地方公共団体における
情報資産のリスク分析・評価
に関する手引き

平成２１年３月

総務省

目　次

総　則

第1章 総則

1.1 手引き作成の背景及び目的

現在、各地方公共団体において、住民サービスの向上及び行政の簡素・効率化等を図る目的で、電子自治体の構築が進められている。一方、電子自治体の構築に伴う業務の情報システム・ネットワークへの依存度の高まりにより、ウェブサーバ等への攻撃による情報システムの緊急停止による自治体業務の中断、個人情報等の漏えい・紛失等による住民の権利・利益の侵害の危険性が高まっている。

このような状況の下で、各地方公共団体では、個人情報をはじめとする情報資産を適切に保護するため、制度的側面、技術的側面及び人的側面における情報セキュリティ対策を推進しているところである。例えば、情報セキュリティ責任者・管理者の任命、担当者の設置、情報セキュリティポリシーの策定については、ほぼ全ての地方公共団体で実施されているところである。しかしながら、実施手順書の策定、情報資産の調査及びリスク分析の実施、情報セキュリティ監査の実施、情報セキュリティポリシーや情報セキュリティ対策の見直しについては、低い実施状況にある。特に、情報資産の調査及びリスク分析の実施は、都道府県では５５．３％、市区町村では２０．２％という低い状況にある[1]。

図表１－１　主な情報セキュリティ対策の実施状況（平成20年4月1日現在）

対策項目	対策の状況
情報セキュリティの責任者・管理者の任命、担当者の設置	都道府県:(100%) 市区町村1,615団体（89.2%）
情報セキュリティポリシーの策定	都道府県:(100%) 市区町村:1,759団体（97.1%）
セキュリティ対策実施手順の策定	都道府県:42団体（89.4%） 市区町村:731団体（40.4%）
情報セキュリティ研修の実施	都道府県:46団体（97.9%） 市区町村:1,217団体（67.2%）
情報資産の調査及びリスク分析の実施	都道府県:26団体（55.3%） 市区町村:366団体（20.2%）

[1] 地方自治情報管理概要「第２章 電子自治体の現況　第 4 節　情報セキュリティ対策の実施状況」（総務省自治行政局地域情報政策室(平成 20 年 10 月 31 日)）を基に作成。

内部監査又は外部監査の実施	都道府県: 40団体（85.1%） 市区町村: 553団体（30.5%）
情報セキュリティポリシーや情報セキュリティ対策の見直し	都道府県:45団体（95.7%） 市区町村:699団体（38.6%）

本手引きは、情報資産のリスク分析・評価の実施の促進のため、各地方公共団体が情報セキュリティに係るリスク管理の基本であるリスク分析・評価を実施する際の参考となるよう、リスク分析・評価に係る具体的な方法論を解説するものである。

また、本手引きは、すべての地方公共団体が実施すべきリスク分析・評価の手法として取りまとめたものである。

1.2 手引き集の構成、特徴及び利用方法

本手引きは、リスク分析・評価の方法論を記述した本書以外に、リスク分析・評価の作業で使用するシート等の付属資料(以下、「分析・評価シート[2]」という。)及び分析・評価シートの使用方法を解説した「(別冊) 分析・評価シート操作マニュアル(以下、「操作マニュアル」という。)」から構成されている。本書では、これら全体を総称して「手引き集」と呼ぶこととする。

[2] 付属資料は、【Microsoft® Excel 2003】で作成し、提供する。

1.2.1 本書の構成

本書は、リスク分析・評価の意義、対象となる組織範囲等について解説した第１章、情報資産に関わらない情報セキュリティ対策の現状に対するリスク分析・評価を解説した第２章、情報資産に関わる情報セキュリティ対策の現状に対するリスク分析・評価を解説した第３章の３つの章から構成される。各章の概要は以下のとおりである。

図表１－２　本書の構成

章	目次	概要
第１章	総則	・リスク分析・評価の意義及び対象となる組織範囲、実施組織体制等リスク分析・評価作業の前提として理解すべき事項を解説する。
第２章	基本リスク分析・評価	・情報資産に関わらない、庁内における情報セキュリティ対策の現状に対するリスク分析・評価の方法を解説する。 ・基本リスク分析・評価に関する改善計画の策定及び実施の方法を解説する。
第３章	(広義の)詳細リスク分析・評価[3]	・情報資産の洗い出し、情報資産台帳の作成に関する方法を解説する。 ・情報資産に関するリスク分析・評価の方法を解説する。 ・詳細リスク分析・評価に関する改善計画の策定及び実施の方法を解説する。

本書では、基本リスク分析・評価及び(広義の) 詳細リスク分析・評価の２つの分析・評価方法を解説する。それぞれの概要は以下のとおりである。

図表１－３　リスク分析・評価の方法

方法	概要
基本リスク分析・評価	規程・規則等の策定、組織体制の確立等の情報セキュリティ対策の現状に係るリスク分析・評価をいう。
詳細リスク分析・評価	情報資産を特定[4]し、当該資産の利用や保管等に関する情報セキュリティ対策の現状に係るリスク分析・評価をいう。

[3] 本書では、リスク分析・評価という用語を狭義と広義で使い分けている。情報資産の洗い出し、情報資産台帳作成等を含んだ概念の広義のリスク分析・評価は、「(広義の)リスク分析・評価」としてこれ以降表記する。情報資産の洗い出し、情報資産台帳作成の実施後に行う(狭義の) リスク分析・評価は、「詳細リスク分析・評価」としてこれ以降表記する。

[4] 情報資産を特定する作業が、情報資産台帳の作成及び更新に当たる。

上記２つの方法を双方とも実施するのか、どちらか１つを選択するのか、その判断については、「1.3 リスク分析・評価の実施のフロー及び２つの分析・評価方法の選択」(9 頁) で説明する。

1.2.2　手引き集の利用方法

本手引き集は、基本的に以下のように利用する。

（１）　本書の総則部分を読み、リスク分析・評価の意義、考え方を理解した上で、リスク分析・評価の作業の流れを習得する。

（２）　本書の第２章及び第３章で実施すべき作業内容を把握し、分析・評価シートを活用して作業を進める。分析・評価シートの利用に当たっては、操作マニュアルを参照する。なお、本書では、作業が発生する箇所を「ステップ」として表示し、作業箇所であることが理解できるようにしている。

