電子消費者契約に関する民法の特例 第4条　電子承諾通知に関する民法の特例
特定商取引に関する法律施行規則の一部を改正する省令	全般
特定電子メールの送信の適正化等に関する法律	全般
古物営業法の一部を改正する法律	全般
インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律	全般

ANNEX B.　医療機関向けｶﾞｲﾄﾞﾗｲﾝ（一部）と JIS Q 27001 及び JIS Q 27002 の位置付け



相関イメージ図についての解説

本イメージ図は JIS Q 27001:2006 及び JIS Q 27002:2006 と医療機関向けのガイドライン（一部）の位置づけを表したものです。目的は各規格やガイドラインが対象としている範囲がどういうものなのか、対象とする情報資産の範囲（水平方向）と対応の考え方（垂直方向）をイメージとして捉え、それぞれの特徴を踏まえた上で自組織における情報セキュリティマネジメントの構築の参考にしてもらうことにあります（本図はあくまで相関関係のイメージであり、この位置づけで 100%一致しているわけではありません）。

この円錐全体のうち、上層部が JIS Q 27001:2006（ISMS マネジメント部分(確立･導入及び運用･監視及びレビュー･維持及び改善)の要求事項)、その上層部から半分が JIS Q 27002:2006（ISMS を実践するための具体的な管理策実践の手引き）となります。

すなわち、円錐の上位にいくほどマネジメント要素（方針、組織、規定･ルール）が強くなり、下位にいくほど具体的な対策とその実践の意味合いが強くなります。(従って、包含関係的には、上層部が配下の部位を包含すると捉えることになります。)

これをベースに医療機関向けの一部のガイド･ガイドラインとの位置づけの例を以下に示

すと、

（１）医療･介護関係事業者における個人情報の適切な取扱いのためのガイドライン（厚生労働省）

・当ガイドラインは個人情報取扱いに関する法律（個人情報保護法）にあわせて、どのような対応を取るべきかの考え方が書かれています。反面、マネジメントシステムとして計画(Plan)、実装(Do)、評価(Check)、見直し(Act)の構築サイクルには触れてはいません。

・このことからイメージ図の位置づけとしてはガイドラインの対象が情報資産全体のうち、個人情報に関する部分のため、水平方向では円錐の一部分(左側)であり、対応の考え方については具体的な対応例も記載されていることから垂直方向では下側の位置付けと考えられます。

（２）医療情報システムの安全管理に関するガイドライン（厚生労働省）

・当ガイドラインは個人情報を含む医療情報を扱う情報システムやネットワークでのセキュリティの考え方とその安全対策についてのガイドラインとして新規に作られ、これに従来の診療録等の電子媒体による保存や外部保存、スキャナ等での電子化保存における指針などのガイドラインを統合したものとなっています。

・情報システムセキュリティマネジメントの基本的な構築として ISMS(JIS Q 27001:2006)に基づいた PDCA サイクルを紹介しており、リスク分析から組織的、物理的、技術的、人的な安全対策の具体例も挙げて説明しています。

・従って、位置付けとして ISMS 系と情報技術系の両方をカバーしつつ、適用範囲を医療機関のネットワークや情報システムと限定しているため、図のようなカバー範囲であると考えられます。

（３）ISO/FDIS 27799

・当規格は ISO/IEC 27002:2005（JIS Q 27002:2006）をベースに ISMS の具体的な実践について、医療機関向けのポイントを挙げて解説する予定です。

・医療機関で扱われている情報（怪我や疾病などの機微の度合いと重要性)、情報に触れる可能性のある対象者（医師、看護師、技師などの有資格者から出入り業者、パートや研修医など入れ替わりの激しい対象者等)、ゾーン（企業と異なり、部外者が自由に出入りできる外来・病棟から中央検査・救急・オペ室などの患者の生命に重大な影響を与えるゾーン等）その特徴と ISMS の具体的な実践について解説する予定です。

・したがって位置づけ例としては JIS Q 27002:2006 と同格です（医療機関向けの具体的な実践について解説している分、医療機関における ISMS の体系的、総合的な構築に有効であると考えられます)。

Annex C.　補足資料：情報漏洩等の事故に関する損害賠償と ISMS 適合性評価制度

個人情報の漏洩などの情報セキュリティインシデントに伴い、損害賠償請求などの金銭的損害が発生することが考えられますが、医療機関が保有する個人情報はその中でもその情報の価値や機微度から考えて、情報１件あたりの損害額も相当なものになることが想像できます。

仮に、医療機関のシステムに存在する患者情報などが、アクセス制御の不備などで、第三者に無断で持ち出され、露呈したような場合、損害額の見積算出の１例が、「個人情報保護に役立つ監査証跡ガイド ーあなたの個人情報を守るためにー　出典：(財)医療情報システム開発センター」の付録３で紹介されている「NPO 日本ネットワークセキュリティ協会（JNSA)」の 2005 年度情報セキュリティインシデントに関する調査報告書に紹介されています。本調査報告書によると、1 件当たりの損害額として下記の算定式が記載されています。

