

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

第1章 総則	1
1.1 手引き作成の背景及び目的.....	1
1.2 手引き集の構成、特徴及び利用方法.....	2
1.2.1 本書の構成.....	3
1.2.2 手引き集の利用方法.....	4
1.2.3 分析・評価シートの構成.....	5
1.2.4 手引きと分析・評価シートとの関連.....	6
1.2.5 分析・評価シート相互の関連図.....	6
1.2.6 リスク分析・評価ファイルの構成.....	7
1.2.7 特徴.....	8
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
1.3.1 本書におけるリスク分析・評価の実施フロー.....	9
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.....	10
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.....	12
1.4.1 リスク分析・評価の位置.....	12
1.4.2 リスク分析・評価の意義.....	13
1.5 リスク分析・評価の効果.....	14
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.....	16
1.6.1 モデル団体.....	16
1.6.2 実施組織体制.....	17
1.6.3 リスク分析・評価の検討・実施チームの編成.....	18
1.6.4 リスク分析・評価の役割分担(担当).....	19
1.6.5 最高情報統括責任者(CIO)の関与.....	19
1.7 リスク分析・評価の対象となる組織範囲.....	20
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.....	20
1.8.1 情報資産の対象範囲.....	20
1.8.2 情報資産の種類及び例.....	20
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.....	21
1.9.1 リスク分析・評価項目.....	21
1.9.2 情報セキュリティ対策の分類.....	21
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.....	23
第2章 基本リスク分析・評価	26
2.1 本章の趣旨.....	26

2.2	基本リスク分析・評価の対象範囲.....	26
2.3	基本リスク分析・評価の事前作業(リスク分析・評価項目表の見直し).....	27
2.4	基本リスク分析・評価の実施.....	33
2.4.1	基本リスク分析・評価の実施方法の検討.....	33
2.4.2	基本リスク分析・評価シート(様式2)のレイアウト.....	33
2.4.3	基本リスク分析・評価の実施.....	34
2.5	基本リスク分析・評価に関する改善計画の策定と実施.....	40
2.5.1	基本リスク分析・評価に関する改善計画の策定から実施までの流れ.....	40
2.5.2	基本リスク分析・評価に関する改善計画表の作成.....	42
2.5.3	基本リスク分析・評価に関する改善計画の承認及び実施.....	43
第3章	(広義の) 詳細リスク分析・評価.....	46
3.1	本章の趣旨.....	46
3.2	情報資産の洗い出し及び情報資産台帳の作成.....	47
3.2.1	情報資産管理者.....	47
3.2.2	情報資産を洗い出す範囲.....	49
3.2.2.1	対象範囲の決定.....	49
3.2.2.2	対象範囲に関する情報セキュリティ委員会等の承認.....	53
3.2.3	情報資産洗い出し対象の決定.....	54
3.2.3.1	情報システムを対象とした洗い出しに関する留意事項.....	54
3.2.3.2	情報資産洗い出し対象設定表の作成.....	55
3.2.4	情報資産の洗い出し、不要な情報資産の処分等情報資産台帳作成の準備作業.....	57
3.2.4.1	情報資産の洗い出しに関する項目の決定.....	57
3.2.4.2	情報資産の価値である重要度による抽出に関する検討.....	58
3.2.4.3	不要な情報資産の処分又は回収等の明確化.....	58
3.2.4.4	情報資産の分類の表示方法の検討.....	60
3.2.4.5	情報資産の重要度による抽出及び情報資産の分類の表示方法に関する情報セキュリティ委員会等の承認.....	60
3.2.4.6	情報資産洗い出しに関する資料の配付と情報資産管理者への実施要請.....	61
3.2.4.7	情報資産の洗い出し及び情報資産台帳(様式6)の作成に関する作業分担.....	62
3.2.5	情報資産台帳の作成.....	63
3.2.5.1	情報資産台帳(様式6)のレイアウト.....	63
3.2.5.2	情報資産台帳(様式6)作成.....	63
3.2.6	情報資産台帳(様式6)の確認及び情報資産の分類の表示作業の実施.....	84
3.3	詳細リスク分析・評価の実施.....	85
3.3.1	リスクの3要素.....	85
3.3.2	詳細リスク分析・評価の事前作業(脅威の分析・評価).....	86

3.3.2.1	脅威の分析・評価に関する3つ要素.....	86
3.3.2.2	脅威の分析・評価の実施.....	86
3.3.3	詳細リスク分析・評価の事前作業(リスク分析・評価項目表の見直し).....	94
3.3.4	詳細リスク分析・評価の事前作業(実施単位の決定).....	95
3.3.5	詳細リスク分析・評価の事前作業(情報資産管理者への実施要請).....	98
3.3.6	詳細リスク分析・評価の実施.....	99
3.3.6.1	詳細リスク分析・評価シート(様式8)のレイアウト.....	99
3.3.6.2	詳細リスク分析・評価の実施概要.....	101
3.3.6.3	課室からの詳細リスク分析・評価シート(様式8)の回収と確認.....	107
3.3.6.4	リスク受容水準の決定と残留リスク.....	107
3.3.6.5	リスク対応の選択.....	115
3.4	詳細リスク分析・評価に関する改善計画の策定と実施.....	119
3.4.1	詳細リスク分析・評価に関する改善計画の策定から実施までの流れ.....	119
3.4.2	詳細リスク分析・評価に関する改善計画表の作成.....	120
3.4.3	詳細リスク分析・評価に関する改善計画の確認、承認及び実施.....	122
付録1：情報資産台帳サンプル		124
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）		

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	<ul style="list-style-type: none"> ・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。 <div style="border: 1px dashed black; padding: 5px; margin: 5px 0;"> <p>手順1 ○○は、□□する。</p> <p>手順2 ○○は、△△する。</p> </div> <ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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。

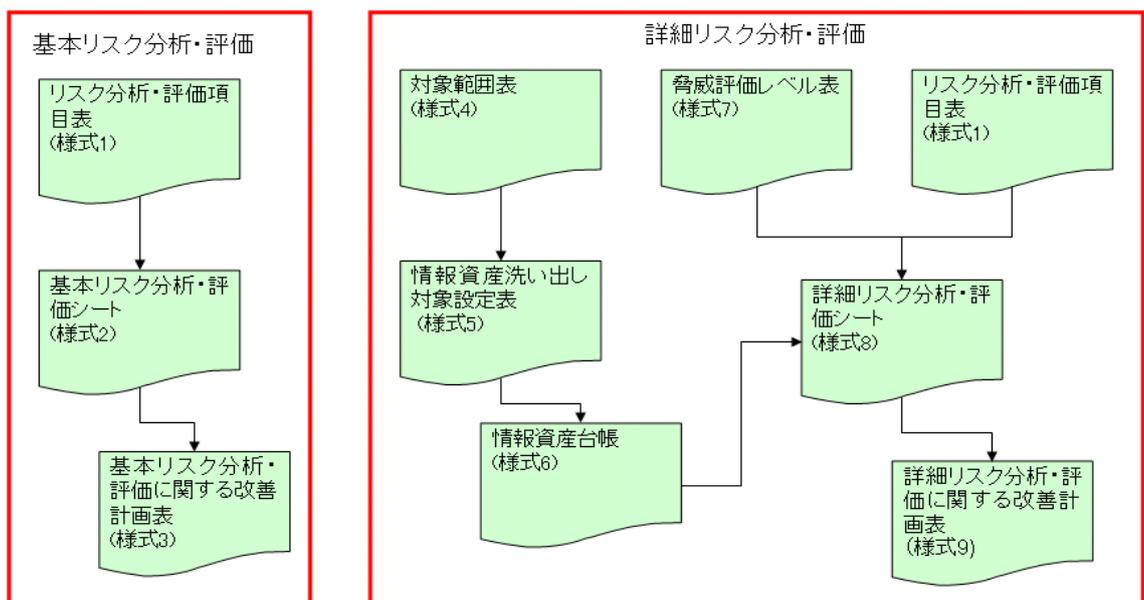
図表 1-6 手引きと分析・評価シートの関連

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)
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。	・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。

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。

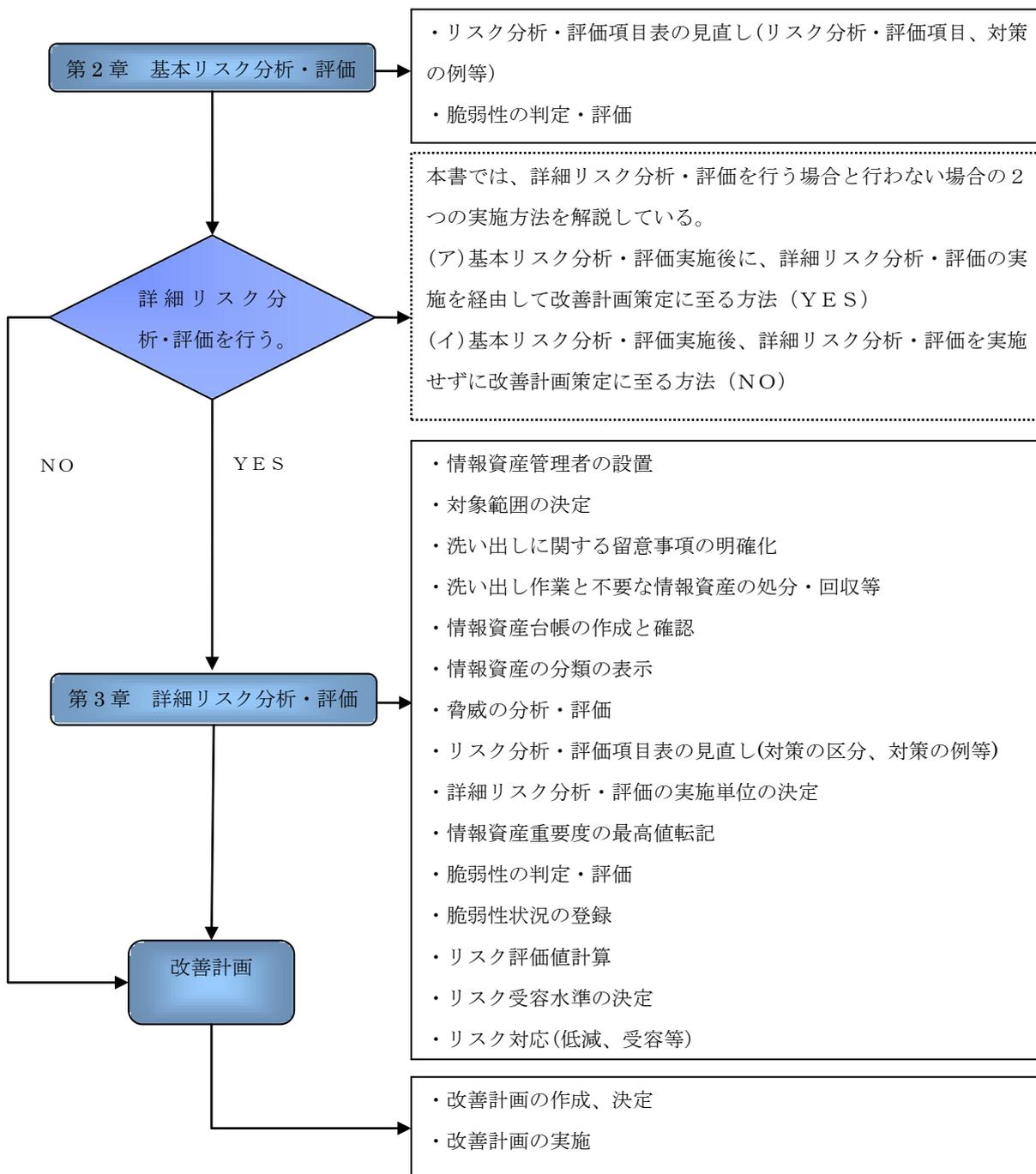
- (1) 基本リスク分析・評価、詳細リスク分析・評価の2つのリスク分析・評価の方法を紹介し、各地方公共団体の事情、状況に応じて、選択して実施できるものとしている。
- (2) リスク分析・評価では、情報資産のリスクが高い状態に対して、リスクの低減を図るため、各地方公共団体の情報セキュリティ対策の現状を把握する必要がある。その際の参考となるよう、対策の例、脆弱性評価レベルの例を提供し、リスク分析・評価の実施を支援するものとしている。
- (3) リスク分析・評価作業を効率的に実施できるよう、作業で使用する様式（分析・評価シート）を添付している。分析・評価シートは、作業しやすいようにExcel（以下、表計算ソフトウェアと呼ぶ。）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



