第1章

情報セキュリティマネジメント

CONTENTS

SECTION 1-1

情報セキュリティの基礎知識

情報セキュリティの概念

(1) 情報セキュリティとは

情報セキュリティ（information security）とは、企業や組織が保有する情報資産の機密性、完全性、可用性を確保し、それをバランスよく維持することです。具体的には、企業や組織がもっている情報資産を、危害や損傷を受けないように保護し、不測の事態が発生したときは速やかに正常な状態に回復することを意味します。情報セキュリティで保護される情報資産には、コンピュータや通信装置などの物理的資産、業務用ソフトウェアやシステムソフトウェアなどのソフトウェア資産、データベースやファイルなどの電子化された情報、マニュアルや契約書・同意書などの紙媒体の情報、人が保有する知識や技能、組織の評判やイメージなど、幅広い範囲のものが含まれます。

JIS Q 27001:2006では、情報セキュリティを次のように定義しています。

> 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。

(2) 情報セキュリティの3要素

情報セキュリティの主要な特性には、機密性、完全性、可用性の三つがあります。これらの三つの要素のことを、アルファベットの頭文字を取って「情報セキュリティのC.I.A.」と呼ぶこともあります。

機密性（confidentiality）

JIS Q 27001:2006では、機密性を「**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**」と定義しています。**エンティティ**とは、情報システムにアクセスする人、ほかの情報システム、装置などの総称のことです。すなわち、機密性を簡単に表現すると、アクセスを認められた者だけが、決められた範囲内で情報資産にアクセスできる状態を確保することです。具体的には、情報資産に対するアクセス権限をもつ者ともたない者を明確に区別し、アクセス権限をもつ者だけが許可された範囲内で使用できるように管理することを指します。

完全性（integrity）

JIS Q 27001:2006では、完全性（インテグリティ）を「**資産の正確さ及び完全さを保護する特性**」と定義しています。簡単に表現すると、情報資産の内容が正しく、矛盾がないように保持されていることです。完全性には、**情報そのもの**が正しいことと、**情報処理の方法**が正しいことの二つを満たすことが要求されます。具体的には、データが処理される過程で、データの欠落や重複、改ざん、破壊などの異常が発生しないようにすることを指します。

可用性（availability）

JIS Q 27001:2006では、可用性を「**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**」と定義しています。簡単に表現すると、アクセスを認められた者が、必要なときにはいつでも、中断することなく、情報資産にアクセスできる状態を確保すること（**使用可能性**）です。具体的には、システムの二重化や冗長化、構成機器のグレードアップ、重要データのバックアップ、定期保守や予防保守の実施などによって、システム障害が発生しないように管理することを指します。

（3）情報セキュリティのその他の特性

JIS Q 27001:2006では、情報セキュリティのその他の特性として、**真正性、責任追跡性、否認防止、信頼性**の四つを挙げています。これらの四つの特性は、主要特性の「機密性」、「完全性」、「可用性」から導くことができるものとされています。

真正性（authenticity）

JIS Q 13335-1:2006では、真正性を「ある主体または資源が、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」と定義しています。例えば、利用者が本人であると主張したとき、その利用者が主張する身元の正しさを検証する手段を備えており、確実に本人だけを認証できることを指します。

責任追跡性（accountability）

JIS X 5004では、「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」と定義しています。例えば、情報システムやネットワーク、データベースなどのログを体系的に取得しておき、どの利用者が、いつ、どの情報資産に、どのような操作を行ったかを追跡できるようにすることを指します。

否認防止（non-repudiation）

JIS Q 13335-1:2006では、否認防止を「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」と定義しています。例えば、PKIを利用したディジタル署名やタイムスタンプを付与することによって、文書作成者が、その文書を作成した事実を後から否認できないようにすることを指します。

信頼性（reliability）

JIS Q 13335-1:2006では、信頼性を「意図した動作及び結果に一致する特性」と定義しています。例えば、ある条件下で情報システムを稼働させたとき、故障や矛盾の発生が少なく、指定された達成水準を満たしていることを指します。

例題　情報セキュリティの定義

ISMSでは、情報セキュリティは三つの事項を維持するものとして特徴付けられている。それらのうちの二つは機密性と完全性である。残りの一つはどれか。

ア　安全性　　イ　可用性　　ウ　効率性　　エ　信頼性

（情報セキュリティアドミニストレータ試験　平成18年度午前　問34）

解説

ISMSでは、情報セキュリティを、情報の機密性、完全性、可用性を維持するものとして定義しています。したがって、正解はイです。

前述のように、JIS Q 27001:2006では、この三つを次のように定義しています。

- 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、情報を使用不可または非公開にする特性
- 完全性（integrity）：資産の正確さ及び完全さを保護する特性
- 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

例題　インテグリティを脅かす攻撃

インテグリティを脅かす攻撃はどれか。

ア　Webページの改ざん
イ　システム停止をねらうDoS攻撃
ウ　システム内に保管されているデータの不正取得

エ　通信内容の盗聴

（情報セキュリティアドミニストレータ試験　平成16年度午前　問31）

解説

インテグリティ（完全性）は、情報セキュリティの3要素（機密性、完全性、可用性）のうちの一つであり、情報資産の内容が正しく、矛盾がないように保持されていることです。具体的には、データが処理される過程で、データの欠落や重複、改ざんなどの異常が発生しないようにすることを指します。よって、インテグリティを脅かす攻撃は、選択肢の中では「Webページの改ざん」が該当します。したがって、正解はアです。

なお、選択肢のイは可用性を脅かす攻撃、選択肢のウとエは機密性を脅かす攻撃です。

情報セキュリティ対策

情報セキュリティ対策は、**技術的セキュリティ**、**物理的セキュリティ**、**人的セキュリティ**、**組織的セキュリティ**の四つに分類されます。情報セキュリティ対策を策定・運用する上で重要なことは、この四つの視点から対策を検討し、できるだけ漏れがないように全体を見通した設計を行い、バランスがとれた実効性の高い対策を実装し、組織の中に定着させることです。

技術的セキュリティ対策

技術的セキュリティ対策は、IT（情報技術）を利用して情報資産を保護するセキュリティ対策です。サーバやクライアントコンピュータ、ネットワークシステム、データベース、OSやアプリケーションソフトなど、情報システムを構成するさまざまな要素を対象としているので、非常に多くの対策があります。

・主体認証（IDとパスワード、IDカード、指紋などによる利用者認証）
・アクセス制御
・権限管理
・ログ管理
・暗号技術の利用
・認証技術（ディジタル署名、メッセージ認証、タイムスタンプなど）の利用
・通信データの暗号化（SSL、IPsecなど）、電子メールの暗号化（S/MIMEなど）
・ファイアウォール、DMZ（非武装地帯）
・コンテンツフィルタ

・ウイルスなどの不正プログラム対策
・ぜい弱性対策（セキュリティホール対策）
・サービス不能攻撃対策（DoS ／ DDoS攻撃対策）

物理的セキュリティ対策

物理的セキュリティ対策は、情報資産に対する物理的な不正アクセス、災害、盗難、損傷、妨害などを防止するためのセキュリティ対策です。施設・設備や装置などに対するもの、セキュリティ境界を利用するもの、記憶媒体（書類などの紙媒体も含む）に対するものなどがあり、次のような対策が挙げられます。

・コンピュータ（サーバ、パソコンなど）や通信装置の保護
・情報資産の施錠管理（施錠付きのロッカー等に情報資産を保管する）
・ゾーニング（セキュリティレベルに応じて区域を分け、物理的に分離する）
・アクセスできる区域の制限
・IDカード、バイオメトリクス認証、監視カメラなどを用いた入退室管理
・クリアデスク／クリアスクリーン（デスク上に不要なものを残さない／画面上に不要なものを表示したままにしない）
・訪問者や情報資産の受け渡し業者の管理
・情報資産の安全な処分または再利用

人的セキュリティ対策

人的セキュリティ対策は、人による誤り、盗難、不正行為、システムの誤操作・誤用など、人が原因で発生する事故・事件を防止するためのセキュリティ対策です。手続き的なもの、管理的なもの、ルールの徹底などがあり、次のような対策が挙げられます。

・情報セキュリティポリシ、各種社内規定、マニュアルなどの遵守
・情報セキュリティに関する意識向上、教育・訓練
・アクセス権の設定などのアクセス管理
・機密保持契約（例：雇用契約書、誓約書、就業規則等で守秘義務条項を明示する）
・懲戒手続（例：セキュリティ違反時における懲戒手続を就業規則や誓約書に明示する）
・雇用終了後における情報資産の返却、アクセス権の削除

組織的セキュリティ対策

組織的セキュリティ対策は、技術的セキュリティ対策、物理的セキュリティ対策、

人的セキュリティ対策を、組織として体系的に管理し、実施し、維持するためのセキュリティ対策です。具体的には、次のような対策が挙げられます。

・情報セキュリティのための組織体制づくり
・情報資産に対する責任、分類
・情報資産の持ち出し管理（例：管理者の許可のない情報資産の持ち出しを禁止する）
・情報セキュリティインシデントの管理
・事業継続管理
・コンプライアンス、内部監査、内部統制

関連知識　管理的セキュリティ対策

人的セキュリティ対策と組織的セキュリティ対策は、どちらも組織のポリシやルールを設定し、それを遵守するために行われる管理面を重視した対策です。そのため、人的セキュリティ対策と組織的セキュリティ対策を合わせて、**管理的セキュリティ対策**と呼ぶことがあります。

セキュリティコントロール

セキュリティコントロール（security control）とは、組織の情報セキュリティを維持するために、組織体の内部や情報システムに組み込まれた仕組みのことです。セキュリティコントロールは、情報セキュリティ対策基準における具体的なセキュリティ対策（管理策）として具現化されます。したがって、

セキュリティコントロール＝情報セキュリティ対策（管理策）

と考えてよいでしょう。

セキュリティコントロールの機能を大別すると、**抑止**、**予防**、**検知**、**復旧**の四つの機能に分類することができます。なお、抑止と予防を区別せず、予防、検知、復旧の三つの機能に分類する場合もあります。

・**抑止**：セキュリティリスクを意図的に顕在化させようとする者に対し、そうした不正行為をけん制し、思いとどまらせること。
・**予防**：意図的であるか、偶発的であるかにかかわらず、セキュリティリスクが顕在化する原因を取り除くこと
・**検知**：セキュリティリスクが顕在化していないかを監視し、顕在化したリスクを早

