ＩＳＭＳユーザーズガイド

-JIS Q 27001:2014(ISO/IEC 27001:2013)対応-

-リスクマネジメント編-

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

2015 年 3 月 31 日

一般財団法人　日本情報経済社会推進協会

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、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 を活用し、多くの企業が情報セキュリティマネジメントを実施し、また、認証取得されています。ISMS ユーザーズガイド リスクマネジメント編（以下、「本ガイド」という。）は、ISMS におけるリスクマネジメント（注記）をより深く理解し、スムーズに実施していただくために、従来の認証基準である JIS Q 27001:2006 から JIS Q 27001:2014 への移行を機に改訂いたしました。

本ガイドの主な読者として想定しているのは、ISMS 認証取得を検討若しくは既に取得している組織において、実際に ISMS の構築・運用に携っている担当者又はその責任者、特にリスクアセスメント及びその結果に基づくリスク対応を行う責任者です。本ガイドがリスクマネジメント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。

本ガイドでは、リスクマネジメントについてできるだけ丁寧な解説を試みましたが、JIS Q 27001:2014 の全ての要求事項を網羅している訳ではありません。本ガイドのほか、JIS Q 27001:2014、ISMS ユーザーズガイド（JIS Q 27001:2014 対応）を併せてご利用下さい。

本ガイドの作成にあたり、ご協力頂いた ISMS 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。

2015 年 3 月

ISMS 適合性評価制度技術専門部会
一般財団法人日本情報経済社会推進協会

注記　本ガイドで用いる「リスクマネジメント」という用語については、「情報セキュリティに関するリスクを対象とし、そのリスクを JIS Q 27001:2014 を活用してどのように取り扱うのか。」という意味で用いることにご留意ください。なお、情報セキュリティリスクを含む、様々なリスク全般に対応する一般的な方法論として、国際規格の中では、例えば ISO 31000(リスクマネジメント-原則及び指針)が挙げられます。

目 次

１．序文

１.１ 本ガイドの位置付け

本ガイドは、既にJIS Q 27001:2006に基づいた情報セキュリティマネジメントシステム（Information Security Management System：ISMS）（以下、「ISMS」という。）を構築し、運用しているユーザにおいて、JIS Q 27001:2014の要求事項、とりわけリスクマネジメントに関する要求事項の変更に対応することを目的に作成したものです。

今回の認証基準の改訂のポイントは、従来の認証基準であるJIS Q 27001:2006が、「ISO/IEC専門業務用指針 第1部 統合版ISO補足指針」の「附属書SL（規定）マネジメントシステム規格の提案」の「Appendix 2（規定）上位構造、共通の中核となるテキスト、共通用語及び中核となる定義」を採用し、ISMSの要求事項の構成を変更した点とJIS Q 31000:2010（ISO 31000:2009）及びJIS Q 0073:2010（ISO Guide73:2009）との整合を図った点が挙げられます。（「ISO/IEC専門業務用指針 第1部 統合版ISO補足指針」については、ISMSユーザーズガイドの「0.2.3 ISO MSS共通要素の概要」を参照してください。）
特に、本ガイドはリスクマネジメント編ですので、「リスクマネジメント－原則及び指針」を展開するJIS Q 31000:2010及び「リスクマネジメント－用語」を提供するJIS Q 0073:2010をJIS Q 27001:2014が採用したことによる影響を理解していただくには、JIS Q 31000：2010のリスクに関する考え方を理解していただくことがポイントとなります。

JIS Q 31000：2010(リスクマネジメント－原則及び指針)とは、リスクの運用管理のためのプロセスを組織の全体的な統治、戦略及び計画策定、運用管理、報告プロセス、方針、価値観並びに文化の中に統合することを目的とした枠組みを、組織が構築、実践及び継続的に改善するための原則及び指針を与えるものです。この指針では、組織の事業活動に関連する、広範なリスクを取り扱い、安全衛生、保安、法律及び規制の順守、社会的受容、環境保護、製品品質、統治、世評などに関連するリスク、すなわち「経営リスク全般」に適用することができ、ERM（Enterprise Risk Management）のフレームワークを構築する上で役立つものです。この規格の主要な特徴は、「組織の状況の確定」を、リスクマネジメントプロセスの開始時点で行う活動として含めている点にあります。組織の状況を確定することにより、組織の目的、組織が自らの目的を達成しようとする状態を取り巻く環境、組織のステークホルダ及びリスク基準の多様性を把握することとなり、これらすべては、組織のリスクの特質及び複雑さを明らかにし、アセスメントを行うことを援助します。すなわち、組織は、自らが置かれた状況を理解することで、組織の内外に存在する課題や利害関係者からのニーズや期待について掌握し、課題解決のため、又はニーズに応えるための活動などについての具体的な「目的」を明らかにすることができます。このように「目的」を明らかにした上で、その目的が達成できないことによる影響をリスクとして捉えることが、リスクアセスメントを実施する上で重要だとしています。

従来の JIS Q 27001:2006 の箇条 4.1 におきましても、「組織は、その組織の事業活動全般及び直面するリスクに対する考慮のもとで、文書化した ISMS を確立、….」と記載しており、PDCA サイクルを紹介した図中に、利害関係者からの情報セキュリティの要求事項及び期待を ISMS プロセスのインプットとし、それらの要求や期待に応えたアウトプット、すなわち利害関係者に対して運営管理された情報セキュリティを提供するために必要なリスクマネジメントの実践を要求しており、従来のユーザーズガイドにおきましても、その重要性について解説してきました。このため、この考え方を基にリスクマネジメントを実践されていた組織にとっては、認証基準の改訂によるインパクトは、小さいものだと思われます。一方、今回の改訂で、この考え方がより明確になったことで、「何のために ISMS を構築するのか」ということについて再確認する良い機会となると考えられます。

また、JIS Q 31000：2010 の採用に伴い、リスクマネジメントに関する用語の定義が変更されました（詳細は本ガイドの 1.2 参照）。リスクマネジメントの主体であるリスクは、「目的に対する不確かさの影響」と定義づけられ、その注記の一つに、「（注記４）リスクは、ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組み合わせとして表現されることが多い」との記載が加わりました。そのため、これを受け、JIS Q 27001:2014 では、リスクを分析するにあたり、情報の機密性、完全性及び可用性の喪失に伴うリスクを特定し、特定されたリスクが実際に生じた場合に起こり得る結果及び、リスクの現実的な起こりやすさについてアセスメントをすることで、リスクレベルを決定する（JIS Q 27001:2014 の箇条 6.1.2 の c）から d）までの要約）との要求事項になりました。（詳細は本ガイドの 3 章参照）。
JIS Q 31000：2010 の他の特徴としては、上記のようなリスクマネジメントに関する考え方や用語の定義はするものの、リスクアセスメントの手法や取組み等に関しては触れておらず、組織の状況や設定した目的に基づいて、これらの手法を選択しても良いとの柔軟な姿勢を示していることが挙げられます。このことは、リスクアセスメントを実施するための手法について幅広い選択肢ができたことを意味する一方、従来の認証基準に基づいて、リスクレベルを機密性、完全性、可用性の喪失からくる影響の度合い及び、事象の起こりやすさを、「脅威」と「ぜい弱性」の組み合わせにより算定する方式を採用し続けても良いということを意味します（詳細は本ガイドの 3 章参照）。

本ガイドでは、上記に記載した内容について、その詳細を各章に振り分け、わかりやすく解説しました。JIS Q 27001:2014 に移行する際の手助けとして、ご参照ください。

1.2 リスク全般

JIS Q 27001:2014 では、「6. 計画」の「6.1 リスク及び機会に対処する活動」において、対処する必要があるリスク及び機会について、次のとおりに記述しています。

6 計画

6.1 リスク及び機会に対処する活動

6.1.1 一般

ISMS の計画を策定するとき，組織は，4.1 に規定する課題及び 4.2 に規定する要求事項を考慮し，次の事項のために対処する必要があるリスク及び機会を決定しなければならない。

(中略)

6.1.2 情報セキュリティリスクアセスメント

組織は，次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め，適用しなければならない。

(中略)

6.1.3 情報セキュリティリスク対応

組織は，次の事項を行うために，情報セキュリティリスク対応のプロセスを定め，適用しなければならない。

（JIS Q 27001:2014 6.計画より一部引用）

ここで、JIS Q 27000:2014 で示されているリスクマネジメントに関係した用語の一覧を示します。これらの用語の定義の詳細は、JIS Q 27000:2014 を参照してください。
これらの用語は、JIS Q 0073:2010 から引用されたものです。

<table>
<tr><td rowspan="11">リスクマネジメントに関する用語の定義</td><td colspan="3">2.68 リスク（risk）</td></tr>
<tr><td colspan="3">2.76 リスクマネジメント（risk management）</td></tr>
<tr><td colspan="3">2.77 リスクマネジメントプロセス（risk management process）</td></tr>
<tr><td rowspan="3">（組織の状況に関する用語）</td><td colspan="2">2.42 内部状況（internal context）</td></tr>
<tr><td colspan="2">2.27 外部状況（external context）</td></tr>
<tr><td colspan="2">2.73 リスク基準（risk criteria）</td></tr>
<tr><td rowspan="6">2.71 リスクアセスメント（risk assessment）</td><td rowspan="2">2.75 リスク特定（risk identification）</td><td>2.25 事象（event）</td></tr>
<tr><td>2.78 リスク所有者（risk owner）</td></tr>
<tr><td rowspan="3">2.70 リスク分析（risk analysis）</td><td>2.45 起こりやすさ（likelihood）</td></tr>
<tr><td>2.14 結果（consequence）</td></tr>
<tr><td>2.44 リスクレベル（level of risk）</td></tr>
<tr><td>2.74 リスク評価（risk evaluation）</td><td>2.69 リスク受容（risk acceptance）</td></tr>
</table>

	2.79 リスク対応 （risk treatment）	2.16 管理策（control）
		2.64 残留リスク（residual risk）
		2.65 レビュー（review）

これらの用語は、本ガイドの「2.リスクマネジメントを取り巻く状況」以降で説明します。

今回の改訂では、ISMS を構築する際には、幅広い視点から ISMS に影響を与える可能性がある外部及び内部の課題を俯瞰することがより明確となり、そのためには、リスク全般を考慮し、把握する必要があります。このことを理解する上において、まず、リスク全般に関連する用語とその定義を理解することが重要です。
リスクに関する規格は、従来 TR Q 0008 を基に構築されておりましたが、今回の改訂によって、JIS Q 0073:2010(ISO Guide 73:2009)及び JIS Q 31000:2010(ISO 31000:2009)の用語及びリスクマネジメントプロセスを採用することになりました。次に示す JIS Q 27000:2014 の用語及びその定義も JIS Q 31000:2010 をそのまま採用しています。

JIS Q 27001:2014 で使用される用語を定義した「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 － 用語（JIS Q 27000：2014）」では、リスクを次のとおりに定義しています。

2.68 ：リスク（risk）
目的に対する不確かさの影響。
（JIS Q 0073:2010 の 1.1 参照）
注記 1 影響とは，期待されていることから，好ましい方向又は好ましくない方向にかい（乖）離することをいう。
注記 2 不確かさとは，事象（2.25），その結果（2.14）又はその起こりやすさ（2.45）に関する，情報，理解又は知識が，たとえ部分的にでも欠落している状態をいう。
注記 3 リスクは，起こり得る事象（2.25），結果（2.14）又はこれらの組合せについて述べることによって，その特徴を記述することが多い。
注記 4 リスクは，ある事象（周辺状況の変化を含む。）の結果（2.14）とその発生の起こりやすさ（2.45）との組合せとして表現されることが多い。
注記 5 ISMS の文脈においては，情報セキュリティリスクは，情報セキュリティ目的に対する不確かさの影響として表現することがある。
注記 6 情報セキュリティリスクは，脅威（2.83）が情報資産のぜい弱性（2.89）又は情報資産グループのぜい弱性（2.89）に付け込み，その結果，組織に損害を与える可能性に伴って生じる。

2.83 ：脅威（threat）
システム又は組織に損害を与える可能性がある，望ましくないインシデントの潜在的な原因。

2.89 ：ぜい弱性（vulnerability）
一つ以上の脅威（2.83）によって付け込まれる可能性のある，資産又は管理策（2.16）の弱点。

（JIS Q 27000:2014 2 用語及び定義 より引用）

リスクの特性は、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、その期待値や目標値に対してどの様な分布を持つか、またそれによりどのような影響を取り得るかにより規定されます。

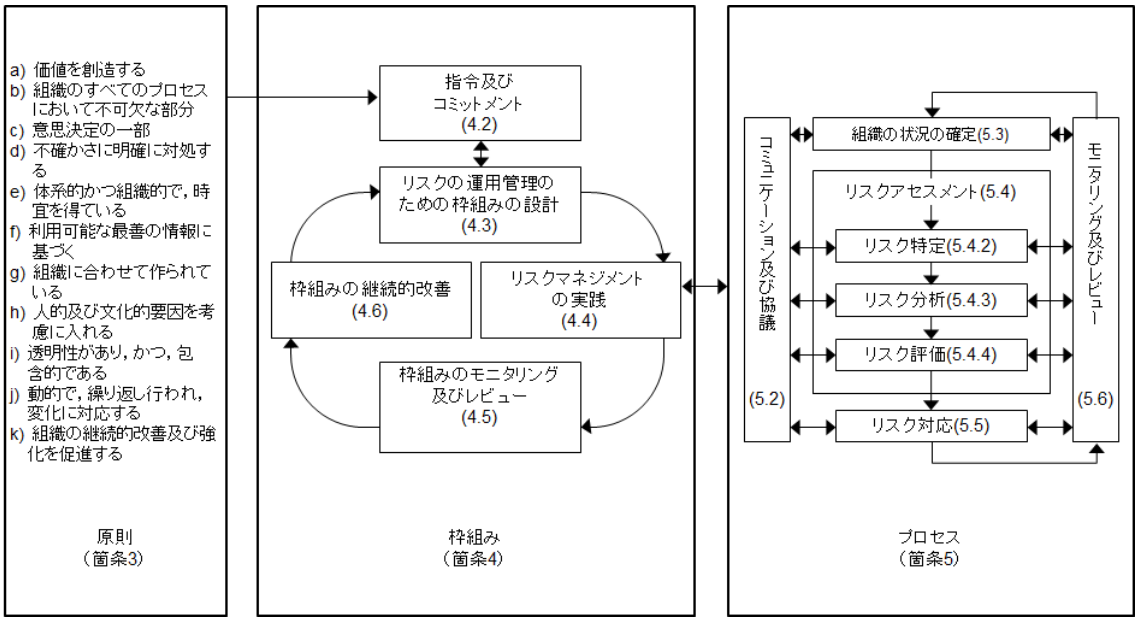
JIS Q 31000:2010 によると、「リスク及び機会」の定義について、リスクは「目的に対する不確かさの影響」のことであり、「影響とは、期待されていることから、好ましい方向又は好ましくない方向に乖離すること」としています。一方、この規格では、「機会（opportunity）」については、特に定義をしていません。「機会（opportunity）」が好ましい方向への乖離に対する処置の意味と解釈される場合もあるようですが、そうするとリスクの定義にある「好ましい方向への乖離への対応」と 6.1 のタイトルにある「機会（opportunity）」はダブることになります。従って、この「機会（opportunity）」については、その意味をどのように解釈するかということよりも、リスクマネジメントにおける事業リスクを理解することが重要であると考えられます。事業リスクを理解する上では、JIS Q 31000:2010 の「5.3 組織の状況の確定」を考慮して「4.1 組織及びその状況の理解」との整合を確保することがリスクマネジメントの重要なポイントであると考えられます。