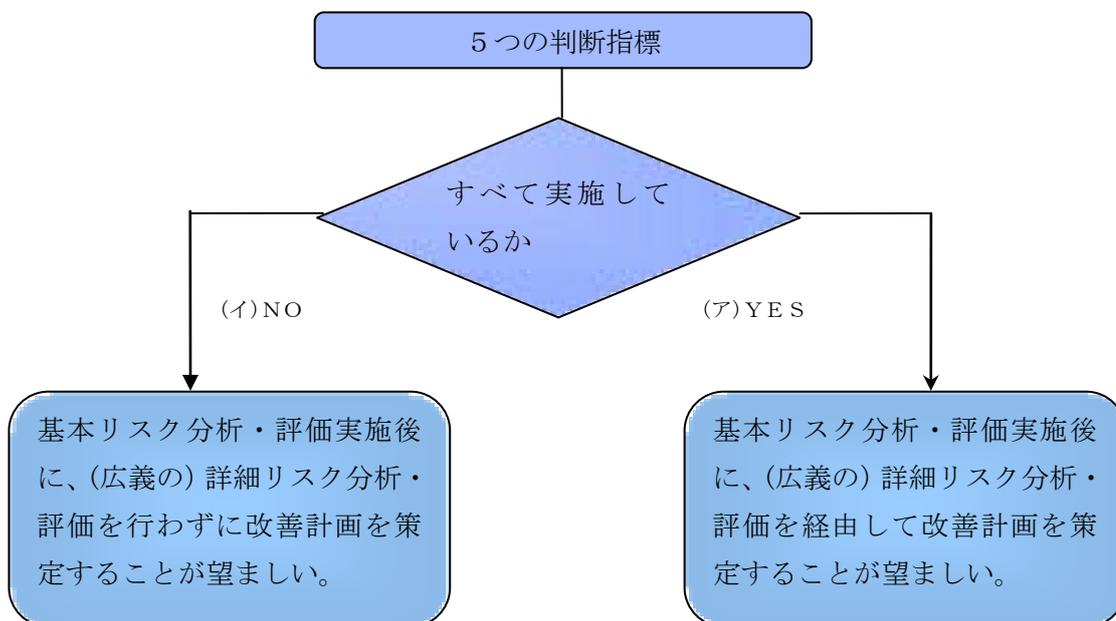
1.3.2 基本リスク分析・評価及び(広義の) 詳細リスク分析・評価の選択

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用するのか、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用のかどうかは、「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。

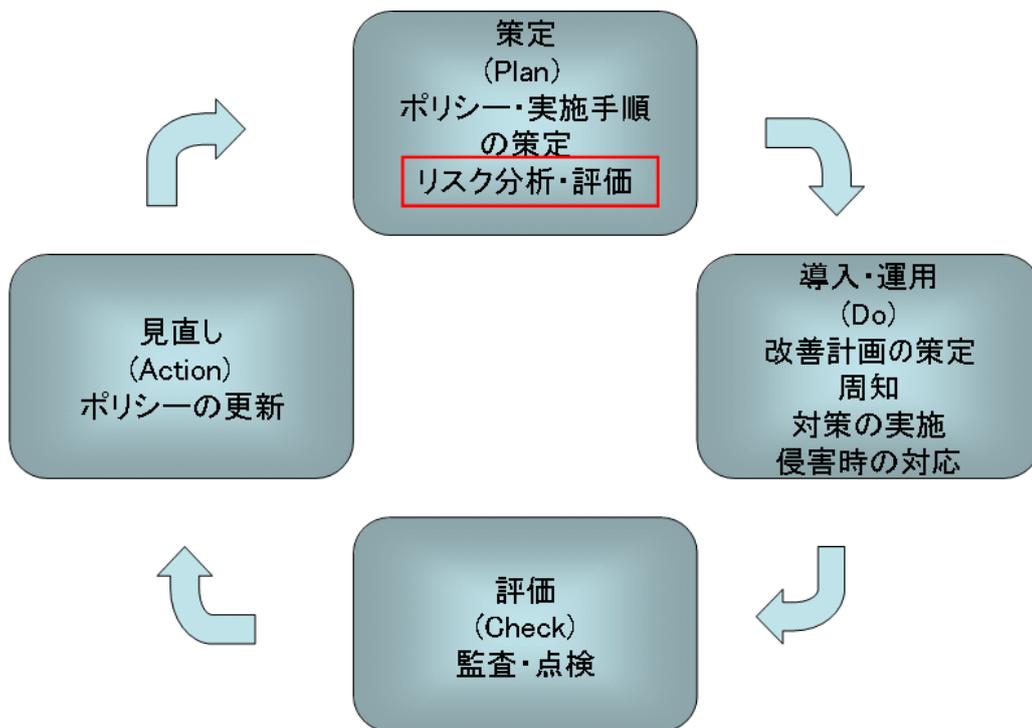
1.4 情報セキュリティ対策のPDCAサイクルとリスク分析・評価の関係

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か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ェ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事故の件数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、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の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 I SMS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I SMSを導入している例が見られる。

I SMS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。I SMS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

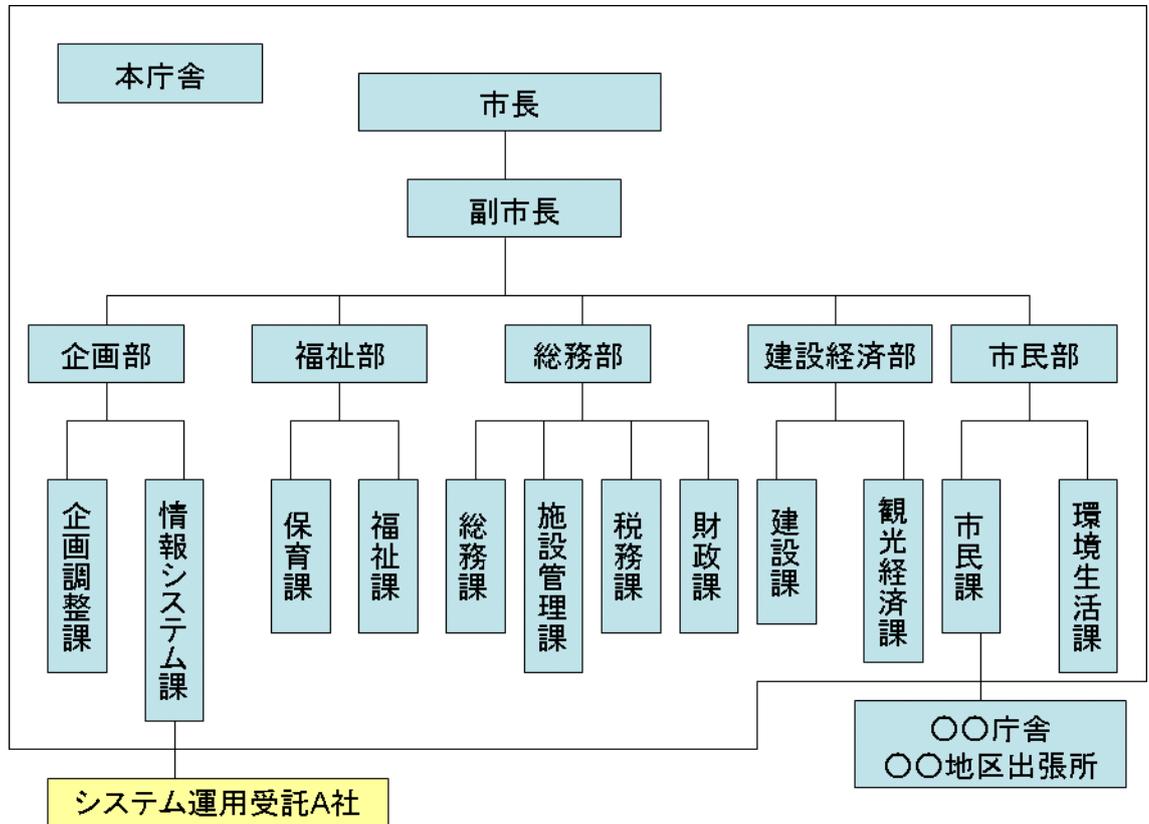
本書を展開するに当たってモデルとして設定する地方公共団体の属性は、以下のとおりである。ただし本モデルは、リスク分析・評価の実施について、小規模な地方公共団体を対象から除くことを意図しているものではなく、本書の説明上あくまでも便宜的に設定したものである。

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ェア及びソフトウェ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、グループウェア等の情報収集、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用した地方公共団体は、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用した地方公共団体は、「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	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）
	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(ソフトウェ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ェアとする。

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ととする。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(ソフトウェア、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。)
設置型ハードウェア ※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
移動型ハードウェア ※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、ソフトウェ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、安定稼働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	設置型ハードウェア	移動型ハードウェア
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、I SMS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るリスクを分析・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。

基本リスク 分析・評価

第2章 基本リスク分析・評価

2.1 本章の趣旨

本章は、庁内の情報資産に直結しない情報セキュリティ対策である、組織体制の確立、規程・規則等の策定及び見直し、情報セキュリティの教育・研修等の管理的対策及び人的対策の現状を調査する基本リスク分析・評価の方法を解説する。

本章の最後では、基本リスク分析・評価の結果から必要となる改善計画の策定及び実施に関する方法を解説する。

2.2 基本リスク分析・評価の対象範囲

基本リスク分析・評価の対象範囲は、全庁の情報セキュリティ対策の現状である。基本リスク分析・評価は、事務局が主体となって実施するが、リスク分析評価・項目の内容によっては、特定の課室の管理的対策や人的対策を調査する場合がある。

2.3 基本リスク分析・評価の事前作業(リスク分析・評価項目表の見直し)

ステップ (第2章-1)	
<p><作業の概要></p> <p>手順1 事務局は、リスク分析・評価項目表(様式1)の対策の区分の初期設定の段階を確認し、「採用」の区分を見直す。また対策の区分を「採用」から「不採用」に変更した場合は、必要に応じてその理由をメモする。</p> <p>手順2 事務局は、リスク分析・評価項目表(様式1)のリスク分析・評価項目、対策の例及び脆弱性評価レベルの例の表現を、必要に応じて見直し、庁内で使用している用語等を踏まえたものに変更する。</p>	
分析・評価シート	リスク分析・評価項目表(様式1)
操作マニュアル目次	2.1 基本リスク分析・評価に関する事前作業

(1) レイアウト

「リスク分析・評価項目表(様式1)」のレイアウトは、以下のとおりである。表示の都合上4分割している。

(その1/4)¹³

基本リスク分析・評価シート(様式2)では、脅威及び対策の区分の文書用対策から移動型ハードウェア用対策まで列の非表示設定

表示	表示	表示	表示	選択	表示	表示	表示	採用時選択	採用時選択	採用時選択	採用時選択	採用時選択	採用時選択	採用時選択	
リスク分析・評価項目表				脅威				対策の区分							
連番	評価項目番号(No.)	必須	リスク分析・評価項目 (監査ガイドラインの監査項目)	脅威の項目	機密性	完全性	可用性	管理的対策	人的対策	文書用対策	電磁的記録媒体用対策	電子データ用対策	設置型ハードウェア用対策	移動型ハードウェア用対策	
1	1	○	i)行政機関の範囲 最高情報統括責任者によって、情報セキュリティポリシーを適用する行政機関の範囲が定められ、文書化されている。					採用	不採用	不採用	不採用	不採用	不採用	不採用	

¹³ 連番を除く、評価項目番号(No.)、必須、リスク分析・評価項目(監査項目)の解釈は、「監査ガイドライン」と同様である。またリスク分析・評価項目の内容は、「ポリシーガイドライン」の対策基準の【例文】の(解説)を参照のこと。

(その 2/4)

基本リスク分析・評価シート(様式2)では、対策の例の文書用対策から移動型ハードウェア用対策まで列の非表示設定

文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正
対策の例(情報セキュリティの機能含む)						
管理的対策	人的対策	文書用対策	電磁的記録媒体用対策	電子データ用対策	設置型ハードウェア用対策	移動型ハードウェア用対策
・情報セキュリティポリシーに適用する行政機関の範囲に関する規定の文言(抑制)		情報セキュリティ対策の機能				

(その 3/4)

文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正
脆弱性評価レベルの例 管理的対策				脆弱性評価レベルの例 人的対策			
1	2	3	4	1	2	3	4
・情報セキュリティポリシーに、行政機関の範囲に関する規定がされていて、職員等に周知している。また、見直しを行っている。	・情報セキュリティポリシーに、行政機関の範囲に関する規定がされていて、職員等に周知している。但し、見直しは行っていない。	・情報セキュリティポリシーに、行政機関の範囲に関する規定がされていて、職員等に周知している。但し、見直しは行っていない。	・情報セキュリティポリシーに、行政機関の範囲に関する規定がされていない。				

(その 4/4)

基本リスク分析・評価シート(様式2)では、すべて列の非表示設定

文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正	文言訂正		
脆弱性評価レベルの例 文書用対策				脆弱性評価レベルの例 電磁的記録媒体対策				脆弱性評価レベルの例 電子データ用対策				脆弱性評価レベルの例 設置型ハードウェア用対策				脆弱性評価レベルの例 移動型ハードウェア用対策				
1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	

(2) 見直しに関する項目

見直しに関する項目を整理すると、以下のとおりとなる。

図表 2-1 見直しに関する項目について

見直しの項目	内容
リスク分析・評価項目	情報資産のリスク分析・評価の具体的な項目である。
対策の区分	「採用」表示は、分析・評価が必要なこと、「不採用」表示は、分析・評価が不要であることを表す。
対策の例	課題と改善案を考える場合の参考例である。
脆弱性評価レベルの例	対策又は管理の状況について、レベル判断する場合の参考例であり、4段階のレベルで記述している。 ※4段階のレベルは変更することはできない。

(3) 事前作業内容

手順 1	実施主体：事務局
------	----------

ア 対策の区分の見直しと当該区分「不採用」時の対応

事務局は、リスク分析・評価項目表(様式1)の対策の区分の初期設定情報を確認し、必要に応じて次の見直しを行う。

リスク分析・評価項目表(様式1)のリスク分析・評価項目ごとに設定されている対策の区分の「採用」を団体の事情に応じて変更する。例えば、「採用」が設定されている対策を実施しないと判断する場合は、「不採用」を選択する。

注：「採用」と「不採用」の変更について

初期設定の段階で「採用」となっている項目は、「不採用」に変更できるが、初期設定の段階で「不採用」となっている項目は、情報セキュリティ対策と関連付けの必要がないリスク分析・評価項目のため、「採用」に変更できないこととしている。また、対策の区分が初期設定の段階で「不採用」の場合は、対策の例及び脆弱性評価レベルの例は空欄となっている。