期に検出し、通知すること

・**復旧**：セキュリティリスクが顕在化した場合、発生した損害を局所化し、速やかに原状に復帰させること

例題　情報システムのセキュリティコントロール

情報システムのセキュリティコントロールを予防、検知、復旧の三つに分けた場合、復旧に該当するものはどれか。

ア　オンラインアクセスにおけるパスワードの利用
イ　コンピュータオペレータとプログラマの職務分離
ウ　コンピュータセンタのコンティンジェンシープラン
エ　メッセージ認証

（テクニカルエンジニア（情報セキュリティ）試験　平成18年度午前　問50）

解説

ア　オンラインアクセスにおいてパスワードを利用することにより、正当な権限をもたない第三者のアクセスを防止することができるので、"予防"に該当します。

イ　プログラムを作成するプログラマが、本番用のコンピュータを操作できるコンピュータオペレータを兼任すると、プログラマに悪意がある場合、不正なプログラムを作成して本番用のシステム上で実行させることが可能になります。コンピュータオペレータとプログラマの職務分離は、このような事態の発生を未然に防ぐことになるので、"予防"に該当します。

ウ　コンティンジェンシープラン（緊急時対応計画）とは、重大な障害や災害が発生した場合を想定し、その被害の影響から重要な業務手続を保護するために策定される計画のことです。コンティンジェンシープランを策定し、訓練を実施することによって、火災や地震等で情報システムに緊急事態が発生した場合でも、速やかに情報システムを修復できるので、"復旧"に該当します。

エ　メッセージ認証を用いることによって、メッセージの改ざんの有無を検出することができるので、"検知"に該当します。

したがって、正解はウです。

例題 機密データの漏えい対策

機密データの漏えいを検知することを目的とした対策はどれか。

ア　機密データにアクセスできる利用者を限定し、パスワード管理を徹底させる。
イ　機密データに対する利用者のアクセスログを取り、定期的にチェックする。
ウ　機密データの取扱マニュアルを作成し、利用者に対して教育を行う。
エ　機密データのバックアップを取得し、その媒体を安全性の高い場所に保管する。

（情報セキュリティアドミニストレータ試験　平成19年度午前　問36）

解説

ア　機密データにアクセスできる利用者を限定し、パスワード管理を徹底させることによって、第三者が機密データにアクセスする危険性を低減することができます。したがって、機密データの漏えいを"予防"することを目的とした対策です。

イ　利用者のアクセスログを定期的にチェックすることによって、第三者が機密データにアクセスした事実を速やかに検出することができます。したがって、機密データの漏えいを"検知"することを目的とした対策です。

ウ　利用者に対して情報セキュリティ教育を行うことによって、利用者のセキュリティ意識が高められるので、不用意に機密データを漏らすことを防ぐことができます。したがって、機密データの漏えいを"予防"することを目的とした対策です。

エ　機密データのバックアックが取得された媒体を安全性の高い場所に保管することによって、地震や火災といった緊急事態が発生した場合でも、速やかに機密データを復元することができます。したがって、機密データの漏えいを"復旧"することを目的とした対策です。

したがって、正解はイです。

SECTION 1-2

情報セキュリティマネジメント

情報セキュリティマネジメントの概要

情報セキュリティマネジメント（Information Security Management）は、企業などの組織体において情報セキュリティ対策を計画し、それを確実に実践することで、情報セキュリティのレベルを維持・改善する一連の活動です。この情報セキュリティマネジメントを組織的に推進するための管理の仕組みを、**ISMS**（Information Security Management System、**情報セキュリティマネジメントシステム**）といいます。

(1) マネジメントシステムとプロセスアプローチ

製品やサービスの品質の維持・向上を図るための活動を、検品や検査、テストといった最終プロセスだけに頼るのではなく、計画、設計、開発、製造などのプロセスごとに目的や役割を明確にし、各プロセス間の相互関係を整理し、有効に機能させることによって、製品やサービスの品質向上につなげていこうという考え方を「**プロセスアプローチ**（process approach）」といいます。プロセスアプローチでは、継続的な改善活動を行うことが前提となっているため、プロセスを管理するための方法として**PDCAサイクル**を用いるのが一般的です。

このプロセスアプローチの考え方は、**ISO 9000**（品質マネジメントシステム）、**ISO 14000**（環境マネジメントシステム）、**ISO/IEC 20000**（ITサービスマネジメントシステム）、**ISO/IEC 27001**（情報セキュリティマネジメントシステム）などの**ISOのマネジメントシステム規格**で採用されています。

(2) ISMSプロセスのPDCAモデル

ISMSの国内規格であるJIS Q 27001では、組織においてISMSプロセスを確立、導入、運用、監視、維持し、さらに改善するために、**Plan-Do-Check-Act**（**計画−実行−点検−処置**）からなるPDCAモデルによるプロセスアプローチを採用しています。

ISMSプロセスでは、顧客や取引先といった利害関係者から情報セキュリティに対する要求事項と期待をインプットとして受け取り、アウトプットとして運営管理された情報セキュリティを生み出します。また、ISMSプロセスの内部においても、Plan（計画）、Do（実行）、Check（点検）、Act（処置）のPDCAサイクルを繰り返すことによって、ISMSプロセスを継続的に改善することが可能になります。

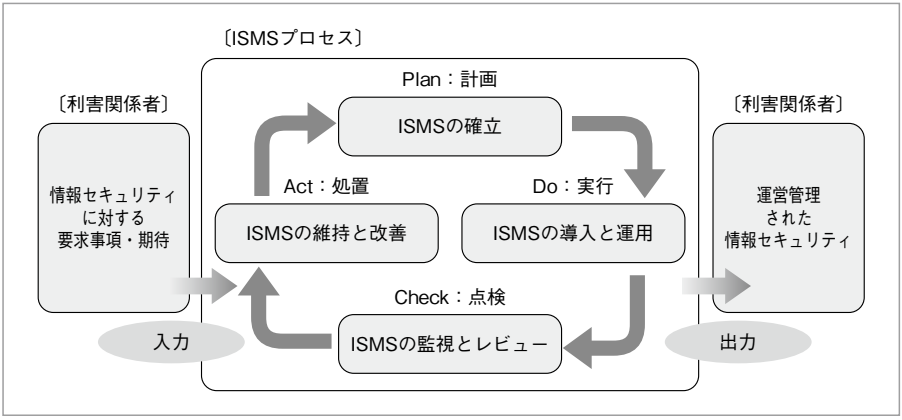

図　ISMSプロセスのPDCAモデル

Plan：計画

ISMSを**確立**します。

ISMS適用範囲の決定、ISMS基本方針や情報セキュリティ基本方針の策定、ISMS構築のための組織体制の整備、情報資産のリスクアセスメント、リスク対応、情報セキュリティ対策基準の策定などが該当します。

Do：実行

ISMSを**導入**し**運用**します。

管理策の実施と有効性測定、情報セキュリティ教育・訓練の実施、ISMS実施に必要な手順書の策定、運用状況の管理、ISMSの経営資源の管理、情報セキュリティインシデントへの対応などが該当します。

Check：点検

ISMSを**監視**し**レビュー**します。

あらかじめ定めた間隔で、**管理策の有効性測定**、**ISMSの内部監査**（**セキュリティ監査**）、**ISMSのマネジメントレビュー**（経営陣によるISMS改善のための意思決定プロセス）を実施します。これらの結果をインプット情報として、ISMSの有効性、残留リスクと受容リスク基準などについて、定期的にレビューを実施します。

Act：処置

ISMSを**維持し改善**します。

ISMSの内部監査やマネジメントレビューの結果に基づき、重要な不適合部分の**是正処置、予防処置、改善策**を実施します。

例題　ISMSプロセスのPDCAモデル

ISMSプロセスのPDCAモデルにおいて、PLANで実施するものはどれか。

ア　運用状況の管理
イ　改善策の実施
ウ　実施状況に対するレビュー
エ　情報資産のリスクアセスメント

（情報セキュリティアドミニストレータ試験　平成19年度午前　問38）

解説

ISMSプロセスのPDCAモデルは、次のような「Plan（計画）－Do（実行）－Check（点検）－Act（処置）」の四つで構成されています。

・Plan-計画　：ISMSの確立
・Do-実行　　：ISMSの導入と運用
・Check-点検：ISMSの監視とレビュー
・Act-処置　　：ISMSの維持と改善

アの「運用状況の管理」はDo（実行）、イの「改善策の実施」はAct（処置）、ウの「実施状況に対するレビュー」はCheck（点検）、エの「情報資産のリスクアセスメント」はPlan（計画）で実施される作業です。したがって、正解はエです。

ISMSの確立（Plan-計画）

ISMSの確立では、ISMSの基盤となる適用範囲を定義し、基本方針を策定します。これらに基づき、リスクアセスメント（リスク分析からリスク評価までのすべてのプロセス）を実施し、リスクに対応するための管理目的と管理策を選択します。残留リスクの承認を経営陣から得た上で、ISMSの導入・運用の許可を得ます。