JIS Q 27000 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。

2.76 リスクマネジメント（risk management）
リスク（2.68）について，組織（2.57）を指揮統制するための調整された活動。
（JIS Q 0073:2010 の 2.1 参照）

（JIS Q 27000:2014 2 用語及び定義 より引用）

ISMS の目的は、リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性を維持し、かつ、情報セキュリティに関するリスクを適切に管理しているという信頼を利害関係者に与えることにあります。
JIS Q 31000:2010 のリスクマネジメントの活動及びプロセスを導入し、JIS Q 27001:2014 の要求事項として、ISMS に統合したテキストとしています。
図 1-1 は、プロセス間の情報の流れを示しています。



（JIS Q 31000:2010 より引用）

図 1-1　JIS Q 31000:2010 のリスクマネジメント

【補足】リスクコミュニケーション

リスクコミュニケーションは、「意思決定者と他のステークホルダの間における、リスクに関する情報の交換又は共有」と説明されています。ステークホルダとは、リスクに影響を与え、リスクの影響を受け、又は影響を受けると認識する個人、グループ又は組織のことです。他のステークホルダとは、具体的には、顧客、所有者、組織内の人々、供給者、銀行家、組合、パートナー又は社会といった利害関係者が中心となります。情報セキュリティにおいて、リスクコミュニケーションが重要となるのは、業務レベルでは、外部委託先にリスクの移転を行っている場合等が考えられます。また、経営レベルでは、株主、投資家に対してリスクコミュニケーションを十分に行わなければならない場合も想定されます。また、リスクコミュニケーションは広義の意味合いでは、経営陣と事業部門間、事業部門と IT 部門間、IT 部門とユーザ部門間などのコミュニケーションも当然、重要な要素として含まれます。組織内の意思統一なしに、真のリスクコミュニケーションは達成されないからです。情報セキュリティにおいては、経営陣の目指す情報セキュリティレベルが、組織内または、関連組織などに十分浸透していない点が課題として上げられることがあります。経営陣は、その様な認識の違いが起こらない様、積極的にコミュニケーションを維持していく責任があります。なお、本ガイドでは、リスクコミュニケーションについては詳細な説明を行っていません。

情報セキュリティリスクの考え方

情報セキュリティリスクを特定する際に、脅威やぜい弱性という考え方を適用することができ、これらとリスクとの関係を図示すると図 1-2 のとおりになります（情報セキュリティリスクについては、リスクの定義の注記 6 に説明があります）。

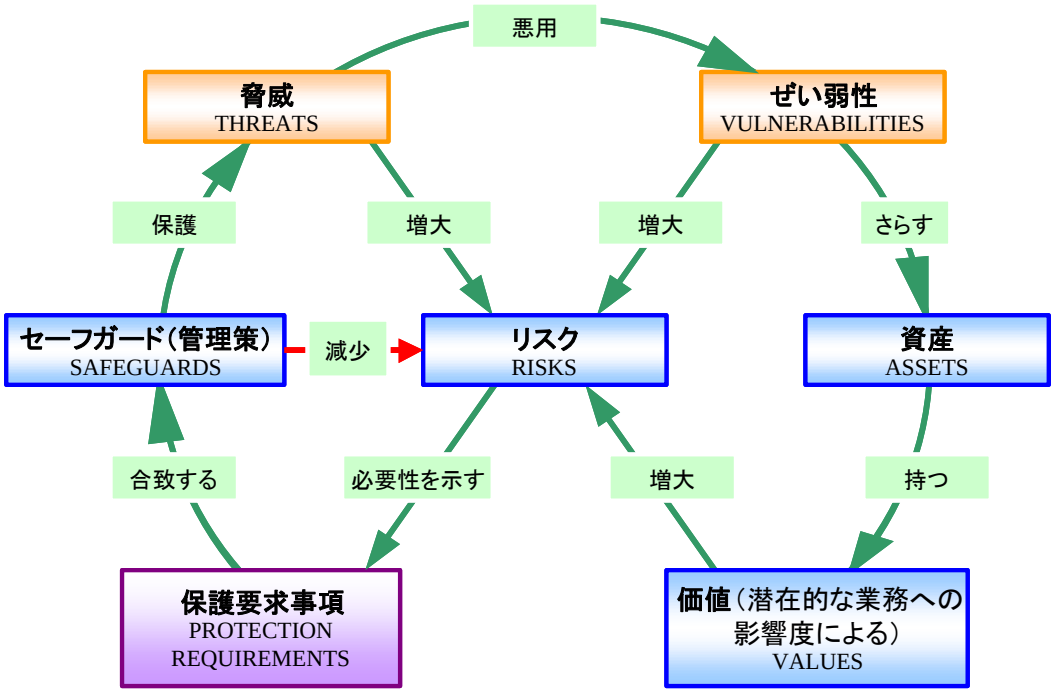


図 1-2 脅威、ぜい弱性とリスクの関係

この図では、脅威、ぜい弱性、（資産）価値のいずれかが増加するとリスクが増大することを示しています。また、脅威、ぜい弱性、（資産）価値を識別することで、リスクに対する保護要求事項が明確にされ、それに対応するセーフガード（管理策）を適切に講じることによりリスクが減少することを示しています。

上記の JIS Q 27000:2014 のリスクの定義の注記 4 には、リスクは、ある事象の結果とその発生の起こりやすさとの組合せとして表現されることが多いとありますが、（資産）価値は事象の結果に関係し、脅威やぜい弱性は発生の起こりやすさに関係することになります。

なお、JIS Q 27000:2014 では、リスク特定を以下のように定義しています。

> 2.75 リスク特定（risk identification）
>
> リスク（2.68）を発見，認識及び記述するプロセス。
>
> （JIS Q 0073:2010 の 3.5.1 参照）
>
> 注記 1 リスク特定には，リスク源，事象，それらの原因及び起こり得る結果の特定が含まれる。
>
> 注記 2 リスク特定には，過去のデータ，理論的分析，情報に基づいた意見，専門家の意見及びステークホルダ

> のニーズを含むことがある。
>
> （JIS Q 27000:2014　2 用語及び定義　より引用）

また、上記の定義にあるリスク源について、JIS Q 31000:2010 では以下の通り定義しています。

> 2.16　：リスク源（risk source）
> それ自体又はほかとの組合せによって，リスク（2.1）を生じさせる力を本来潜在的にもっている要素。
> 注記 リスク源は，有形の場合も無形の場合もある。
>
> （JIS Q 31000:2010　2 用語及び定義　より引用）

リスク源の典型的な例としては、資産に対する脅威やぜい弱性等が考えられます。また、リスクの定義の注記で示されている、リスクの特徴や、結果の発生の起こりやすさを、脅威とぜい弱性を組合わせることで、表現することができます。

なお、JIS Q 27000:2014 では資産という表現が使われておりませんが、情報セキュリティに関する重要な情報または、重要な情報を含むプロセスやシステムととらえ、それらは外部委託先に委託しているプロセスなどにも適用すると考えることができます。

１.３ ISMS 構築ステップとリスクアセスメント、リスク対応、リスク受容

JIS Q 27001 では、前述のとおり、JIS Q 31000:2010 におけるリスクの考え方を基礎として、JIS Q 27000 の用語を採用しています。
JIS Q 27000 によれば、「リスクマネジメント」とは、「リスクについて，組織を指揮統制するための調整された活動」と定義されており、また JIS Q 31000:2010 によると、リスクマネジメントのプロセスは一般に組織の状況の確定、リスクアセスメント、リスク対応、リスクコミュニケーションを含む活動によって形作られていると説明されています。
この定義に従えば、情報セキュリティのリスクマネジメントは、図 1-1 で示した JIS Q 31000:2010 におけるリスクマネジメントと同様に考えることができます。

JIS Q 27001:2014 では、ISMS のリスクマネジメントプロセスの中で、特に、リスクアセスメント及びリスク対応の計画については、図 1-3 で示すとおり、箇条 6 で要求しています。
また、組織の状況については、JIS Q 27001:2014 の箇条 4 で要求しており、ISMS のリスクマネジメントを実施する際に重要です（本ガイドの 2.1 参照）。

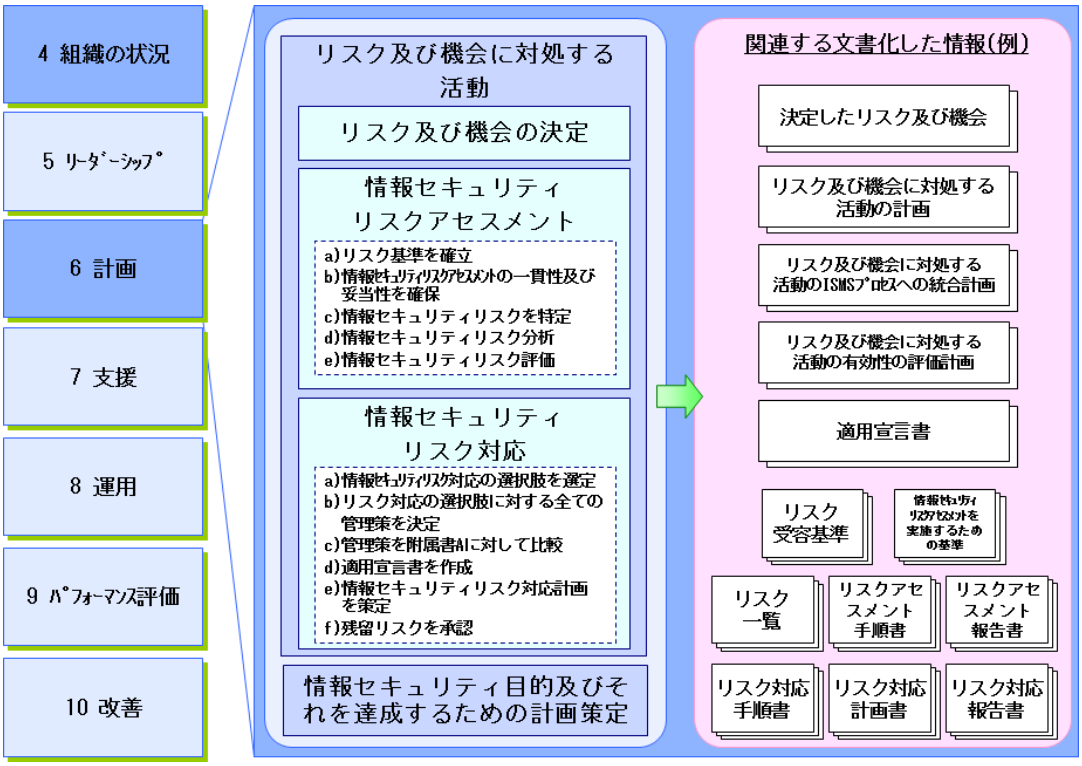


図 1-3 リスクアセスメント及びリスク対応の計画　注）文書名は全て例示

上図で示す ISMS の活動は、以下の図 1-4 に示すように、リスクアセスメント及びリスク対応に関する作業と関連づけして整理することが可能です。

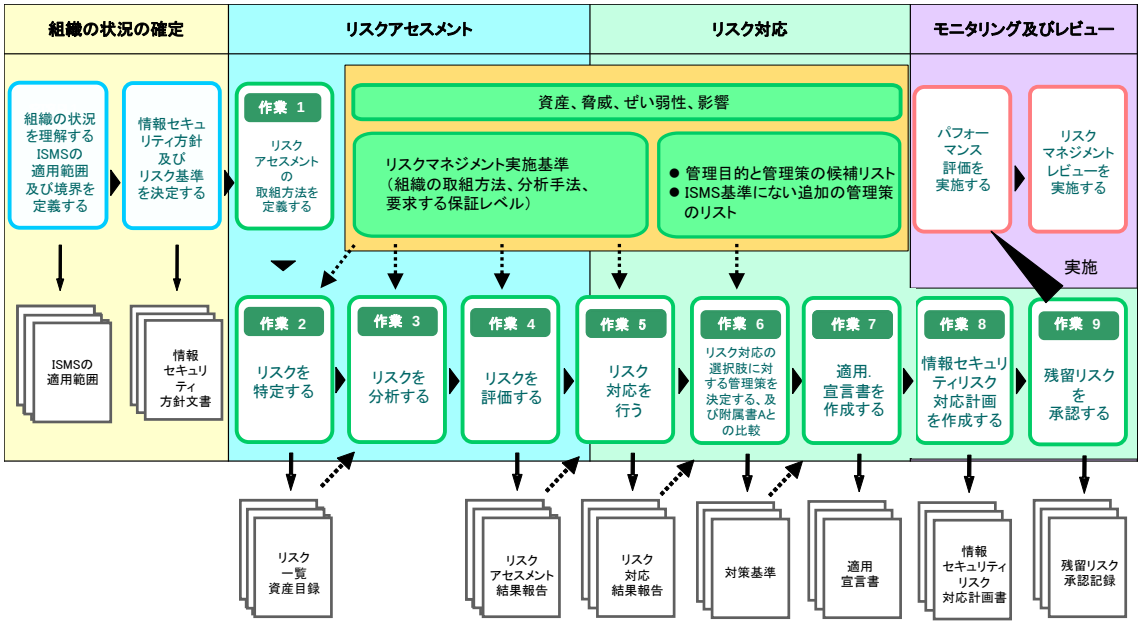


図 1-4 リスクアセスメント及びリスク対応に関する作業

上図を参考に、本ガイドの構成を説明すると、「組織の状況の確定」については、本ガイドの「2.リスクマネジメントを取り巻く状況」で説明します。
また、リスクアセスメント及びリスク対応に関する作業 1～9 については、本ガイドの「3.情報セキュリティリスクアセスメントとリスク対応」で説明します。
なお、本ガイドの 3.1 にも記載致しますが、作業 1～9 までを実施する順番（流れ）は、この例に限られるものではありません。

