【情報資産】
組織にとって価値のある情報のことである。記載される媒体は紙、電子媒体等の形態を問わない。情報資産を漏れなく識別し、その資産価値及びリスクを評価し、保護レベルを決定することがＩＳＭＳ構築において不可欠である。
【機密性、完全性、可用性】
機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）はＣＩＡとも呼ばれ、情報セキュリティ上の要求事項の中でも最たるものと位置づけられる。ＩＳＭＳ適合性評価制度における機密性とは「認可されていない個人、エンティティ（団体等）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」、完全性とは「資産の正確さ及び完全さを保護する特性」、可用性とは「認可されたエンティティ（団体等）が要求したときに、アクセス及び使用が可能である特性」と定義されている。
【安全管理策】
リスクに対応するために実施される手順等のことを指す。
【適用宣言書】
組織の確立するＩＳＭＳに関して適用される管理目的及び安全管理策を記述した文書のこと。一般にはＪＩＳ　Ｑ　27001付属書Ａに沿って記述する。
【専用線】
特定の事業者間を接続する専用の回線であり、他事業者の通信の影響を受けず、通信回線上の機密性が高い性質を持つ。
【ＶＰＮ（仮想私設網）、ＩＰ－ＶＰＮ（閉域ＩＰ網／閉域網ＶＰＮ）、インターネットＶＰＮ】
不特定事業者が接続されるネットワーク上に構築された、特定の事業者間のみを接続する仮想的な閉域網のことをＶＰＮ（仮想私設網）と呼ぶ。
ＶＰＮのうち、通信事業者が保有する広域ネットワーク網と医療機関等に設置されている通信機器とを接続する通信回線が他のネットワークサービス等と共用されていない接続方式を提供する接続サービスを、特に、ＩＰ－ＶＰＮ（閉域ＩＰ網／閉域網ＶＰＮ）と呼ぶ。
また、オープンなネットワークであるインターネット上に構築されたＶＰＮを、特に、インターネットＶＰＮと呼ぶ。
なお、本ガイドラインでは、回線の種別を表す用語として、専用線、ＩＰ－ＶＰＮ、インターネットＶＰＮの三種類を用いることにする。
【電子媒体】
電子情報を保存、記録する媒体の総称であり、ハードディスクドライブ、ＵＳＢメモリのような、情報を記録、記憶する媒体と装置が一体となった記憶装置、光学ディスク（ＣＤ－Ｒ、ＤＶＤ－Ｒ等）や磁気ディスク（フロッピーディスク等）、光磁気ディスク（ＭＯ）、磁気テープ等の、情報を記録、記憶する記憶媒体等を含む。
【ＡＳＰ・SaaS】
ＡＳＰ及びSaaSは、ともにネットワークを通じてアプリケーション・サービスを提供するものであり、基本的なビジネスモデルに大きな差はないものと考えられる。
したがって、本ガイドラインでは、ＡＳＰ・SaaSインダストリ・コンソーシアム・ジャパンの発行した2005年版『ＡＳＰ白書』によるＡＳＰの定義『ネットワークを通じて、アプリケーション・ソフトウェア及びそれに付随するサービスを利用させること、あるいはそうしたサービスを提供するビジネスモデルを指す』を採用するとともに、ＡＳＰとSaaSを特に区別せず、「ＡＳＰ・SaaS」と連ねて呼称することとする。またＡＳＰ・SaaSを行う事業者及び団体等を「ＡＳＰ・SaaS事業者」と呼ぶこととする。

1.3. 本ガイドラインで用いる独自用語の説明
この他に、本ガイドラインで用いる用語のうち、特定の意味を持たせている用語について以下に示す。
【作業者】
情報処理事業者において情報処理装置を操作するものを作業者と呼ぶ。
【情報処理事業者】
医療情報処理を受託する情報処理事業者を意味する。
【医療情報処理施設】
情報処理装置及び配置される物理的施設（データセンター、サーバラック等）を含んだ情報処理施設全体を意味する。

２．医療情報を受託管理する情報処理事業者における安全管理上の要求事項

2.1. 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定
医療情報に係る情報処理事業を受託する機関においては、医療情報の安全確保を目的として、合理的・客観的な基準による公正な第三者認証を取得すること。

2.2. 情報資産管理

2.2.1. 資産台帳
医療情報が完全な状態にあることを保証するために、資産台帳等を適切に維持管理することを目的として、以下の管理策を適用すること。なお、資産台帳等の媒体は、紙文書、電子ファイルのいずれでも良いが、媒体特有の脅威について把握し、適切な管理策を追加すること。
⑴　医療機関等から預かる情報を管理するための管理台帳の整備について文書化して管理すること。
⑵　預託された情報の全てを資産台帳に記録すること。
⑶　必要に応じて資産台帳の閲覧が速やかに行うことができる状態で管理しておくこと。
⑷　資産台帳等へのアクセスについては、閲覧・編集が必要な作業者に制限すること。
⑸　資産台帳等を電磁的記録として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について記録すること。

2.2.2. 情報の分類
⑴　情報を分類するための指針を決定し、情報の所有者、管理責任者が指針に従って適切な分類を行うことができるようにしておくこと。
⑵　情報の所有者、管理責任者は情報の分類が正しく行われていることを定期的に確認すること。
⑶　預託される情報に対して分類にもとづいたリスク分析を実施すること。
⑷　リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること。
⑸　分類がわかるように情報にラベルをつけること（電磁的な記録にラベルをつける方式には様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得ること）。
⑹　各ラベルに応じた処理方式（保存、配送、閲覧、廃棄等）を定めること。

2.3. 組織的安全管理策（体制、運用管理規程）
⑴　医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。
⑵　個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。
⑶　個人情報保護に関しては、医療機関等の監督の下に行うこと。
⑷　情報処理の安全管理に関わる手順書、運用管理規程を整備すること。
⑸　運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内の体制及び施設、医療機関及び清掃事業者等の外部事業者との契約書の管理、情報処理に関わるハードウェア・ソフトウェアの管理方法、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理（保管・授受等）、第三者による情報セキュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載しておくこと。