ISMS確立の手順は次の①～⑩のステップからなり、さらにこの10のステップは三つのフェーズに分けられます。

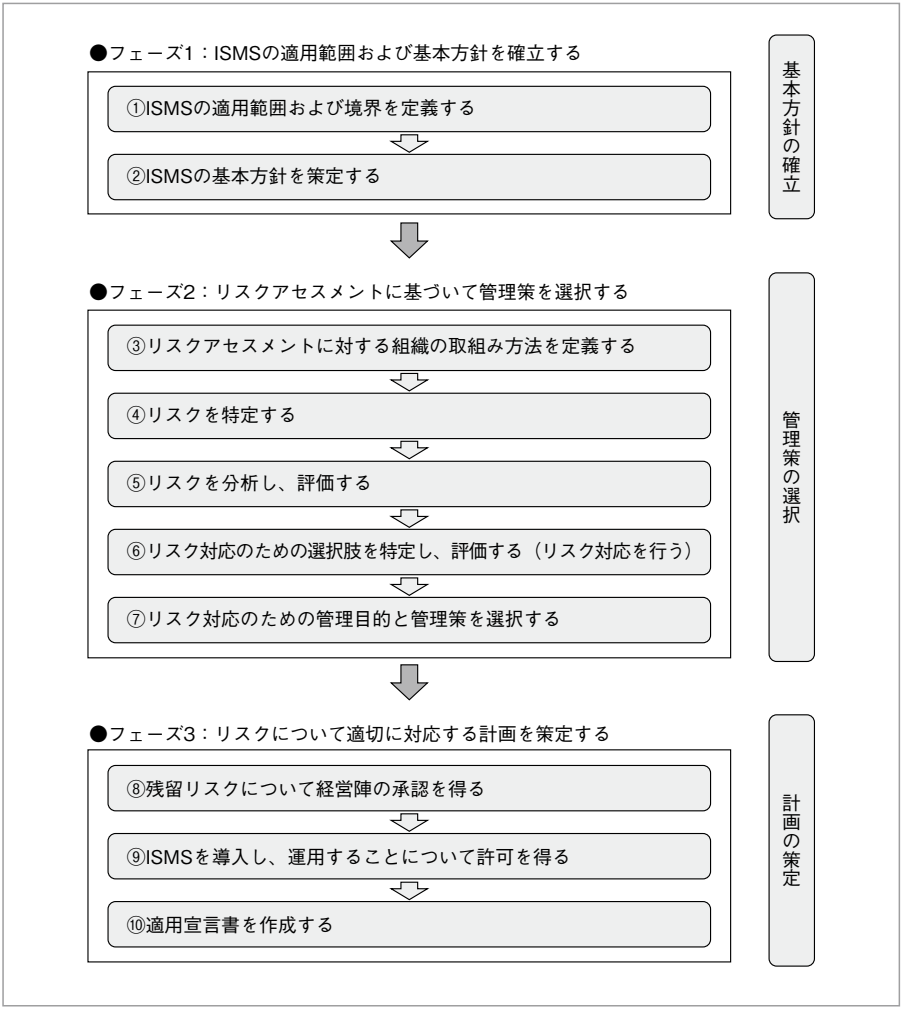

図　ISMS確立の手順

フェーズ1：ISMSの適用範囲および基本方針を確立する

〔フェーズ1の概要〕

組織のどの部分をISMSの適用範囲とするかを定義し、文書化します。ISMS基本方針を策定し、経営陣の承認を得ます。

①ISMSの適用範囲および境界を定義する

組織としてどの範囲にISMSを構築すべきかを、事業の特徴、組織、所在地、資産、技術などの観点から検討し、**ISMSの適用範囲**として定義し文書化します。

ISMSの適用範囲として、組織全体を対象とすることも、組織内のある一部門だけを対象とすることもできます。また、同じ業務やサービスを提供する複数の部門を対象とすることもできます。なお、ISMSの適用範囲を決定する際のポイントは、一つのマネジメントシステムを構成できること、適用範囲の境界線が明確であること、合理的な説明ができることです。

②ISMSの基本方針を策定する

情報セキュリティに関連する諸活動の基本方針を確立し、ISMS構築のための組織体制を構築し、これらについて経営陣から**コミットメント**（組織として実施責任があることを利害関係者に宣言すること）を得ます。

ISMS基本方針は、その企業や組織の情報セキュリティに対する基本的な考え方を示したものであり、ISMSの位置付け、ISMSの目的、枠組み、情報セキュリティに関する活動の方向性（指針）と行動の諸原則などの内容を明記します。なお、ISMS基本方針は、情報セキュリティポリシにおける**情報セキュリティ基本方針**とほぼ同じ内容のものです。

フェーズ２：リスクアセスメントに基づいて管理策を選択する

〔フェーズ２の概要〕

リスクアセスメントを実施する手順を策定し、情報資産、脅威、ぜい弱性を洗い出してリスクを識別します。リスクアセスメントを実施してリスクを算定し、その結果に基づき、それぞれのリスクについて、どのような優先順位でどのような対策を講じるかを決定します（リスク対応）。リスク対応の結果に基づき、ISMS認証基準から必要な管理目的と管理策を選択したり、その組織に独自の管理策を追加したりします。

③リスクアセスメントに対する組織の取組み方法を定義する

フェーズ１で決定したISMSの適用範囲およびISMS基本方針に基づき、組織としてどのように**リスクアセスメント**（リスク分析からリスク評価までのすべてのプロセス）を行うかを定義します。具体的には、次のような作業を実施します。

［1］リスク分析の方法（ベースラインアプローチ、詳細リスク分析、組合せアプローチなど）の中から、その組織にとって最も適切なものを選択する。

［2］リスクアセスメントの方法（情報資産の価値判断基準、脅威・ぜい弱性の評価基

準、リスク値の算出方法など）を決定し、作業を実施するための手順を文書化する。
[3] 算出されたリスク値に基づき、どのようなリスク対応をとるかという方針や目標を設定する
[4] 受容リスク基準（受容可能なリスクの水準）を定義し、経営陣の承認を得て決定する

④リスクを特定する

まず、情報資産を洗い出して**情報資産目録**を作成し、資産価値に基づいてクラス分け（公開、社外秘、秘密、極秘など）を行います。次に、脅威とぜい弱性を識別し、その大きさに従ってランク付け（低い、中程度、高いなど）を行います。

⑤リスクを分析し、評価する

④で特定したリスクについて、③で定義したリスクアセスメントの手順に従い、実際にリスクを分析し評価して、それぞれのリスクごとにリスクの大きさを算定します。

⑥リスク対応のための選択肢を特定し、評価する（リスク対応を行う）

⑤で明らかになったリスクについて、どのような優先順位でどのような対策を講じるかを決定します。具体的には、⑤で算定したリスクに基づき、リスク回避、リスク最適化（リスク低減）、リスク保有、リスク移転の中から適切な方法を選択します。なお、この作業のことを**リスク対応**といいます。

⑦リスク対応のための管理目的と管理策を選択する

⑥のリスク対応の結果に基づき、ISMS認証基準（JIS Q 27001）の附属書A「管理目的及び管理策」から必要な**管理目的**と**管理策**を選択したり、その組織に独自の管理策を追加したりします。ここでいう「管理策」とは、個々の組織員が守るべき具体的な遵守事項（ルール）のことであり、情報セキュリティポリシの**情報セキュリティ対策基準**に記載されている個々の対策の内容と同レベルのものです。

フェーズ3：リスクについて適切に対応する計画を策定する

〔フェーズ3の概要〕

経営陣によって残留リスクが承認され、ISMSの導入・運用の許可が経営陣から得られた場合には、適用宣言書を作成します。

⑧残留リスクについて経営陣の承認を得る

残留リスクとは、リスク対応を行った後にまだ残っているリスクのことです。残留リスクが受容リスク基準(受容可能なリスクの水準)を満たしているかどうかを検証・確認し、残留リスクについて経営陣の承認を得ます。

⑨ISMSを導入し、運用することについて許可を得る

残留リスクの承認を得た上で、ISMSを導入し、実際に運用することについて経営陣からの許可を得ます。

⑩適用宣言書を作成する

適用宣言書とは、その組織のISMSで適用する管理目的や管理策などが記載された文書です。⑦で選択した管理目的と管理策、これらを選択した理由を文書化し、適用宣言書にまとめます。なお、ISMS認証基準の附属書Aの管理策で除外したものがある場合には、その除外理由とそれに代わる管理策についても記載します。

ISMSの導入と運用(DO-実行)

ISMSの導入と運用では、リスクアセスメントに基づき作成したISMS基本方針、管理策(情報セキュリティ対策基準)、プロセス、手順を導入し運用します。また、導入したこれらの基本方針や管理策について有効性を測定する方法を規定します。ISMSの導入と運用の手順は、右図の①～⑧のステップからなります。

(1)リスク対応計画と経営陣の責任

リスク対応計画は、リスクアセスメントの結果に基づき選択した、リスク対応のための管理策や管理目的について、**実際の業務や情報システムに実装するための実行計画**です。リスク対応計画には、管理策や管理目的を実装するための日程表、優先順位、作業計画、管理策を実施する責任などを記載します。なお、リスク対応計画には、リスクを低減するための管理策・管理目的だけでなく、導入した管理策や管理目的が有効に機能しているかを検証するための管理策・管理目的や、異常を検出するための管理策・管理目的なども含める必要があることに留意します。

経営陣には策定されたリスク対応計画を確実に実施する責任があり、計画の実行に必要な経営資源を割り当てるとともに、経営陣自身の役割や責任を明確にすることが要求されます。

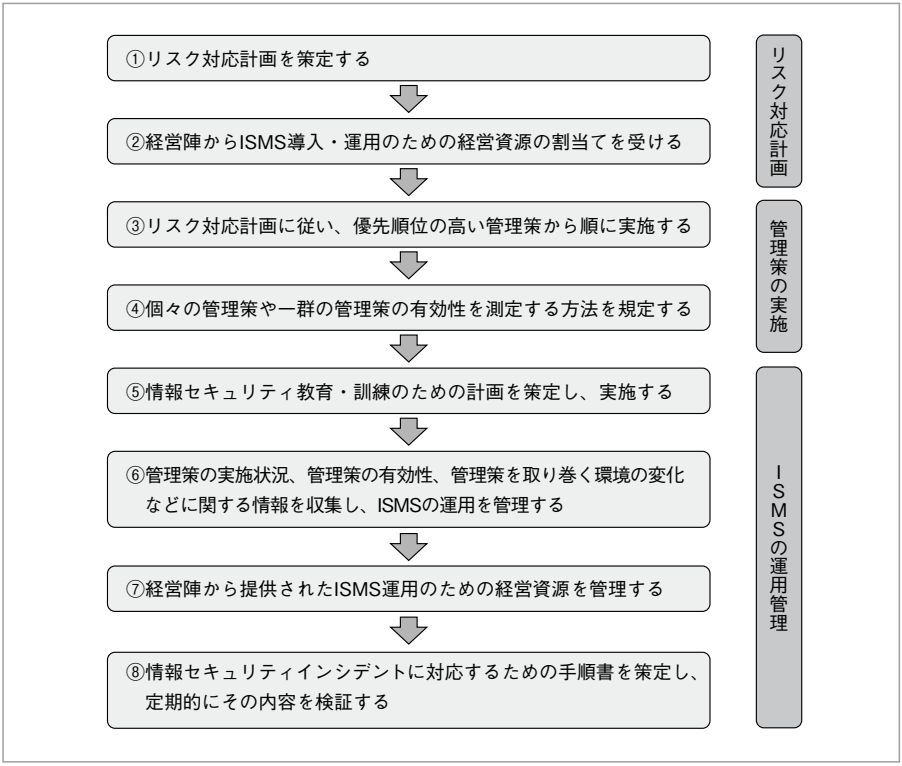

図　ISMS導入と運用の手順

(2) 管理策の有効性の測定

情報セキュリティマネジメントを維持・改善するためには、導入した管理策や管理目的について有効性を測定し、管理目的が達成されているかどうかを評価する必要があります。有効性を測定する対象は、次の二つのレベルに分けられます。