※本書では、リスク分析・評価の流れの理解を助けるため、必要な個所に以下のマークを表示している。各マークの意味するところは以下のとおりである。

図表１－４　マーク表示とその内容

マーク表示	内容
ステップ	・作業の概要 リスク分析・評価に関して、本書の利用者が実際に作業する内容の手順を明確にして解説している。 本文では以下のように記述している。 手順１○○は、□□する。 手順２○○は、△△する。 ・分析・評価シート 使用する分析・評価シートを表示している。 ・操作マニュアル目次 操作マニュアルの参照目次を表示している。
ここがポイント	・リスク分析・評価を実施するに当たって、ポイントとなる事項を解説している。
参考	・リスク分析・評価の実施に当たって、利用者の参考となる点を解説している。作業の実施上特に読み飛ばしても構わない。
実施主体	・実際の作業主体の例を表示している。

以下のように、本文中で、作業の手順と、それを実施する組織等を明示している。

手順１	実施主体：事務局

1.2.3 分析・評価シートの構成

分析・評価シートは、以下の様式から構成されている。

図表１－５　分析・評価シートの構成

様式	シート名	用途
1	リスク分析・評価項目表	基本リスク分析・評価シート及び詳細リスク分析・評価シートに反映する項目や値があらかじめ入力されたものであり、各団体の事情に応じて項目や値を変更する際に使用する。
2	基本リスク分析・評価シート	基本リスク分析・評価を行う際に使用する。
3	基本リスク分析・評価に関する改善計画表	基本リスク分析・評価を行った後に、改善計画を策定する際に使用する。
4	対象範囲表	詳細リスク分析・評価を行う際に、情報資産を洗い出す業務、組織範囲（課室等）の決定に使用する。
5	情報資産洗い出し対象設定表	情報資産を管理する者が、実際に洗い出しを行う実施範囲を明確にするために使用する。
6	情報資産台帳	詳細リスク分析・評価を行う際の情報資産台帳の作成に使用する。
7	脅威評価レベル表	詳細リスク分析・評価シートで脅威の特定の設定等に反映する項目や値が、あらかじめ入力されたものであり、各団体の事情に応じて項目や値を変更する際に使用する。
8	詳細リスク分析・評価シート	詳細リスク分析・評価を行う際に使用する。
9	詳細リスク分析・評価に関する改善計画表	詳細リスク分析・評価を行った後に、改善を行う際に使用する。

1.2.4　手引きと分析・評価シートとの関連

本書と分析・評価シートの関連は、以下のとおりである。

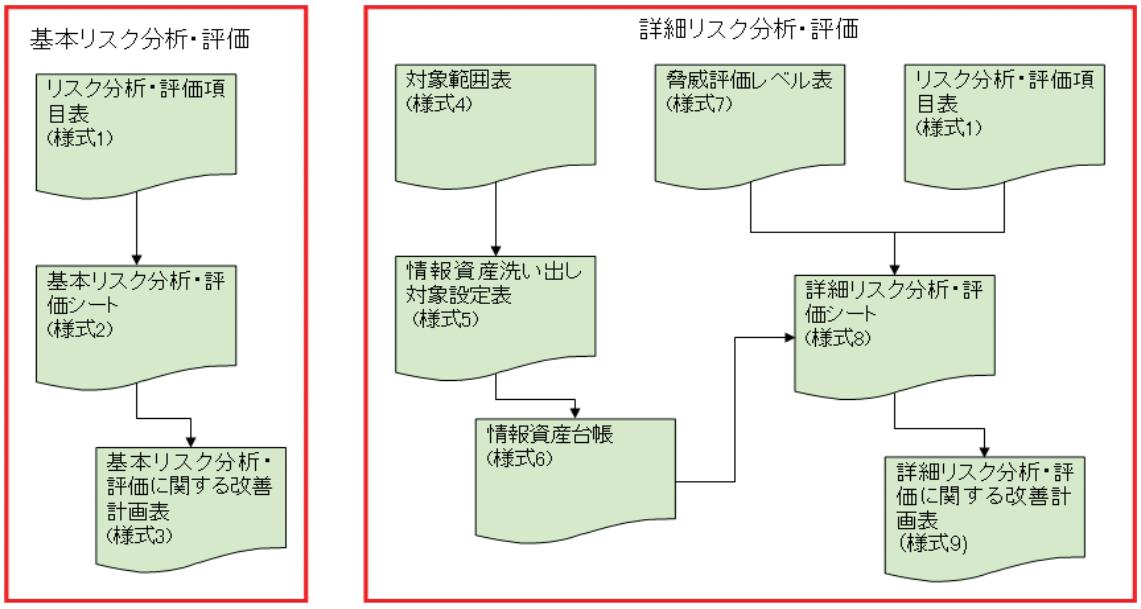
図表１－６　手引きと分析・評価シートの関連

章	目次	関連する分析・評価シート
第１章	総則	なし
第２章	基本リスク分析・評価	リスク分析・評価項目表（様式１） 基本リスク分析・評価シート(様式２） 基本リスク分析・評価に関する改善計画表（様式３）
第３章	（広義の）詳細リスク分析・評価	リスク分析・評価項目表（様式１） 対象範囲表（様式４） 情報資産洗い出し対象設定表（様式５） 情報資産台帳（様式６） 脅威評価レベル表（様式７） 詳細リスク分析・評価シート(様式８） 詳細リスク分析・評価に関する改善計画表（様式９）

1.2.5　分析・評価シート相互の関連図

分析・評価シート相互の関連は、以下の図のとおりである。

図表１－７　分析・評価シート相互の関連図



1.2.6　リスク分析・評価ファイルの構成

本手引き集においては、分析・評価シートの様式を格納している「リスク分析・評価ファイル」を３種類用意している。

「リスク分析・評価ファイル」を３種類用意した趣旨は、基本リスク分析・評価では、規程・規則等の策定、組織体制の確立等は、情報資産の管理・保管状況に直接関連付くものではないため分離し、詳細リスク分析・評価では、情報資産の管理・保管状況について、情報システム主管課室とそれ以外の課室では大きく異なる(特にサーバ、ネットワーク管理に関して)ことにある。これによって、情報システム主管部門以外の課室が行うリスク分析・評価の作業工数の削減を図っている。