想定損害賠償額
＝*漏洩個人情報価値　×　情報漏洩元組織の社会的責任度　×　事後対応評価

*漏洩個人情報価値　＝基礎情報価値　×　機微情報度　×　本人特定容易度

医療機関の場合の上記パラメータの値は以下のように紹介されています。

基礎情報価値	･･･500	
機微情報度	･･･101	
本人特定容易度	･･･6	（氏名+住所があるデータのとき）
	3	（氏名 or 住所+電話番号があるデータのとき）
社会的責任度	･･･2	
事後対応評価	･･･1	（対応が適切なとき）
	2	（対応が不適切なとき）

一例として、医療機関が第三者に本人を特定することが容易なデータを漏洩し、対応が不適切なときには１件当たり

損害額＝　500　×　101　×　6　×　2　×　2　＝1,212,000　円／件

となります。これが仮に 1000 人相当の患者（個人）情報であれば、損害額の可能性として 10 億円を上回ることも考えられ、医療機関の経営に重大なダメージが与えられるものと思われます。

このような被害が発生する可能性を低くするためにもISMSの仕組みを構築し、第三者審査機関による定期的な審査を受け評価してもらうことで、改善の機会を得ながら、安全を確保・維持することになると考えられます、このような姿勢は、患者さんのみならず医師や関係者から信頼を獲得することに繋がり、経営の安定にもつながるのではないでしょうか。

さらにISMS適合性評価制度の認証を取得していることで、万が一インシデントが発生し、損害賠償問題になった際に適用可能な賠償責任保険へ加入するときの保険料が割引になる可能性があります(割引率は会社によって異なりますが50%以上の割引率を設定している場合もあるようです)。

最後に、情報漏洩の原因の多くは、設備やシステムによる対策があるにも係らず、それらを利用するユーザの人為的ミスや従業員の不正行為など「ヒト」に関わる部分が寄与していることが現状です。

日頃から機器や設備だけでなく人･組織の情報セキュリティ管理の仕組みを総合的に構築し定期的なチェックと対応を通して地域社会に貢献できる医療機関をなっていただくためにもISMS適合性評価制度の意味･価値を是非ご検討いただければと思います。

おわりに

本ガイドの作成は、ISMS 適合性評価制度技術専門部会のもとに設置した ISMS 医療 WG で行いました。ISMS 医療 WG の皆様に対し厚く御礼申し上げます。

また、本ガイドを作成するにあたり、ISMS 医療 WG で以下のような提言があったことをご紹介します。

「予防処置をより適切に行うためには、自院内のみならず、医療機関間、医療機関・薬局間などとの情報セキュリティに関する事例の共有化がはかれ、各種情報システムのとの連携を強めることがポイントになると思います。現状では、情報セキュリティインシデントに対する報告ルール、そのために記載される項目等が定義されていない状態です。情報セキュリティインシデントの事例の内容を、どの機関に対しても理解されやすく活用しやすいように整備することが重要です。」

標準的なルールがない現状で、担当者による手書きの報告書などによる事例収集では、このような実現は困難であると思われますし、医療機関の経営陣によるマネジメントレビューも難しいということになります。

このような問題を解決するために、国、産業界、学会、医療機関の各々が協力して、情報セキュリティインシデントの標準化や報告ルールの策定を行うべきだと考えます。このような活動を継続的に実施し、情報セキュリティインシデントの収集、分析などが効率的に行われる環境が構築されることにより、情報セキュリティ事故が削減し、より安全な医療サービスが提供されることが期待されます。

ISMS 医療 WG メンバー

氏名	所属／役職
メンバー	
駒瀬　彰彦	情報マネジメントシステム運営委員会 *（㈱アズジェント　取締役　技術本部長）*
野津　勤	日本画像医療システム工業会(JIRA) *（(財)理工学振興会　特別研究員）*
丸山　満彦	ISMS 適合性評価制度技術専門部会 *（監査法人　トーマツ　エンタープライズ リスク サービス部* *パートナー　公認会計士）*
茗原　秀幸	保健医療福祉情報システム工業会(JAHIS) *（三菱電機㈱　インフォメーションシステム事業推進本部* *情報セキュリティ推進センター）*
山仲　聡	ISMS 適合性評価制度技術専門部会 *（日揮㈱　第２プロジェクト本部* *ライフサイエンス事業部　メディカルプロジェクト部）*
オブザーバー	
喜多　紘一	東京工業大学　統合研究院　ソリューション研究機構 特任教授
町田　悦郎	財団法人 医療情報システム開発センター　研究開発部 研究開発第一課　課長
吉村　仁	日本画像医療システム工業会(JIRA) *（コニカミノルタ エムジー株式会社　商品企画センター* *MI 商品企画室　担当課長）*

2008 年 5 月

情報マネジメントシステム運営委員会／
ISMS 適合性評価制度技術専門部会
財団法人日本情報処理開発協会
財団法人医療情報システム開発センター