【補足】

情報セキュリティリスクアセスメント／リスク対応を中心とした事例

図 1-6 は情報セキュリティリスクアセスメント/リスク対応の手法を中心に、プロセスの事例を示したものです。

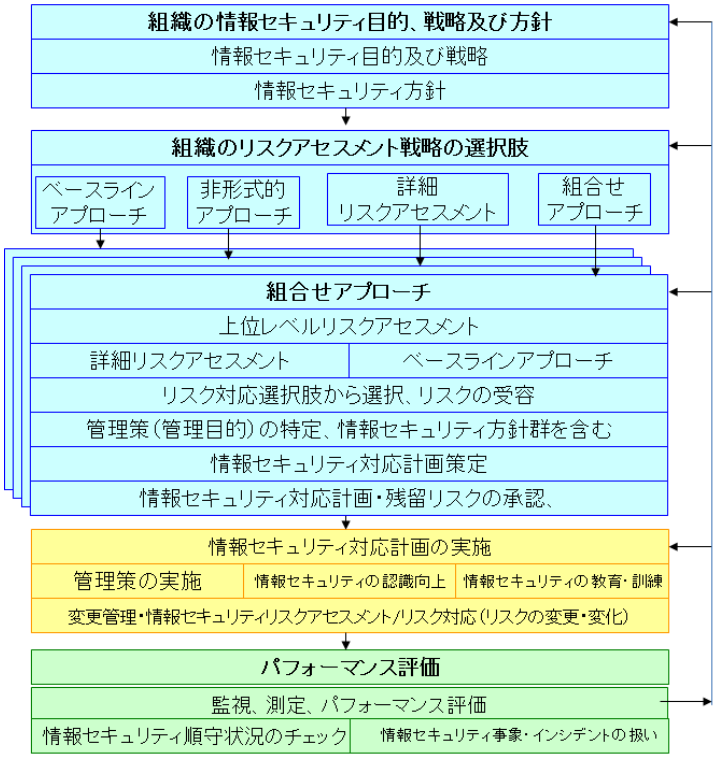


図 1-6　情報セキュリティリスクアセスメント/リスク対応を中心とした事例

次に、情報セキュリティリスクアセスメントを実施するための基準として 4 つのアプローチを紹介します。

■　**ベースラインアプローチ（Baseline Approach）**

あらかじめ一定の確保すべきセキュリティレベルを設定し、実装するのに必要な対策を選択し、対象となるシステムに一律に適用することを指す

■　**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ことを指す

■　**詳細リスク分析（Detail Risk Analysis）**

システムについて詳細なリスクアセスメントを行うアプローチで、資産に対し、「資産価値」、「脅威」、「ぜい弱性」やセキュリティ要件を識別し、評価することを指す

■　**組合せアプローチ（複合アプローチ）（Combined Approach）**

複数のアプローチを併用し、それぞれのアプローチの長所短所を相互に補完し、作業の効率化や分析精度の向上を図る

２．リスクマネジメントを取り巻く状況

２.１　組織の状況

ISMS を構築する重要な目的の 1 つは、その活動が予防的な役割をもつことです。JIS Q 27001:2014 では、箇条 4.1 と箇条 6.1 の 2 つの要求事項が、「予防的活動」というコンセプトをカバーすると考えられます。4.1 は「組織」の「目的に関連し、意図した成果（規格、プロセスなどの適用の結果）を達成する組織の能力に影響を与える、外部及び内部の課題」を評価することを要求し、箇条 6.1 は、「ISMS が、その意図した成果を達成できることを確実にするため、望ましくない影響を防止又は低減するため、及び継続的改善を達成するため、それらに対処するリスク及び機会の決定」を実施することを要求しています。
ここでは、箇条4.1の要求事項にもとづき、リスクアセスメントに必要な「組織及びその状況を理解」するための方法を例示します。

> 組織は，組織の目的に関連し，かつ，その ISMS の意図した成果を達成する組織の能力に影響を与える，外部及び内部の課題を決定しなければならない。
>
> 注記　これらの課題の決定とは，JIS Q 31000:2010 の 5.3 に記載されている組織の外部状況及び内部状況の確定のことをいう。
>
> （JIS Q 27001:2014　4.1　組織及びその状況の理解　より引用）

箇条 4.1 で使用されている用語及び表現のうち、留意すべきものについて説明します。まず、「組織」については次のように定義されています。組織の定義自体に「目的を達成するため、独自の機能をもつ」という表現があることに注目して下さい。

> 2.57　組織（organization）
> 自らの目的（2.56）を達成するため，責任，権限及び相互関係を伴う独自の機能をもつ，個人又は人々の集まり。
>
> 注記　組織という概念には，法人か否か，公的か私的かを問わず，自営業者，会社，法人，事務所，企業，当局，共同経営会社，非営利団体若しくは協会，又はこれらの一部若しくは組合せが含まれる。ただし，これらに限定されるものではない。
>
> （JIS Q 27000:2014　2　用語及び定義　より引用）

「ISMS の意図した成果」は、その ISMS を確立しようとする組織が定めるものであり、ISMS 導入の目的及び効果を考慮すると、以下を含むものであると考えられます。

- リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性を維持する。

– リスクを適切に管理しているという信頼を利害関係者に与える。

また、組織の「外部及び内部の課題の決定」とは、組織の外部状況及び内部状況の確定とされていますが、外部状況、内部状況とは、以下にように定義されています。

2.27 外部状況（external context）

組織が自らの目的を達成しようとする場合の外部環境。

（JIS Q 0073:2010 の 3.3.1.1 参照）

注記 外部状況には，次の事項を含むことがある。

– 国際，国内，地方又は近隣地域を問わず，文化，社会，政治，法律，規制，金融，技術，経済，自然及び競争の環境
– 組織（2.57）の目的（2.56）に影響を与える主要な原動力及び傾向
– 外部ステークホルダ（2.82）との関係並びに外部ステークホルダの認知及び価値観

（JIS Q 27000:2014 2 用語及び定義 より引用）

2.42 内部状況（internal context）

組織が自らの目的を達成しようとする場合の内部環境。

（JIS Q 0073:2010 の 3.3.1.2 参照）

注記 内部状況には，次の事項を含むことがある。

– 統治，組織体制，役割及びアカウンタビリティ
– 方針，目的及びこれらを達成するために策定された戦略
– 資源及び知識としてみた場合の能力（例えば，資本，時間，人員，プロセス，システム，技術）
– 情報システム，情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む。）
– 内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観
– 組織の文化
– 組織が採択した規格，指針及びモデル
– 契約関係の形態及び範囲

（JIS Q 27000:2014 2 用語及び定義 より引用）

（１）外部状況

組織の外部状況には、例えば、次のようなものが考えられます。

政治的性格の状況、戦略的性格の状況、地勢的状況、経済及び政治動向から発生する状況、方法に関連する状況、文化的性格の状況などです。表 2-1 に「組織の外部状況の構成要素の例」を示します。

表 2-1　組織の外部状況の構成要素の例

構成要素	内容
政治的性格の状況	この状況は、行政府、公共機関又はより広範に、政府の決定を適用しなければならない組織にかかわるものです。この状況は通常、戦略又は運用の方向性に関して、政府省庁又は意思決定機関が下す決定であり、適用することが望ましいものです。例えば、請求書又は管理文書のコンピュータによる処理によって、内部統制などに関するような情報セキュリティ問題が発生します。
戦略的性格の状況	この状況は、組織の構成又は方向性の変更計画又は変更の可能性からも発生することがあります。この状況は、組織の戦略計画又は運用計画の中で表されます。例えば、取扱いに慎重を要する情報の共有に関する国際協力のためには、安全な情報交換に関する合意が必要となります。
地勢的状況	組織の構成及び/又は目的は、国土全体又は外国に広がったサイトの分布のような固有の状況を生み出すことがあります。郵便事業、大使館、銀行、大手企業グループの子会社などの例が挙げられます。
経済及び政治動向から発生する状況	組織の運営は、ストライキ又は国内外の危機のような特別の事象によって大きな変更を余儀なくされることがあります。例えば、ある種のサービスは、重大な危機のときも継続して運営されることが望まれます。
方法に関連する状況	プロジェクト計画、要件定義、開発などの側面には、組織のノウハウに適した方法を用いる必要があります。例えば、この種の代表的な状況は、組織の法的義務をセキュリティ方針に盛り込む必要性などがあります。
文化的性格の状況	組織によっては、社会的慣習、宗教、労働習慣又は主要な事業が組織内に固有の「文化」を生み出し、これがセキュリティ管理策と相容れないということが起こることがあります。この文化は、要員が一般的に拠り所とする枠組みであり、これは教育、指示、専門家としての経験、仕事以外の経験、意見、哲学、信念、社会的地位など、数多くの側面によって決定されます。

（2）内部状況

次に、内部状況について説明します。

JIS Q 31000:2010 の箇条 5.3 によれば、組織の状況を確定することによって、組織は、目的を明確に表現し、リスクの運用管理において考慮するのが望ましい外部及び内部の要因を定め、それ以降のプロセスに関する適用範囲及びリスク基準を設定することができます。

組織の内部状況の調査では、組織のアイデンティティを定義する特徴的な要素を確認することが該当します。調査は、組織の目的、事業、使命、価値及び戦略を対象とします。これらは、その発展に寄

与する要素（下請負契約など）と合わせて特定することが望ましいようです。表 2-2 に「組織の特徴的な構成要素の例」を示します。

表 2-2　組織の特徴的な構成要素の例

構成要素	内容
組織の主要な目的	組織が何のために存在するか。活動領域、マーケットセグメント等。
組織の事業・業務	事業・業務の分野・内容、保有する技術・ノウハウにより定義する。
組織の使命	提供する製品・サービスとエンドユーザを関連付けて特定することが望ましい。
組織の価値	事業・業務の実践に当たり適用する原則／行動規範。
組織の構成	①　部門としての構成　②機能的な構成（例：設計、製造、調達、営業、IT、人事等） 組織の構成は組織図等で図式化する。 レポートライン、権限委譲関係等の情報の流れが分かるようにすることが望ましい。
組織の戦略	組織の主導原則を公式に表明したもの

組織の外部及び内部の状況を把握するポイントは、組織がどのように構成されているかを正確に理解することにあります。その実際の構成を特定すれば、組織の目的を達成するうえで各事業部門の役割及び重要性の理解が得られます。

組織の外部及び内部の要因には、リスクマネジメントの枠組みの設計において検討する要因と類似したものも多いのですが、リスクマネジメントプロセスに関して組織の状況を確定する場合には、要因を一層詳細に考慮する必要があります。特に、情報セキュリティのリスクマネジメントプロセスの適用範囲とどのように関係し合うのかについて考慮する必要があります。
例えば、要因の代表的な例として、情報及び情報に関連する資産、事業、組織、所在地、技術の特徴という視点があります。JIS Q 27001:2006 では、これら 5 つの視点を適用範囲と境界として定義するよう示されていました。JIS Q 27001:2014 では、これらの視点は示されなくなりましたので、ISMS のリスクマネジメントに関する規格 ISO/IEC 27005:2011 を参考にして、組織の目的を明確に表現し、リスクの運用管理において考慮するのが望ましい外部及び内部の要因を定め、それ以降のプロセスに関する適用範囲及びリスク基準を設定することで、課題や意思決定の過程を明らかにすることも可能です。
「外部及び内部の要因と課題の例」を表 2-3 に示します。

表 2-3　外部及び内部の要因と課題の例

要因の例	内容	課題の例
情報及び情報に関連する資産	営業秘密（顧客情報、個人情報、製造技術・ノウハウ、販売ノウハウ、製造原価、販売原価、など）文書（方針、規程、手順書、記録等）	機密性の確保 保管情報の完全性

事業	定款や会社案内に示す事業の内容	顧客への信頼性提供、説明責任
組織	会社案内や組織表に示す内容	委託先のセキュリティ確保
所在地	会社案内や事業拠点に示す内容	業務委託やテナントの安全確保
技術	利用するソフトウェア、ハードウェア、ネットワーク、クラウド環境	社内のセキュリティ、安全確保、クラウドサービス利用の安全

（3）適用範囲に影響する制約条件

適用範囲の決定には、さらに技術的制約、資金的制約、環境的制約、時間的制約、方式的制約、法的規制、組織的制約、既存プロセスからの影響などを考慮します。「適用範囲に影響する制約条件の例」を表 2-4 に示します。

表 2-4　適用範囲に影響する制約条件の例

制約条件の例	内容
技術的制約	IT インフラ基盤に関わる制約（ファイル、アーキテクチャ、ソフトウェア、ハードウェア、通信ネットワーク、建物・ユーティリティ）
資金的制約	セキュリティへの予算配分
環境的制約	国・地域、気象、自然災害リスク、地理状況
時間的制約	セキュリティ管理策導入に要する時間
方式的制約	当該組織のノウハウに適したプロジェクト計画、要件定義、開発
法的規制	法令及び規制上の要求事項、契約上の義務
組織的制約	運用、メンテナンス、人的資源管理、業務管理、開発管理、渉外管理
既存プロセス	既存プロセスからの影響

（参考：ISO/IEC 27005:2011　附属書 A4）

２.２　情報セキュリティ方針及びリスク基準を決定する

２．２．１　情報セキュリティ方針

JIS Q 27001:2014 では、トップマネジメントは、情報セキュリティ方針を確立することが求められています。

> トップマネジメントは，次の事項を満たす情報セキュリティ方針を確立しなければならない。
>
> a）組織の目的に対して適切である。
>
> b）情報セキュリティ目的（6.2 参照）を含むか，又は情報セキュリティ目的の設定のための枠組みを示す。
>
> c）情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。
>
> d）ISMS の継続的改善へのコミットメントを含む。
>
> 情報セキュリティ方針は，次に示す事項を満たさなければならない。
>
> e）文書化した情報として利用可能である。
>
> f）組織内に伝達される。
>
> g）必要に応じて，利害関係者が入手可能である。
>
> （JIS Q 27001:2014　5.2 方針　より引用）

情報セキュリティ方針は、情報セキュリティに対する組織の意図を示し、方向付けをするものであり、組織の目的と整合をとる必要があります。

情報セキュリティ方針では、上記の「JIS Q 27001:2014　5.2 方針 b)項」に記載されている、「6.2 項に記載される、 情報セキュリティ目的及びそれを達成するための計画策定」で決定する情報セキュリティ目的を含むか、又は情報セキュリティ目的の設定のための枠組みを示すことが要求されます。6.2 では、情報セキュリティ目的は情報セキュリティ方針と整合することを要求しており、組織にとって有益な情報セキュリティ目的を設定するためにも、ここで組織の事業目的に沿った情報セキュリティ方針を策定する必要があります。

そのためにも、トップマネジメントは、自ら ISMS の運用に積極的に関与すること（コミットメント）を情報セキュリティ方針で表明しなければなりません。表明する際、トップマネジメントが確立した情報セキュリティ方針を文書化して利用可能とし、組織内に伝達し、各従業員がそれに従って行動できるように組織内の意識を高めることが必要となります。逆に、各従業員が方針を理解せず、各々の感覚で情報セキュリティに取り組んでしまった場合、組織としての ISMS にほころびが生まれ、情報漏えいなどが起きてしまう可能性があります。
また、利害関係者が必要に応じて情報セキュリティ方針を入手可能な状態にしておくことも必要です。

従来の JIS Q 27001:2006 では、上位概念の ISMS 基本方針（ISMS policy）と下位概念の情報セキュリティ基本方針（Information security policy）の 2 つがありましたが、JIS Q 27001:2014 では、これらを区別することなく情報セキュリティ方針（Information security policy）としています。JIS Q 27001:2014 では、方針は ISO のマネジメントシステム規格共通の要求事項になり、他のマネジメントシステムの方針と整合するような要求事項となっています。

２．２．２ 情報セキュリティ方針の策定

情報セキュリティ方針は、トップマネジメント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、企業としての使命、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。情報セキュリティ目的を含むか、又は情報セキュリティ目的の設定のための枠組みを示す必要があります。

情報セキュリティ方針を策定するためには、組織の状況の把握（例えば、組織の目的、事業、使命、価値観、事業遂行上の主要な原理及び行動規範、想定された適用範囲に含まれる組織の人員構成、規程類の整備状況、情報及び情報に関連する資産の保有状況、情報システムの利用状況等、広範に情報と情報関連の資産とそれを取り巻く環境）、並びに利害関係者からの要求事項を確認する必要があります。