表示	表示	表示	表示	選択	表示	表示	表示	採用時選択	採用時選択	採用時選択	採用時選択	採用時選択	採用時選択	採用時選択
リスク分析・評価項目表				脅威				対策の区分						
連番	評価項目番号(No.)	必須	リスク分析・評価項目 (監査ガイドラインの監査項目)	脅威の項目	機密性	完全性	可用性	管理的対策	人的対策	文書用対策	電磁的記録媒体用対策	電子データ用対策	設置型ハードウェア用対策	移動型ハードウェア用対策
1	1	○	i)行政機関の範囲 最高情報統括責任者によって、情報セキュリティポリシーを適用する行政機関の範囲が定められ、文書化されている。					採用	不採用	不採用	不採用	不採用	不採用	不採用
<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 0 auto;"> 対策の区分の「採用」は、プルダウンになっている。 </div>														

(リスク分析・評価項目表)

ここがポイント 対策の区分の「採用」と「不採用」について

採用 リスク分析・評価項目に照らして、管理的対策、人的対策、情報資産「文書、電磁的記録媒体、電子データ、設置型ハードウェア、移動型ハードウェア」に関連する対策の中で適合する場合をいう。

不採用 リスク分析・評価項目に照らして、管理的対策、人的対策、情報資産「文書、電磁的記録媒体、電子データ、設置型ハードウェア、移動型ハードウェア」に関連する対策の中でいずれにも適合しない場合をいう。

対策の区分を、「採用」から「不採用」に変更した場合には、後日その理由を把握することができるように別途メモすることが望ましい。様式は任意である。

図表 2-2 「不採用」に変更した場合のメモの例

評価項目番号とリスク分析・評価項目	「採用」→「不採用」に変更した理由
1 1 2 iii) 認証用 I C カード等の放置禁止 認証用 I C カード等を業務上必要としないときは、カードリーダーやパソコン等の端末のスロット等から抜かれている。	本市においては、認証用 I C カード等は、利用していないため。

イ リスク分析・評価項目、対策の例及び脆弱性評価レベルの例の変更・修正

手順 2	実施主体：事務局
------	----------

必要に応じて、リスク分析・評価項目表(様式 1)のリスク分析・評価項目、対

策の例及び脆弱性評価レベルの例欄の表現を変更・修正する。例えば、情報セキュリティポリシーという表現ではなく、「〇〇管理規程」という表現を用いている場合は、そのような正確な表現に変更・修正する。

参考▶ 情報セキュリティ対策の機能

(28 頁)のレイアウト(その 2/4)の対策の例の末尾の括弧は、情報セキュリティ対策の機能を表している。情報セキュリティ対策の機能には、抑制、予防、防止、検知及び回復の 5 つの局面がある。情報セキュリティ対策の機能を識別できるよう、本書では、対策の例に関連付けている。この機能は、情報セキュリティ対策の実施によって得られる効果を意味する。

図表 2-3 情報セキュリティ対策の機能、意義及び具体例

機能	意義	具体例
抑制	規則の遵守等による牽制や犯罪防止への啓発を職員に働きかける機能	規則の作成と遵守、組織体制の活動、マネジメント系の監査等
予防	コンピュータ、ネットワーク等のシステムに関する脆弱性の改善を図る機能	パッチの適用、ウイルス定義ファイルの更新、不要な I D 等の削除、ネットワーク侵入検査等
防止	不正アクセス、コンピュータウイルス感染等の直接的な脅威に対抗する機能	認証機能の活用、アクセス制御、暗号化、ファイアウォールの利用等
検知	不正アクセス等の悪意の行為や異常な状態の速やかな発見により、被害の拡大を抑制する機能	ログの点検、侵入検知システムの導入、コンピュータウイルス検知ソフトウェアの常駐等
回復	障害等が発生した場合に、速やかに、正常な元の状態に戻す機能	バックアップ、データリストア、緊急時対応訓練等

参考▶ 情報セキュリティ対策の機能の複合的な効果

情報セキュリティ対策の機能について、対策の実施により 1 つの機能を果たす個別効果だけではなく、2 つ以上の機能を果たす複合的な効果が得られる例がある。

例えば、コンピュータウイルス検知ソフトウェアの導入により、多くの場合、コンピュータウイルス感染の「**予防**」(ウイルス定義ファイルの自動更新)だけでなく、「**検知**」(感染の検知)と「**回復**」(ウイルスの駆除)といった複合的な効果が得られる。

2.4.3 基本リスク分析・評価の実施

手順	実施主体：事務局
----	----------

(1) 基本リスク分析・評価シート(様式2)のヘッダ項目の入力

基本リスク分析・評価シート(様式2)のヘッダ項目に必要事項を入力する。

ア 実施組織

事務局等実施する組織名を入力する。

イ 実施完了日

基本リスク分析・評価の実施が完了した年月日を入力する。

(2) 2つの実施ケース

基本リスク分析・評価を実施する上で、リスク分析・評価項目に応じて事務局が庁内全般の情報セキュリティ対策の状況を把握しているケースと、庁内全般の情報セキュリティ対策状況を把握しきれないケースがあると考えられるため、2つのケースに分けて実施手順を解説する。

ア 庁内全般の情報セキュリティ対策の状況を把握しているケース

基本リスク分析・評価シート(様式2)をそのまま利用して実施する。

(ア) 脆弱性評価レベルの判定

対策の区分の管理的対策又は人的対策で「採用」となっている項目について、脆弱性評価レベルの判定を1～4の選択肢から選択する。選択に当たっては、脆弱性評価レベルの例で例示されている内容を参考として、1～4までの評価レベルを判定する。

図表2-5 脆弱性評価レベルの選択肢

選択肢

評価レベル	選択肢の内容
1	できている
2	大半はできている
3	一部できている
4	できていない

(イ) 脆弱性の判定で、値が「1(できている)」以外の場合には、「脆弱性状

況の登録(メモ)」欄に、課題の把握や改善計画の作成に役立てるため、より詳しい脆弱性に関する情報をメモする。ただし、この作業は任意である。

参考 基本リスク分析・評価の脆弱性状況の登録のメモの例

- ・(課題) 情報セキュリティポリシーに、行政機関の範囲を規定していない。
- ・(改善案) 情報セキュリティポリシーに、行政機関の範囲を規定する。

課題と改善案の登録が難しい場合は、対策の例を参考にするとよい。

イ 庁内全般の情報セキュリティ対策状況を把握していないケース

事務局が、(i)庁内の情報セキュリティ対策の状況について、関係課室にヒアリングによって確認を行う場合と、(ii)アンケート方式によって全庁又は関係課室の情報セキュリティの対策状況を把握する場合を説明する。

(i) 庁内の情報セキュリティ対策の状況について、関係課室にヒアリングによって確認を行う場合

- (ア) リスク分析・評価項目に関して、関係課室にヒアリングを行う。
- (イ) 関係課室と協議の上、ヒアリングの回答を基に、脆弱性評価レベルの判定を前述した選択肢から行う。
- (ウ) 脆弱性の判定で、値が「1(できている)」以外の場合には、「脆弱性状況の登録(メモ)」欄に、ヒアリングした課室の回答を基に、課題の把握や改善計画の作成に役立てるため、より詳しい脆弱性に関する情報をメモする。ただし、この作業は任意である。

(ii) アンケート方式によって全庁又は関係課室の情報セキュリティの対策状況を把握する場合

アンケート方式を実施する場合、リスク分析・評価項目に関して、一つの質問でアンケートを構成するか、複数の質問でアンケートを構成するかは、庁内の状況をどこまで精緻に調査するかを考慮して事務局が決定する。

(ア) アンケートの実施

脆弱性評価レベルの判定の基礎資料を得るため、全庁又は関係課室を対象としたアンケートを行う。

全庁又は関係課室へのアンケートを行う場合の例として、以下のリスク分析・評価項目が挙げられる。

リスク分析・評価項目の例
 ii) 机上の端末等の取扱い
 離席時には、パソコン等の端末や記録媒体、文書等の第三者使用又は情報セキュリティ管理者の許可なく情報が閲覧されることを防止するための適切な措置が講じられている。

例えば、「リスク分析・評価項目：ii) 机上の端末等の取扱い」に関して、1つの質問でアンケートを行う場合と、複数の質問でアンケートを行う場合の脆弱性評価レベルの判定への反映方法は以下のとおりとなる。

(イ) アンケート結果の脆弱性評価レベルの判定への反映方法

アンケートの結果を基に、脆弱性評価レベルの判定を行い、選択肢から評価レベルを選択する。(a) 及び (b) それぞれの反映方法を以下に解説する。

(a) 1つの質問でアンケートを行う場合の反映方法
 <アンケートの例>
 質問例1：長時間離席は、端末画面をロックしていますか。
 ・ 選択肢
 イ ロックしている。
 ロ 大半はロックしている。
 ハ 一部はロックしている。
 ニ ロックしていない。

アンケートの回答結果を集計し、その結果と脆弱性評価レベルの判定を関連付ける。

選択肢	回答数	計算式 (注) (回答数×係数)	計
イ	3	3 × 1	3
ロ	4	4 × 2	8
ハ	7	7 × 3	21
ニ	6	6 × 4	24
計	20		56

(注) 選択肢をそれぞれ係数(重み)として数値化して集計する。
 例：選択肢イ→1
 選択肢ロ→2
 選択肢ハ→3
 選択肢ニ→4

集計式：56(係数計) ÷ 20(回答数計) = 2.8

2.8を四捨五入すると3になるため、集計値は「3」(選択肢ニ)とする。

- ・集計値が「1」の場合、脆弱性評価レベルを「1」と判定する。
- ・集計値が「2」の場合、脆弱性評価レベルを「2」と判定する。
- ・集計値が「3」の場合、脆弱性評価レベルを「3」と判定する。
- ・集計値が「4」の場合、脆弱性評価レベルを「4」と判定する。

(b) 複数の質問でアンケートを行う場合の反映方法

この場合は、(a)に比較し、複数の手順が加わることになる。

<アンケートの例>

質問例1:長時間離席は、端末画面をロックしていますか。

(選択肢の作りこみを、脆弱性評価レベルの強弱に対応して設定する。)

- ・選択肢

イ ロックしている。

ロ 大半はロックしている。

ハ 一部はロックしている。

ニ ロックしていない。

質問例2:帰宅時には、机上の書類を引き出し等に入れてありますか。

- ・選択肢

イ 引き出し等に入れている。

ロ 引き出し等に大半は入っていない。

ハ 引き出し等に一部は入っていない。

ニ 引き出し等に入っていない。

アンケートの回答結果を集計し、その結果と脆弱性評価レベルの判定を関連付ける。

選択肢	回答数 (質問1)	回答数 (質問2)	計算式(注) (回答数×係数)	計
イ	3	9	$(3+9) \times 1$	12
ロ	4	8	$(4+8) \times 2$	24
ハ	7	2	$(7+2) \times 3$	27
ニ	6	1	$(6+1) \times 4$	28
計	20	20		91

(注) 選択肢をそれぞれ係数(重み)として数値化して集計する。

例: 選択肢イ→1
 選択肢ロ→2
 選択肢ハ→3
 選択肢ニ→4

集計式：91(係数合計) ÷ 40(回答数合計) = 2.275

2.275 を四捨五入すると 2 になるため、集計値は「2」(選択肢ロ) とする。

- 集計値が「1」の場合、脆弱性評価レベルを「1」と判定する。
- 集計値が「2」の場合、脆弱性評価レベルを「2」と判定する。
- 集計値が「3」の場合、脆弱性評価レベルを「3」と判定する。
- 集計値が「4」の場合、脆弱性評価レベルを「4」と判定する。

(ウ) 脆弱性の判定で、値が「1(できている)」以外の場合には、課題の把握や改善計画の作成に役立てるため、「脆弱性状況の登録(メモ)」欄に、アンケートの集計結果から窺える状況を記載する。

なお、基本リスク分析・評価については、リスク分析・評価項目に沿った分析・評価を一度に実施することが理想的であるが、人的または時間的な制約から一度に実施することが困難であれば、複数回に分けて実施するといった方法も考えられる。

参考 リスク分析・評価項目表（様式1）と基本リスク分析・評価シート（様式2）との関係

リスク分析・評価項目表（様式1）と基本リスク分析・評価シート（様式2）との関係は以下のようにになっている。

対策の区分						
管理的対策	人的対策	文書用対策	電磁的記録媒体用対策	電子データ用対策	設置型ハードウェア用対策	移動型ハードウェア用対策
採用	不採用	不採用	不採用	不採用	不採用	不採用

リスク分析・評価項目表(対策の区分)

自動的に転記される。

対策の例(情報セキュリティの観点含む)						
管理的対策	人的対策	文書用対策	電磁的記録媒体用対策	電子データ用対策	設置型ハードウェア用対策	移動型ハードウェア用対策
・情報セキュリティポリシーに適用する行政機関に関する規定の文書化(印刷)						

リスク分析・評価項目表(対策の例)

脆弱性評価レベルの例 管理的対策			
1	2	3	4
・情報セキュリティポリシーに、行政機関の範囲に関する規定がされていて、職員等に周知している。また、見直しを行っている。	・情報セキュリティポリシーに、行政機関の範囲に関する規定がされていて、職員等に周知している。但し、見直しは行っていない。	・情報セキュリティポリシーに、行政機関の範囲に関する規定がされていて、職員等に周知していない。	・情報セキュリティポリシーに、行政機関の範囲に関する規定がされていない。

リスク分析・評価項目表(脆弱性評価レベルの例)