・ISMSプロセス全体を対象とした有効性の測定
・個々の管理策や一群の管理策を対象とした有効性の測定

個々の管理策の有効性を測定することは、ISMS全体のプロセスの有効性を測定することに貢献するものであり、最終的にはISMSプロセス全体の改善のために寄与します。

なお、有効性を測定する方法を決定する際には、次の点に留意します。

・有効性の測定は定期的に行う必要があることから、繰り返し測定できること
・測定結果の比較が可能であること

ISMS適合性評価制度

(1) ISMS適合性評価制度とは

ISMS適合性評価制度は、組織体が構築したISMS（Information Security Management System、情報セキュリティマネジメントシステム）が**ISMS認証基準**に準拠していることを第三者機関が認証する制度です。ISMS認証基準として国際規格との整合性がとられた国内規格を採用していることにより、国際的に整合性のとれた情報セキュリティマネジメントシステムに対する第三者適合性評価制度となっています。なお、実際の認証審査は、**JIPDEC**（情報処理開発協会）が認定した第三者機関である審査登録機関が行っています。

(2) ISMS認証基準

ISMS適合性評価制度では、**JIS Q 27001:2006（ISO/IEC 27001:2005）**を認証のための基準として用いています。また、実際にISMSを構築・運用する上で欠かせない国内規格として、**JIS Q 27002:2006（ISO/IEC 27002:2005）**があります。JIS Q 27001とJIS Q 27002はペアで用いられるもので、JIS Q 27001で要求している管理策を実施するための具体的な手引きがJIS Q 27002に規定されています。

JIS Q 27001:2006（ISO/IEC 27001:2005）

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）は、ISMSの国際規格であるISO/IEC 27001:2005を国内規格化したものです。ISMSの構築・運用に関する認証基準であり、**組織がISMSを構築・運用するための要求事項**が、次のような枠組みで体系的にまとめられています。

0　序文（Introduction）
1　適用範囲（Scope）
2　引用規格（Normative references）
3　用語及び定義（Terms and definitions）
4　情報セキュリティマネジメントシステム（Information security management system）

5 経営陣の責任（Management responsibility）
6 ISMS内部監査（Internal ISMS audits）
7 ISMSのマネジメントレビュー（Management review of the ISMS）
8 ISMSの改善（ISMS improvement）

また、附属書A「管理目的及び管理策」にはJIS Q 27002の概略が示されており、管理領域、管理目的、管理策などが記載されています。

JIS Q 27002:2006（ISO/IEC 27002:2005）

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）は、ISMSの国際規格であるISO/IEC 27002:2005を国内規格化したものです。ISMSの構築・運用に関する実施基準（ガイドライン）であり、組織の情報セキュリティに責任をもつ人々に向けて、**効果的なISMSを実施するための規範（ベストプラクティス＝最良の事例）**がまとめられています。JIS Q 27001の附属書A「管理目的及び管理策」の内容がより詳細に記述されており、それぞれの管理策ごとに「**実施の手引き**」や「**関連情報**」が示されています。そのため、ISMSの構築時において管理策を導入する際には、このJIS Q 27002を参照する必要があります。

関連知識　認証基準と実施基準

ISOのマネジメントシステム規格には、**ISO 9001**、**ISO 14001**、**ISO/IEC 20000-1**、**ISO/IEC 27001**などがあります。これらは**認証基準**（審査の際に使用される認証用規格）であり、認証を取得するに当たって「満たさなければならない**要求事項**」が記述されています。

一方、**ISO/IEC 20000-2**や**ISO/IEC 27002**などの規格は**実施基準**（ガイドライン）であり、認証取得を目指す組織にとって「実施することが望ましいとされる**推奨事項**」が記述されています。

例題　JIS Q 27001:2006（ISO/IEC 27001:2005）

“JIS Q 27001:2006（ISO/IEC 27001:2005）情報セキュリティマネジメントシステム－要求事項”に規定されているものはどれか。

ア ISMSが適切に運用されているかどうかを評価するために、定期的に外部監査を受けなければならない。

イ　経営者の責任が重要であり、コミットメント、経営資源の提供、マネジメントレビューなどに関与しなければならない。
ウ　附属書の管理策は、すべて適用しなければならない。
エ　リスクアセスメントで明らかになったすべてのリスクに対して、リスク管理策を適用しなければならない。

（テクニカルエンジニア（情報セキュリティ）試験　平成19年度午前　問54）

解説

ア　JIS Q 27001では、Check（点検）フェーズにおいてISMSの有効性を確認するために、定期的に「内部監査」を行うことを規定しています。
イ　JIS Q 27001では、経営者の責任として、ISMSの実効性を担保するために、コミットメント、経営資源の提供、マネジメントレビューなどに関与しなければならないことが規定されています。
ウ　附属書の管理策をすべて適用する必要はなく、組織の実情に合わせて必要な管理策を選択します。
エ　リスクアセスメントで明らかになったすべてのリスクのうち、その組織における受容リスク基準を満たしているものについては、リスク管理策を適用する必要はありません。

したがって、正解はイです。

SECTION 1-3 情報セキュリティポリシ

情報セキュリティポリシ

(1) 情報セキュリティポリシとは

情報セキュリティポリシとは、**企業や組織が保護すべき情報資産と、それを保護する理由を明示したもの**です。企業や組織が、情報セキュリティに対する考え方や取組みを示すために策定します。そのため、情報セキュリティポリシの策定作業は経営陣(代表取締役など)が中心となって行うべきであり、次の二つの内容を含んでいることが要求されます。

・情報セキュリティに対する経営陣の基本方針や考え方が明確に示されていること
・情報セキュリティのレベルを適切に維持・管理するために遵守すべきルールが具体的に示されていること

また、策定した情報セキュリティポリシは、文書化してすべての社員や従業員に配布し、**組織員全員に周知徹底させる**ことが重要です。情報セキュリティポリシを周知徹底させるためのポイントとして、次の二つの事項が挙げられます。

・責任者や従業員を含めたすべての利用者が、情報セキュリティの脅威および懸念を認識していること
・すべての利用者が、通常の仕事のなかで組織のセキュリティ基本方針を維持することの重要性を認識していること

情報セキュリティポリシを策定し、それを実践して適切に運用管理することによって、次のような効果が期待できます。

・体系的で合理的なセキュリティ対策を実施できる
・組織員の情報セキュリティに対する意識を高められる
・顧客などからの対外的な信頼度が向上する

(2) 情報セキュリティポリシの構成と位置付け

情報セキュリティポリシの構成や位置付けなどを明確に定義しているものはありません。なお、情報処理技術者試験では、情報セキュリティポリシを**「情報セキュリティ基本方針」と「情報セキュリティ対策基準」の二つを合わせたもの**として定義してい

ます。

なお、情報セキュリティ基本方針は、組織の情報セキュリティに取り組む姿勢を宣言するものなので、一般には外部からの信頼を得るために公開します。一方、情報セキュリティ対策基準や実施手順は、具体的なセキュリティ対策や防御方法が記述されているので、外部からの攻撃の足がかりにされないように非公開にします。

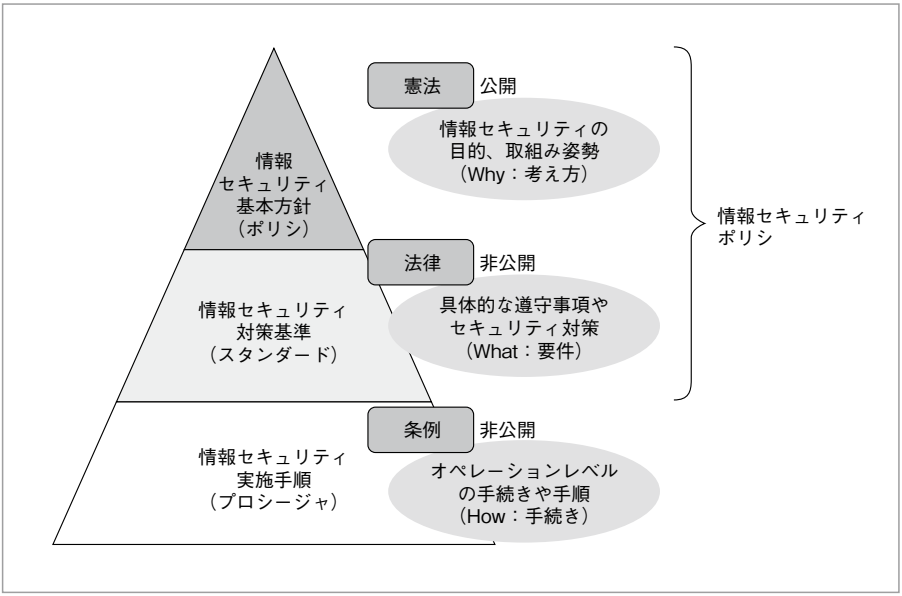

図　情報セキュリティポリシの位置付け

情報セキュリティ基本方針（ポリシ）

情報セキュリティ基本方針は、**企業や組織の情報セキュリティに取り組む姿勢や基本的な考え方を明文化したもの**であり、情報セキュリティにおける憲法のような役割をもっています。情報セキュリティの目的と、その目的を達成するためにとるべき行動を社内外に宣言する文書であり、いったん作成された後はほとんど改訂されることはありません。

情報セキュリティ基本方針には、基本理念や目的、情報セキュリティポリシの役割と位置付け、適用範囲、組織体制、法令等の遵守、情報セキュリティポリシに違反したときの罰則などが記述されています。また、情報セキュリティ対策基準に規定されていないような事態が発生したときの行動や判断の指針となります。

情報セキュリティ対策基準（スタンダード）

情報セキュリティ対策基準は、情報セキュリティ基本方針を実現するために必要となる、**個々の組織員が守るべき具体的なルールやセキュリティ対策を示したもの**です。情報セキュリティ対策基準に規定されている個々の具体的なルールや対策のことを「**管理策**」ともいいます。