また、「情報セキュリティに関連する、組織として適用可能とされている情報セキュリティ要求事項を満たすこと」、及び「ISMS の継続的改善」への誓約（コミットメント）がなされることが示される必要があります。情報セキュリティ方針は、文書として利用可能とし、組織全体に伝え、認知させることが重要です。

２．２．３ 情報セキュリティ方針の策定事例

情報セキュリティ方針は、情報セキュリティに対する組織の方向付けをするものです。

JIS Q 27002:2014 の「5.1.1 情報セキュリティのための方針群」には、最上位の情報セキュリティ方針に含まれる事が望ましい内容が提示されています。以下は、それを参考にして策定した情報セキュリティ方針の事例です。

（情報セキュリティ方針、策定事例）

情報セキュリティ方針文書では，トップマネジメントの責任を含む、各責任者の責任を明記し，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とする。この情報セキュリティ方針文書には，次の事項に関する記述を含む。

a）情報セキュリティの定義，情報セキュリティ目的及び適用範囲，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
b）事業戦略及び事業目的に沿った情報セキュリティ目的及び原則を支持するトップマネジメントの意思を示す記述
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）情報セキュリティ方針群への違反に対する処置
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とする。

これらの事項は、例示であり、必ずしもその全てが策定する方針に含まれる必要はありません。4.3 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。
上記の策定事例は、方針の内容を検討する際に考慮すべきポイントを示すものです。

２．２．４ リスク評価基準とリスク基準

従来のリスクマネジメント編では、TR Q 0008 の定義を用いて、リスクの重大さを決定するために算定されたリスクと比較する尺度としてリスク評価基準を使っていました。

旧リスクマネジメント編 補章 1 TR Q 0008 に基づくリスクマネジメントの用語と解説（52/61）
②リスクアセスメント
「リスク評価」は「リスクの重大さを決定するために、算定されたリスクを与えられたリスク評価基準と比較するプロセス」と定義されています。リスク評価を行うということは、組織にとって、リスクがどの程度重大であるかを、リスク評価基準（リスククライテリア：リスクの重大さを評価するために適用される尺度）と照らし合わせることをいいます。リスク評価基準は、関連するコストと利益、法規制の要求事項、社会への経済的な影響、環境への影響、ステークホルダの関心事、優先度などを考慮して決定されることになります。

一方、JIS Q 27001:2014 ではリスク評価基準という用語がなくなりリスク基準となっています。このリスク基準は従来のリスク評価基準を含んだ概念です。それは、6.1.2 情報セキュリティリスクアセスメントの次の要求事項を確認していただければ、理解しやすいと考えられます。

> 6.1.2 情報セキュリティリスクアセスメント
> a) 次を含む情報セキュリティのリスク基準を確立し，維持する。
> 1) リスク受容基準
> 2) 情報セキュリティリスクアセスメントを実施するための基準
> （JIS Q 27001:2014 6.1.2 情報セキュリティリスクアセスメント より引用）

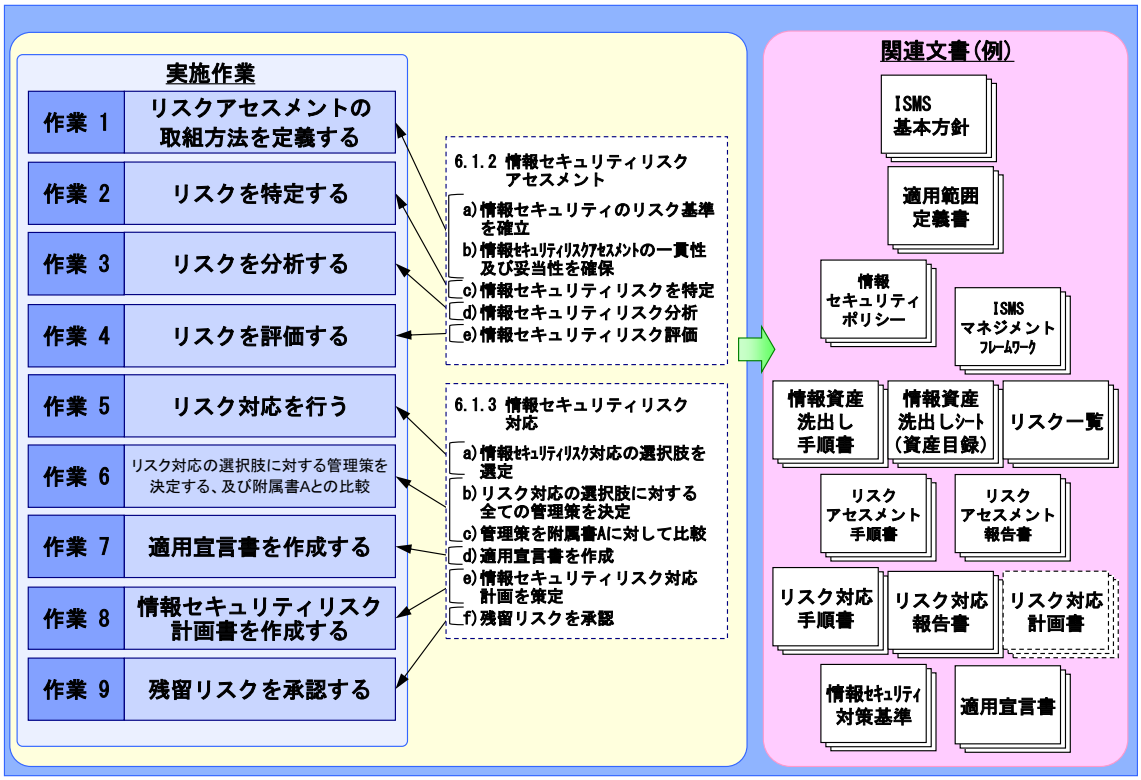
改訂された基準でいうリスク基準は、リスク受容基準及び情報セキュリティリスクアセスメントを実施するための基準を含むより広い概念といえます。この概念には、旧リスクマネジメント編で用いられていたリスク評価基準、すなわち、「リスクの重大さを決定するために算定されたリスクと比較する尺度（リスククライテリア）」も含まれるといえます。このガイドでは、これ以降、リスク基準という用語を用いますが、旧リスクマネジメント編のリスク評価基準を含みます。

３．情報セキュリティリスクアセスメントとリスク対応

JIS Q 27001:2014 の「6.1 リスク及び機会に対処する活動」は、ISMS の全体のリスクを考慮し、取扱いますが、その中で「6.1.1　一般」では、ISMS の計画を策定するとき、組織が対処する必要のあるリスク及び機会について述べています。リスクマネジメント活動においては、ISMS の意図した成果を達成するために、情報セキュリティに関連する固有のリスクだけでなく、マネジメントシステムのリスクを含めた ISMS 全体に対するリスクを対象とします。詳細は、ISMS ユーザーズガイドの 6.1 を参照してください。
また、JIS Q 27001:2014「6.1.1　一般」では、ISMS で解決する必要のある課題を決定して、その課題を ISMS で解決できるように 7 つのプロセス（JIS Q 27001:2014 の箇条 4～10 までのプロセス）をしっかりと動かすための仕組みを作ることを要求しています。
まず、ISMS で解決する必要のある課題を決定するために、リスク及び機会を抽出する手順を策定します。抽出にあたっては、箇条 4 で把握した組織の内外の環境と利害関係者からの情報セキュリティのニーズと期待の調査を一連のものとして行います。できるだけ網羅的にリスク及び機会を抽出します。
次に求められるのは、組織固有の ISMS の仕組みを構築することです。JIS Q 27001:2014 では組織のプロセスに組み込むことを要求しています。そこで、7 つのプロセスで必要とする文書を準備することになります。その結果として、ISMS の課題に対する活動計画、運用計画、有効性やパフォーマンスの測定計画などの様式を準備することができます。

３．１　作業の流れ

JIS Q 27001:2014 の「6.1.2 情報セキュリティリスクアセスメント」及び「6.1.3 情報セキュリティリスク対応」について、図 3-1 に実施作業の例を示します。作業１～９までを実施する順番はこの例に限られるものではありません。たとえば、細分化した個別リスクごとに、各作業を進捗することができますし、関連する個別リスクについては、それらに必要な作業項目を他の個別リスクの結果に基づいて繰り返すなど、帰納法的に進捗することも考えられます。



注）文書名は全て例示

図 3-1　実施作業の例

【補足】

情報セキュリティリスクアセスメントとリスク対応の手法改善の重要性

リスクアセスメントとリスク対応の手法は、当初に決めた方法を採用し続けなければならないということではなく、適切なマネジメントの手続きに従って、改善していくことが重要です。

脅威の程度、ぜい弱性の程度、事業上の損害の評価、リスクレベルの決定の方法など、多くの場面で、経営陣、情報管理者、担当者の判断が介在します。また、リスク基準の最終的な設定は経営陣に依存します。経営陣のリスクマネジメントについての力量が十分でない場合には、経営的な視点から見て不適切なリスク基準が選定されているかもしれません。これは、リスクマネジメントが経営の一部であることを考えれば当然のことです。しかし、ISMS の枠組みに従い継続的にリスクマネジメントを実施することにより、この様な判断に関する力量も高まっていきます。

リスクアセスメントとリスク対応についてのみならず、リスクマネジメント全体についての改善が行われていくことが ISMS の重要なポイントといえます。

3．2　情報セキュリティリスクアセスメント

3.2.1　作業 1　リスクアセスメントの取組方法を定義する

組織は，次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め，適用しなければならない。

a) 次を含む情報セキュリティのリスク基準を確立し，維持する。

1) リスク受容基準

2) 情報セキュリティリスクアセスメントを実施するための基準

（JIS Q 27001:2014　6.1.2 情報セキュリティリスクアセスメント　より引用）

本ガイドの「2.1　組織の状況」、「2.2　情報セキュリティ方針及びリスク基準を決定する」に関連する作業を終えたら、適用範囲におけるリスクアセスメントを実施する上での体系的な取組方法を明らかにし、文書化する必要があります。「組織の状況」、「情報セキュリティ方針及びリスク基準を決定する」で決定した方針を基に、「組織及びその状況の理解」や「利害関係者のニーズ及び期待の理解」に基づき作業のフレームワークやそれぞれの目標を決定し、文書化します。

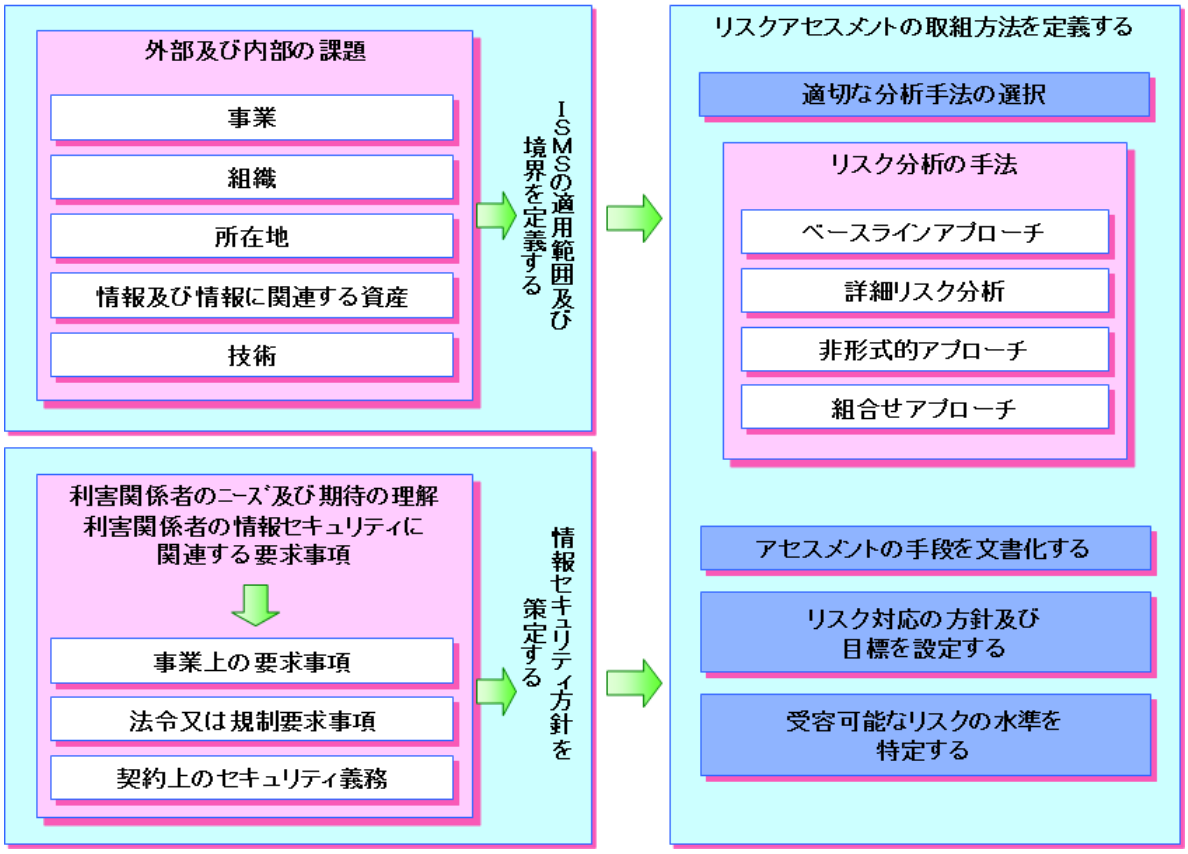


図 3-2　リスクアセスメントの取組方法の定義（例）

（１）リスクアセスメント

「リスクアセスメント」とは「リスク特定からリスク分析を実施、リスク評価するまでの全てのプロセス」を指します。つまり、リスクアセスメントにおいては、どのようなリスクが存在し（「リスク特定」）それがどの程度発生しやすいか、そして発生した時どの程度の影響をもつかを明らかにし（「リスク分析」）あらかじめ定められているリスク受容基準と比較する「リスク評価」までのプロセスを実施します。

（２）リスクアセスメントの方法を特定する

JIS Q 27001:2014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、「組織は情報セキュリティリスクアセスメントのプロセスを定めなければならない」として次のとおり規定しています。

> 組織は，次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め，適用しなければならない。
> a) 次を含む情報セキュリティのリスク基準を確立し，維持する。
> 1) リスク受容基準
> 2) 情報セキュリティリスクアセスメントを実施するための基準
> b) 繰り返し実施した情報セキュリティリスクアセスメントが，一貫性及び妥当性があり，かつ，比較可能な結果を生み出すことを確実にする。
> （JIS Q 27001:2014 6.1.2 情報セキュリティリスクアセスメント より引用）

組織は、「組織の状況（内外の課題や利害関係者のニーズや期待（法令・規制の要求事項を含む））」や「情報セキュリティ方針」を踏まえて以下を決定し、情報セキュリティリスクアセスメントに関して文書化する必要があります。

- 誰が行うのか
- いつ行うのか
- 段階に応じてどの手法をとるのか
  - 例えば、リスクアセスメントのプロセスの過程で、著しくコンプライアンス違反が判明した際は、分析を一時中断し、管理策の検討、導入の工程に速やかに入るベースラインアプローチ的手法をとる
- 発生のしやすさをどのような基準で分類するか
- 影響の大きさをどのようにはかるか
- 発生のしやすさや影響の大きさからどのようにリスクレベルを算定するか
- 算定されたリスクレベルに対する受容可能な範囲はなにか
- 受容を承認するのは誰かなど