図表１－８　分析・評価ファイルの利用者及び格納シート

リスク分析・評価ファイルの種類	利用者	関連する目次及び分析・評価シート
基本リスク分析・評価用	事務局が利用する。 ※事務局の編成例は、後述する。	第２章　基本リスク分析・評価 ・リスク分析・評価項目表（様式１） ・基本リスク分析・評価シート(様式２) ・基本リスク分析・評価に関する改善計画表（様式３）
詳細リスク分析・評価（情報システム管理者[5]用）	情報システムを主管している課室が利用する。	第３章　詳細リスク分析・評価 ・リスク分析・評価項目表（様式１） ・対象範囲表（様式４） ・情報資産洗い出し対象設定表（様式５） ・情報資産台帳（様式６） ・脅威評価レベル表（様式７） ・詳細リスク分析・評価シート(様式８) ・詳細リスク分析・評価に関する改善計画表（様式９） ※対象範囲表（様式４）及び情報資産洗い出し対象設定表（様式５）は情報システム管理者用のファイルのみに格納している。
詳細リスク分析・評価（情報セキュリティ管理者用）	情報システムを主管以外の課室が利用する。	

[5] 情報セキュリティ管理者及び情報システム管理者の権限及び責任については、(総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン(平成 18 年 9 月版)」(以下、「ポリシーガイドライン」という。) の「3.2. 組織体制」(27 頁～29 頁) 参照。

1.2.7　特徴

本手引き集の特徴は、以下のとおりである。

（1）　基本リスク分析・評価、詳細リスク分析・評価の２つのリスク分析・評価の方法を紹介し、各地方公共団体の事情、状況に応じて、選択して実施できるものとしている。

（2）　リスク分析・評価では、情報資産のリスクが高い状態に対して、リスクの低減を図るため、各地方公共団体の情報セキュリティ対策の現状を把握する必要がある。その際の参考となるよう、対策の例、脆弱性評価レベルの例を提供し、リスク分析・評価の実施を支援するものとしている。

（3）　リスク分析・評価作業を効率的に実施できるよう、作業で使用する様式（分析・評価シート）を添付している。分析・評価シートは、作業しやすいようにＥｘｃｅｌ(以下、表計算ソフトウエアと呼ぶ。)を利用し、随所に工夫を採り入れ、分析・評価シートに大幅な変更を加えなくても利用できるようにしている。

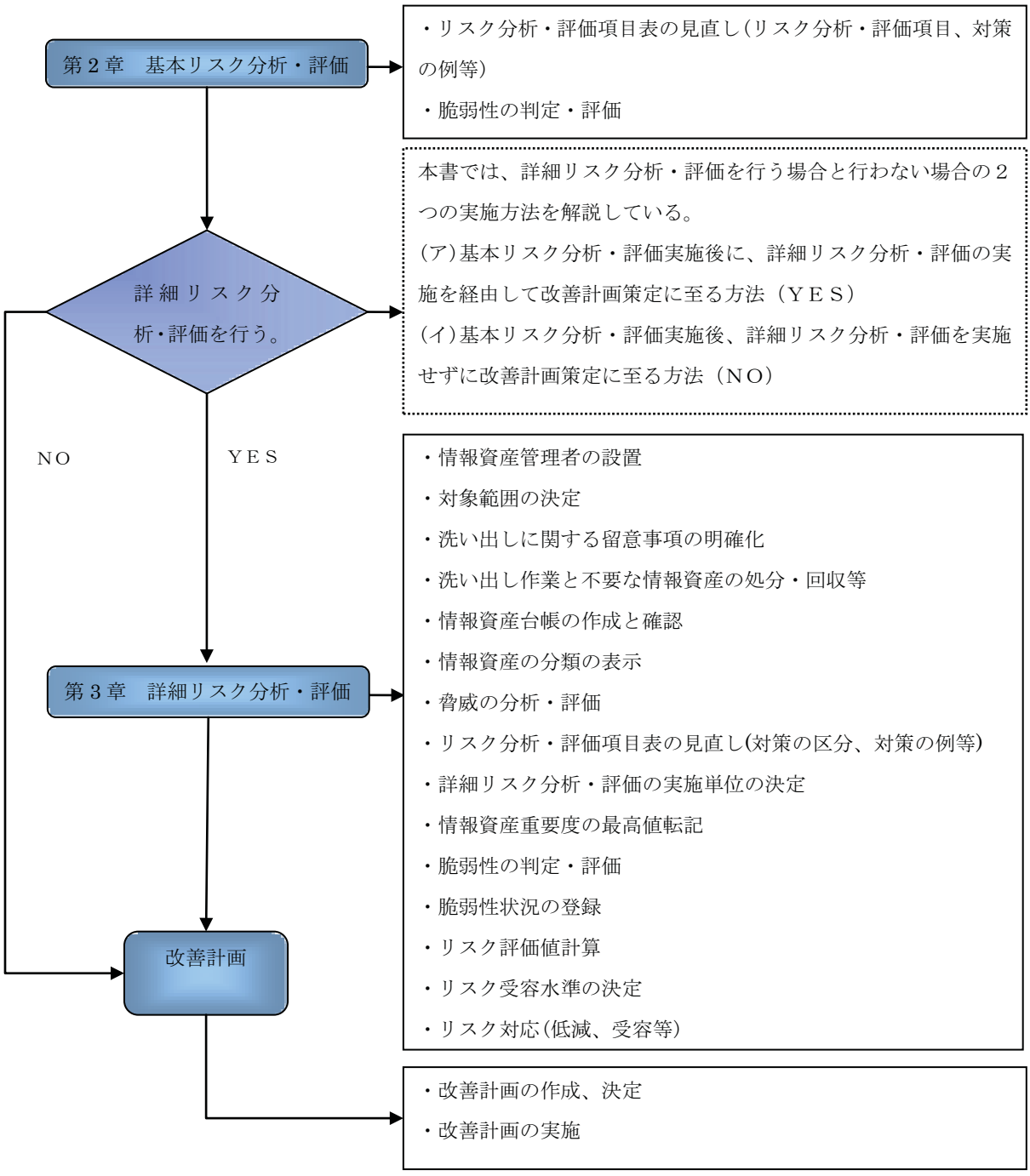
（4）　総務省が公表している情報セキュリティに関する各種ガイドライン(以下、「関連ガイドライン」という。)との整合性を確保しながら、実際の作業負担軽減を図っている。