情報セキュリティ対策基準には、目標とする情報セキュリティのレベルを維持・確保するための具体的な管理策が記述されています。その組織に特有のセキュリティ環境に合うようにカスタマイズされた管理策を集めたものであり、一般には**技術的対策、物理的対策、人的対策、組織的対策**に分類して記述します。

情報セキュリティ実施手順（プロシージャ）

情報セキュリティ実施手順は、**情報セキュリティ対策基準を実施するための詳細な手順や手続きを記述したもの**です。マニュアル的な文書であり、特定の部署や業務を対象とした運用手順書／実施手順書、ハードウェアやソフトウェアの設定手順書／操作マニュアル、利用者ガイドなどが該当します。

情報セキュリティポリシの策定

(1) 情報セキュリティポリシ策定のポイント

実効性のある情報セキュリティポリシを策定するには、次のようなポイントに留意します。

・情報セキュリティポリシの対象範囲は組織全体とすること

組織全体で統一した情報セキュリティポリシを策定することによって、情報セキュリティに対する認識を全組織員が共有できるので、情報セキュリティの実効性を高めることができます。

・組織の実情に即した情報セキュリティポリシが策定されていること

それぞれの組織ごとに、置かれている経営環境やもっている経営資源が異なるので、他社のものをまねたり、ひな形をそのまま適用したりするのではなく、実情に即した内容にカスタマイズする必要があります。

・経営陣の承認が得られていること

経営陣自らが情報セキュリティの重要性を認識し、経営陣の強いリーダシップのもとで情報セキュリティポリシを策定することによって、必要な経営資源が提供さ

れ、情報セキュリティポリシの実効性を高めることができます。

・情報セキュリティを推進する体制が構築されていること

組織全体として情報セキュリティを推進するためには、「全社横断的な組織体制が存在すること」、「情報セキュリティに関する役割と責任が明確に定められていること」、「情報セキュリティポリシが周知徹底されていること」などの条件が満たされている必要があります。情報セキュリティを推進する中心的な役割を担い、経営陣や各部門の代表者が参加する全社横断的な組織として**情報セキュリティ委員会**があり、組織内に設置することが推奨されています。

・組織活動を行う上で遵守すべき法令等が網羅されていること

コンプライアンスの重要性は非常に高まっており、法令等に違反した場合には企業の存続そのものが危ぶまれます。そのため、遵守すべき法令等の内容を正確に把握するとともに、定期的に情報収集を行い、適宜情報セキュリティポリシに反映させる必要があります。

関連知識　情報セキュリティポリシにおける基本原則

情報セキュリティポリシを策定する際には、次の原則に配慮します。

- **必要の原則（need to knowの原則）**
  情報を開示するときは、業務上において知る必要がある人にだけに限定すること。
- **最小権限の原則**
  利用者やプロセスに権限を与えるときには必要最小限の権限を付与すること。特に特権を与えるときには注意が必要であり、必要な管理者だけに限定するとともに、特権を与える時間や範囲をできるだけ限定して必要最小限に付与する。
- **リスク評価の原則**
  セキュリティ対策（管理策）は、リスクアセスメント（リスク分析からリスク評価までのすべてのプロセス）に基づいて策定されること

(2) 情報セキュリティ基本方針策定のポイント

情報セキュリティ基本方針は、**企業や組織の情報セキュリティに対する基本的な考え方や姿勢**を明示したものです。情報セキュリティ基本方針に記載する項目の例を、右ページの枠内に示します。

なお、従業員などが情報セキュリティポリシに違反した場合に備え、**就業規則に基づく正式な懲戒手続**を整備しておく必要があります。具体的には、情報セキュリティポリシの中に罰則規定を盛り込み、これを従業員に周知徹底させることであり、正式

な懲戒手続があることによってポリシ違反に対する**抑止力**が働きます。なお、罰則規定が明文化されていない場合には、情報セキュリティポリシが形骸化したり、懲戒処分になった従業員の間で不公平感が生じたりするなどの弊害が発生することにも注意します。

1. 基本理念および目的
   組織が情報セキュリティに取り組む姿勢や目的などを示します。
2. 用語の定義
   情報セキュリティポリシで使用されている主な用語の定義を記載します。
3. 情報セキュリティポリシの役割と位置付け
   情報セキュリティポリシが担う役割や、組織における情報セキュリティポリシの位置付けを示します。
4. 適用範囲
   情報セキュリティポリシが適用される範囲を示します。
5. セキュリティ対策の方針
   経営方針との整合性を図り、セキュリティ対策の方針を示します。
6. 組織体制、責任と権限
   情報セキュリティを推進するための組織体制、各組織のもつ責任と権限を示します。
7. 教育
   組織員に対して情報セキュリティ教育を定期的に実施することを明文化します。
8. 法令等の遵守
   関係法令等を遵守することを明文化します。
9. 罰則
   情報セキュリティポリシに違反した場合には罰則が適用されることを明文化します。
10. 関連文書
    文書管理規定や各種社内規定など、他の文書との関連を示します。

(3) 情報セキュリティ対策基準策定のポイント

情報セキュリティ基本方針が理念や考え方といった抽象的な内容であるのに比べ、情報セキュリティ対策基準には**個々の組織員が守るべき具体的なルール**(**管理策**)が規定されます。情報セキュリティ対策基準に規定する管理策は、物理的セキュリティ、

技術的セキュリティ、人的セキュリティ、組織的セキュリティに大別されます。

一般的な企業の場合の情報セキュリティ対策基準には、次のような内容が盛り込まれます。

1. 組織および体制
   最高責任者（社長）、情報セキュリティ委員会の設置、実施責任者、情報セキュリティ管理者、ネットワーク管理者などに関する規定
2. 情報の分類と管理
   重要度による情報資産の分類基準、分類された情報資産の管理方法に関する規定
3. 物理的セキュリティ
4. 人的セキュリティ
5. 技術的セキュリティ
6. 運用
   情報システムの監視とポリシの遵守状況の確認（運用管理）、運用管理における留意点、侵害時の対応策などに関する規定
7. 法令遵守
8. セキュリティポリシ違反への対処
   就業規則に基づく懲罰規定や罰則規定
9. 評価と見直し

(4) ベースラインアプローチ

従業員数が多く関連する企業が多い場合には、情報セキュリティ対策基準に盛り込むべき管理策は大きく膨れ上がり、カバーする範囲も多岐にわたるので、自組織だけで一からすべてを作成するには大変な労力がかかります。そのため、情報セキュリティ対策基準を策定する際には、記述漏れが発生しないようにするため、既存の対策基準のひな形や管理策集を上手に利用し、それを自組織の実情に合わせてカスタマイズする方法が推奨されています。なお、このような対策基準の作成方法のことを**ベースラインアプローチ**といいます。

管理策集の代表的なものにJIS Q 27002があり、その概略が示されているJIS Q 27001の附属書A「管理目的及び管理策」は次のような項目で構成されています。

A.5. 情報セキュリティ基本方針
A.5.1 情報セキュリティ基本方針
A.6. 情報セキュリティのための組織
A.6.1 内部組織
A.6.2 外部組織
A.7 資産の管理
A.7.1 資産に対する責任
A.7.2 情報の分類
A.8 人的資源のセキュリティ
A.8.1 雇用前
A.8.2 雇用期間中
A.8.3 雇用の終了又は変更
A.9 物理的及び環境的セキュリティ
A.9.1 セキュリティを保つべき領域
A.9.2 装置のセキュリティ
A.10 通信及び運用管理
A.10.1 運用の手順及び責任
A.10.2 第三者が提供するサービスの管理
A.10.3 システムの計画作成及び受入れ
A.10.4 悪意のあるコード及びモバイルコードからの保護
A.10.5 バックアップ
A.10.6 ネットワークセキュリティ管理
A.10.7 媒体の取扱い
A.10.8 情報の交換
A.10.9 電子商取引サービス
A.10.10 監視
A.11 アクセス制御
A.11.1 アクセス制御に対する業務上の要求事項
A.11.2 利用者アクセスの管理
A.11.3 利用者の責任
A.11.4 ネットワークのアクセス制御
A.11.5 オペレーティングシステムのアクセス制御
A.11.6 業務用ソフトウェア及び情報のアクセス制御
A.11.7 モバイルコンピューティング及びテレワーキング
A.12 情報システムの取得、開発及び保守
A.12.1 情報システムのセキュリティ要求事項
A.12.2 業務用ソフトウェアでの正確な処理
A.12.3 暗号による管理策
A.12.4 システムファイルのセキュリティ
A.12.5 開発及び支援プロセスにおけるセキュリティ
A.12.6 技術的ぜい弱性管理
A.13 情報セキュリティインシデントの管理
A.13.1 情報セキュリティの事象及び弱点の報告
A.13.2 情報セキュリティインシデントの管理及びその改善
A.14 事業継続管理
A.14.1 事業継続管理における情報セキュリティの側面
A.15 順守
A.15.1 法的要求事項の順守
A.15.2 セキュリティ方針及び標準の順守、並びに技術的順守
A.15.3 情報システム監査に対する考慮事項

例題　機密データの漏えい対策

ISMS適合性評価制度における情報セキュリティポリシに関する記述のうち、適切なものはどれか。

ア　基本方針は、事業の特徴、組織、その所在地、資産及び技術を考慮して策定する。
イ　重要な基本方針を定めた機密文書であり、社内の関係者以外の目に触れないようにする。
ウ　セキュリティの基本方針を述べたものであり、ビジネス環境や技術が変化しても変更してはならない。
エ　特定のシステムについてリスク分析を行い、そのセキュリティ対策とシステム運用の詳細を記述したものである。

（情報セキュリティアドミニストレータ試験　平成17年度午前　問29）

解説

情報セキュリティポリシは、企業や組織が保護すべき情報資産と、それを保護する理由を明示したものであり、企業や組織が情報セキュリティに対する考え方や取組みを示すために策定されます。ISMS適合性評価制度のISMS認証基準（Ver.2.0）では、「第4　情報セキュリティマネジメントシステム」の「4.2 ISMSの確立及び運用管理」において、ISMS基本方針を策定する手順として、基本方針は「事業の特徴、組織、その所在地、資産及び技術の観点から」策定することが記載されています。