を考慮して、適したリスクアセスメントの方法を特定する必要があります。
同一組織において、その体系的な取組み方法は一意に決定されますが、リスクアセスメントを実施する際、用いる手法は、想定されるリスクに応じて複数ある場合があります。リスクアセスメントの結果が実

施する人や部門でバラツキが出たり、実施した時で同一条件であるにもかかわらず異なる結果がでたりすると、リスクに対する適切な対応がとれなくなる恐れがあります。
この様なことを踏まえ、一貫性及び妥当性があり，かつ，比較可能な結果を生み出すことを確実にするリスクアセスメントの手順を文書化しておく必要があります。
なお、リスクアセスメントの方法については、ISMS ユーザーズガイド　付録 2 を参照してください。

（３）適切な分析手法の選択

リスクはリスク源に事象が作用して発生すると考えることもできますし、資産にとって「発生しては困る事象（脅威）」が「固有の弱点（ぜい弱性）」につけ込んで発生すると考えることもできます。
このいずれにおいてもリスクは発生のしやすさと影響の大きさから算定することができます。
発生のしやすさと影響の大きさを算定するに当たってはプロセスベースでリスクを特定し、算出することが極めて有効です。情報はどのプロセスで扱われるかによって、リスクが異なります。異なるリスクに対応するためにも、プロセスとの関係でリスクを捉えることで情報やその情報を扱う情報システム、人や組織を同時に捉えることができます。規格では資産に限定してリスク分析をすることを要求していませんので、プロセスベースで発生の起こりやすさと影響の大きさを考慮してリスクアセスメントをすることも有効です。
またこれらのプロセスを念頭に置いた上で、そのプロセスで作成されたり、使用されたりする資産に注目して、以下のように資産にとって「発生しては困る事象（脅威）」と「固有の弱点（ぜい弱性）」を明確にすることでリスク分析を実施することも具体的で有効です。この方法では、個別の資産の価値と、脅威、ぜい弱性を総合的に分析し、リスク算定を行います。算定したリスクに応じて、資産を脅威から適切に保護する対策を実施することが必要になります。
リスク分析の手法の特徴を理解し、前のステップで情報セキュリティ方針を定義する際に明らかになった「組織の保有する情報及び情報に関連する資産」や「情報セキュリティ上の要求事項」に基づいてリスク分析の手法を決定します。

（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では、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を特定する」には、次のような作業手順や判断基準、分類基準が含まれます。

- 資産目録の作成手順
- 事業上の損害（資産の価値）の評価基準
- 脅威の分類基準や評価基準
- ぜい弱性の分類基準や評価基準
- リスクレベルの算出方法
- リスク基準（リスク受容基準として）
- リスク基準（リスクアセスメントを行う頻度など、リスクアセスメントを実施するための基準）

上記の例は、脅威の発生可能性の評価と、ぜい弱性の評価を別々に行う場合の例です。
従来からプロセスに注目してリスクアセスメントすることは可能でしたが、今回の規格改訂でプロセスベースでリスクアセスメントしても良いことがより明確になりました。

プロセスベースでの「リスクアセスメントの方法」には、次の様な作業手順や判断基準、分類基準が含まれます。

- プロセスフローの作成手順
- 発生のおこりやすさを評価する基準
- 影響の大きさを評価する基準
- リスクレベルの算出方法
- リスク基準（リスク受容基準として）
- リスク基準（リスクアセスメントを行う頻度など、リスクアセスメントを実施するための基準）

（５）リスク対応の方針及び目標を設定する

組織は、リスク分析を実施し算出されたリスクレベルとリスク基準（リスク受容基準）を比較し、算出されたリスクレベルに基づきリスクマネジメントの枠組みの中でどの様な対応を実施する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 JIS Q 31000:2010 に次の７つが紹介されています。

- リスクを生じさせる活動を、開始又は継続しないと決定することによってリスクを回避すること
- ある機会を追求するために、リスクを取る又は増加させること
- リスク源を除去すること
- 起こりやすさを変えること
- 結果を変えること
- 一つ以上の他者とリスクを共有すること（契約及びリスクファイナンシングを含む）

■ 情報に基づいた選択によって、リスクを保有すること

「リスク対応」の内容については、3.3 で詳細に説明します。
ここで決定したリスク対応の選択肢も、文書化す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」が存在します。
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されます。
ここでは、（４）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レベルを用いてリスク評価を実施する際、その水準を再度明らかにし、リスク受容またはリスク対応の意思決定の水準の確認を行い、その上で、経営陣は受容可能なリスクの水準を最終的に承認することになります。

３.２.２ 作業２ リスクを特定する

c) 次によって情報セキュリティリスクを特定する。
1) ISMS の適用範囲内における情報の機密性，完全性及び可用性の喪失に伴うリスクを特定するために，情報セキュリティリスクアセスメントのプロセスを適用する。
2) これらのリスク所有者を特定する。
（JIS Q 27001:2014　6.1.2 情報セキュリティリスクアセスメント より引用）

リスクアセスメントは、資産にとって「発生しては困る事象（脅威）」と「固有の弱点（ぜい弱性）」を特定することから始めます。図 3-3 は、リスクレベルがそれを取り巻く「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。

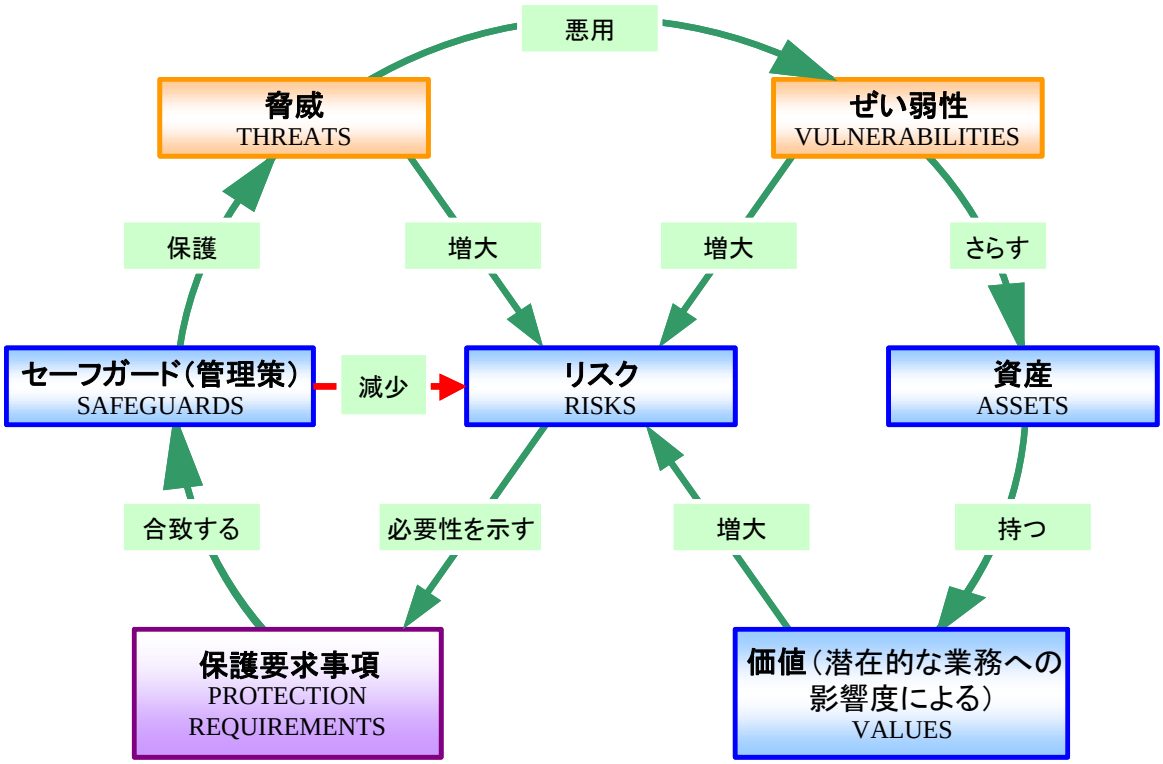


図 3-3　脅威、ぜい弱性とリスクの関係

リスクの特定では、具体的には次の 2 つの作業が実施されます。

- 資産の洗い出し（または、特定）
- 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 JIS Q 27002:2014 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」を特定することが望ましいとしています。

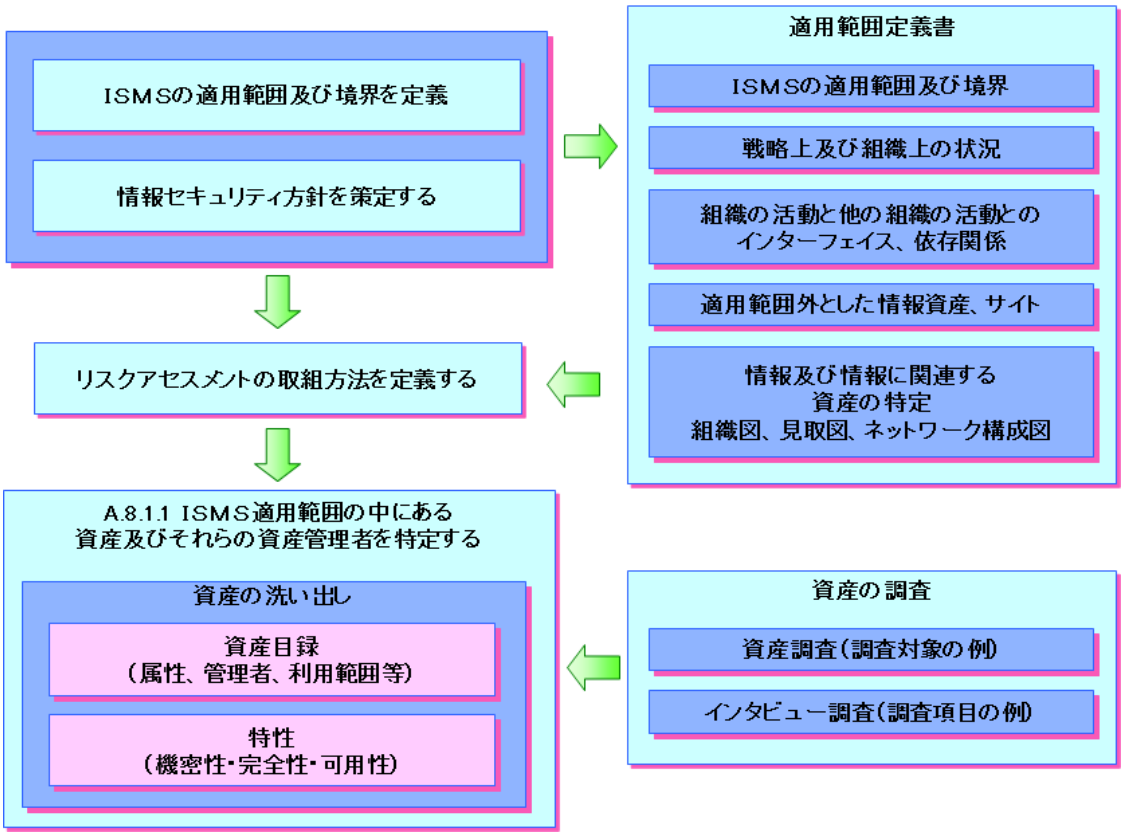


図 3-4　資産の洗い出し（例）

①　資産目録の作成

「資産目録」を作成することを、JIS Q 27002:2014 では、「8.1.1 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，情報のライフサイクルに関連した資産を特定し，その重要度を文書化することが望ましい。情報のライフサイクルには，作成，処理，保管，送信，削除及び破棄を含めることが望ましい。文書は，専用の目録又は既存の目録として維持することが望ましい。
> 資産目録は，正確で，最新に保たれ，一貫性があり，他の目録と整合していることが望ましい。
> 特定された各資産について，管理責任者を割り当て（8.1.2 参照），分類する（8.2 参照）ことが望ましい。
> （JIS Q 27002:2014　8.1.1 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次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（利用する業務プロセス）
- 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、後の作業とな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

情報、情報を支援する資産として表 3-1 のように主要資産、全種類の支援資産（適用範囲の主要要素が依拠する）に分類して整理することも有効です。

表 3-1 資産の例示

資産の種類	例示
主要資産	事業プロセス及び事業活動、情報
全種類の支援資産（適用範囲の主要要素が依拠する）	ハードウェア、ソフトウェア、ネットワーク、要員、サイト、組織の構成

（ISO/IEC 27005:2011 附属書 B B1 資産の特定の例 より引用）

また、主要資産及び支援資産について、ISO/IEC 27005:2011 では次のように説明しています。

B.1.1 主要資産の特定

この活動は，適用範囲をより正確に記述するために，主要資産（事業プロセス及び事業活動，情報）を特定することにある。この特定活動は，プロセスの活動グループの代表（マネージャ，情報システムの専門家及びユーザ）が実施する。

主要資源は通常，適用範囲の活動の中核プロセス及び情報である。情報セキュリティ基本方針又は事業継続計画を策定するのにより適していれば，組織のプロセスのような、これ以外の主要資産も検討することができる。目的に応じて，調査には，適用範囲を構成する全要素の徹底的な分析を必要としない場合がある。このようなケースでは，適用範囲の主要要素に調査の境界を限定することができる。

主要資産には，二つのタイプがある。

1-事業プロセス（又はサブプロセス）及び事業活動，例えば：

・その損失又は低下によって，組織の使命達成が不可能となるプロセス

・機密プロセス又は占有技術を伴っているプロセス

・修正された場合，組織の使命の達成に大きく影響するプロセス

・組織が契約，法令又は規制の要求事項を順守するために必要となるプロセス

2-情報：

より一般的には，主要情報は主に次のものを含む

・組織の使命又は事業の遂行に不可欠の情報

・プライバシーに関する国内法にいう意味で，特別に定義することができる個人情報

・戦略的方向性によって決定される目的の達成に必要となる戦略情報

・収集，保管，処理及び送信に長時間を要する高コスト情報及び／又は高い取得費用を伴う高コスト情報

この活動後に，取扱いに慎重を要すると特定されなかったプロセス及び情報は，残りの調査で明確な種別をもたない。すなわち，このようなプロセス又は情報が危機にさらされるとしても，組織は指名の達成に成功する。

ただし、このようなプロセス及び情報は，多くの場合，取扱いに慎重を要すると特定されたプロセス及び情報の保護のために導入される管理策に引き継がれる。

B.1.2 支援資産のリスト及び説明

適用範囲は，特定され，説明を加えられるべき資産で構成される。このような資産は，適用範囲の主要資産（プロセスと情報）を損なうことを狙いとした脅威につけ込まれる可能性のあるぜい弱性をもつ。このような資産は，様々なタイプのものがある。