1.3　リスク分析・評価の実施のフロー及び２つの分析・評価方法の選択

1.3.1　本書におけるリスク分析・評価の実施フロー

リスク分析・評価の実施フロー(以下、「実施フロー」という。)は、以下のとおりである。

図表１－９　リスク分析・評価実施フロー図



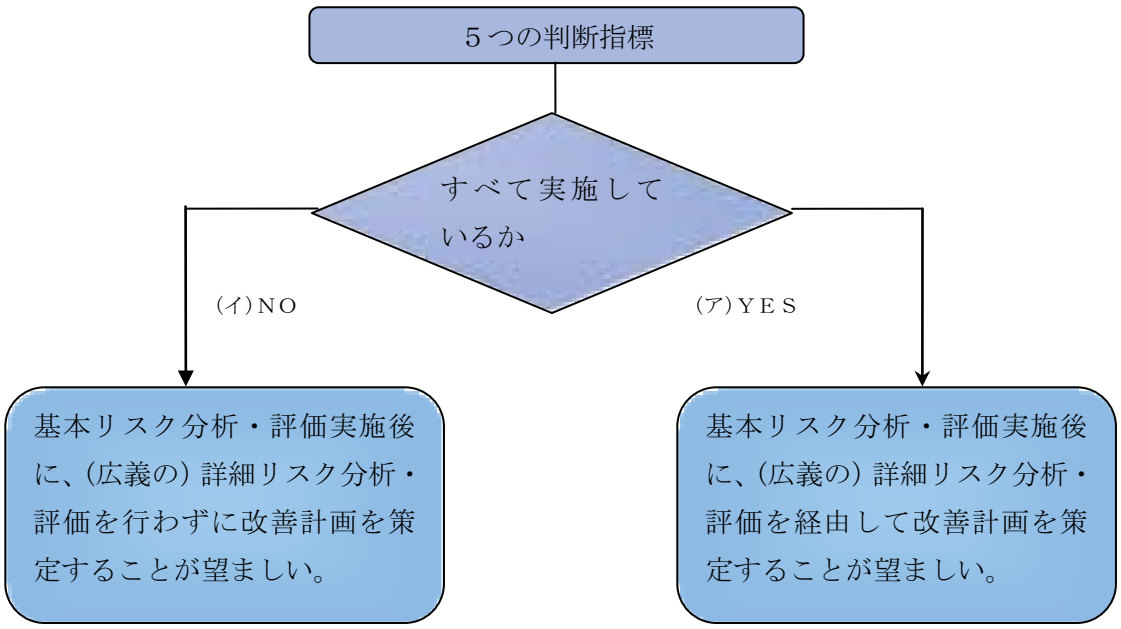
1.3.2　基本リスク分析・評価及び(広義の）詳細リスク分析・評価の選択

前頁の実施フローにあるように、基本リスク分析・評価実施後に、(広義の）詳細リスク分析・評価の実施を経由して改善計画策定に至る方法を採るのか、基本リスク分析・評価実施後に、(広義の）詳細リスク分析・評価を実施せずに改善計画策定に至る方法を採るのかどうかは、「図表１－１０　リスク分析・評価実施の判断について」に示す基本的な情報セキュリティ対策の状況によって判断することができる。

図表１－１０　リスク分析・評価実施の判断について

５つの判断指標
情報セキュリティポリシーを策定している。
情報セキュリティ研修を定期的に職員に実施している。
情報セキュリティ委員会等を定期的に開催し、次年度活動計画の策定又は方針を決定している。
(広義の）詳細リスク分析・評価を行う目的を明確にしている。
(広義の）詳細リスク分析・評価を行う資源（人、予算等）を確保している。

図表１－１１　リスク分析・評価実施の判断に関するフロー図



ここがポイント 実施の判断

「５つの判断指標」は、リスク分析・評価の実施フローを選択するための判断の視点を示したものであるが、これはあくまでも目安であることに注意が必要である。基本リスク分析・評価とその改善計画の実施にとどめるのか、あるいは基本リスク分析・評価から情報資産の洗い出し、情報資産台帳の作成、詳細リスク分析・評価とその改善計画まで一貫して実施するのかは、各地方公共団体の事情に応じて判断する。

基本リスク分析・評価とその改善計画を実施する方法を選択した場合においても、将来的には、「５つの判断指標」を確実に実施し、漸次、基本リスク分析・評価から詳細リスク分析・評価まで行える体制を確立することが望ましい。