自動的に転記される。

基本リスク分析・評価シート		実施経緯		審査期											
表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示
区分種別	区分種別	区分種別	区分種別	区分種別	区分種別	区分種別	区分種別	区分種別	区分種別	区分種別	区分種別	区分種別	区分種別	区分種別	区分種別
対策の区分	対策の区分	対策の区分	対策の区分	対策の区分	対策の区分	対策の区分	対策の区分	対策の区分	対策の区分	対策の区分	対策の区分	対策の区分	対策の区分	対策の区分	対策の区分
番号	番号	番号	番号	番号	番号	番号	番号	番号	番号	番号	番号	番号	番号	番号	番号
採用	不採用	採用	不採用	採用	不採用	採用	不採用	採用	不採用	採用	不採用	採用	不採用	採用	不採用
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

リスク分析・評価項目表のリスク分析・評価項目が自動的に転記される。

自動的に転記される。

基本リスク分析・評価シート

2.5 基本リスク分析・評価に関する改善計画の策定と実施

ステップ (第2章-3)	
<p><作業の概要></p> <p>手順1 事務局は、基本リスク分析・評価に関する改善計画表（様式3）を利用し、素案を作成する。</p> <p>手順2 事務局は、改善計画の素案を、情報セキュリティ委員会等に諮り、承認を得る。</p> <p>手順3 事務局は、改善計画に基づき、改善を実施する。</p>	
分析・評価シート	基本リスク分析・評価に関する改善計画表（様式3）
操作マニュアル目次	なし

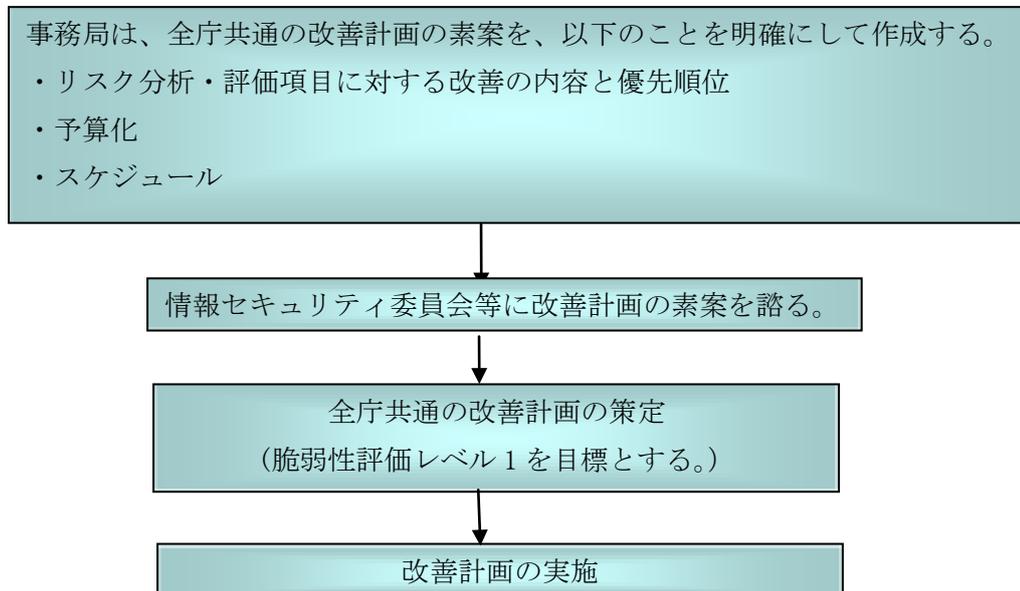
2.5.1 基本リスク分析・評価に関する改善計画の策定から実施までの流れ

情報セキュリティ対策では、管理的対策としての規程の策定、組織体制の確立等の環境の整備や、人的対策としての教育・研修等の職員の意識向上策が継続的に行われることが重要である。事務局は、基本リスク分析・評価の結果で脆弱性評価レベルが「1」以外の結果となった項目について、全庁に共通する改善計画を策定する。計画の策定に当たっては、基本リスク分析・評価に関する改善計画表（様式3）を利用し、対策の緊急性、経済性、有効性を検討した上で、リスク分析・評価項目の脆弱性評価レベルが2、3及び4の項目について、当該脆弱性に対する改善内容、優先順位、実施のスケジュール等を決定する。また、対策の実施に当たって予算化をしなければならないものもあることから、必要に応じて予算化のための作業を行う。

基本リスク分析・評価シート（様式2）の「脆弱性状況の登録」に必要なメモが取られている場合は、当該情報を参考とし、改善計画を策定する。

最終的には、改善計画を情報セキュリティ委員会等に諮り、その承認を得て全庁的に実施していくことになる。

図表 2-6 基本リスク分析・評価結果を基にした改善計画策定から実施までのフロー図



脆弱性評価レベルが「4」、「3」及び「2」の場合における改善計画の例としては、以下ようになる。(ここでは例として、情報セキュリティ組織体制に関する項目を取り上げている)。

図表 2-7 脆弱性評価レベルの判定による改善案の例

脆弱性評価レベルの判定	改善案の例
脆弱性評価レベルの判定が4の場合	全庁の情報セキュリティ組織体制を確立する。
脆弱性評価レベルの判定が3の場合	全庁の情報セキュリティ組織体制を確立しているが、情報セキュリティ委員会等が活動をしていないため、年1回以上当該委員会等を開催する。
脆弱性評価レベルの判定が2の場合	全庁の情報セキュリティ組織体制を確立しており、年1回以上組織的な活動を行っているが、業務組織体制の変更に對して、速やかな見直しが行われていないため、年1回の情報セキュリティ組織体制の見直しを行う。

2.5.2 基本リスク分析・評価に関する改善計画表の作成

(1) 基本リスク分析・評価に関する改善計画表(様式3)のレイアウト

レイアウトは、以下のとおりである。

基本リスク分析・評価に関する改善計画表				実施組織	事務局								
				作成日	平成21年1月14日								
				情報セキュリティ委員会 承認日	平成21年1月23日								
表示	表示	表示	表示	表示	表示	入力	入力	入力	入力	入力	入力	入力	入力
番号	対策の区分		評価項目番号	リスク分析・評価項目	脆弱性状況の登録 (基本リスク分析・評価シートとのリンク)	改善の実施内容			予算 (単位:千円)	スケジュール			
	管理的対策	人的対策				優先順位	開始日 (YYYY/MM/DD)	終了予定日 (YYYY/MM/DD)		終了日 (YYYY/MM/DD)			
											優先度高	優先度低	
1	採用	不採用	42	3	1)行政機関の範囲 最高情報統括責任者によって、情報セキュリティポリシーを適用する行政機関の範囲が定められ、文書化されている。	行政機関の範囲の文書化していない。行政機関の範囲を情報セキュリティポリシーに追記する。	高	情報セキュリティポリシーを改正して、行内の対象の組織範囲を定め、次回の情報セキュリティ委員会に諮る。		平成21年1月26日	平成21年2月27日		

(2) 基本リスク分析・評価に関する改善計画の素案の作成

手順 1	実施主体：事務局
------	----------

事務局は、基本リスク分析・評価に関する改善計画表(様式3)の素案を作成する。

ア ヘッド項目の作成

(ア) 実施組織

事務局等組織名を入力する。

(イ) 作成日

改善計画を作成した年月日を入力する。

(ウ) 承認日

情報セキュリティ委員会等が改善計画を承認した年月日を入力する。

イ 明細項目の作成

(ア) 優先順位

以下の観点から、優先度高、低を選択する。

図表 2-8 改善計画の優先順位の観点

優先順位の観点	内容
緊急性	リスク評価値が高く、速やかな対応をしなければならない状況にあるかどうか。
経済性	改善の実施に当たって必要な費用はどのくらいか。別途予算措置の必要があるか。
有効性	改善を実施した場合のリスク軽減効果はどの程度か。

(イ) 改善内容

各リスク分析・評価項目ごとに改善内容を作成する。詳細な計画とする場合は、別紙として作成する。

<改善内容の例>

(a) 管理的対策

- ・情報セキュリティポリシーを、庁内の情報セキュリティの状況を踏まえ、2年に1度見直す。

(b) 人的対策

- ・職員に対して、年に1度、情報セキュリティ上の事故を踏まえた情報セキュリティポリシーに関する研修を実施する。

(ウ) 予算

改善計画を作成する上で、情報システムの改修や物品購入等のために予算措置が必要になる場合に、必要経費の概算額を入力する。本書では、千円単位としているが、各地方公共団体において、入力する金額単位を修正してもよい。

(エ) 開始日、終了予定日及び終了日

改善計画の実施開始年月日とその終了予定年月日を入力する。また、改善計画の実施が終了した際に終了年月日を入力する。

なお、改善計画の作成では、番号、対策の区分、評価項目番号、リスク分析・評価項目及び脆弱性状況の登録(メモ)に関して、リスク分析・評価項目表(様式1)と同じ内容が表示されているため、入力は不要である。

2.5.3 基本リスク分析・評価に関する改善計画の承認及び実施

(1) 全庁共通の改善計画の素案に関する情報セキュリティ委員会等の承認

手順 2	実施主体：事務局
------	----------

事務局は、全庁共通の改善計画の素案を情報セキュリティ委員会等に諮り、承認を得る。庁内横断的な情報セキュリティに係る意思決定組織である情報セキュリティ委員会等の承認を得ることにより、円滑に改善計画を実施することができるようになると考えられる。

(2) 改善計画の実施

手順3	実施主体：事務局
-----	----------

事務局は、必要に応じて関係課室の協力を得ながら、全庁共通の改善計画を実施する。また、改善計画の進捗状況を監査等で確認し、情報セキュリティ委員会等に、定期的に報告していくことが望ましい。

詳細リスク 分析・評価

第3章（広義の）詳細リスク分析・評価

3.1 本章の趣旨

本章は、情報資産の洗い出し、情報資産台帳(様式6)の作成及び詳細リスク分析・評価の実施方法について解説する。

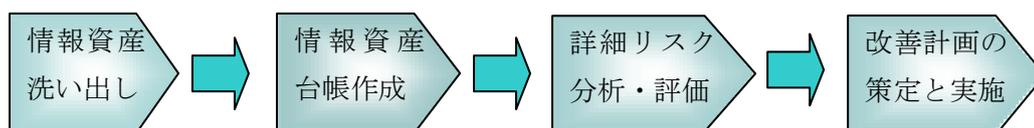
情報資産の洗い出し、情報資産台帳(様式6)の作成については、情報資産の洗い出し対象範囲の決定、情報資産を管理する者の権限及び責任等について解説する。

詳細リスク分析・評価については、情報資産台帳(様式6)に登録された文書、電磁的記録媒体、電子データ、設置型ハードウェア及び移動型ハードウェアに関する情報セキュリティ対策の現状を調査する方法を解説する。詳細リスク分析・評価は、方法によっては相当な労力や時間を費やすことにもなるため、本書では、作業負担の軽減が図れるような方法を解説する。

本章の最後では、詳細リスク分析・評価の結果から必要となる改善計画の策定及び実施に関する方法を解説する。

情報資産の洗い出し、情報資産台帳(様式6)の作成及び詳細リスク分析・評価の流れを図示すると、以下のとおりとなる。

図表 3-1 （広義の）詳細リスク分析・評価の流れ



ここがポイント 情報資産の洗い出しとリスク分析・評価との関係について

情報資産の洗い出し及び情報資産台帳(様式6)の作成は、詳細リスク分析・評価につながっているが、基本リスク分析・評価には直接関係していない(「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」(23 頁)参照)。

3.2 情報資産の洗い出し及び情報資産台帳の作成

情報資産の洗い出しとは、各課室における文書、電磁的記録媒体の利用や保管の状況、電子データの利用や保存の状況、機器の設置や保管等の状況を調べることをいう。情報資産台帳とは、洗い出した情報資産を登録する台帳のことである。

3.2.1 情報資産管理者

(1) 情報資産管理者の役割

情報資産の洗い出しや情報資産台帳の作成は、基本的に情報資産管理者が責任をもって行うことになる。

情報資産管理者の役割は、課室の情報資産を適正かつ安全に取り扱い、当該資産の機密性、完全性及び可用性を確保することである。情報資産の洗い出し及び情報資産台帳(様式6)の作成は、基本的に課室単位で実施することとなるため、課室の長たる情報資産管理者が、その実施の役割を担うこととなる。

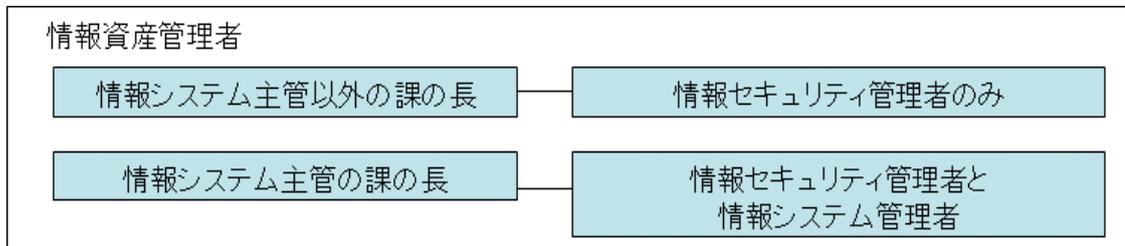
(2) 情報資産管理者の位置づけ

情報資産の管理は、実務的に情報資産を取り扱う組織の長に権限及び責任を付与することが職分として妥当である。これを踏まえて本書では、ポリシーガイドラインとの整合性を確保することも加味して、情報資産管理者を、情報システム主管外の課室長である情報セキュリティ管理者と、情報システムを主管している課室長である情報システム管理者とする。