ア　適切な記述です。
イ　情報セキュリティポリシは、情報セキュリティに対する考え方や取組みを示すために策定されるものであり、組織の構成員全員に周知されなければなりません。
ウ　情報セキュリティポリシは、ビジネス環境や技術の変化に柔軟に対応させるため、定期的な見直しを行い、継続的に改善する必要があります。
エ　情報セキュリティポリシは、特定のシステムだけを対象とするのではなく、組織全体として保護すべき情報資産を対象としたものであり、それを保護する理由や行動指針を明文化したものです。

したがって、正解はアです。

SECTION 1-4 リスクマネジメント

リスクとリスクマネジメント

(1)リスクの概念

一般にリスクというと「予期しないことが発生する可能性」のことをいい、「事象の発生確率と事象の結果の組合せ(JIS TR Q 0008:2003)」と定義されています。組織活動におけるリスクは、**純粋リスク**と**投機的リスク**に分けられます。

- **純粋リスク**　：災害、事故、盗難、障害などのように、マイナスの影響(損失)のみが発生するリスク。
- **投機的リスク**：事業や投資などのように、マイナスの影響(損失)が発生する可能性もあれば、プラスの影響(利益)が発生する可能性もあるリスク。

情報セキュリティにおけるリスクマネジメントでは、純粋リスクのみを対象とします。

(2)情報セキュリティにおけるリスク

情報セキュリティにおけるリスクとは、「**情報資産にマイナスの影響を与える事象が起きて、それが原因で組織に損失が発生する可能性**」のことです。また、リスクの大きさは、「リスクと考えていた事態が実際に起きる確率(**事象の発生確率**)」と「その事態が起きたことによって発生する損失の大きさ(**事象の影響度**)」の組合せで測定されます。

リスクを理解する上で重要なことは、「リスクが組織にただ存在している」だけでは何も起こらず、

- **ぜい弱性**(情報セキュリティ上の弱点)
- **脅威**　(ぜい弱性につけ込んで情報資産を脅かすもの)

の二つが結びついたときに、リスクが現実のものとなって損失が発生するという考え方です。すなわち、リスクを正しく捉えるためには、情報資産、脅威、ぜい弱性の三つの要素を識別し、それぞれの大きさを算定する必要があります。「事象の発生確率」は**ぜい弱性と脅威の大きさ**(**脅威×ぜい弱性**)によって決まり、「事象の影響度」は**情報資産の価値**によって決まります。

(3)リスクマネジメント

情報セキュリティにおける**リスクマネジメント**(risk management)とは、情報資産に対するセキュリティリスクを分析・評価し、優先順位を付けて適切な管理策を決定することによって、**許容されるコストの範囲内でリスクを最小限に抑え、除去するようにコントロールする一連の活動**です。リスクマネジメントでは、情報資産、脅威、ぜい弱性の三つの視点でリスクの大きさを評価し、そのリスクにどのように対応すべきかを決定し、適切なリスク対応策を決定します。具体的には、次のような一連のプロセスをPDCAサイクルで回します。

①リスクアセスメントを行う
②リスク対応を行う
③リスク対応計画を策定し、管理策を導入する
④導入した管理策の妥当性を評価し、見直しと改善を行う

リスクアセスメントとは「リスク分析を行い、算定されたリスクについてリスク評価を行うこと」であり、**リスク対応**とは「リスク評価の結果に基づき、特定したリスクが受容可能なリスクの水準以下になるように適切な管理策を選択すること」です。

リスクマネジメントに関連する用語をJIS TR Q 0008:2003などに基づいて整理すると、右ページの図のようになります。なお、図中の**リスク因子**(risk source)とは、情報資産にマイナスの影響を与える原因である「脅威」と、情報資産が抱える情報セキュリティ上の弱点や欠陥である「ぜい弱性」を組合せたものです。

(4)リスクマネジメントにおける留意点

リスク分析で明らかになったすべてのリスクについて対応策を講じることは、時間と費用がかかり過ぎて現実的ではありません。リスクマネジメントでは、限られた予算を有効に活用し、損失発生の可能性を最小限に抑えられるような対応策を講ずる必要があります。そのためには、損失額と発生確率を予想し、**リスクの大きさに従って優先順位を付ける**ことが重要になります。

<table>
<tr><td colspan="4">リスクマネジメント(risk management)</td></tr>
<tr><td></td><td colspan="3">リスクアセスメント(risk assessment)</td></tr>
<tr><td></td><td></td><td colspan="2">リスク分析(risk analysis)</td></tr>
<tr><td></td><td></td><td></td><td>リスク因子の特定</td></tr>
<tr><td></td><td></td><td></td><td>リスク算定</td></tr>
<tr><td></td><td></td><td colspan="2">リスク評価(risk evaluation)</td></tr>
<tr><td></td><td colspan="3">リスク対応(risk treatment)</td></tr>
<tr><td></td><td></td><td colspan="2">リスク回避</td></tr>
<tr><td></td><td></td><td colspan="2">リスクの最適化(リスクの低減)</td></tr>
<tr><td></td><td></td><td colspan="2">リスク移転</td></tr>
<tr><td></td><td></td><td colspan="2">リスク保有</td></tr>
<tr><td></td><td colspan="3">リスクの受容(risk acceptance)</td></tr>
<tr><td></td><td colspan="3">リスクコミュニケーション(risk communication)</td></tr>
</table>

図　リスクマネジメントに関連する用語(JIS TR Q 0008:2003)

例題　情報システムのリスクマネジメント

情報システムのリスクマネジメント全体の説明として、最も適切なものはどれか。

ア　事故や災害の発生を防止したり、それが万一発生した場合には損失を最小限にしたりする手段であり、回避、最適化、移転、保有などの手段がある。

イ　情報システムの機能特性を損なう不安定要因やシステムに内在するぜい弱性を識別して、企業活動に生じる損失を防止、軽減するとともに、合理的なコストでの対策を行う。

ウ　情報システムの機能に障害が発生した際に、業務の中断や機密漏えいを、防止又は軽減する緊急時対策を行う。

エ　リスクを経済的な範囲で最小化するコントロールを設計するために必要な情報を提供する。

(情報セキュリティアドミニストレータ試験　平成20年度午前　問33)

解説

情報システムのリスクマネジメントでは、システムに内在するぜい弱性とぜい弱性につけ込む脅威を識別してリスクの大きさを算定し(リスクアセスメント)、リスクを受容可能な水準まで低減させる対策を策定し(リスク対応)、合理的なコストで対策を行う、という一連のプロセスを実施します。したがって、正解はイです。

そのほかの選択肢に関する説明は、次のとおりです。

ア　リスクマネジメントの一部である「リスク対応」の説明です。
ウ　リスクマネジメントの一部である「緊急時対応計画（コンティンジェンシープラン）」の説明です。
エ　「リスクを経済的な範囲で最小化するコントロール（管理策）を設計する」ことは、リスク対応の方法のうちの「リスク最適化（リスク低減）」に該当します。

午後問題の演習

情報セキュリティ対策とリスクの要素

問　題

情報セキュリティ対策の検討に関する次の記述を読んで、設問に答えよ。

C主任：情報セキュリティ対策を検討するには、どのような観点で整理するのがよいのでしょうか。
D課長：そうだな。例えば、リスクを低減するための情報セキュリティ対策を、抑止、予防、検知、回復の四つの観点から検討するという考え方がある。
C主任：すみませんが、抑止、予防、検知、回復について、もう少し詳しく教えていただけないでしょうか。
D課長：抑止とは、リスクを［　a　］に発現させようとする者に対して、そうした行為を［　b　］し、思いとどまらせるために実施する対策をいう。予防とは、［　a　］であるか、［　c　］であるかにかかわらず、リスクが発現する原因を取り除くために実施する対策をいう。さらに、検知とは、発現したリスクを早期に発見するために実施する対策であり、回復は、損害を局所化し、原状への復帰を図るために実施する対策をいう。
C主任：リスクの要素には、［　d　］と［　e　］が含まれているという話は聞いたことがあるのですが、それらとの関係はどう考えればよいのでしょうか。
D課長：抑止は人的な［　d　］の発生を減少させるためのもの、予防は［　d　］に付け込まれる［　e　］を減少させるためのものと考えれば分かりやすい。
C主任：分かりました。早速、検討を始めます。

設 問

本文中の［ a ］～［ e ］に入れる適切な字句を解答群の中から選び、記号で答えよ。

解答群

ア 意図的　イ 可用性　ウ 看過　エ 完全性　オ 機密性
カ 脅威　キ 偶発的　ク 継続的　ケ けん制　コ 資産価値
サ ぜい弱性

（情報セキュリティアドミニストレータ試験 平成19年度午後Ⅰ 問2改題）

設問の解説

空欄a～空欄c

情報セキュリティ対策（セキュリティコントロール）には多様な分類方法がありますが、対策の機能面に着目した場合、一般には「抑止、予防、検知、回復」の四つに分類します。四つのうちの抑止とは、リスクを「意図的」に発現させようとする者に対して、そうした行為を「けん制（ある行為をさせないように抑制すること）」し、思いとどまらせるために実施する対策です。

抑止と予防は似ており、両方ともリスクを発現させないために実施する対策という点で共通しています。この二つの違いは、抑止がリスクを「意図的」に発現させようとする者を対象としているのに対し、防止は「意図的」であるか、「偶発的」であるかにかかわらず、すべての利用者を対象としていることです。

したがって、空欄aには「意図的」、空欄bには「けん制」、空欄cには「偶発的」が入ります。

空欄d、空欄e

リスクの要素は、情報セキュリティで保護すべき「情報資産」、情報資産にマイナスの影響を与える潜在的な原因である「脅威」、組織や情報資産に内在する情報セキュリティ上の弱点や欠陥である「ぜい弱性」からなります。脅威とぜい弱性はリスク因子とも呼ばれ、脅威がぜい弱性に付け込み、この二つが結び付いたときにリスクが発現します。したがって、空欄dと空欄eには、「脅威」と「ぜい弱性」のいずれかが入ります。ここで、問題文中の「［ d ］に付け込まれる［ e ］」という表現に

着目しましょう。脅威がぜい弱性に付け込むので、付け込む側の空欄dは「脅威」、付け込まれる側の空欄eは「ぜい弱性」になります。

解答

a：ア　　b：ケ　　c：キ　　d：カ　　e：サ

リスクアセスメント

リスクアセスメント（risk assessment）は、JIS Q 27001:2006によると「リスク分析からリスク評価までの全てのプロセス（TR Q 0008:2003）」と定義されています。すなわち、リスクアセスメントとは「リスク分析を行い、算定されたリスクについてリスク評価を行うこと」であり、単にリスク評価を行うだけでなく、その前のプロセスであるリスク分析も含んでいます。