ハードウェア

ハードウェアのタイプは，プロセスを支援するすべての物理的要素で構成される。

データ処理機器（アクティブ）

単体で動作する必要のある品目を含めた自動情報処理機器

可搬形機器

ポータブルコンピュータ機器

例：ラップトップコンピュータ，パーソナルデジタルアシスタント（PDA）

固定機器

組織の構内で使用するコンピュータ機器

例：サーバ，ワークステーションとして使用するマイクロコンピュータ

周辺機器

入力，持ち出し又は送信用データとして通信ポート（シリアル，パラレルリンクなど）によりコンピュータに接続される機器

例：プリンタ，脱着可能なディスクドライブ

データ媒体（パッシブ）

データ又は機能を保存する媒体

電子媒体

データ保存用にコンピュータ又はコンピュータネットワークに接続可能な情報媒体。サイズはコンパクトでも，大量のデータを含むことがある。標準のコンピュータ機器で使用することができる。

例：フロッピーディスク，CD-ROM，バックアップカートリッジ，脱着可能なハードディスク，メモリキー，テープ

その他の媒体

データを含む非電子媒体，静電媒体

例：紙，スライド，透明度の高いスライド，文書，ファックス

ソフトウェア

（以下、省略）

（ISO/IEC 27005:2011 附属書 B より引用）

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。

例えば、経理関連書類には、発表前の財務諸表から、試算表、売掛金元帳、売掛金回収リスト、顧客マスタなど、様々なものが存在します。しかし、これらを洗い出した後、重要性や属性が同じものを経理関連書類としてまとめればよいでしょう。そして、重要性などが異なるために、別途管理が必要なもの（例えば、発表前の財務諸表など）を別に取り出して管理すればよいと思われます。

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最終目標ではありません。

（２） 脅威・ぜい弱性の明確化

リスクの発生のしやすさは、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」の組合せで表現されます。

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。ISO/IEC 27005:2011 では表 3-2 のとおりに大別して説明しています。

表 3-2 脅威の分類例

故意によるもの	偶発的なもの	環境的なもの
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と同様、情報利用者や他事業部門の関係者、外部の専門家から提供される脅威に関する情報をもとに、自らが管理する資産がさらされる脅威を識別し、表 3-3 の例示の様な一覧表を作成します。

表 3-3 脅威の例示とその分類例

類型	脅威	原因
物理的損傷	火災	A, D, E
	水害	A, D, E
	汚染	A, D, E
	大事故	A, D, E
	機器や媒体の破壊	A, D, E
	粉塵(ダスト)，腐食，凍結	A, D, E
自然事象	気候	E
	地震	E
	火山活動	E
	気象現象	E
	洪水	E
重要なサービスの喪失	空調や給水システムの故障	A, D
	電力供給の停止	A, D, E
	電気通信機器の故障	A, D
放射による妨害	電磁放射	A, D, E
	熱放射	A, D, E
	電磁パルス	A, D, E
情報を危うくすること	危険にさらされている干渉信号の傍受	D
	遠隔スパイ行為	D

	盗聴	D
	媒体や文書の盗難	D
	機器の盗難	D
	再利用又は廃棄した媒体からの復元	D
	漏洩	A, D
	信頼できない情報源からのデータ	A, D
	ハードウェアの改ざん	D
	ソフトウェアの改ざん	A, D
	位置検知	D
技術的な故障	機器の故障	A
	機器の誤動作	A
	情報システムの飽和	A, D
	ソフトウェアの誤作動	A
	情報システムの保守に関する違反	A, D
認可されていない行為	認可されていない機器の使用	D
	ソフトウェアの不正コピー	D
	海賊版又は(不正)コピーソフトウェアの使用	A, D
	データの破壊	D
	データの違法な処理	D
機能を危うくすること	使用時のミス	A
	権限の乱用	A, D
	権限の詐称	D
	アクションの拒否	D
	要員の可用性に関する違反	A, D, E

（ISO/IEC 27005:2011 より引用）

脅威の洗い出しは、表 3-3 の例などを参考に実施します。例えば、故意によるものは、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、どの様な要因が脅威であるかを識別します。
偶発的なものは、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。

【補足】

脅威の分類と管理策の選択

人為的脅威（意図的脅威、偶発的脅威）と環境的脅威を区分して把握することにより、どの様な性質のセキュリティ対策を実施すればよいのかが整理しやすくなります。

環境的脅威は、脅威の発生そのものを人間が低減することが困難なものが多くあります。例えば、環境的脅威として地震や高潮がありますが、地震や高潮の発生そのものを人間がコントロールすることはできません。従って、地震の発生可能性が低い場所を選択する、地震が発生した場合に素早く検知し、災害から回復する対策を重視する、などのセキュリティ対策が選択されることになります。

意図的脅威の例としては、「（内部者が営業秘密を）漏洩する」という脅威が考えられます。この様な脅威については、当該行為が犯罪行為（不正競争防止法違反）であり、法的に罰せられること、会社は就業規則により漏洩者を罰すること、場合によっては損害賠償請求を行うということを規程で明確に示し、教育を実施するという抑止的な対策が有効となります。また、漏洩を早期に検知するといった発見的な対策も重要となります。

偶発的脅威としては、「入力ミス」がありますが、入力ミスが生じない様に、二回ずつ入力する、一定の範囲の値しか入力できない様にする、チェックデジットやチェックサム※を設けるといった技術的な対策が有効となります。

この様に、意図的脅威、偶発的脅威、環境的脅威を区分して把握することは、どの様な対策が有効であるかを考える上で有用といえます。

※チェックデジットやチェックサム：データを送受信する際の誤り検出方法の一つ。

② ぜい弱性の識別

ぜい弱性とは、脅威の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 3-4 に示します。また、ぜい弱性をリスト化する際には、表 3-4 のとおりに脅威と関連付けて整理する必要があります。

表 3-4 ぜい弱性の識別

類型	ぜい弱性の例	脅威の例
ハードウェア	記憶媒体の不十分な保守/不適当な設置	情報システムの保守に関する違反
	定期的な交換計画の欠如	機器や媒体の破壊
	湿気，ホコリ，汚れに対する影響の受けやすさ	粉塵(ダスト)，腐食，凍結
	電磁放射に対する影響の受けやすさ	電磁放射
	有効な構成変更管理の欠如	使用時のミス
	電圧の変化に対する影響の受けやすさ	電力供給の停止
	温度変化に対する影響の受けやすさ	気象現象
	保護されない保管	媒体や文書の盗難
	廃棄時の注意の欠如	媒体や文書の盗難

	管理されないコピー作成	媒体や文書の盗難
ソフトウェア	ソフトウェアのテストをしない，又は不十分なソフトウェアのテスト	権限の濫用
	ソフトウェアの公知の欠陥	権限の濫用
	ワークステーションから離れる際に“ログアウト”しない	権限の濫用
	適切に削除されていない記憶媒体の処理又は再利用	権限の濫用
	監査証跡の欠如	権限の濫用
	アクセス権の誤った割当て	権限の濫用
	分散配布しているソフトウェア	データの破壊
	時間の観点からみると誤ったデータのアプリケーションプログラムによる処理	データの破壊
	複雑なユーザインタフェース	使用時のミス
	文書化の欠如	使用時のミス
	不正確なパラメタ設定	使用時のミス
	日付の誤り	使用時のミス
	ユーザの識別及び認証メカニズムの欠如	権限の詐称
	保護されていないパスワードファイル	権限の詐称
	不十分なパスワード管理	権限の詐称
	不要なサービスが実行可能	データの違法な処理
	成熟度の低いソフト又は新しいソフトウェア	ソフトウェアの誤作動
	開発者のための不明確又は不完全な仕様書	ソフトウェアの誤作動
	効果的な変更管理の欠如	ソフトウェアの誤作動
	管理されていないソフトウェアのダウンロード及び使用	ソフトウェアの改ざん
	バックアップコピーの欠如	ソフトウェアの改ざん
	建物，ドア及び窓の物理的保護の欠如	媒体や文書の盗難
	管理報告書を作成しないこと	認可されていない機器の使用
……	……	……

（ISO/IEC 27005:2011 より引用）

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、情報のライフサイクルに応じた処理プロセス形態、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（社内利用）」、「ノートPC（社外利用）」などと分けて識別して管理した方が、より効果的な対策を導入できる場合もあることに留意しなければなりません。

また、表 3-4 のぜい弱性の内容を見ていただければわかりますが、ぜい弱性は管理策の欠如を同時に意味します。例えば、バックアップコピーの欠如というぜい弱性とバックアップコピーの取得という管理策は裏表の関係になっています。ぜい弱性を識別することは、必要となる管理策の識別にも役立ちます。ぜい弱性を識別するために、JIS Q 27001:2014 の附属書 A「管理目的及び管理策」、JIS Q 27002:2014 の管理策、情報セキュリティ管理基準等のコントロールを参考にするとよいでしょう。

【補足】

■プロセスベースの情報セキュリティリスクアセスメント

今まで資産に注目して、その資産に対する脅威やぜい弱性を考慮したリスクアセスメントについて述べてきましたが、今回の規格改訂によりリスクアセスメントの方法が汎用的になり、色々なリスクアセスメント方法が可能になっています。

その１つとしてプロセスベースのリスクアセスメント方法について以下に解説します。

プロセスベースのリスクアセスメントとは仕事（業務）の流れにそってリスクアセスメントをすることです。

プロセスに沿って以下の視点でリスクを特定します。

１）機密性の視点

そのプロセスや活動で情報が漏れるかの視点でリスクを特定します。

２）完全性の視点

そのプロセスや活動で情報の完全性が失われるかの視点でリスクを特定します。

３）可用性の視点

そのプロセスや活動で情報が使えなくなるかの視点でリスクを特定します。

４）法令・規制を順守の視点

そのプロセスや活動で法令・規制が不順守になるかの視点でリスクを特定します。

特定にあたっては、そのプロセスで使用する情報だけでなく、ハードウェア、ソフトウェア、ネットワーク、要員、サイト、組織の構成にも注目して特定します。

プロセスベースのリスクアセスメントは、仕事（業務）の流れでリスクを特定するため、品質マネジメントシステム等の他のマネジメントとの親和性の高いリスクアセスメントが行われ、統合したマネジメントシステムが構築しやすくなります。

プロセスベースの情報セキュリティリスクアセスメントの例を以下に示します。

① プロセスを明確にする

仕事（業務）の流れを明確にし、業務プロセスを明らかにします。どの程度細かくするかは組織によりますが、階層を分けて明確にすることができます。例えば、第一レベルでは営業プロセスの後、設計・開発のプロセスがあり、その後、製造プロセスがあり、検査プロセスを経て出荷プロセスで顧客に製品を届けるといった具合です。更に第二レベルは例えば営業プロセスを 1)顧客から要件書を受領し、2)見積りのついた提案書をメールで送付し、3)契約するといった具合です。

これらプロセスを明らかにするにあたり、誰が、どんな機器やシステムを使用して、どんな情報を扱うかを明確にする必要があります。例えば、上記 2)では、営業担当者が顧客管理システムに登録されているメールアドレスを使って、見積書という情報を添付ファイルとしてメーラーを使用して顧客先に送付するといった具合です。

② リスクを特定する

プロセスと個々の活動に注目してリスクを特定します。

たとえば、上記 1)では顧客から資料を受領したかしないかでの紛争リスクがあり、２）ではメールで見積書を送付する時に誤送信をするリスクや提案書に他社に著作権がある情報を記載してしまうリスクがあり、3)の契約では契約書に機密保持条項が欠落するリスクがあります。

プロセスと活動に注目することでどんなリスクがあるかが想定しやすくなると同時に、情報だけでなく、人や IT 機器や IT システムも含めたリスク特定ができます。さらに、上記著作権に触れるリスクのように法令に違反するリスクも明確にすることができます。

さらに、例えば営業プロセスに関するリスクであれば営業部長がリスク所有者だといったようにリスク所有者を明確にさせやすいといった特徴があります。

3.2.3 作業 3 リスクを分析する

d）次によって情報セキュリティリスクを分析する。

1）6.1.2 c）1）で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。

2）6.1.2 c）1）で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。

3）リスクレベルを決定する。

（JIS Q 27001:2014　6.1.2 情報セキュリティリスクアセスメント より引用）

作業 2 で特定したリスクについて、分析をします。

（1）起こり得る結果のアセスメント （参考：JIS Q 27001:2014 6.1.2 d）1))

資産目録に基づき事業上の損害を評価します。資産の価値を評価するというより、資産の機密性（C）、完全性（I）、可用性（A）が損なわれた時の事業上の影響（損害）を評価すると考えたほうがよいでしょう。

このプロセスは、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、主要な事業上の損害の評価は、組織のビジネスをよく理解した情報の管理責任者（一般にはビジネスオーナがなります。）によって行われなければなりません。

組織は、事業上の損害を判定する際に組織独自の判断基準を明確にしなければなりません。

情報セキュリティは、CIA それぞれについて事業上のリスクが異なります。従って、CIA それぞれの観点から、事業上の損害を評価することが非常に重要です。例えば、企業紹介用のホームページについては、機密性は高くないですが、完全性は高くなければなりません。また、資金決裁システムなどでは、可用性や完全性については非常に高くなければなりませんが、機密性についてはそれほど高くなくてもよいかもしれません。

従って、事業上の損害の評価を機密性、完全性、可用性の平均点で評価する様な方法は、論理的ではなく、誤った対策を導くことになりますので不適切です。その点を明確にするために、機密性、完全性、可用性のそれぞれの観点から事業上の損害を評価することとなります。

表 3-5 及び表 3-6 に、影響度評価の判断基準の例を示します。

表 3-5 機密性の評価基準例

資産価値	クラス	説明
1	公開	内容が漏洩した場合でも、ビジネスへの影響はほとんど無い
2	社外秘	内容が漏洩した場合、ビジネスへの影響は少ない
3	秘密	内容が漏洩した場合、ビジネスへの影響は大きい

4	極秘	内容が漏洩した場合、ビジネスへの影響は深刻かつ重大である

表 3-6 影響度の評価基準例

価値評価	影響度	金銭・機会損失（短期）	金銭・機会損失（中長期）	信用・ブランド損失
1	非常に小さい	当期経営にはほとんど影響はない	中長期的な経営には影響はない	ほとんど影響がない
2	小さい	当期経営に軽微な影響（当期利益の１％以下）を及ぼす	中長期的な経営には影響はない	限定された人に対して悪い風評が及ぶ
3	中程度	当期経営に影響（当期利益の３％以下）を及ぼす	中長期的な経営にはほとんど影響はない	多くの人に対して悪い風評が及ぶ
4	大きい	当期経営に重大な影響（当期利益の１０％未満）を及ぼす	２年程度の経営に影響が及ぶ	限定された人に長期的に悪いイメージが残る
5	非常に大きい	当期経営に極めて重大な影響（当期利益の１０％以上）を及ぼす	３年以上の経営に影響が及ぶ	多くの人に対し長期的に悪いイメージが残る

上記はあくまでも例示です。この例は評価レベルを５段階とし、３つの視点から総合的に評価することを想定したものです。利益と信用を価値評価の中心としています。自治体であれば、利益やブランドではなく、予算総額、住民からの信頼という視点を取り入れるほうがよいでしょう。この様な評価の視点はその組織の重要な利害関係者の利益に関連する視点にあわせるとよいでしょう。
事業上の損害の評価は、主に情報の管理責任者の主観で判定され、情報セキュリティ委員会等で全体のバランスを調整することになります。