(3) 情報システム管理者と情報セキュリティ管理者による情報資産の管理範囲の相違

情報システム管理者は、情報システムを主管しているため、サーバ、通信機器、情報システムのソースコード等の管理責任を有している。情報セキュリティ管理者は、情報システム管理者と異なり、サーバ、通信機器、情報システムのソースコード等の管理責任を持たずに情報システムから業務を利用するためサービスの提供を受ける立場にある。このため、情報システム管理者と情報セキュリティ管理者とでは、情報資産の洗い出しの対象範囲が異なる。ポリシーガイドラインにおける情報システム管理者及び情報セキュリティ管理者の権限・責任と情報資産管理者との関係を示すと、以下のとおりとなる。

図表 3-2 情報システム管理者及び情報セキュリティ管理者と情報資産管理者との位置関係



3.2.2 情報資産を洗い出す範囲

ステップ (第3章-1)	
＜作業の概要＞	
手順1 事務局は、対象範囲表(様式4)を利用し、情報資産を洗い出す範囲について決定する。	
手順2 事務局は、情報資産を洗い出す範囲に関して、情報セキュリティ委員会等に諮り、承認を得る。	
分析・評価シート	対象範囲表(様式4)
操作マニュアル目次	なし

3.2.2.1 対象範囲の決定

手順1	実施主体：事務局
-----	----------

事務局は、情報資産を洗い出す範囲に関して、業務、組織(課室)、場所及び外部委託先の面を明確にして、情報資産の洗い出しの対象範囲表(様式4)を作成する。

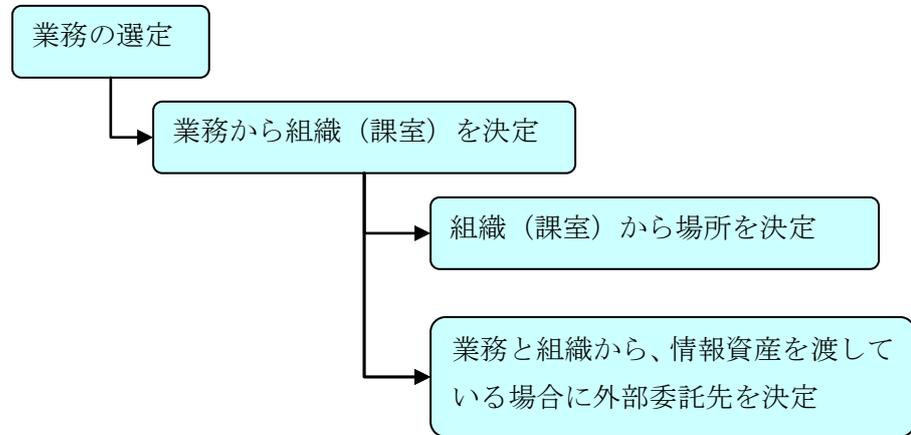
対象範囲を区切らず、全庁で情報資産の洗い出しを行うことが本来あるべき姿である。しかしながら、情報資産の洗い出しは、実施方法の確立段階において試行錯誤も多く、職員の作業負担も大きく、さらに習熟度が低い状況で対象範囲を拡大すると、作業手順や内容面において混乱を招くことも想定される。そのため、最初の取組段階においては、対象範囲を限定してまずは試行的に実施することが、継続的な取組みの観点からは重要である。最初の段階で対象範囲を区切って試験的に行うことは、民間でもよく行われているケースである。

本書では、対象範囲を区切って行う場合と全庁で一斉に行う場合を解説する。

(1) 対象範囲を区切って行う場合

対象範囲を区切って洗い出しを実施する場合は、業務における個人情報の漏えいや情報システムの故障等による業務への影響等を考慮して、その対象範囲を決定する。対象範囲を決定するための要素は、業務、組織(課室)、場所、外部委託先による情報資産の利用である。

図表 3-3 対象範囲決定の要素と各要素間の関係



例えば、対象業務を決定した場合は、これに応じて、対象となる組織（課室）、場所、外部委託先も自ずと決まることになる。ただし、特定の課室の協力が得られないから洗い出しの対象から除外したなどのことが生じると、対象業務の一部が洗い出しの範囲外となってしまうため、対象範囲の業務で利用する重要な情報資産が特定されないことになる。このような事態を回避するため、業務（対象範囲）を選定した理由を明確にし、対象となる課室によく説明することが重要である。

業務（対象範囲）を選定する理由としては、以下のようなものが考えられる。

- ・ 事務局が、情報資産の洗い出し、情報資産台帳（様式6）の作成の全庁展開に向けての手法を確立するため。
- ・ 市民への影響が大きい住民記録システム等の特定の情報システムに関する情報セキュリティ状況を調査するため。
- ・ 市民のプライバシーに直接影響が及ぶ個人情報を取り扱う業務と処理全般の情報セキュリティ状況を調査するため。

事務局は、対象範囲を区切る場合に、「図表 3-4 対象範囲を区切って行う場合の対象範囲表（様式4）の例」を参考に、対象範囲表（様式4）を作成する。

ア 作成者

事務局等対象範囲を検討する組織名を入力する。

イ 作成日付

対象範囲表（様式4）を作成した年月日を入力する。

ウ 承認日

情報セキュリティ委員会等が対象範囲を承認した年月日を入力する。

エ 業務と選定理由

情報資産の洗い出し対象とする業務名を入力する。また、その業務を選定した理由を入力する。

オ 課室

対象とする業務に従い、情報資産を洗い出す対象の課室を入力する。

カ 場所

対象とする課室の場所（執務室等）を入力する。

キ 外部委託先

対象とする業務及び課室において、外部委託先に情報資産が移送されている場合、情報資産を洗い出す対象として入力する。ただし、外部委託先に関する情報資産の洗い出しは、委託業務契約の内容を踏まえて検討する必要がある。

ク 対象範囲を区切って行う場合の留意事項

項目中「管理外の情報資産の状況」は、庁内全体で(広義の) 詳細リスク分析・評価を実施する際に、何らかの理由で対象から除外する組織等がある場合の留意事項として入力する欄であるため、対象範囲を区切って行う場合、入力は不要である。

以下に、対象範囲を区切って行う場合の対象範囲表(様式4)の例を示す。

図表3-4 対象範囲を区切って行う場合の対象範囲表(様式4)の例

項目	作成の例
作成者	事務局
作成日付	平成21年1月20日
情報セキュリティ委員会 承認日	平成21年1月23日
業務と選定理由	住民記録等に関する業務 選定理由：住民の家族構成等の個人情報を利用するため
課室	・市民課及び関連出張所 ・庁内LANとサーバ室を管理している情報システム課
場所	・本庁舎 市民課(1階執務室)及び関連出張所 ・本庁舎 情報システム課(4階執務室) ・住民記録システムのサーバ、通信機器等が設置してあるサーバ室
外部委託先(指定管理者を含む)	住民記録データベースのテープ保管を委託している〇〇社

管理外の情報資産 の状況	除外する業務
	-
	除外する組織
	-
	除外する場所
-	
除外する外部委託先	
-	

参考 対象範囲の決定について

取組みの最初の段階では、情報資産の洗い出しやその後の資産台帳の作成作業等のノウハウが完全に習得できないことが想定される。そこで、まずは情報セキュリティを担当する情報システム課等において、本書を活用して、実際に作業を実施することを推奨する。

その後、作業のノウハウが蓄積された後に、情報セキュリティ委員会等の場において、実施範囲の拡大について検討することが望ましい。範囲拡大の考え方としては、リスクが顕在化した場合の地域住民等への影響を考慮し、情報資産への各種の脅威に対して適切な対策を講じることが情報資産のリスク分析・評価の主たる目的であることから、情報資産管理の視点として重要な個人情報を取り扱う業務を対象とすることが考えられる。具体的には、住民情報を扱う業務（市民課等）、住民の資産情報や所得情報を扱う業務（税務課等）、住民の健康に関する情報を扱う業務（福祉課等）である。その後、個人情報を扱うことが少ないと考えられる業務（例えば、建設業務を行う建設課や予算、起債、決算業務を担当する財政課等）に対象範囲を広げていくことが考えられる。また、情報漏えい対策の観点から、情報システムに依存する業務を優先的に対象範囲と設定することも一案である。例えば、業務のシステム依存度が高い¹⁴、住民関係業務（住民課）、税務業務（税務課）等を優先的に対象とし、システム依存度が低い観光業務（観光経済課）や環境保全業務（環境生活課）をその後の対象範囲とすることも考えられる。

参考 民間の I SMS 認証取得で対象範囲を区切る場合のケース

民間における I SMS 認証取得では、データセンタや重要な情報資産を利用

¹⁴「電算処理システムの導入状況について、都道府県においては、人事・給与システム、法人都道府県民税システム、法人事業税システム、自動車税システム、軽油引取税システム、不動産取得税システム、予算執行システム、工事設計・進行管理システムが全団体に導入されており、市区町村においては個人市区町村民税システムが1,781団体（98.3%）と最も多かった。」地方自治情報管理概要（平成20年10月31日 総務省自治行政局地域情報政策室）30頁参照。

及び保管している業務、組織、場所等で対象範囲を区切ることが多い。最初の取組みとして、リスクが顕在化した場合に大きな影響を受ける可能性の高い、重要な情報システムや多くの情報資産を利用及び保管している業務や場所を対象範囲として区切ることは、よく行われている。

(2) 全庁で一斉に行う場合

対象範囲を区切らず全庁で一斉に実施する場合、広域連合、協議会等の情報資産で、地方公共団体の情報セキュリティポリシーの対象範囲外であるならば、対象から除外する。¹⁵これに該当する業務、組織、場所、外部委託先は除外することに留意する必要がある。例えば、除外する対象範囲を決定した後、対象範囲表（様式4）の「管理外の情報資産の状況」に、情報セキュリティポリシー等に定めている対象範囲外の業務、組織、場所等を入力する。

3.2.2.2 対象範囲に関する情報セキュリティ委員会等の承認

手順2	実施主体：事務局
-----	----------

事務局は、対象範囲を示した表等の素案を情報セキュリティ委員会等に諮り、承認を得る。事務局が独断的に決定するのではなく、関係各部課室のメンバーから構成される情報セキュリティ委員会等が関与することで、情報資産の洗い出しの範囲が明確になるとともに、作業対象となる関係課室の理解も得やすいと思われる。

¹⁵ ポリシーガイドラインの「3.1. 対象範囲」25頁参照。なお、ポリシーガイドラインでは、各団体で、情報セキュリティポリシーの対象範囲として、「行政機関」及び「情報資産」を明確にすることが求められている。

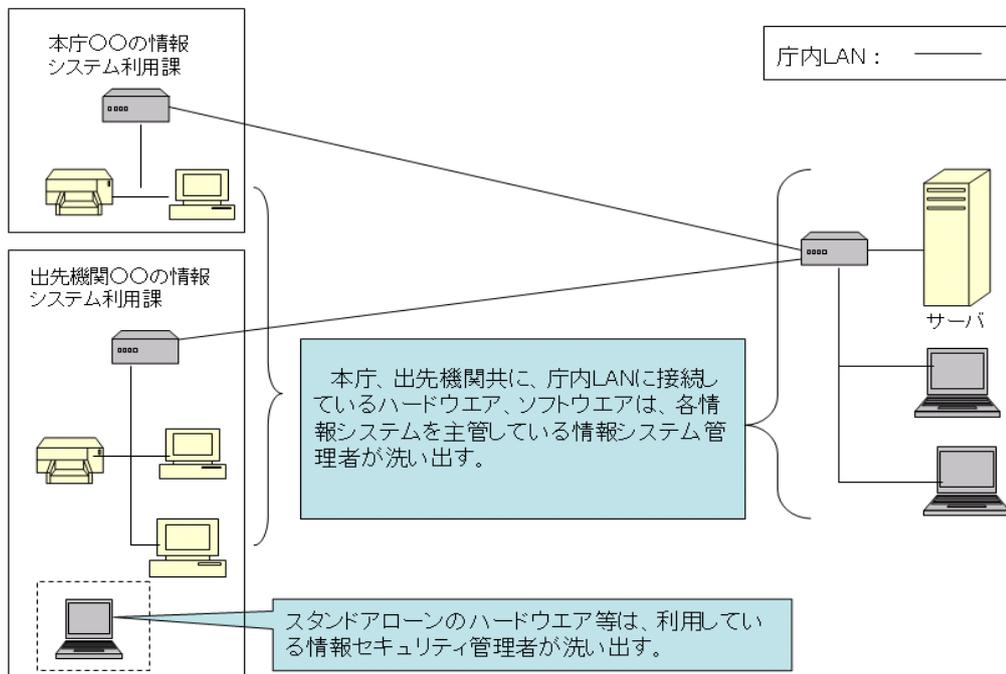
3.2.3 情報資産洗い出し対象の決定

ステップ (第3章-2)	
<p><作業の概要></p> <p>手順 事務局は、情報システムを対象とした洗い出しに関する留意事項を踏まえ、情報資産洗い出し対象設定表(様式5)を作成する。</p>	
分析・評価シート	情報資産洗い出し対象設定表(様式5)
操作マニュアル目次	なし

3.2.3.1 情報システムを対象とした洗い出しに関する留意事項

情報システム管理者は、主管する情報システムに関連する情報資産、及び庁内LANに接続している他の課室が利用している情報システム(ハードウェア、ソフトウェア両方)も洗い出しの対象とする。ただし、庁内LANに接続していないパソコン等各情報セキュリティ管理者で管理しているスタンドアロンのハードウェアは、情報セキュリティ管理者が洗い出す。