（1）リスク分析とリスク評価

リスク分析は、組織や情報資産に潜在する多様なリスクを洗い出し、その大きさを算定することです。リスク分析の結果を受けて、その企業の経営判断によって定めた独自の判定基準（**リスク評価基準**）と比較し、そのリスクの重大さを決定することを**リスク評価**といいます。リスク評価では、算定されたリスクについて受容リスク基準を満たしているかどうかを評価し、それぞれのリスクについてリスク対応を行うかどうかも決定します。

リスク分析では、まず情報セキュリティで保護すべき情報資産を洗い出し、重要度ごとに分類します。その次に、その情報資産に対する脅威とぜい弱性を徹底的に洗い出します。そして、情報資産、脅威、ぜい弱性の関連性を明らかにし、想定されるセキュリティリスクの損失額と発生確率を予測し、それぞれのリスクの大きさを算定します。

なお、リスクの損失額を予測する際には、セキュリティ事故によって発生する**直接的損失**（紛失や破壊によって被った直接的な被害）や**対応費用**（システムの復旧費用や復旧するまでの間の代替手段にかかる費用など）だけでなく、**間接的損失**（事故によって失った信用を回復するためにかかる費用）についても考慮する必要があります。

（2）リスクアセスメントの重要性

ISMSで保護すべき情報資産には、その組織に独自の特性や固有のリスクがあり、情報セキュリティ対策（管理策）にはそれらが反映されていなければなりません。も

し、リスクアセスメントを実施せずに情報セキュリティ対策が策定された場合には、その対策は、**組織に固有のリスクに対応していないため、不適切なものになってしまう**という問題が生じます。そのため、情報セキュリティ対策を策定する際には、必ずリスクアセスメントを実施して受容リスク基準を満たしていないリスクを判別し、そのリスクに対してどのような対応方法をとるかを決定するという手順を経る必要があります。

(3)リスク分析方法

ISMSにおける代表的なリスク分析方法には、次の四つがあります。ここでは、これらの四つの方法について概要を説明します。

ベースラインアプローチ(baseline approach)

ベースラインアプローチは、公表されている各種の基準やガイドラインなどに基づいて一定のセキュリティレベルを設定し、実施している管理策とのギャップ分析を行ったうえで、リスクを評価する方法です。詳細リスク分析とは異なり、個々の情報資産に対するリスクの分析・評価は行いません。公表されている基準やガイドラインなどをベースライン(セキュリティ対策の標準)として一律に適用するので、リスク分析にかかる労力や時間を軽減することができるというメリットがあります。

詳細リスク分析(detail risk analysis)

詳細リスク分析は、個々の情報資産ごとにリスクの分析・評価を行う方法です。ISMSの適用範囲に含まれる情報資産を洗い出し、それぞれの情報資産に対して、情報価値、脅威、ぜい弱性、セキュリティ要件を識別し、情報資産ごとにリスクを評価します。詳細リスク分析では、情報資産ごとにきめ細かいリスクアセスメントを行うことができる反面、作業量が多くなるので手間と労力がかかります。

非形式アプローチ(informal approach)

非形式アプローチは、リスク分析を行う組織や担当者の経験や判断に基づき、リスクを評価する方法です。体系的なアプローチをとらないため、担当者の主観や考え方に影響を受けやすく、リスクアセスメントの結果の正当性を保証するのが難しいというデメリットがあります。

組合せアプローチ(複合アプローチ:combined approach)

組合せアプローチは、複数のリスク分析方法を併用し、それぞれの短所と長所を相

互に補完できるように組合せる方法です。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ことが多く、基本的な情報資産についてはベースラインアプローチを採用し、重要な情報資産に限って詳細リスク分析を適用するという方法がとられます。組合せアプローチでは、それぞれのリスク分析方法の長所を生かせるので、作業効率や分析精度の向上を図ることができるというメリットがあります。

(4)リスクの特定

リスクアセスメントでは、最初に「リスクを特定する」ための作業を行います。

まず、情報資産を洗い出して情報資産目録を作成し、資産価値に基づいてクラス分け(公開、社外秘、秘密、極秘など)を行います。次に、脅威とぜい弱性を識別し、その大きさに従ってランク付け(低い、中程度、高いなど)を行います。

情報資産

情報資産は、**情報セキュリティで保護すべき対象物**のことです。情報資産には、電子化された媒体だけでなく、ノウハウや人の記憶など電子化されていないものも含まれます。具体的には、サーバやパソコンなどのハードウェア、ネットワーク、データベース、OSやプログラムなどのソフトウェア、設計書や操作手順書などのドキュメント類、顧客情報や営業情報、経営情報や人事情報、ノウハウ、企業イメージや信用など、幅広い範囲のものが含まれます。

脅威

脅威は、**情報資産にマイナスの影響を与え、損失を発生させる潜在的な原因となるもの**です。一般には、地震や火災、落雷、水害などの「**自然災害**」、ハードウェアの故障や誤動作、ソフトウェアのバグ、電源異常などの「**システム障害**」、機器の不正使用、破壊、盗聴、情報の改ざん、なりすましなどの「**不正行為**」、システム使用時のミスや誤操作などの「**人為的過失**」に大別されます。

なお、TR X 0036-1:2001(ITセキュリティマネジメントのガイドライン)では、第1部(ITセキュリティの概念およびモデル)において、脅威について「**脅威は、資産に既存のぜい弱性を悪用して、財産に危害を与える**」と定義し、情報資産に対する脅威の例を次の表のように分類しています。

表 TR X 0036-1:2001による脅威の例

脅威の分類		脅威の例
人間	意図的	盗聴、情報の改ざん
	偶発的	誤り及び手落ち、物理的な事故
環境		地震、落雷

ぜい弱性

ぜい弱性は、**組織や情報資産に内在する情報セキュリティ上の弱点や欠陥**のことです。ぜい弱性が大きければ、情報資産が被害に遭ったり、損失が発生したりする危険性が高くなります。具体的には、建物の構造上の欠陥などの「**設備面のぜい弱性**」、ソフトウェアのバグなどの「**技術面のぜい弱性**」、ユーザ教育やマニュアル不備などの「**管理面のぜい弱性**」があります。

(5)リスクの算定

情報セキュリティを脅かすセキュリティリスクは、情報資産、脅威、ぜい弱性の三つの要素で構成されています。この三つの要素がすべて存在し、脅威とぜい弱性がともに成立したときに、「損失が発生するかもしれない状態」から「実際に損失が発生した状態」に変化します(これを「**リスクが顕在化する**」といいます)。すなわち、リスクとは、「**脅威が情報資産のぜい弱性を利用して、情報資産への損失または損害を与える可能性**」のことであると表現できます。

リスクの大きさを数値化する際には、次の数式がよく用いられます。

リスク値 ＝ 情報資産の価値 × 脅威 × ぜい弱性

なお、リスクが顕在化したときの損失額やリスクの発生確率を数値化できるときは、次の数式を用いることもできます。

リスク値(リスク評価額) ＝ 予想損失額 × 発生確率

例題 情報システムのリスク分析

情報システムのリスク分析に関する記述のうち、適切なものはどれか。

ア リスクには、投機的リスクと純粋リスクとがある。情報セキュリティのためのリスク分析で対象とするのは、投機的リスクである。

イ　リスクの予想損失額は、損害予防のために投入されるコスト、復旧に要するコスト、及びほかの手段で業務を継続するための代替コストの合計で表される。
ウ　リスク分析では、現実に発生すれば損失をもたらすリスクが、情報システムのどこに、どのように潜在しているかを識別し、その影響の大きさを測定する。
エ　リスクを金額で測定するリスク評価額は、損害が現実のものになった場合の1回当たりの平均予想損失額で表される。

（情報セキュリティスペシャリスト試験　平成21年度春期午前Ⅱ　問8）

解説

ア　リスクには、利益と損失のどちらも発生する可能性がある「投機的リスク」と、損失のみが発生する可能性がある「純粋リスク」があります。情報セキュリティのためのリスク分析で対象とするのは、純粋リスクだけです。
イ　リスクの予想損失額には、損害予防のために投入されるコストは含めません。
ウ　適切な記述です。
エ　リスクを金額で測定するリスク評価額は、損害が現実のものになった場合の1回当たりの平均予想損失額とリスクの発生確率の積（1回当たりの平均予想損失額×発生確率）で表されます。

したがって、正解はウです。

例題　情報システムのリスク分析における作業

情報システムのリスク分析における作業①～⑤の、適切な順序はどれか。

①損失の分類と影響度の評価
②対策の検討・評価と優先順位の決定
③事故態様の関連分析と損失額予想
④ぜい弱性の発見と識別
⑤分析対象の理解と分析計画

ア　④→⑤→②→③→①　　イ　④→⑤→③→②→①
ウ　⑤→④→②→③→①　　エ　⑤→④→③→①→②

（テクニカルエンジニア（情報セキュリティ）試験　平成19年度午前　問51）

解説

情報システムのリスク分析では、まず、「分析対象の情報システム（情報資産）を理解し、分析計画を立案すること（作業⑤）」から始めます。次に、情報システムに内在する

弱点やセキュリティホールであるぜい弱性を発見し識別します（作業④）。識別したぜい弱性にどのような脅威が結び付き、どのような事故が発生するかを分析し、リスクが発現したときの損失額を予想します（作業③）。以上の結果を受けて、損失を分類し、リスクの発生確率、ぜい弱性、脅威などを参考にリスクの影響度を評価します（作業①）。最後に、それぞれのリスクを受容可能な水準まで低減させるための対策を検討・評価し、対策を実施する順番を明らかにするために優先順位を決定します（作業②）。

なお、この問題ではリスク分析の作業範囲をやや広く捉えており、リスクアセスメントからリスク対応までのプロセスを含んでいます。JIS Q 27001によると、作業⑤、④、③が（狭義の）リスク分析、作業①がリスク評価、作業②がリスク対応に該当します。