（２）起こりやすさのアセスメント　（参考：JIS Q 27001:2014 6.1.2 d）2)）

ここでは、起こり得るセキュリティ障害などの現実的な発生可能性を評価するために、認識されている脅威及びぜい弱性を評価します。但し、脅威とぜい弱性の評価は、個別に行っても組み合わせて評価しても構いません。その際、資産に影響を及ぼす脅威や連動して起こりうる脅威などを洗い出し、現在実施されている管理策からぜい弱性を考慮する必要があります。

① 脅威の評価

脅威の評価は、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す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です。表 3-7 に 3 つに区分した場合の分類基準を、表 3-8 に 5 つに区分した場合の分類基準を例示します。

表 3-7 脅威の分類基準例（１）

脅威		
レベル	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。

表 3-8 脅威の分類基準例（２）

脅威			
レベル	意図的（計画的）脅威	偶発的脅威	環境的脅威
1	実施による利益はない	通常では発生しない	3 年以内に一度も発生しない
2	実施による利益はあまりない	特定の状況下での発生が考えられる	3 年に一度程度発生する
3	実施による利益は多少ある	専門能力のあるものの不注意で発生する	1 年に一度程度発生する
4	実施による利益がある	一般者の不注意で発生する	1 ヶ月に一度程度発生する
5	発生が具体的に予想される	通常の状態で発生する	1 ヶ月に一度以上発生する

表 3-8 は、脅威の内容に応じて脅威レベルの評価軸を区分しています。あくまで例ですので、自らのマネジメントシステムにおいて、もっとも適切な評価方法を確立することが重要です。

② ぜい弱性の評価

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。つまり、現在実施されている対策を考慮してぜい弱性の評価を行うことになります。十分な管理策が実施されている場合は、ぜい弱性が少なくなります。一方、管理策を実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。
表 3-9 に５つに区分した場合のぜい弱性の分類基準を例示します。

表 3-9 ぜい弱性の分類基準例

ぜい弱性			
レベル	意図的（計画的）脅威に対するぜい弱性	偶発的脅威に対するぜい弱性	環境的脅威に対するぜい弱性
1	最高程度の対策を実施済み	最高程度の対策を実施済み	最高程度の対策を実施済み
2	高度な専門知識や設備を持つ者によって可能な状況	通常の利用状況ではほとんどリスクが顕在化する恐れがない状況	通常の利用環境ではほとんどリスクが顕在化する恐れがない状況
3	専門能力を持つ者によって可能な状況	専門能力がある者の不注意によりリスクが顕在化する恐れがある状況	専門能力がある者の不注意によりリスクが顕在化する恐れがある状況
4	一般者が調査を実施すれば可能な状況	一般者の不注意によりリスクが顕在化する恐れがある状況	一般者の不注意によりリスクが顕在化する恐れがある状況
5	一般者が普通に実施可能な状況	特段の対策を実施しておらず、いつリスクが顕在化してもおかしくない状況	特段の対策を実施しておらず、いつリスクが顕在化してもおかしくない状況

ぜい弱性を評価するに当たっては、資産に対して実施している管理策を資産毎にリストアップし、その結果をみてぜい弱性を評価するという方法も考えられます。
表 3-10 にこの方法により評価する場合のワークシート例を表示します。この表には資産、脅威も記載されていますので、リスク分析及びリスク対応後のリスク分析にも利用可能です。

表 3-10 ぜい弱性の分析と低減対策検討ワークシート例

資産	脅威	CIA	実施している対策	現在のぜい弱性	追加する対策	対策後のぜい弱性
顧客リスト（紙）	盗難	C	業務時間外はキャビネットに保管している。 （施錠はしていない）	4	業務時間外は施錠された金庫に保管する。 その鍵は営業課長及び主任が携帯する。 業務時間内は施錠されたキャビネットに保管する。 その鍵は営業課員の机の引き出しに保管する。	2

					….	

※：資産と脅威の列は、あくまでぜい弱性を分析・評価し、対策をイメージするための補足情報（前提条件）であり、表 3-10 としてはリスクを算出している訳ではありません。但し、表 3-10 に脅威等の値を入れることによりリスク分析表として展開することも可能といえます。

脅威やぜい弱性の評価は、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をすることも考えられます。

【補足】

評価作業上の留意点について

脅威やぜい弱性の分類

脅威やぜい弱性の分類数は概ね 3 ～ 5 である場合が多いようです。分類をより細かくするほど、より正確なリスクレベルの決定を実施できる様な錯覚に陥りがちです。また、統計データに基づき客観的な定量評価をしたくなりがちです。しかし、ほとんどの脅威やぜい弱性の評価は限られた事実に基づく評価者の主観的な判断にならざるを得ず、それらを正確に予測することは困難であることは明らかです。従って、分類数を細かく設定したり、統計データを駆使して見積もることは、リスクアセスメントの作業負荷を増加させる割には、効果が少ないと思います。なぜならば、分類を細かく分けてもセキュリティ対策実施段階では、ほとんど影響がないことが多いからです。

評価が中央に集中する問題

資産の重要性（損害時の影響）の評価、脅威やぜい弱性の評価を分類する場合に、中央の数値（平均値：いわゆる大でも小でもないといった値）に評価が集まりがちになるという問題があります。特に分類数を 3 つにする場合は、この傾向性が多く見られます。一般に、評価基準があいまいである場合、評価者が十分な知識をもって評価できない場合に、その傾向が見られます。この様な問題を避けるために、評価基準を明確にする、評価者に対して評価についての適切な教育を行うことが重要なります。また、分類数を偶数（例えば、4 つ）にすることにより、中央の値に評価が集中するのを避けるという方法もあります。

評価者によるバラツキの問題

資産の重要性（損害時の影響）の評価、脅威やぜい弱性の評価を一人の担当者が行う場合はあまり問題となりませんが、複数の担当者が評価を行う場合、評価値を高めにとる傾向のある人、低めにとる傾向のある人が混在するため、評価にバラツキが生じるという問題があります。この様な問題を防ぐため、

- 評価基準を明確にする
- 評価者の評価についての教育・訓練を行う
- 情報セキュリティ委員会といった場で、評価全体の調整をする

などの対策が必要となります。

また、それぞれ分類したレベルに関して例を示すのもよいでしょう。個人情報の漏洩に伴う損害の評価はレベル５、個人情報の改ざんに伴う損害の評価はレベル４、個人情報が利用できないことに伴う損害の評価はレベル３などといった例示を分類例として示すことによりバラツキをある程度抑えることができます。また、部門間などに発生するバラツキを調整するために、整合性のとれた部門毎の分類表を策定し、バラツキを抑えることも考えられます。このことは、人事考課などで用いられる手法と似ているともいえるでしょう。

（３）リスクレベルの決定　（参考：JIS Q 27001:2014 6.1.2 d）3)）

リスクレベルは、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、簡易的に次の様な式で算出します。

リスクレベル　＝「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　2（一部の作業担当者に特権が付与されていたので）

この場合のリスクレベルは、次のとおりになります。

機密性に関わるリスクレベル：4×3×2＝24

完全性に関わるリスクレベル：2×3×2＝12

可用性に関わるリスクレベル：1×3×2＝6

図 3-5 リスクレベルの計算例

また、リスクレベルを算出するために、表 3-11 の例の様なマトリクス「リスクレベル早見表」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 3-11 リスクレベル早見表例

	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

【補足】

体系的なリスクレベルの決定の重要性

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～」ではリスクレベルの決定をリスクの算定として次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）

経営的な視点に立てば、リスクアセスメントは組織が直面する全てのリスクについて行われるべきです。情報セキュリティは組織が直面するリスクの一分野にすぎません。全てのリスクについてのリスクアセスメントを実施する上では、特に体系だったリスクアセスメントの手法を確立することが重要となります。その一部としてのリスクレベルの決定も体系的に行うことが重要となります。

【補足】

リスクレベルを決定することの意味

JIS Q 27001:2014 では、リスクレベルを決定することが要求事項に規定されています。上記の例では、リスクレベルを決定するために次の計算を行いました。

リスクレベル ＝「資産の価値」×「脅威」×「ぜい弱性」

しかし、この計算式には厳密な理論性はありません。脅威を評価した値は脅威の大きさを順位づけるために便宜的につけた数値にすぎません。損害を評価するための値、ぜい弱性を評価した値も同じです。この様な数値に過ぎない数字を四則演算してリスクレベルを決定することに理論性が乏しいことはあきらかです。このリスクレベルを決定するための算定式が教条的に利用され、単なるリスク計算遊びになってしまっては、本来の主旨から大きくはずれることになりかねません。したがって、この様な算定式や他の手法から得られた数値だけに頼ってリスクレベルを決定せず、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や、決定されたリスクレベルの妥当性を再度検討し、異常が発見されればその場で修正するなども、選択肢のひとつとなると思います。

3.2.4 作業４ リスクを評価する

> e) 次によって情報セキュリティリスクを評価する。
>
> 1) リスク分析の結果と 6.1.2 a) で確立したリスク基準とを比較する。
>
> 2) リスク対応のために，分析したリスクの優先順位付けを行う。
>
> （JIS Q 27001:2014　6.1.2 情報セキュリティリスクアセスメント より引用）

（１）リスク分析の結果とリスク基準との比較

作業 3 で分析し決定したリスクレベルについて、リスク基準と比較して評価します。リスク基準は経営陣が受容可能なリスクの水準として最終的に承認することになるものです。例えば、リスク基準で、受容可能なリスクレベルを 9 未満と決めた場合、リスク対応が必要となる資産は脅威とぜい弱性の観点から表 3-12 のとおりになります。なお、表 3-12 のリスクレベルの計算例では、可用性に関わるリスクレベルは受容できる範囲となります。 また、受容可能なリスクレベルを 4 未満とした場合は、表 3-13 のとおりになります。

表 3-12 リスク受容一覧の例(1)

起こりやすさ / 影響（結果）	脅威								
	1			2			3		
資産の価値	ぜい弱性								
	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6 A	9
2	2	4	6	4	8	12	6	12 I	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24 C	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 3-13 リスク受容一覧の例(2)

起こりやすさ / 影響(結果)	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

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す。残留リスクについても、何も管理をしなくてもよいというわけではありません。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、適宜リスクレベルの見直しを実施しなければなりません。その結果、受容可能なリスクとして判断されていたものも、追加的なリスク対応が必要となる場合もあります。

（２）リスク対応のための優先順位付け

リスクについては、リスク対応のために優先順位付けをします。リスク対応の順番の決め方は、リスク所有者の判断で行います。一般にはリスクレベルの高いものからリスク対応をしますが、リスクレベルが同じ場合に、どちらを先に対応すべきかの判断も重要です。

３．３　情報セキュリティリスク対応

３.３.１　作業５ リスク対応を行う

リスク対応は、リスクアセスメントで明確になった管理対象となるリスクに対して、リスクマネジメントの枠組みの中でどのような対応を実施するかを決定し、リスクを組織が受容できる水準に修正するプロセスです。JIS Q 27000:2014 では（JIS Q 0073 を引用し）、「リスクを修正するプロセス」と定義されています。また、この定義の注記 1 では、リスクを修正するための方策として、JIS Q 31000:2010 で例示されている次の 7 つの選択肢が示されています。

- リスクを生じさせる活動を、開始又は継続しないと決定することによってリスクを回避すること
- ある機会を追求するために、リスクを取る又は増加させること
- リスク源を除去すること
- 起こりやすさを変えること
- 結果を変えること
- 一つ以上の他者とリスクを共有すること（契約及びリスクファイナンシングを含む）
- 情報に基づいた選択によって、リスクを保有すること

リスク対応では、管理対象とするリスクに対し、適切なリスク対応の選択肢を選出し、さらにそれを実施する管理策を決定します。この選択肢として上記の 7 つを用いることができます。管理対象としないリスクに対しては、「受容する」という選択肢を選出します。ここでは、リスク対応における選択肢の選出について説明します。

（１）リスクレベルを低減する選択肢

「適切な管理策を適用し、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、JIS Q 27001:2014 の附属書 A に記載されている 114 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。前述の７つの選択肢のうち、「リスク源を除去すること」、「起こりやすさを変えること」及び「結果を変えること」の 3 つがこれに相当します。すなわち、リスクレベルそのものを修正し、低減する選択肢です。3 つの選択肢では、それぞれ低減するための対策が異なります。

リスク低減について概念的に示したものを図 3-6 に示します。
図中で、

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。
この例では、リスク（R）は、「リスクの発生の可能性を低減させる」ことと「リスクが顕在化した場合の影響度を低減させる」ために有効な管理策（C）により低減されることが示されています。

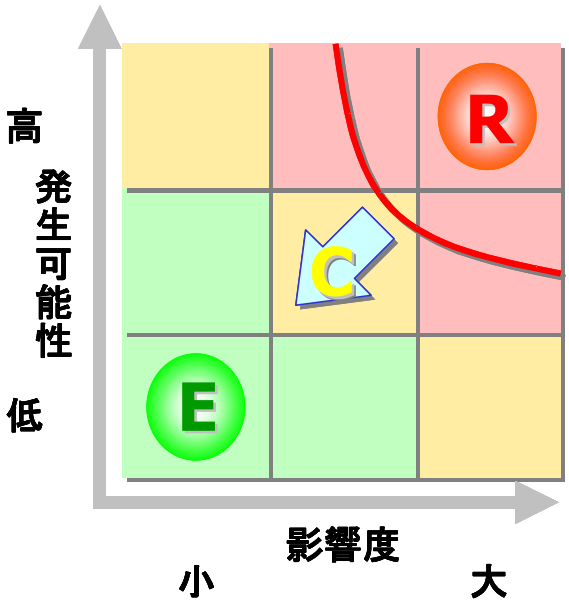


図 3-6 リスク低減の概念

この場合、それぞれの概念に相当する具体的な対策の例として次を挙げることができます。

リスクの発生の可能性を低減させる例

a)「入退室をより厳重に管理する」

b)「セキュリティパッチ適用により既知のぜい弱性を迅速に排除する」

リスクが顕在化した場合の影響度を低減させる例

c)「バックアップ頻度を増やし、修復可能なデータを増やす」

d)「情報資産の棚卸を行い必要ないものを整理する」

これらの例を前述の 7 つの選択肢と対照すると、それぞれ、b)及び d)は「リスク源を除去すること」、a)及び b)は「起こりやすさを変えること」、c)及び d)は「結果を変えること」に関する対策と見ることができます。b)が「起こりやすさを変えること」に加え「リスク源を除去すること」にも該当することは、「ぜい弱性が内在するシステム」をリスク源と見做すことで理解できます。

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ので対策を講じたあとのリスク（E）が存在します。多くの場合、利便性の確保や、対策に要す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

「情報に基づいた選択によって、リスクを保有すること」の選定により保有されるリスクは、次の 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

組織はリスクを識別している、していないに関わらず、何らかのリスクを保有しています。従って、上記の 2 種類のリスクが存在していることになります。
JIS Q 27001:2014 のリスクを保有するとは、前者の「識別され受容されるリスク」が対象です。リスクが組織の情報セキュリティ方針及びリスクの受容のための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

「リスクを生じさせる活動を、開始又は継続しないと決定することによってリスクを回避すること」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、対象となる業務を廃止したり、対象資産を全て破棄するといった方法をとることです。

例えば、個人情報は漏えい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えいしたり、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）リスクを共有する

「一つ以上の他者とリスクを共有する」とは、契約等によりリスクを他者（他社）と共有することです。リスクを共有する方法は大別すると 2 種類あります。

- 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）
- 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