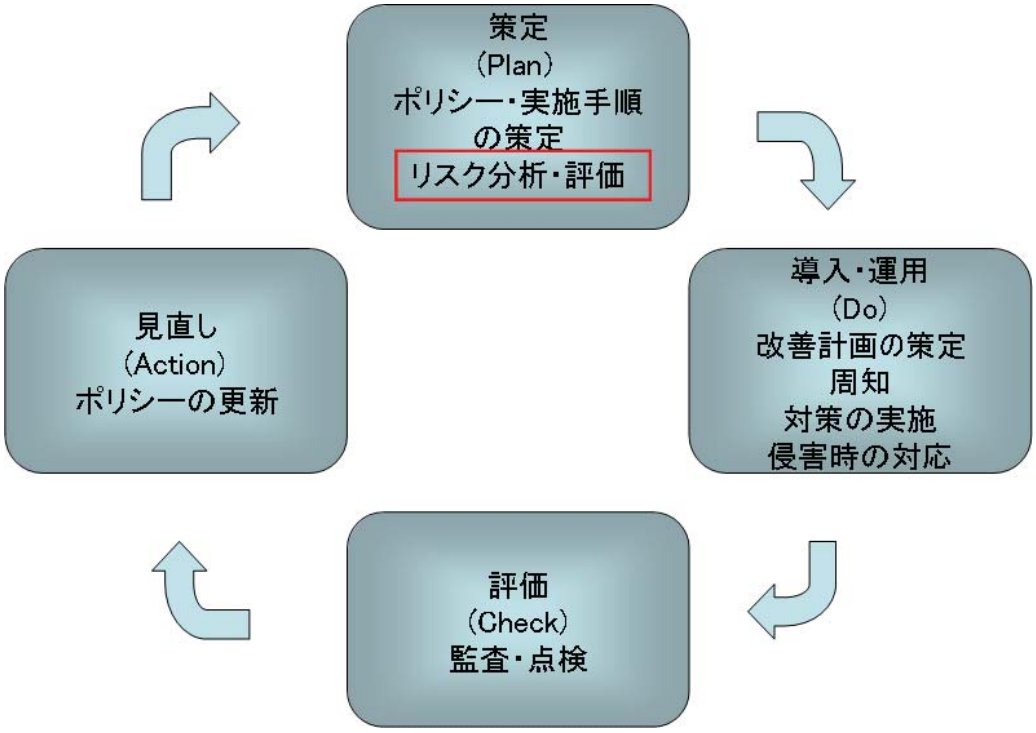
1.4　情報セキュリティ対策のＰＤＣＡサイクルとリスク分析・評価の関係

1.4.1　リスク分析・評価の位置

リスク分析・評価は、定期的に、又は組織及び業務の変更、情報セキュリティの動向、ネットワーク及び情報システムの構成変更等の面を検討の上、必要に応じて行うことが望まれる。本来業務への影響を考慮しても、情報セキュリティ対策のＰＤＣＡサイクル及び情報資産の増減等を踏まえると、年１回以上は行う必要がある。

リスク分析・評価の結果、情報資産に対するリスクが高いと判断した場合は、リスクを低減するなどの改善計画を策定し実施することが必要となる。このようなリスク分析・評価及び改善計画の策定プロセスの情報セキュリティ対策のＰＤＣＡサイクルにおける位置付けは、以下のとおりである。

図表１－１２　情報セキュリティ対策のＰＤＣＡサイクル



1.4.2 リスク分析・評価の意義

情報セキュリティ対策の目的は、業務で利用する情報資産を様々な脅威から保護することにある。情報資産の保護とは、情報資産の機密性、完全性及び可用性[6]を確保することである。情報資産の機密性、完全性及び可用性を確保するためには、まず、情報資産を洗い出し、情報資産が被害を受けた場合の重要度を評価し、何が保護すべき情報資産かを特定する。次に、特定した情報資産に対するリスクの状況を的確に把握し(脅威と脆弱性を識別する)、現在実施している対策について、改善の必要性の有無を検討する。これが、情報セキュリティ対策における重要なプロセスの一つである情報資産のリスク分析・評価である。

リスク分析・評価を実施することで、全庁における情報セキュリティ対策(組織体制の確立、規程等の策定、研修の実施等)の現状調査及び情報資産の特定を行い、当該資産の利用や保管等につけ入る脅威に対する情報セキュリティ対策(セキュリティ技術の導入、情報資産の無許可持ち出し制限等)の現状調査を通してリスクの状況を認識することで、現状の対策で何が不足しているのか、どこまで行えばよいのかが把握できることになる。

もし、情報資産の特定及び対策状況の把握が組織的になされていない場合は、リスクの状況を認識不足が原因となり、情報流出事件が発生する可能性がある。

例えば、業務で利用している住民情報が記録されているＵＳＢメモリが無造作に庁内で保管されている場合は、媒体管理がなされていないことによる紛失時の検出の遅延や職員等による許可を得ない持ち出しも横行する。さらに自宅のパソコンで住民情報を扱う作業を行った場合は、自宅のパソコンのファイル交換ソフトウエアがコンピュータウイルスに感染することにより、インターネットを通じて、これらの住民情報が漏えいする可能性が高くなる。このような事案は、各種報道からも知るところであるが、庁内に所在する情報資産の特定ができていないこと(住民情報が記録されているＵＳＢメモリを守るべき情報資産として特定していないなど)、情報資産に対する脅威や情報資産が抱える脆弱性を分析せずにその取扱いがなされていること(紛失や無断持ち出しの脅威、ＵＳＢメモリを自由に使用できる管理体制の不備の脆弱性など)に問題の所在がある。

現に、平成２０年度上半期の地方公共団体及び国などの公的機関におけるセキュリティ事故事案の件数[7]は、１８２件(うち、地方公共団体では１４７件[8])と前年同

---

6 機密性とは、情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。完全性とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。可用性とは、情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。「ポリシーガイドライン」20 頁参照。

7 「平成２０年度上半期　情報セキュリティ関連事故の分析」((財) 地方自治情報センター調査結果より)

8 地方公共団体の母数が、1800 団体以上と大きいことが数に影響を与えているものと考えられる。

期８１件に比べ倍増している。特に、情報漏えいの件数が１６７件で９割以上に上る。内訳を見ると、書類の紛失（３３件)、ＵＳＢメモリの紛失（２７件)、電子メールやＦＡＸの誤送信（２５件)、盗難（２５件）などの人的な事案が上位を占めている。このことからも、地方公共団体の各職員が、情報資産のリスクの状況を認識し、情報資産の適切な取扱いをすることが重要である。

リスク分析・評価の実施により、地方公共団体にとって限りある資源である「人・物・予算」をどの程度情報セキュリティ対策に割り当てることが適正かどうかを判断する根拠・資料を得ることも可能となる。反対に、リスク分析・評価を実施していない場合には、前述のような事案に対する抑止の改善が一向に進まない事態も想定される。また、情報資産の特定と的確な対策が行われないことで、どこまでセキュリティ対策を実施すべきか、また、どこに重点的に行うべきかが把握できないために、総花的な対策、過剰な対応等に陥りやすくなる可能性もある。

参考 ＩＳＭＳについて

一部の企業や地方公共団体等において、情報を適切に管理し機密等を守るための包括的なセキュリティ対策の取組みとしてＩＳＭＳを導入している例が見られる。ＩＳＭＳとは、情報セキュリティマネジメントシステム(Information Security Management System)の略であり、組織の情報セキュリティのマネジメントシステムの構築・運用に関する取組みが認証基準に適合しているかを第三者が審査する制度である。審査に合格すると、一定の情報セキュリティ水準を確保した組織とみなされる。ＩＳＭＳを導入する際には、リスク分析・評価の実施が不可欠のプロセスとなっている。認証基準としては、現在「ISO/IEC27001:2005 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）」が定められている。