図表3-5 情報システムを対象とした洗い出しを行う範囲



3.2.3.2 情報資産洗い出し対象設定表の作成

手順	実施主体：事務局
----	----------

対象範囲に保管している文書、電磁的記録媒体、サーバ等に保存している電子データ、設置・保管しているハードウェアについては、作業の範囲が不明瞭なまま情報資産の洗い出しを実施すると、登録漏れや二重登録が発生することがある。事務局は、このような事態を極力避けるため、前述の留意事項を検討し、情報資産洗い出し対象設定表（様式5）を作成する。以下に、「図表1-14 モデルとした地方公共団体の組織図」を参考とした情報資産洗い出し対象設定表（様式5）作成の例を、情報システム管理者に関する権限と情報システム管理者に関する権限別に示す。ただし、情報システム管理者は、情報セキュリティ管理者を兼ねることになるため、その権限に応じた洗い出しを行うこととなる。

図表3-6 情報資産洗い出し対象設定表（様式5）作成の例

情報資産洗い出し対象設定表（様式5）	
情報資産の種類	洗い出しの主体と対象
文書	<主体> ・各課室 <対象> ・利用・保管している文書 ・管理している書庫内に保管している文書
電磁的記録媒体	・各課室が、利用・保管している電磁的記録媒体を洗い出す。
電子データ	<主体その1> ・情報システム課その他情報システムを主管している課室が <対象> ・情報システムに導入・利用しているソフトウェア ・管理しているサーバに保存された主要なデータベース及びファイル <主体その2> ・情報システム課 <対象> ・ファイルサーバシステムにおける課室の領域名（各課室に割り当てたフォルダー名）

	<p><主体その3></p> <ul style="list-style-type: none"> ・各課室 <p><対象></p> <ul style="list-style-type: none"> ・ファイルサーバシステムに割り当てられた当該課室が利用するフォルダー内のファイル ・職員等のパソコンに保存されている重要な電子データ
設置型ハードウェア	<p><主体></p> <ul style="list-style-type: none"> ・情報システム課その他情報システムを主管している課室 <p><対象></p> <ul style="list-style-type: none"> ・庁内LANに接続しているサーバ、デスクトップパソコン、プリンタ、通信機器等の設置型ハードウェア
	<p><主体></p> <ul style="list-style-type: none"> ・各課室 <p><対象></p> <ul style="list-style-type: none"> ・庁内LANに接続していないデスクトップパソコン、プリンタ等の設置型ハードウェア ・ファクシミリ、コピー機等の事務機器
移動型ハードウェア	<p><主体></p> <ul style="list-style-type: none"> ・情報システム課その他情報システムを主管している課室 <p><対象></p> <ul style="list-style-type: none"> ・庁内LANに接続しているノートパソコン等の移動型ハードウェア
	<p><主体></p> <ul style="list-style-type: none"> ・各課室 <p><対象></p> <ul style="list-style-type: none"> ・庁内LANに接続していないノートパソコン等の移動型ハードウェア ・利用・保管しているデジタルカメラ、ICレコーダ等の移動型ハードウェア
外部委託先にある情報資産	<p><主体></p> <ul style="list-style-type: none"> ・情報システム課 <p><対象></p> <ul style="list-style-type: none"> ・情報システム運用受託先A社に移送した文書、電磁的記録媒体等の情報資産（上段に記載した情報資産の種類に応じて洗い出す）

3.2.4 情報資産の洗い出し、不要な情報資産の処分等情報資産台帳作成の準備作業

ステップ (第3章-3)	
<p><作業の概要></p> <p>手順1 事務局は、情報資産を洗い出すための項目を決定する。</p> <p>情報資産の洗い出しを行うために、次の事項を明確にしておく。</p> <ul style="list-style-type: none"> ・情報資産台帳(様式6)の作成に当たって、情報資産の価値である重要度で抽出するか否か ・不要な情報資産について、廃棄等の処分又は回収等に関する留意事項 ・情報資産の分類の表示方法 <p>手順2 事務局は、情報資産台帳(様式6)の作成のための情報資産の重要度による抽出の有無と情報資産の分類の表示方法を、情報セキュリティ委員会等に諮り、承認を得る。</p> <p>手順3 事務局は、情報資産の洗い出しに関する文書を作成し、これまでに作成してきた対象範囲表(様式4)、情報資産洗い出し対象設定表(様式5)とともに関係する情報資産管理者に配付し、洗い出しの作業と情報資産台帳(様式6)の作成を要請する。</p> <p>手順4 情報資産管理者は、作業量に応じて、課室における情報資産洗い出し及び情報資産台帳(様式6)の作成に係る作業分担を行う。</p>	
分析・評価シート	情報資産台帳(様式6)
操作マニュアル目次	なし

3.2.4.1 情報資産の洗い出しに関する項目の決定

手順1	実施主体：事務局
------------	----------

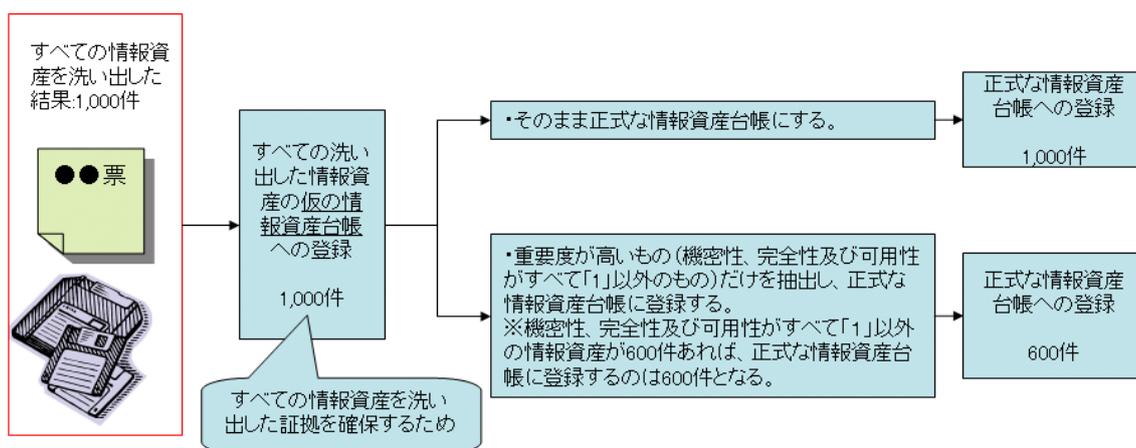
事務局は、情報資産の洗い出しに関する項目を決定する。情報資産の洗い出しに関する項目は、情報資産台帳(様式6)の必須項目を基に設定し、仮の情報資産台帳(様式6)に登録を行う。任意項目の取捨選択については、事務局が、どの程度詳細に情報資産の管理を行うかどうかを検討した上で決定する。なお、仮の情報資産台帳(様式6)に関する項目等は、後述の「3.2.5 情報資産台帳の作成」(63頁)を参照する。

3.2.4.2 情報資産の価値である重要度による抽出に関する検討

情報資産台帳(様式6)の作成に当たっては、情報資産台帳の項目に基づき、対象範囲の情報資産をすべて洗い出した結果を仮の情報資産台帳(様式6)に登録し、それをそのまま正式な情報資産台帳(様式6)とする場合と、仮の情報資産台帳(様式6)に登録した情報資産をその価値である重要度を基に抽出し、正式な情報資産台帳(様式6)を作成する方法が存在する。仮の情報資産台帳(様式6)を作成する趣旨は、情報資産を洗い出した証拠を確保することにある。

本来は、今後の情報セキュリティ対策を重点的に進めるためにも、仮の情報資産台帳(様式6)に登録した情報資産の中から重要度の高いものを抽出した上で正式な情報資産台帳(様式6)を作成することが望ましい。事務局は、この2つの方法のどちらを選択するか検討する必要がある。

図表3-7 情報資産台帳(様式6)の登録に関する2つの方法



すべての情報資産の洗い出しを行うとしても不要な情報資産まで仮の情報資産台帳(様式6)に登録すべきではない。例えば、不要な複製文書があれば、細かく裁断等を行い廃棄し、不要なフロッピーディスク等があれば破碎処理などの処分を行うべきである。

3.2.4.3 不要な情報資産の処分又は回収等の明確化

事務局は、情報資産の洗い出しの過程で、業務上利用しない、又は保管不要な情報資産や、職員個人が保有する必要のない情報資産が発見された場合の処分・回収等の際の留意事項を明確にする。

図表 3-8 不要な情報資産の処分の留意事項

項目	実施内容
処分	<ul style="list-style-type: none"> 不要な情報資産は、廃棄等の処分を行う。 個人情報等が記録されている電磁的記録媒体等の情報資産を利用しない場合は、情報を消去した後に廃棄等の処分を行う。
回収	<ul style="list-style-type: none"> USBメモリ等の電磁的記録媒体を職員が独占的に保有している場合は、当該媒体を回収し、所定の場所に保管する。
パソコンからの情報消去	<ul style="list-style-type: none"> 職員が利用しているパソコンに記録している個人情報等の中で、業務に利用しないものは消去する。必要な場合は、ファイルサーバに格納した上でパソコン上の情報は消去する。今後は、一時的に利用する電子文書等以外は、すべてファイルサーバに格納するようにする。 ファイルサーバを利用していない場合は、バックアップとして、電磁的記録媒体を利用することもある。このような場合は、課室（組織）で媒体を管理するようにし、職員個人が機の引き出し等で保管することは極力避ける。また、定期的にこれらの電磁的記録媒体の保有本数を点検する。

ここがポイント 情報資産の洗い出しと不要な情報資産の処分等の作業関係

情報資産の洗い出し作業時に、業務利用又は保存義務の必要がない不要な情報資産であることが判明すれば、処分作業も並行的に行うことができる。

参考 ファイルサーバの容量の限界

ファイルサーバが利用されていても、各課室に割り当てられた領域が少なく、さらに容量の増設をしようとも予算措置が困難な場合もあると思われる。このような場合は、課室として、電磁的記録媒体や外付け磁気ディスク装置を利用することも考えられる。これは本来推奨すべき方法ではないが、実際に使用している場合には、以下の3点の対策を行う必要がある。

- 電磁的記録媒体の場合、職員個人に管理させるのではなく、前述のとおり、課室（組織）で管理する。
- 外付け磁気ディスク装置の場合、セキュリティワイヤが取り付けられる製品を選定する。
- ファイルサーバに割り当てられた領域に保存している情報のうち不要なものは、定期的に削除するようにする。このようにしないと、不要な情報をいつまでも残置することとなり、無駄にサーバの容量を使用することになる。

参考 情報資産の洗い出しによる副次的効果

情報資産台帳(様式6)の作成の副次的効果として、不要な文書等の処分が行われ、執務室内の文書、電磁的記録媒体、不要な電子データ等の整理整頓が進む効果もある。また、職員の誰も知らない古い文書等で埋没していた個人情報が発見されることもある。

3.2.4.4 情報資産の分類の表示方法の検討

情報資産の分類の表示とは、文書の表紙や電磁的記録媒体のレーベル面に、機密性のレベル表示のラベル等を貼付することである。

情報資産台帳(様式6)を作成した後、当該台帳に記載された情報資産の機密性を基に、文書や電磁的記録媒体に関する利用制限、又はアクセス制限を確保するため、情報資産の分類の表示方法を明確にしておく必要がある。

そこで、庁内の情報資産の取扱いを統一化するため、事務局において、表示方法の素案を作成し、情報セキュリティ委員会等で決定しておく必要がある。

分類の表示の単位は、ファイリング単位、文書1枚単位など、組織の運用の実情を勘案して、職員に情報資産毎の機密性が分かるような単位とする。

地方公共団体において、「文書管理規程」等による既に表示単位が定められている場合は、これに拠ることとしてもよい。

なお、電磁的記録媒体の中に複数の電子データが記録されている場合は、最も高い機密性に依じて分類の表示をする。

また、ハードディスク等内部記憶装置に記録されている電子データについては、ソフトウェア又は情報システムでアクセス制御を行い機密性を確保するため、情報資産の分類の表示の対象外とする。

ここがポイント 保管場所(位置)による情報資産の分類

文書や電磁的記録媒体に個別に情報資産の分類の表示をすることは、かなりの労力を要する。そこで、個々の文書や電磁的記録媒体に直接情報資産の分類の表示をすることが困難な場合は、機密性レベルが一目で識別できるようにロッカーやキャビネットにマーキングするなど、機密性が異なる情報資産の保管場所(位置)を設定し、文書等を該当の場所(位置)に保管することも一案である。

3.2.4.5 情報資産の重要度による抽出及び情報資産の分類の表示方法に関する情報セキュリティ委員会等の承認

手順2	実施主体：事務局
-----	----------

(1) 情報資産の重要度による抽出について

事務局は、情報資産の重要度による抽出するか否かを、情報セキュリティ委員会等に諮り、承認を得る。重要度による抽出を行うことを選択した場合は、この後の作業工程であるリスク分析・評価の作業負担の軽減が図れることになる。

(2) 情報資産の分類の表示方法について

事務局は、情報資産の分類の表示方法についても、情報セキュリティ委員会等に諮り、承認を得る。これによって、庁内の情報資産の取扱いを統一的に行えるようになる。

3.2.4.6 情報資産洗い出しに関する資料の配付と情報資産管理者への実施要請

手順3	実施主体：事務局
-----	----------

事務局は、以下の資料を情報資産管理者に配付し、情報資産の洗い出しと情報資産台帳(様式6)の作成を要請する。

- (ア) 対象範囲表(様式4)
- (イ) 情報資産洗い出し対象設定表(様式5)
- (ウ) 情報資産の洗い出しの方法に関する文書

上記2つの表以外に、実際の情報資産洗い出しに作業に関連する事項を文書で情報資産管理者に通知する必要がある。

- ア 仮の情報資産台帳(様式6)の項目
- イ 情報資産の重要度による抽出の有無
- ウ 不要な情報資産の処分等の方法
- エ 情報資産の分類の表示方法

例を示せば、以下のとおり。

図表3-9 情報資産の洗い出しの方法に関する文書の記載事項例

ア 仮の情報資産台帳(様式6)の項目	仮の情報資産台帳(様式6)に記載する明細項目は、以下のとおりとする。 ・必須項目 ・任意項目のうち、情報資産の利用範囲、個人情報記録の有無
イ 情報資産の重要度による抽出の有	仮の情報資産台帳(様式6)には、対象とする情報資産をすべて登録する。ただし、正式な情報資産台帳(様式6)に登録す