アウトソーシングの例
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。一般にデータセンター、インターネットサービスプロバイダー、アプリケーションサービスプロバイダー、マネジメントサービスプロバイダーといわれている事業者がこの様なリスクの共有先となります。

※コロケーションサービス：顧客の通信機器や情報発信用のコンピュータ（サーバ）を、自社の回線設備の整った施設に設置するサービス。

組織は、この様なアウトソーシング等にリスクを共有する場合、

- 「共有したリスク及び共有後のリスクレベル」
- 「共有しなかったリスク」
- 「共有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、共有したリスクを明確にするために、情報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。

JIS Q 27001:2014 の附属書 A には次の様な管理策が記載されており、リスクを共有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.15.1 供給者関係における情報セキュリティ 目的：供給者がアクセスできる組織の資産の保護を確実にするため。		
管理策		
A.15.1.1	供給者関係のための情報セキュリティの方針	管理策 組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化しなければならない。

A.15.1.2	供給者との合意におけるセキュリティの取扱い	管理策 関連する全ての情報セキュリティ要求事項を確立しなければならず，また，組織の情報に対して，アクセス，処理，保存若しくは通信を行う，又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と，この要求事項について合意しなければならない。

（JIS Q 27001:2014　A.15.1 供給者関係 より引用）

リスク管理上は、JIS Q 27001:2014 附属書 A の管理策に相当する管理策を適用できない場合や、適用してもリスクレベルが受容水準以上の場合、リスク共有を検討します。

■リスクファイナンスとして保険を採用する例
地震等の不可避な脅威については、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になります。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。

（５）リスクを取る又は増加させる

「ある機会を追求するために、リスクを取る又は増加させる」とは、リスク顕在化時のリターンとして大きな機会（好影響をもたらすもの）が望める場合に、新たなリスクを取ったり、既存のリスクを増加させたりすることです。 ビジネスリスクの検討時によく適用され、例えば、新たな事業をはじめるために必要な投資に対して、その事業により大きな利益が見込める場合などに選定される選択肢です。情報セキュリティにおいて、この選択肢を選定するケースとしては、次のような場合が考えられます。

■ あるリスクに対する対策の適用により、新たな別のリスクの発生が想定される場合
「あるリスク」の低減後のリスクレベルと、新たに発生したリスクのリスクレベルを比較し、新たなリスクをとることを決定する場合には、「（新たな）リスクを取る」選択をすることになります。このようなケースは、リスクに対する対策を検討する際に多く発生します。具体的な例を挙げます。メールの宛先アドレスの入力時に、過去に送受信したアドレスから候補を推測表示することで入力を支援する機能が設定されている場合、この機能が誤送信を誘発するとして、機能を無効にする対策をとる場合があります。この対策により、メールアドレスの選択ミスは減りますが、すべてを手入力するために、メールアドレスをミスタイプするリスクは増加することになります。この例では、誤ったメールアドレスを選択し、想定しなかった相手にメールを送信するリスクと、メールアドレスのミスタイプにより、想定した相手にメールが届かないリスクを比較して、前者のリスクの影響がより大きいと判断し、この機能を無効にする選択をした場合に、新たなリスクを取る選択をしたことになります。

この例に限らず、あるリスクに対する対策をとることで、別のリスクが発生するケースはよくあります。そのような場面では、元々のリスクを受容するのか、新たに発生するリスクを取るのか、あるいはさらに別の対策を検討するのかなど、多面的に検討することが重要となります。

3.3.2 作業 6 リスク対応の選択肢に対する管理策を決定する、及び附属書 A との比較

組織は、選定した情報セキュリティリスク対応の選択肢の実施に必要な管理策を決定します。その際、組織は必要な管理策を設計するか、任意の情報セキュリティに関する情報源の中から特定することもできます。従来通り、JIS Q 27001:2014 の附属書 A（規定）「管理目的及び管理策」より、リスク対応に関する管理策を選択することも可能です。適切な管理策が附属書 A に記載されていない場合は、独自に追加の管理策を決定することができます。

また、この決定については、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。
JIS Q 27001:2006 に従って、管理策を選択されている組織の場合、JIS Q 27001:2014 において、それらがどの管理策に移行したのかを考慮して、変更する必要があります。

具体的にどの様な管理策を決定すべきかについては、リスクアセスメントを実施した複数の担当者等や情報システム管理者、外部コンサルタントなどとコミュニケーションを図りながら、可能な限り具体的に決定していきます。

また、決定した管理策を JIS Q 27001:2014 の附属書 A「管理目的及び管理策」と比較し、必要な管理策が見落とされていないことを検証しなければなりません。この際、「何をどこまでするか」ということを経営陣と担当者間で明確に意識あわせするために、コミュニケーションを図ることは重要です。特に、リスクアセスメントの実施には通常数ヶ月かかりますので、その間、発生した問題点や意識のずれなどを随時調整する必要があります。コミュニケーション不足のまま管理策を決定すると、プロジェクトが形骸化し、意図するセキュリティ目的とは異なる管理策が決定される場合もあるので注意が必要です。

なお、一つの管理策を導入することを想定した場合においても、その管理策を導入することに関連する他の管理策が存在する場合があります。

例えば、JIS Q 27001:2014 の附属書 A「管理目的及び管理策」の「A.10.1.1 暗号による管理策の利用方針」管理策を決定すると、それに関連する「A.10.1.2 鍵管理」も通常、同時に選択する必要があります。また、そもそも、「A.10.1.1 暗号による管理策の利用方針」管理策に記載されている「情報を保護するための・・・」の部分が組織で明確化されていない場合は、「A.8.2.1 情報の分類」、「A.8.2.2

情報のラベル付け」、及び、「A.8.2.3 情報の取扱い」なども追加の管理策として決定する必要があります。この際、「A.10.1.1 暗号による管理策の利用方針」管理策とそれに関連する「A.10.1.2 鍵管理」管理策は「A.10.1 暗号による管理策」内に存在し、それらに付随する管理目的は「情報の機密性、真正性または完全性を保護するため」ですが、「A.8.2.1 分類の指針」、「A.8.2.2 情報のラベル付け」及び「A.8.2.3 情報の取扱い」などの管理策は、「A.8 資産の管理」という項目の「A.8.2 情報分類」内に存在し、付随する管理目的は、「情報の適切なレベルでの保護を確実にするため」となります。このとおりに管理策を十分に検討していくと、当初想定していなかった管理策が必要になる場合があります。

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。例えば、JIS Q 27002:2014 の「6.1.2 職務の分離」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ますが、その実施の手引では、「比較的小規模の組織にとって、職務の分離を実現するのは難しい場合がある。」としています。しかし、このような場合でも、組織は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決定し、確実に実装していく必要があります。

決定した管理策については、リスクアセスメントの結果、すなわち資産が保有する脅威やぜい弱性に対してどう効果的なのか、どの程度のリスクレベルが軽減され、残留リスクはどの程度なのかを評価する必要があります。特に、管理策を決定後も残留リスクが高い場合は、追加の管理策を検討し、リスクを受容可能な範囲に落とし込む、または、その旨を明らかにしておく必要があります。

3.3.3 作業 7 適用宣言書を作成する

作業 6 で決定した管理策、並びにこれらを含めた理由、及びこれらの管理策を実施しているか否かを文書化し、適用宣言書を作成します。
また、附属書 A「管理目的及び管理策」に記載された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。

3.3.4 作業 8 情報セキュリティリスク対応計画を作成する

作業 7 で作成した適用宣言書に基づき、受容できないリスクを低減するためにとるべき活動と、選択した管理策の実装に関する実行計画を、情報セキュリティ対応計画として作成することで、情報セキュリティ目的の達成を目指すものです。
この情報セキュリティ対応計画で、リスクマネジメントに必要な経営資源の割当てや実施する作業を定めます。

３.３.５ 作業９ 残留リスクを承認する

リスク所有者は、作業７及び作業８で作成した適用宣言書及び情報セキュリティリスク対応計画の内容に基づき、決定された管理策の有効性、妥当性を確認すると同時に、算出された残留リスクについて、残留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こと、あるいはリスクを保有（受容リスク水準を超える場合を含む）することを確認し、そのために必要な経営資源や実施する作業が適切かどうかを判断し承認する必要があります。

残留リスクが承認されることで、適用宣言書及び情報セキュリティリスク対応計画が確定することになります。

４．パフォーマンス評価

組織は、パフォーマンス評価の一環として、「監視、測定、分析及び評価」、「内部監査」、「マネジメントレビュー」を実施しなければなりません。なお、パフォーマンス評価の詳細については、ISMS ユーザーズガイドをご参照ください。

（１）監視、測定、分析及び評価

監視、測定、分析及び評価では、情報セキュリティパフォーマンス（情報セキュリティの測定可能な結果）及び ISMS の有効性（計画した活動を実行し、計画した結果を達成した程度）を評価します。

監視と測定の対象は、情報セキュリティプロセスと管理策の２つの側面を含めて決定します。その際、監視、測定、分析及び評価の方法、実施時期と実施者も決定する必要があります。

なお、管理策のパフォーマンスを測定する際は、管理策の実施度と、目的の達成度という視点を考慮することが有用と考えられます。

（２）内部監査

内部監査では、ISMS の取組みが、組織の規定した要求事項に従って実施されているか、JIS Q 27001:2014 の要求事項に適合しているか、有効に実施され継続的に維持されているかを評価します。結果は、（３）マネジメントレビューの重要なインプットとなります。

（３）マネジメントレビュー

マネジメントレビューは、トップマネジメントが俯瞰的視点から、ISMS 全体の取組みを定期的に確認し、構築・維持した ISMS を改善する必要があるのか、変更する必要があるのかを判断するプロセスです。

マネジメントレビューは、組織が定めた間隔で実施する必要があります。また、マネジメントレビュー実施時には、前回までのマネジメントレビューの結果を受けて実施した処置の状況、ISMS に関連する外部及び内部の課題の変化、情報セキュリティパフォーマンスに関するフィードバック、利害関係者からのフィードバック、リスクアセスメントの結果及びリスク対応計画の状況、継続的改善の機会を考慮することが必要です。

まとめ

本ガイドでご紹介した「リスクアセスメント」手法は、現段階では最も利用し易く、且つ JIS Q 27001:2014 版に対応した評価手法であると思われます。
企業または組織が求めるセキュリティレベルによっては、もっと簡易な評価手法でよい場合や、逆にもっと厳密かつ詳細に評価する必要もあります。必ずしもこうしなければいけないということではありませんが、いずれにせよ、標準的な手法から派生される手法をカスタマイズして、その企業または組織に合う手法を探し当てることが良いと考えます。
また、将来、有効的な ROSI（Return of Security Investments：セキュリティ投資効果）の手法が開発されれば、新たなリスクアセスメント手法により、定量的なリスク評価が可能となり、セキュリティ投資がより容易になることもあるでしょう。
リスクアセスメントの実施で最終的に期待されることは、個々の資産が持つ「リスク」、「リスクに対する適切な管理策」及び「管理策に投じるべき費用」を識別することです。
リスクレベルは、基本的（理想的）には、「予想損失額」と「発生頻度」から算出され、下記の様な数式から年間損失額を導くことになります。

『リスク（金額／年）』＝『予想損失額（金額）』×『発生頻度（回数／年）』

リスクが大きいということは、資産にダメージ（悪影響）を与える可能性が高く、その影響力も大きいということであり、リスクが小さいということはその逆です。同額のセキュリティ対策費用を投ずるなら、リスクが大きいものから行うのが妥当と考えられます。また、小さなリスクに対して、多大な資産を投じてセキュリティ対策を施すのは効果的ではない、いわゆるコストパフォーマンスが悪いといえます。
しかし、上記の様な考え方でリスクは定義されるものの、「予想損失額」や「発生頻度」をどう見積もるかが問題となります。これらは何らかの統計に基づき算出されることが望ましいといえますが、信頼性の高いデータを入手することは、実務的には困難です。
　またリスクは時間の変化や環境要因などで動的に変化するものなので、適宜リスクアセスメントを行い対策（管理策）の実装状態などをレビューするための手法も必要になります。
従って、本ガイドにおいては、対象となる資産の価値や重要度を階層化（レベル分け）し、また、それらに対してどの様な脅威があり、その脅威を誘引してしまう弱点、または脅威に対する管理策の不備の度合いなどを示すぜい弱性を評価することで、リスクを定性的、または相対的に評価する方法を推奨しています。
本ガイドで紹介した手法やリスクマネジメントの解説が ISMS 構築の一助になれば幸いです。

IMS 運営委員会

（順不同・敬称略）

氏名	会社・機関名
土居　範久	慶應義塾大学【委員長】
大木　榮二郎	工学院大学【副委員長】
島田　洋之	大同火災海上保険株式会社【副委員長】
新　誠一	電気通信大学
伊藤　毅志	独立行政法人　情報処理推進機構
稲垣　隆一	稲垣隆一法律事務所
榎木　千昭	慶應義塾大学大学院
大畑　毅	日本電気株式会社
熊谷　堅	KPMG コンサルティング株式会社
小林　偉昭	技術研究組合　制御システムセキュリティセンター（CSSC）
駒瀬　彰彦	株式会社アズジェント（ISMS 技術専門部会　主査）
小山　條二	特定非営利活動法人 itSMF Japan
金野　千里	独立行政法人　情報処理推進機構(IPA)
佐々木　良一	東京電機大学
塩田　貞夫	洛 IT サービス・マネジメント株式会社（ITSMS 技術専門部会　主査）
杉浦　昌	日本電気株式会社
武中　和昭	日本マネジメントシステム認証機関協議会 (一般社団法人日本能率協会)
田原　幸朗	一般社団法人情報サービス産業協会
出口　幹雄	富士通株式会社
中尾　康二	ＫＤＤＩ株式会社
中野　利彦	株式会社日立製作所
藤本　正代	富士ゼロックス株式会社
八木　隆	株式会社日立製作所

（2014 年 12 月 17 日現在）

ISMS 技術専門部会

（順不同・敬称略）

氏名	会社・機関名
駒瀬　彰彦	株式会社アズジェント【主査】
丸山　満彦	デロイト　トーマツ　リスクサービス株式会社【副主査】
相羽　律子	株式会社日立製作所　情報・通信システム社
小寺くれは	KPMG コンサルティング株式会社
佐藤　慶浩	日本ヒューレット・パッカード株式会社
竹下　和孝	株式会社筑波総合研究所
中村　春雄	日本マネジメントシステム認証機関協議会 （一般財団法人　日本品質保証機構）
平野　芳行	一般社団法人　情報処理学会
松尾　正浩	株式会社三菱総合研究所
事務局	
高取　敏夫	一般財団法人　日本情報経済社会推進協会
中島　博文	一般財団法人　日本情報経済社会推進協会
畔津　布岐	一般財団法人　日本情報経済社会推進協会
星　昌宏	一般財団法人　日本情報経済社会推進協会
野中　武志	一般財団法人　日本情報経済社会推進協会
富永　典子	一般財団法人　日本情報経済社会推進協会

（2014 年 12 月 17 日現在）

一般財団法人日本情報経済社会推進協会

〒106-0032 東京都港区六本木１丁目９番９号 六本木ファーストビル内

TEL 03-5860-7570　FAX 03-5573-0564

URL http://www.jipdec.or.jp/