1.5 リスク分析・評価の効果

リスク分析・評価の実施により、情報セキュリティ上リスクが高いものが明らかとなり、優先的に改善を図るべき事項や予算の投入の程度を明確にするための資料を得ることが可能となる。また、以下のような副次的な効果が得られる。

（１） 自己点検の代用

各業務課室における情報セキュリティの自己点検の実施をリスク分析・評価によって代用することができる。

（２） 重点的・効率的な監査の実施

リスク分析・評価結果を参考に、リスクが高い情報資産や複数の共通課題が検出できた情報資産に対して、重点的な監査を行うことができる。例えば、監査計画を策定する場合には、監査テーマ及び監査項目の設定に、また、監査の

実施では、監査証拠の収集等に活用することができる。

1.6 本書を展開するに当たってモデルとして設定する地方公共団体の属性及び実施組織体制

1.6.1 モデル団体

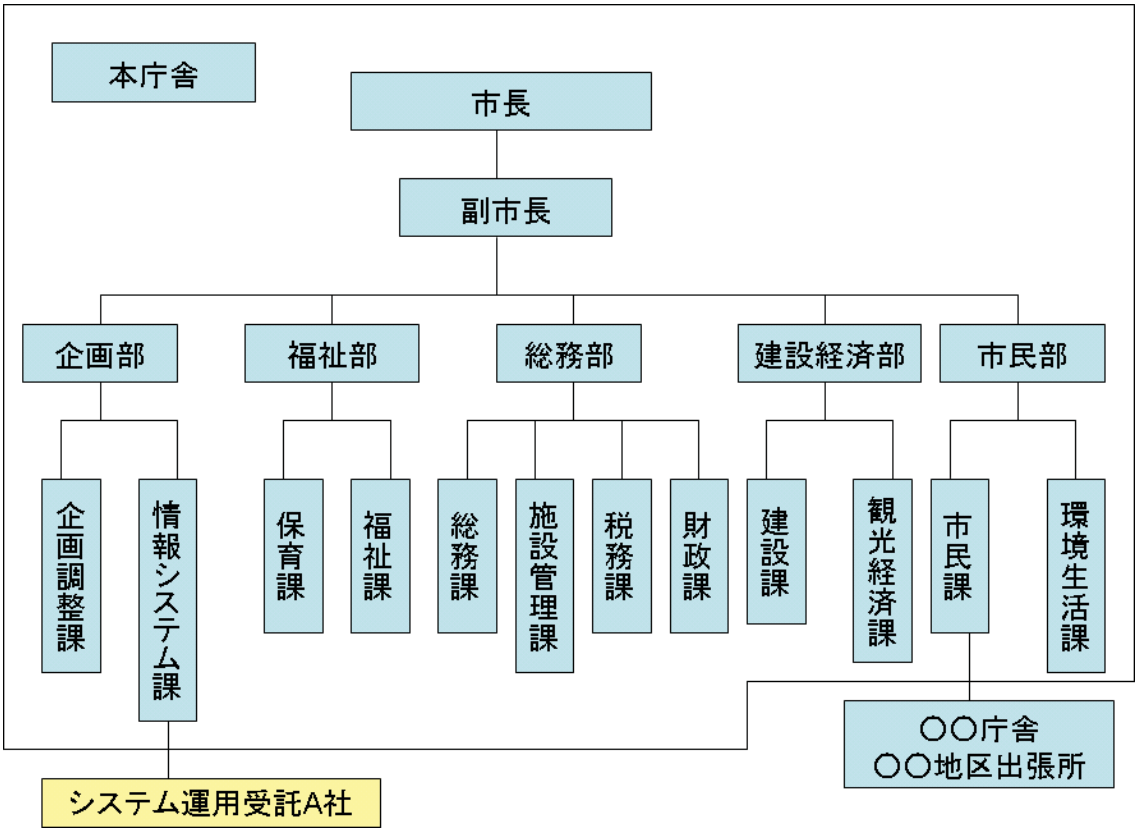
本書を展開するに当たってモデルとして設定する地方公共団体の属性は、以下のとおりである。ただし本モデルは、リスク分析・評価の実施について、小規模な地方公共団体を対象から除くことを意図しているものではなく、本書の説明上あくまでも便宜的に設定したものである。

図表１－１３　モデルとした地方公共団体の属性

地方公共団体の規模	人口５～１０万人を有する地方公共団体の組織を想定。
庁内情報システムの管理状況	庁内ＬＡＮ及びメールシステムその他の情報系システムの主管は情報システム課とし、各業務の情報システム及びスタンドアロンの主管は各業務担当課室を想定。
注：本書における庁内ＬＡＮ、スタンドアロン及び情報系システムの定義 ・庁内ＬＡＮ インターネット等の外部ネットワーク及び庁内のネットワークに接続しているハードウエア及びソフトウエアの構成の総称をいい、ＶＬＡＮ[9]等で論理的に通信を分離している場合も含める。 ・スタンドアロン 庁内ＬＡＮに物理的に接続していないコンピュータをいう。 ・情報系システム メール、Ｗｅｂ、イントラネット、グループウエア等の情報収集、情報共有・交換に利用しているシステムの総称をいう。	

9 Virtual LAN の略。

図表１－１４　モデルとした地方公共団体の組織図



1.6.2　実施組織体制

リスク分析・評価の実施には、庁内横断的な取組みとなることから、幹部職員の関与が必要となる。また、リスク分析・評価は、組織内の様々な部署の情報セキュリティ及び情報資産に係る問題を取り扱うことから、責任の所在を明確にするため、全部長、情報システムを主管する課室長及び情報セキュリティに関する専門的知識を有する者などで構成される情報セキュリティ委員会又はこれに代わる組織(以下、「情報セキュリティ委員会等」という。)が関与することが望ましい。