無	る情報資産は、資産重要度(機密性、完全性及び可用性)の値が、事務局で決定した値以上のものを抽出して行う。
ウ 不要な情報資産の処分等の方法	<p>情報資産の洗い出し作業において、不要と判断した情報資産等がある場合は、以下の手順を進めること。</p> <ul style="list-style-type: none"> ・文書、電磁的記録媒体等は、〇〇課で一括廃棄処分とする。 ・パソコン等の情報機器については、〇〇課に連絡し処分方法等を協議する。 <p>また、職員用パソコンにデータが保存されている場合には以下の手順を進めること。</p> <ul style="list-style-type: none"> ・業務上必要と判断したデータは、各ファイルサーバに移管する。 ・業務上不要と判断したデータは、各自で削除する。
エ 情報資産の分類の表示方法	<p>正式な情報資産台帳(様式6)作成後の文書及び電磁的記録媒体については、以下の分類の表示を行うこと。</p> <ul style="list-style-type: none"> ・文書(機密区分3)の情報資産格納場所(キャビネット棚)に「S」と表示する。 ・電磁的記録媒体(機密区分3)には、媒体のレーベル面に「S」とラベルシールを貼付する。 <p>なお、機密区分3以外には特段の表示は不要とする。</p>

3.2.4.7 情報資産の洗い出し及び情報資産台帳(様式6)の作成に関する作業分担

手順4	実施主体：情報資産管理者
-----	--------------

情報資産の洗い出し及び情報資産台帳(様式6)の作成の作業は、対象範囲の課室で実施するが、ある程度作業量が多いことから、課室内で分担して行うことが必要である。情報資産管理者においては、必要に応じ、例えば情報資産の洗い出しについては各課室の職員全員が協力して実施し、情報資産台帳(様式6)への登録については、業務に精通した職員が実施するなどの方法を採用することが考えられる。

なお、正式な情報資産台帳(様式6)の作成は、仮の情報資産台帳(様式6)に登録されているデータを利用することとなるため、実際の作業上は、情報資産の洗い出しとほぼ同時に正式な情報資産台帳(様式6)の作成も終了していることになる。

3.2.5 情報資産台帳の作成

ステップ (第3章-4)	
<p><作業の概要></p> <p>手順 情報資産管理者が主導して、情報資産台帳(様式6)を作成する。</p>	
分析・評価シート	情報資産台帳(様式6)
操作マニュアル目次	3.1 情報資産台帳(様式6)の作成

3.2.5.1 情報資産台帳(様式6)のレイアウト

レイアウトは、以下のとおりである。

ヘッダ	課室名	市民課			← ヘッダ項目						
	調査者	総務次郎	調査完了日	平成21年2月10日							
	保管・設置場所	本庁舎1階執務室									
	情報資産の種類	設置型ハードウェア									
	情報資産グループ(任意)										
明細項目	必須項目		資産重要度評価と最高値			任意項目					
	番号	個別の情報資産名称	数量	3	2	1	収納場所	情報資産の利用範囲	保存期限	個人情報記録の有無	備考
				機密性	完全性	可用性					
	1	住民記録システムの端末	2	3	2	1	市民課職員				6万人の住民記録を扱う端末
2	公的個人認証サービス受付窓口端末	1	3	2	1	市民課職員					

3.2.5.2 情報資産台帳(様式6)作成

手順	実施主体：情報資産管理者
-----------	--------------

情報資産管理者が主導し、情報資産洗い出しに関連する資料(仮の情報資産台帳(様式6))を基に、情報資産台帳(様式6)を作成する。もし、情報資産の価値である重要度で抽出する方法を採用した場合は(「3.2.4.2 情報資産の価値である重要度による抽出に関する検討」参照)、正式な情報資産台帳(様式6)を別途作成することになる。

情報資産台帳(様式6)の項目は、ヘッダ項目と明細項目により構成されており、さらに必須項目と任意項目に分けている。必須項目とは、情報資産台帳(様式6)として利用する場合に最低限必要な項目(調査者、調査完了日、番号、個別の情報資産名称、数量)と詳細リスク分析・評価に利用する項目(課室名、保管・設置場所、情報資産の種類、資産重要度評価と最高値)である。任意項目とは、それ以外の項目である。

情報資産台帳(様式6)は、情報資産の洗い出し対象とする課室別、保管・設置場所別、情報資産の種類別、情報資産グループ別に作成する。ただし、情報資産の種類別(文書、電磁的記録媒体等)までを必須とし、情報資産グループ別の作成については任意とする。なお、情報資産台帳の作成例は、「付録1：情報資産台帳サンプル」を参照のこと。

ここがポイント 情報資産台帳(様式6)の作成シート枚数

情報資産台帳は、課室×保管・設置場所×情報資産の種類×情報資産グループの乗数分作成する必要がある。例えば、対象課室が1、保管・設置場所が2、情報資産の種類が5、情報資産グループが10である場合、 $1 \times 2 \times 5 \times 10 = 100$ 枚(シート)作成することになる。情報資産グループ別に作成しない場合は、 $1 \times 2 \times 5 = 10$ 枚(シート)の作成となる。

(1) 情報資産台帳(様式6)の作成

ア ヘッダ項目

情報資産台帳(様式6)のヘッダ項目は、以下のとおりである。

ヘッダ	課室名	市民課		
	調査者	総務太郎	調査完了日	平成21年2月10日
	保管・設置場所	本庁舎1階執務室		
	情報資産の種類	設置型ハードウェア		
	情報資産グループ(任意)			

(ア) 課室名(必須)

情報資産を管理している課室名を入力する。

(イ) 調査者、調査完了日(必須)

情報資産台帳(様式6)作成後における台帳内容の誤りの原因や疑問点等を検証できるように、情報資産の調査者名を入力する。

調査完了日は、対象範囲の情報資産について調査が完了した年月日とする。

(ウ) 保管・設置場所(必須)

情報資産(文書、電磁的記録媒体、電子データ、設置型ハードウェア、移動型ハードウェア)を保管又は設置している場所(階数、部屋名等)を入力する。名称は、実際に情報資産を利用する職員が分かるように、「1階執務室」、「2階東南のトイレの隣の書庫」等具体的に入力する。

- a 文書、電磁的記録媒体、設置型ハードウェア、移動型ハードウェアの場合
 情報資産の保管・設置場所を入力する。職員が場所を特定できる名称で入力する。以下に例を示す。

図表 3-10 保管・設置場所の入力例

情報資産	保管・設置場所の例
文書、電磁的記録媒体、設置型ハードウェア、移動型ハードウェアの保管・設置場所	本庁舎〇〇課執務室 〇〇出張所 電子計算機室 書庫（2階東南のトイレの隣）

保管・設置場所の入力は、「〇〇室」などの入力にとどめ、キャビネット等の具体的な収納場所は、別途、収納場所として記録する。

※後述の「ウ. 明細項目(任意項目)」(80 頁)で説明する。

- b 電子データの場合

電子データの保管場所を特定することは大変困難である。なぜなら、その格納場所がシステム構成によって分散している場合などもあるためである。そのため、電子データの保管場所は、便宜上、対象とする電子データを使用するソフトウェアや情報システムとし、その名称を入力する。

なお、電磁的記録媒体に保存されている電子データに関しては、電磁的記録媒体自体を情報資産として台帳に入力するため、電子データとそれが保存されている電磁的記録媒体双方を情報資産台帳(様式6)に二重に入力しないように注意する必要がある。以下に例を示す。

図表 3-11 電子データの保管・設置場所の入力例

情報資産	保管・設置場所の例
電子データの保管・設置場所	<ul style="list-style-type: none"> ・情報系システム ・文書管理システム ・ファイルサーバシステム ・住民記録システム ・国民健康保険システム ・土木工事積算システム

- c 外部委託先に情報資産を移送している場合（外部保管等を含む）

外部委託先に情報資産を移送している場合は、当該情報資産の所在が分かる範囲で、外部委託先の名称及び保管場所を入力する。

外部委託先の入力の例は、以下のようになる。

図表 3-12 外部委託先の保管・設置場所の入力例

外部委託等のケース	保管・設置場所の例
業務委託により、個人情報等が記録された文書や電磁的記録媒体を委託先に移送している場合	「〇〇会社の執務室」
庁舎外にサーバ等のハードウェアを設置している場合	「〇〇会社データセンタ」
A S P ・ S a a S を利用している場合	「〇〇会社の〇〇 S a a S」
文書や電磁的記録媒体を保管業者に預けている場合	「〇〇会社の〇号棟倉庫」

(エ) 情報資産の種類(必須)

以下の情報資産から選択する。

図表 3-13 情報資産の種類を選択肢

<ul style="list-style-type: none"> ・ 文書 ・ 電磁的記録媒体 ・ 電子データ ・ 設置型ハードウェア ・ 移動型ハードウェア
--

(オ) 情報資産グループ(任意)

本項目は、情報資産の利用の形態や保管の形態に応じて、情報資産の種類をさらに細分化して実施する場合に使用するものである。情報資産グループを設定することにより、設定しない場合に比較してより具体的な対策を行うことができるが、(広義の) 詳細リスク分析・評価の作業負担が大きくなることに留意する必要がある。本書では任意項目として扱う。

情報資産グループの例としては、以下のようなものが挙げられる。

図表 3-14 情報資産グループの入力例(掲載件数: 28件)

情報資産の種類	情報資産グループの例
文書	<ul style="list-style-type: none"> ・ 氏名、住所、性別、年齢、家族構成を記録した文書 ・ 納税情報等の住民の重要な財産情報を記録した文書

	<ul style="list-style-type: none"> ・公開前の財政情報等を記録した文書 ・庁内で利用する文書
電磁的記録媒体	<ul style="list-style-type: none"> ・氏名、住所、性別、年齢、家族構成の記録を含んだ電磁的記録媒体 ・納税情報等の住民の重要な財産情報を記録した電磁的記録媒体 ・公開前の財政情報等を記録した電磁的記録媒体 ・システム関係のログを記録した電磁的記録媒体 ・CD等のソフトウェアの原本 ・バックアップに利用した電磁的記録媒体 ・利用していない電磁的記録媒体
電子データ	<ul style="list-style-type: none"> ・個人情報等を記録した電子データ ・オペレーティングシステム等のソフトウェア ・団体に開発・保守・運用している情報システム ・公開前の財政情報等を記録した電子データ ・庁内で利用する電子データ ・文書管理システムの電子文書
設置型 ハードウェア	<ul style="list-style-type: none"> ・サーバ、外付け磁気ディスク装置 ・ルータ等の通信機器 ・デスクトップパソコン一式 ・プリンタ、ファクシミリ、コピー機、スキャナー ・利用していない設置型のハードウェア ・その他の設置型のハードウェア(封入封緘機等)
移動型 ハードウェア	<ul style="list-style-type: none"> ・ノートパソコン一式 ・携帯電話・PHS ・デジタルカメラ、ICレコーダ等の録音、録画機器 ・利用していない移動型のハードウェア ・その他の移動型のハードウェア(PDA等)

イ 明細項目(必須項目)

情報資産台帳(様式6)の明細項目(必須項目)は、以下のとおりである。

明細項目	必須項目					
	番号	個別の情報資産名称	数量	資産重要度評価と最高値		
				3	2	1
				機密性	完全性	可用性
1	住民記録システムの端末	2	3	2	1	
2	公的個人認証サービス受付窓口端末	1	3	2	1	

(ア) 番号

情報資産の区別ができるように算用数字を入力する。

(イ) 個別の情報資産名称

情報資産に記載、記録された情報等の内容からふさわしい名称を登録する。
以下の点に注意して登録する。

a 情報資産名称の付与方法について

個別の情報資産の登録は、課室内における情報資産の管理範囲を明確にし、資産が紛失した場合などの事件・事故の検出を正確かつ迅速に行うために必要である。したがって、最低限課室の職員が共通して認識できる名称を登録することが重要である。また、出先機関が複数ある課室で情報資産台帳(様式6)を閲覧した場合、同じ情報資産か、あるいは違うものかを判別できるよう名称を統一しておく必要がある。できれば、洗い出しを行う出先機関等下部組織において、情報資産の洗い出しに関する共通認識を持てるように、部局等上位組織又は事務局が情報資産の名称付与に関する統一的な基準を定めることが望ましい。

参考 ネーミングの例示

全庁又は部等で横断的に利用している情報資産のネーミングの付け方は、事務局又は部等が通知し、個別名称登録の混乱を極力回避する。

- ・例えば、全庁各課室で利用しているデジタルカメラであれば、「〇〇課用デジタルカメラ」とする。
- ・例えば、〇〇部で利用している〇〇申請書であれば、「〇〇部〇〇用申請書(平成20年度)綴」とする。

b 文書

文書の名称登録については、文書 1 枚単位で登録することでもよいが、文書を保存しているファイルやフォルダー単位毎に付与された名称を登録することが作業の効率的な遂行上便利である。名称登録の際は、極力各担当者が認識できる名称を利用することが望ましい。

c 電磁的記録媒体

電磁的記録媒体の記録情報について、記録情報をそれぞれ個別の情報資産名称として登録すれば重要な情報の登録漏れを防止できるが、その反面、情報資産台帳(様式 6)の更新にかなり労力を要することになる。このため、電磁的記録媒体のレーベル面等に付けた名称等を個別の情報資産名称として登録することが望ましい。