したがって、正解はエです。

例題　情報システムのリスクとその評価

JIS Q 27001:2006における情報システムのリスクとその評価に関する記述のうち、適切なものはどれか。

ア　脅威とは、ぜい弱性が顕在化する確率のことであり、情報システムに組み込まれた技術的管理策によって決まる。
イ　ぜい弱性とは、情報システムに対して悪い影響を与える要因のことであり、自然災害、システム障害、人為的過失及び不正行為に大別される。
ウ　リスクとは、脅威が情報資産のぜい弱性につけ込み、情報資産に損失又は損害を与える可能性のことである。
エ　リスク評価とは、リスクの大きさを判断して対策を決めることであり、リスク回避とリスク低減の二つに分類される。

（テクニカルエンジニア（情報セキュリティ）試験　平成20年度午前　問49）

解説

ア、イ　脅威とは情報システムに対して悪い影響を与える要因のことであり、ぜい弱性とは情報システムに内在する弱点やセキュリティホールです。なお、自然災害、システム障害、人為的過失、不正行為は脅威の分類です。
ウ　適切な記述です。
エ　リスクの大きさを判断して対策を決めることを「リスク対応」といいます。リスク対応は、リスク回避、リスク低減（リスク最適化）、リスク移転、リスク保有（リスク受容）の四つに分類されます。

したがって、正解はウです。

リスク対応

(1)リスク対応の方法

リスクアセスメントの結果を受けてリスクの大きさを判断し、緊急度や重要度の観点から優先順位を付けて適切な対策を決定することを**リスク対応**といいます。簡潔に表現すれば、「**リスクアセスメントの結果に基づいてリスクの対応策を決定すること**」といえるでしょう。リスク対応の方法には、リスク最適化(リスク低減)、リスク保有(リスク受容)、リスク回避、リスク移転の四つの選択肢があります。

リスク最適化(リスク低減)

損失規模が小さく、発生確率が高いリスクの場合には、費用対効果が最適となるような**リスク対策を採用し、リスクを許容範囲内まで低減させる**という考え方です。例えば、ISMSの管理策を適用することによってリスクの発生確率を減少させたり、火災に備えてコンピュータ室に消火設備を設置したりするなどの対策がこれに該当します。

リスク保有(リスク受容)

リスクアセスメントの結果、そのリスクが軽微である場合(損失規模が小さく、発生確率が低いリスクの場合)には、組織として許容できる範囲内であれば受容し、**それ以上の対策を講じず、そのまま保有する**という考え方です。

リスク回避

リスクをもつことによって得られる利益に比べてリスクが非常に大きい場合(損失規模が大きく、発生確率が高いリスクの場合)には、**リスクの要因そのものを排除し、リスク発生の可能性を取り去る**という考え方です。例えば、リスク要因となる情報資産を廃棄したり、業務を廃止したりするなどの対策がこれに該当します。

リスク移転

損失規模が大きく、発生確率が低いリスクの場合には、**リスクそのものを契約によって他者(他社)に転嫁する**という考え方です。リスクが顕在化したときの被害に備えてリスク保険などに加入したり、リスク要因となる情報システムや業務を他社にアウトソーシングしたりするなどの対策がこれに該当します。

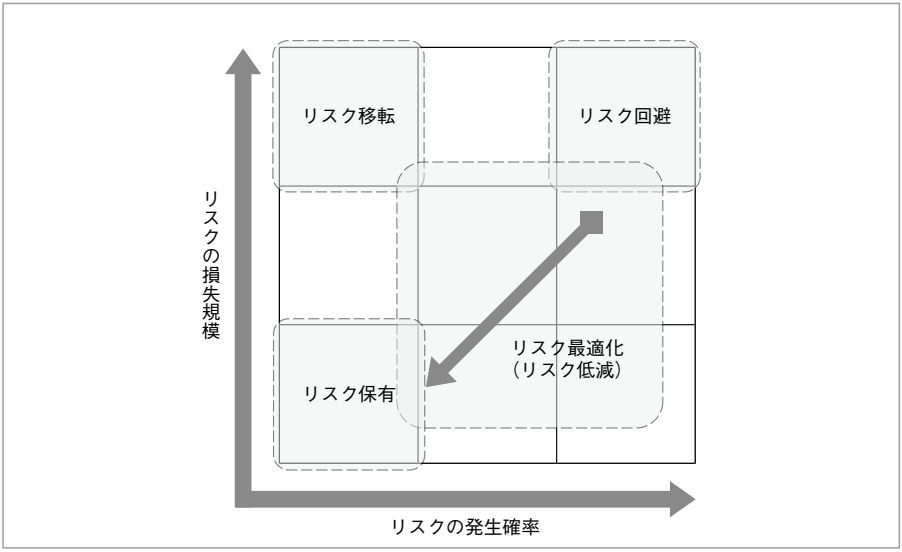

図　リスク対応の方法

(2)リスクコントロールとリスクファイナンス

リスクの対応策については、前述のように四つの選択肢に大別する方法以外に、**リスクコントロールとリスクファイナンス**に分類する方法があります。

リスクコントロール(risk control)

リスクコントロールは、リスクそのものを小さくする管理面の対策であり、次のような方法があります。

- **リスク回避**：リスクの要因そのものを排除する
- **損失予防**　：リスクの発生確率を小さくする
- **損失軽減**　：リスクによる損失の程度を軽減する
- **リスク分散**：情報資産を分散してリスクを軽減する
- **リスク集約**：リスクを集中的に管理してリスクを軽減する
- **リスク移転**：情報資産の管理、情報システムの開発や運用、情報セキュリティ対策を外部に委託する(アウトソーシングする)

リスクファイナンス(risk finance)

リスクファイナンスは、リスクが顕在化したときの損失に備える資金面の対策であ

り、次のような方法があります。

・**リスク移転**：保険や契約を使ってリスクによる損失を外部に転嫁する
・**リスク保有**：リスクによる損失を自社内の資金で対処する

例題　リスクファイナンス

リスクファイナンスを説明したものはどれか。

ア　損失の発生率を低下させることによって保険料を節約し、損失の低減を図る。
イ　保険に加入するなど資金面での対策を講じ、リスク移転を図る。
ウ　リスクの原因を除去して保険を掛けずに済ませ、リスク回避を図る。
エ　リスクを扱いやすい単位に分解するか集約することによって保険料を節約し、リスクの分離又は結合を図る。

（テクニカルエンジニア（情報セキュリティ）試験　平成18年度午前　問51）

解説

リスクファイナンスは、リスクが顕在化したときの損失に備える資金面の対策であり、保険に加入するなどの対策が該当します。したがって、正解はイです。

そのほかの選択肢に関する説明は、次のとおりです。

ア　損失の発生率を低下させる方法は損失予防であり、リスクコントロールに該当します。
ウ　リスクの原因を除去する方法はリスク回避であり、リスクコントロールに該当します。
エ　リスクを扱いやすい単位に分解または集約する方法はリスク分散・リスク集約であり、リスクコントロールに該当します。

例題　リスクファイナンス

　リスク対策をリスクコントロールとリスクファイナンスに分けた場合、リスクファイナンスに該当するものはどれか。

ア　システムが被害を受けた場合を想定して保険をかけた。
イ　システム被害につながるリスクの発生を抑える対策に資金を投入した。
ウ　システムを復旧するのに掛かった費用を金融機関から借り入れた。
エ　リスクが顕在化した場合のシステム被害を小さくする対策に資金を投入した。

（情報セキュリティスペシャリスト試験　平成21年度春期午前Ⅱ　問7）

解説

ア　リスクが顕在化したときの損失に備える資金面の対策であり、リスクファイナンスに該当します。
イ　リスクの発生を抑える対策は損失予防であり、リスクコントロールに該当します。
ウ　システムを復旧するのに掛かった費用を金融機関から借り入れたという事実を述べたものであり、リスク対策に該当しません(リスクコントロール、リスクファイナンスのいずれにも該当しません)。
エ　システム被害を小さくする対策は損失軽減であり、リスクコントロールに該当します。

　したがって、正解はアです。

午後問題の演習

リスクマネジメントの実施手順

問　題

リスクマネジメントの実施手順に関する次の記述を読んで、設問に答えよ。

H主任：当社では、リスクマネジメントを実施する手順として、最初にリスクアセスメントを行い、次にリスク対応を行うことにしている。リスクアセスメントでは、まず、リスク分析を行い、次にリスク評価を行う。リスク分析では、情報資産の重要度、脅威及びぜい弱性をレベルで表し、それぞれのレベルの積をリスク値として算定する。リスク評価では、リスク値が一定値を超えたものを対応すべきリスクとして決定する。

M君　：対応すべきリスクとして決定されたものについては、どうするのですか。

H主任：対応すべきリスクに対して、個々に対応を検討していく。リスク対応には、四つの選択肢がある。第一に、適切な管理策を採用して、リスクを低減するという選択肢がある。第二に、リスクが組織の方針及びリスク［　a　］基準を満たす場合には、そのリスクを［　a　］するという選択肢がある。第三に、リスクの存在する状況から撤退することによって、リスクを［　b　］するという選択肢がある。第四に、関連する事業上のリスクを保険会社や供給者などの他者に［　c　］するという選択肢がある。

現時点でリスク評価までは完了しているので、次の段階では、リスクを低減する選択肢の中で、技術的な管理策を検討していこう。

設　問

本文中の［　a　］～［　c　］に入れる適切な字句を解答群の中から選び、記号で答えよ。

解答群

ア　移転	イ　回避	ウ　管理	エ　拒否
オ　根絶	カ　受容	キ　譲渡	ク　売却

（テクニカルエンジニア（情報セキュリティ）試験　平成20年度午後Ⅰ　問4改題）

設問の解説

リスク対応には、リスク低減(最適化)、リスク受容(リスク保有)、リスク回避、リスク移転という四つの選択肢があります。問題文における第一の方法はリスク低減、第二の方法はリスク受容、第三の方法はリスク回避、第四の方法はリスク移転に該当します。

空欄aはリスク受容(リスク保有)に関するものであり、識別したリスクが軽微なものでリスク「受容」基準を満たす場合には、そのリスクを「受容」するという選択肢です。

空欄bは、リスク回避に関するものであり、リスクの存在する状況から撤退するというリスク要因の除去によって、リスクを「回避」するという選択肢です。

空欄cは、リスク移転に関するものであり、保険やアウトソーシングなどを利用して、関連する事業上のリスクを保険会社や供給者(アウトソーシングサービスの提供者)に転嫁することによって、リスクを他者に「移転」するという選択肢です。

解答

a：カ　　b：イ　　c：ア