また、リスク分析・評価の実施の過程において、情報セキュリティ委員会等を開催し、審議及び承認が必要な場面がある。具体的には、以下のとおりである。

（１）基本リスク分析・評価実施後に、詳細リスク分析・評価の実施を経由して改善計画策定に至る方法を採った地方公共団体は、すべて該当する。

（２）基本リスク分析・評価実施後、詳細リスク分析・評価を実施せず改善計画策定に至る方法を採った地方公共団体は、「項目番号１」のみ該当する。

図表１－１５　情報セキュリティ委員会等の開催場面

項 目番号	開催場面	本書の記載頁
1	基本リスク分析・評価から必要となる改善計画策定に対する承認	43
2	情報資産を洗い出す対象範囲の決定に関する承認	53
3	情報資産台帳を作成するに当たっての情報資産の重要度による抽出の有無	60
4	情報資産の分類の表示方法の決定に関する承認	60
5	リスク受容水準の決定	113
6	詳細リスク分析・評価から必要となる改善計画策定に対する承認	123

本書では、情報セキュリティ委員会等の開催が必要な場面毎に、その都度、作業の流れとして当該委員会等を開催することを記述しているが、委員会等の開催回数を最小限に留めるため、項目番号１から４までを一括して審議することとしてもよい。また、項目番号５及び６についても、同様に一括して審議することとしてもよい。

注：情報セキュリティ委員会を設置していない場合

情報セキュリティ委員会を設置していない場合は、リスク分析・評価の実施に関して、新たに組織を立ち上げるのではなく、「情報化推進委員会」等の既存の類似する組織が代替してもよい。

1.6.3　リスク分析・評価の検討・実施チームの編成

リスク分析・評価の検討・実施作業は、実際には情報セキュリティ委員会等の下にリスク分析・評価のための事務局を設置し、事務局が主導して行うことが想定される。事務局には、すべての部、課等の関係者が関与することが望ましいが、主たる関係課室に絞って構成する場合もある。事務局の編成例としては、以下のような構成が挙げられる。

図表１－１６　事務局の編成例（図表１－１４を基に作成）

課室	選定の理由
情報システム課	・庁内の情報政策の主管
総務課	・個人情報保護条例の主管 ・文書管理規程の主管
施設管理課	・庁内の施設管理の主管

1.6.4　リスク分析・評価の役割分担（担当）

リスク分析・評価の役割分担（担当）の例としては、以下のようになる。図表１－１４を基にすると、情報システム課をはじめ、業務の情報システムを主管している課の長が情報システム管理者となり、それ以外の課の長が、情報セキュリティ管理者となる。

図表１－１７　役割分担の例

実施区分	実施項目	役割分担（担当）
基本リスク分析・評価	基本リスク分析・評価の実施	事務局
	基本リスク分析・評価に関する改善計画	
（広義の）詳細リスク分析・評価	情報資産洗い出しの対象範囲の決定	
	情報資産の洗い出し、情報資産台帳の作成	事務局 情報セキュリティ管理者（各課室長） 情報システム管理者（各課室長）
	詳細リスク分析・評価の実施	
	詳細リスク分析・評価に関する改善計画	

1.6.5　最高情報統括責任者（ＣＩＯ）の関与

リスク分析・評価を庁内で実施するためには、事務局のみならず、庁内の多くの職員の協力を要することから、庁内全体の情報セキュリティに関する責任を有する最高情報統括責任者（ＣＩＯ）の取組姿勢と意識が重要である。最高情報統括責任者は、リスク分析・評価作業に対して、事務局や作業を行う職員に対して指示するだけではなく、作業の進捗管理を定期的かつ直接的に確認するなどの強い関与が必要である。

1.7 リスク分析・評価の対象となる組織範囲

庁内における情報セキュリティポリシーの効力が及ぶ範囲を対象とする。

なお、詳細は、「2.2 基本リスク分析・評価の対象範囲」(26 頁)及び「3.2.2 情報資産を洗い出す範囲」(49 頁)で説明する。

1.8 リスク分析評価の対象となる情報資産の範囲、種類及び例

1.8.1 情報資産の対象範囲

情報資産の対象範囲は、個人情報をはじめとする行政情報、これらの行政情報を記録する文書、電磁的記録媒体[10]、磁気ディスク装置等の記憶装置に記録されている電子データ(ソフトウエアや情報システムのソースコード等を含む。)及び情報を利用するためのハードウエアとする。

建物や倉庫等の施設、空調設備や電源設備等の設備、関連する機器及び什器備品は、情報資産の可用性確保の観点から必要不可欠なものではあるが、業務継続計画[11]において講ずる対策と重なるため除外することとする。

また、各地方公共団体では多くの個人情報を保有しているが、個人情報以外にも、公開前の財政情報や技術情報等の重要な情報も保有していることから、個人情報に限らずすべての保有行政情報を情報資産の対象とする。さらに記録される媒体によって情報の質が異なるものでないため、電子情報の他、文書情報も対象とする。

これ以外にも、「人」、「組織の評判、イメージ等の無形資産」等[12]を情報資産の範囲に取り込むこともある。「人」に対する対策は、可用性についてのみ確保することがあり、例えば、情報システムの技術面で職員等にけが等が生じたときの代替要員確保になるが、この点も業務継続計画において講ずる対策と重なる対策のため除外することとする。さらには無形資産に対する具体的な対策についても、本書に示すのは困難であるため、これについても除外するこことする。このため具体的に対策が行える情報資産に限定する。

1.8.2 情報資産の種類及び例

情報セキュリティ対策が必要となる情報資産の種類とは、前述したとおり、直接的に情報資産に対策が行えるものに限定する。情報資産の種類及び例としては、以下のようなものが挙げられる。

---

[10] ドライバーを内蔵しているＵＳＢメモリ等の電磁的記録媒体は、ＦＤ等とは構造が異なるが、利用方法が同じになるため「電磁的記録媒体」として取り扱う。

[11] 施設、設備等に関する対策については「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」（平成 20 年 8 月）において、具体的な解説をしている。

[12] ISO/IEC 17799：2005 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)(19 頁～20 頁)参照。

図表１－１８　情報資産の種類と例

情報資産の種類	情報資産の例
文書	紙の文書
電磁的記録媒体	ＦＤ、ＭＯ、ＣＤ、ＵＳＢメモリ、ＤＡＴ、ＣＧＭＴ等
電子データ	サーバ又はパソコンの磁気ディスク装置、電磁的記録媒体等に記憶している電子データ（ソフトウエア、組織で運用している情報システムのソースコード、電子文書等を含む。）
設置型ハードウエア ※床置き、机上、ラック等に設置等して使用する資産	サーバ、デスクトップパソコン、ルータ、スイッチ、プリンタ、ファクシミリ、コピー機、スキャナー等
移動型ハードウエア ※持ち出しができるように製造された資産	ノートパソコン、携帯電話、デジタルカメラ、ＩＣレコーダ等

1.9　リスク分析・評価項目及び情報セキュリティ対策の分類

1.9.1　リスク分析・評価項目

本書でいうリスク分析・評価項目とは、庁内における情報セキュリティ対策向上のため、現状の対策との比較において実施状況の強弱を判断するための項目をいう。当該項目は、情報セキュリティ対策のＰＤＣＡのサイクル及び関連ガイドラインとの整合性の確保の観点から、「地方公共団体における情報セキュリティ監査に関するガイドライン（平成１９年７月６日全部改定）」（以下、「監査ガイドライン」という。）の情報セキュリティ監査項目（以下、「監査項目」という。）を利用する。監査ガイドラインの「監査項目」は全部で３１７項目あるが、本書では必須項目である１１０項目をリスク分析・評価項目として利用している。これによって、ＰＤＣＡサイクルにおける後続プロセスである監査に引き継げるようにしている。

参考　ガイドライン間の整合性

ポリシーガイドラインと監査ガイドラインは、互いに整合性を確保して作成されている。また、監査ガイドラインの「監査項目」は、ポリシーガイドラインの対策基準に即して構成されている。

1.9.2　情報セキュリティ対策の分類

リスク分析・評価の実施に際して、情報セキュリティ対策の全体像を明確にして

おく必要がある。具体的には、以下の４つの対策に分類することができる。

図表１－１９　情報セキュリティ対策の分類

情報セキュリティ対策	各対策の内容	対策の例
管理的対策	組織体制の確立、規程・規則等の文書化、運用面での点検・評価等の仕組みがあり、これらの対策が、職員の意識向上のために講じられている。	情報セキュリティポリシー等の策定、組織体制の確立、監査の実施、セキュリティ委員会等の活動等の対策
人的対策	教育の実施、情報セキュリティ事故の原因と対応の周知等の仕組みがあり、これらの対策が、職員の意識向上のために講じられている。	教育の実施、テスト、異動・退職時の情報資産返却等の対策
技術的対策	セキュリティ技術の実装、ログの取得等の開発・保守・運用の仕組みがあり、これらの対策が、ソフトウエアの脆弱性や運用の不備の改善のために講じられている。	認証、アクセス制御、暗号化、バックアップ、フィルタリング、ログの取得等の対策
物理的対策	入退室制限、情報資産の持出・持込制限等の対策の仕組みがあり、これらの対策が、情報資産の紛失、盗難、安定稼動等のために講じられている。	入退室管理、機器の保守、機器の処分、情報資産の持出・持込の制限、電源の供給確保、機器の転倒防止等の対策

注：監査ガイドラインの「情報セキュリティ監査チェックリスト」と本書の情報セキュリティ対策との関連

監査ガイドラインの「情報セキュリティ監査チェックリスト」に「管理的対策」という用語は使用していないが、本書では、監査ガイドラインの「１．対象範囲」、「２．組織体制」等の庁内全体で取り組む、情報資産に直結しない対策を取りまとめた総称として使用する。

本書では、監査ガイドラインで「人的セキュリティ」に区分されている対策であっても、「図表１－１９　情報セキュリティ対策の分類」の「各対策の内容」に照らして妥当と考えられる物理的対策等の区分に組み替えているケースもある。これに関する詳細は、「付録２：監査ガイドライン情報セキュリティ対策別関連表(別冊)」を参考のこと。

1.10 リスク分析・評価における情報セキュリティ対策と情報資産との関連

本書では、管理的対策、人的対策、技術的対策及び物理的対策の各情報セキュリティ対策に関して、情報資産に直結しない対策と直結する対策に分けてリスク分析・評価を行う方法を採用している。

図表１－２０　リスク分析・評価におけるセキュリティ対策と情報資産の関連表

分析・評価方法の名称		基本リスク分析・評価		（広義の）詳細リスク分析・評価				
情報セキュリティ対策と情報資産との関連		情報資産に直結しない対策		情報資産に直結する対策				
リスク分析・評価の対象となる情報資産		—	—	文書	電磁的記録媒体	電子データ	設置型ハードウエア	移動型ハードウエア
情報セキュリティ対策の分類	管理的対策	●						
	人的対策							
	技術的対策					●		
	物理的対策			●	●		●	●

参考 リスク分析・評価の手法

リスク分析・評価の手法としては、一般的に、ＩＳＭＳで活用されている ISO/IEC TR 13335(GMITS: Guidelines for the Management of IT Security)が挙げられる。

図表１－２１　ISO/IEC TR 13335 のリスク分析・評価手法の概要

手法	内容	利点	欠点
ベースラインアプローチ	基準等をもとに、組織で確保すべきセキュリティレベルを設定し、現状との乖離(ギャップ)を分析・評価する手法	基本的な対策を短い時間で、基準等に基づいて実施されているかどうかを検証することができる。	一律に適用することで、設定レベルが高すぎたり、低すぎたりすることが生じる。
詳細リスク分析	情報資産ごとに、脅威と脆弱性を加味してリスクを分析・評価する手法	情報資産ごとに、脅威や脆弱性を検証することかできる。	情報資産ごとに実施するため、分析・評価にかなりの時間を要し、習熟が必要となる。
非形式的アプローチ	基準等を用いるのではなく、個人の経験や長年の勘に依存してリスクを分析・評価する手法	費用対効果に優れ、小規模な組織に適している。	個人の能力に依存するため、客観性に乏しく、見落としが発生しやすい。
組み合わせアプローチ	ベースラインアプローチと詳細リスク分析を組み合わせてリスクを分析・評価する手法	両方の利点を採用することができる。	ベースラインアプローチが不正確な場合、詳細リスク分析・評価で必要な事項が見落とされる。

本書では、「ベースラインアプローチ」及び「詳細リスク分析」の利点を活用した、「組み合わせアプローチ」を参考にしている。