ここがポイント

電磁的記録媒体の個別の情報資産名称の登録の例

例えば、複数の情報が記録された 1 枚の CD の中で最も大量の個人情報記録されているファイルが選挙人名簿情報の場合、「選挙人名簿情報ファイル」と情報資産名称に登録する。その他、情報資産の重要度の高いファイルを基に、その名称を情報資産名称に登録する方法もある。

d 電子データ

情報資産の登録において特に注意を要するものは、常に内容が変化する電子データの登録である。電子データは、どの程度きめ細かく登録をするのかの判断が非常に難しい。あまり細分化して登録すると、情報資産台帳(様式 6)の更新等の作業が膨大になるおそれがある。

そこで、〇〇データベース、〇〇プログラムファイル、〇〇情報、〇〇課業務関係、〇〇課プロジェクト関係等の大枠で登録することが望ましい。

e 設置型ハードウェア

庁内で名付けた名称や課室で認識できる名称を登録するようにする。

f 移動型ハードウェア

設置型ハードウェアと同じ登録方法とする。

g 個別の情報資産名称の登録例

執務室等に同種の情報資産が複数ある場合(例えば、同じ業務関係の綴りが

2冊ある場合)は、「〇〇綴」とする。

個別の情報資産名称登録の例としては、以下のようなものが挙げられる。

図表 3-15 個別情報資産の名称登録例

情報資産の種類	個別の情報資産名称
文書	<ul style="list-style-type: none"> ・住民票交付綴 ・選挙人名簿管理綴 ・〇〇地区道路拡幅工事関係綴 ・ケースワーカ訪問履歴
電磁的記録媒体	<ul style="list-style-type: none"> ・オペレーティングシステムのソフトウェア原本(CD) ・市民税システム日次バックアップ(DAT) ・選挙人名簿データベースバックアップ(MO)
電子データ	<ul style="list-style-type: none"> ・介護保険情報データベース ・市民税情報データベース ・軽自動車税情報ファイル ・職員人事情報ファイル ・(ファイルサーバの)〇〇課フォルダー ・(文書管理システムの)〇〇課事業計画 ・〇〇SaaSのデータ
設置型ハードウェア	<ul style="list-style-type: none"> ・国民健康保険システムサーバ ・ファイルサーバ ・メールサーバ ・福祉課用プリンタ ・情報系システムの端末(デスクトップパソコン) ・住民記録システムの端末(デスクトップパソコン) ・本庁舎用4階レイヤ3スイッチ ・建設課NAS型磁気ディスク装置 ・4階ファクシミリ(〇〇社製)
移動型ハードウェア	<ul style="list-style-type: none"> ・情報系システムの端末(ノートパソコン) ・基幹系システムの端末(ノートパソコン) ・市民課デジタルカメラ ・議会事務局ICレコーダ

- h 保管・設置場所、情報資産の種類及び個別の情報資産名称間の関連付けの例
 以下に、前述した情報資産台帳の項目の中、保管・設置場所、情報資産の種類及び個別の情報資産名称間の関連付けを整理するため、情報システム管

理者、情報セキュリティ管理者の権限別の情報資産名称の登録例を示す。

図表 3-16 情報システム管理者の例(図表 1-14 を基に作成)

保管・設置場所の例	情報資産の種類	個別の情報資産名称の例
情報システム課 執務室	文書	・〇〇システム開発テスト結果綴
	電磁的記録媒体	・〇〇システム開発のテスト結果(MO)
	設置型ハードウェア	・基幹系システムの開発用端末(デスクトップパソコン)
	移動型ハードウェア	・情報系システムの端末(ノートパソコン)
サーバ室	文書	・〇〇システム運用手順書綴
	電磁的記録媒体	・ファイルサーバシステム差分バックアップ(DAT) ・〇〇ソフトウェアCD(原本)
	設置型ハードウェア	・メールサーバ(〇〇社製) ・ファイルサーバ(〇〇社製) ・ウイルス監視サーバ(〇〇社製) ・基幹系システム(〇〇社製) ・大型レザープリンタ(〇〇社製) ・レイヤ3スイッチ(〇〇社製) ・インターネット接続用ルータ(〇〇社製) ・ファイアウォール機器(〇〇社製)
	移動型ハードウェア	・情報系システムの監視端末(ノートパソコン)
ファイルサーバシステム	電子データ	・市民課フォルダー ・総務課フォルダー ・建設課フォルダー ・(すべての構成が同じ時には) 課室割り当てフォルダー
文書管理システム		・市民課フォルダー ・総務課フォルダー ・建設課フォルダー ・(すべての構成が同じ時には) 課室割り当てフォルダー

情報系システム		<ul style="list-style-type: none"> ・オペレーティングシステム(L i n u x 等) ・メールサーバソフトウェア(S e n d m a i l 等) ・D N S ¹⁶ソフトウェア(B I N D ¹⁷ 等) ・W e b サーバソフトウェア(A p a c h e 等) ・ファイルサーバソフトウェア(〇〇社製) ・〇〇イントラネットシステム ・〇〇グループウェア ・〇〇パスワードファイル ・〇〇ログファイル メールサーバの送受信内容(※ I M A P ¹⁸を利用している場合)
住民記録システム		<ul style="list-style-type: none"> ・住民記録データベース ・〇〇データベースソフトウェア(〇〇社製) ・〇〇オペレーティングシステム(〇〇社製) ・住民記録システムプログラムファイル
国民健康保険システム		<ul style="list-style-type: none"> ・国民健康保険データベース ・〇〇データベースソフトウェア(〇〇社製) ・〇〇オペレーティングシステム(〇〇社製) ・国民健康保険システムプログラムファイル
人事給与システム		<ul style="list-style-type: none"> ・職員人事情報データベース ・職員給与マスタファイル ・〇〇データベースソフトウェア(〇〇社製)

¹⁶ DNS:Domain Name System の略。

¹⁷ BIND:Berkeley Internet Name Domain の略。

¹⁸ IMAP:Internet Message Access Protocol の略。

		○社製) ・○○オペレーティングシステム(○ ○社製) ・人事給与システムプログラムファイ ル
外部委託(○○社○ ○号棟倉庫)	電磁的記録媒体	・国民健康保険データベース週次バッ クアップ(DAT)

図表 3-17 情報セキュリティ管理者の例(図表 1-14 を基に作成)

保管・設置場所の例	情報資産の種類	個別の情報資産名称の例
市民課 執務室	文書	<ul style="list-style-type: none"> ・住民票発行綴 ・印鑑証明書発行綴
	電磁的記録媒体	<ul style="list-style-type: none"> ・戸籍情報バックアップ(DAT)
	設置型ハードウェア	<ul style="list-style-type: none"> ・情報系システムの端末(デスクトップパソコン) ・戸籍情報システムの端末(デスクトップパソコン) ・住民記録システムの端末(デスクトップパソコン) ・住民基本台帳ネットワークシステムの端末(デスクトップパソコン) ・公的個人認証サービス受付窓口の端末(デスクトップパソコン) ・住民票発行プリンタ
	移動型ハードウェア	<ul style="list-style-type: none"> ・情報系システムの端末(ノートパソコン) ・市民課 ICレコーダ
ファイルサーバシステムの市民課フォルダー	電子データ	<p>(例:フォルダー単位)</p> <ul style="list-style-type: none"> ・市民課 外部団体との連絡記録 ・市民課 会議召集記録 ・市民課 保護司との連絡調整記録 ・市民課 各職員勤務簿様式 ・市民課 住民票申請様式 ・市民課 印鑑証明申請様式 ・市民課 包括監査報告記録
文書管理システムの市民課フォルダー		<ul style="list-style-type: none"> ・市民課 業務要領 ・市民課 年間事業計画
職員用に付与された情報系システムのパソコンの電子データ		<p>フォルダーの例</p> <ul style="list-style-type: none"> ・市民課勤務データ <p>※ もし課室として共有している重要なデータが格納されていれば登録する。</p>

(ウ) 数量

情報資産の数量は、情報資産の紛失・盗難時の検出や、情報漏えい時におけるデータ件数の公開を求められたとき、迅速な対応を行うに当たって必要となる。

情報資産の種類別の数量の入力方法は以下のとおりである。

なお、個別の情報資産における最低の数量は「1」とする。

a 文書

- ・ 入力単位

「冊」又は「枚」

- ・ 入力方法

同種類の業務関連のファイルが複数ある場合（例：No.1～No.3）は、「3冊」と入力する。

注）連続して管理している文書を1冊（枚）と入力すると、実際の数量と異なる数量で管理されているため、紛失時の検出が遅れる可能性がある。

b 電磁的記録媒体

- ・ 入力単位

「個」又は「枚」

- ・ 入力方法

同種類の業務関連の電磁的記録媒体が複数ある場合（例：No.1～No.4）は、「4個」と入力する。

注1）連続して管理している電磁的記録媒体を1個（枚）と入力すると、実際の数量と異なる数量で管理されているため、紛失時の検出が遅れる可能性がある。

注2）電磁的記録媒体に記録されている電子データの件数を入力する場合には、任意項目の備考欄を活用するとよい。

図表3-18 備考欄活用の例

事例	備考欄
電磁的記録媒体に選挙人名簿が4万人分記録されている場合	「〇〇選挙人名簿 4万件（概数）」

c 電子データ

- ・ 入力単位

「件」

- ・ 入力方法
サーバ、パソコン内の記憶装置にあるデータ件数や情報システムに入力されている主要なデータ件数を概数で入力する。

図表 3-19 電子データの概数登録の例

事例	数量
個別の情報資産名称(選挙人名簿データベース) 40,114 件の場合	「〇〇選挙人名簿データベース 4 万件 (概数)」

注：数量の把握が困難な場合

保管・設置場所が外部委託先、ファイルサーバシステムのフォルター名やメールサーバのIMAPのデータ件数、又はログファイル、〇〇ソフトウェアの場合は、件数の把握が困難なため、「1」とすることでもよい。

d 設置型ハードウェア

- ・ 入力単位
「台」
- ・ 入力方法
同じ業務で使用するハードウェアが10台ある場合は、「10台」と入力する。
ハードウェアで制御装置、磁気ディスク装置等を一体的に構成しているハードウェア群は、「1台」として入力する。
デスクトップパソコン等で、マウス、キーボード等を接続している場合は、マウス、キーボード等を含め全部で「1台」として入力する。

ここがポイント 登録漏れを防ぐ必要のあるハードウェア

【個人情報保存している機器】

ハードウェアで最も大切な機器は、個人情報等を保存するための記憶装置を内蔵しているサーバやパソコンである。また、ネットワークで利用しているルータ、スイッチングハブ、レイヤ3スイッチ等の通信機器である。これらは漏れなく登録する必要がある。

【ケーブル関係の対策】

電源ケーブル、通信ケーブルの情報資産台帳(様式6)の登録に関して、既設のケーブルカバーに覆われている場合、フリーアクセスの場合、天井上に敷設している場合等においてケーブル本数を把握するのは、壁中、床下等に

配線がされていて探索に時間がかかる、また、配線が分岐している等のため、事実上困難である。したがって、電源ケーブル、通信ケーブルは、接続図、配置図、構成図等で管理し、情報資産台帳（様式6）に登録することが現実的である。

- e 移動型ハードウェア
 - ・ 入力単位
「台」
 - ・ 入力方法
設置型ハードウェアと同じ登録方法とする。

(エ) 資産重要度評価と最高値

情報資産台帳(様式6)に登録する重要度は、以下の数字から選択する。最高値とは、情報資産台帳(様式6)の明細の機密性、完全性及び可用性の列の最高の値を意味する。例えば、法令等により保護が求められている情報資産については、当該法令に応じて機密性等の重要度を決定する。また、地方公共団体における文書管理規程、規則等で秘密文書等として管理している情報については、その規定内容に応じて機密性等の重要度を決定する。

図表3-20 重要度評価における入力数値

情報資産の重要度（情報資産価値）	機密性	完全性	可用性
重要度3（高）	3	2	2
重要度2（中）	2		
重要度1（低）	1	1	1

情報資産の重要度は、機密性、完全性及び可用性の3側面に脅威を受け被害が及んだとき、住民に対する行政への信頼・信用や地方公共団体の業務に与える影響の大きさ等を数値化したものである。その影響の大きさをレベルに応じて分類したものが重要度評価基準である。重要度の評価は、情報資産の3側面である機密性、完全性及び可用性に基づいて行うことになるが、対象となる情報資産中文書、電磁的記録媒体、電子データに関しては、記録されている情報自体の内容及び性質に着目して実施する。設置型ハードウェア及び移動型ハードウェアに関しては、情報資産の利用面の特性(例：機器が故障で利用できない場合に生じる影響、部品調達に時間を要する場合に生じる影響、機器制御のファームウェア¹⁹の不具合で生じる影響等)に着目して実施する。

情報資産の重要度は、詳細リスク分析・評価を実施する際の一要素になることから、情報資産台帳(様式6)の作成に当たって情報資産の重要度評価を行う必要がある。本書では、ポリシーガイドライン²⁰の「分類」と「分類基準」との整合性を確保し、「図表3-21 情報資産の重要度評価基準」に示す重要度評価基準を用いて評価を行うこととする。本図表において、「分類」は重要度を表し、「分類基準」が重要度の定義を表す。

¹⁹ ハードウェアの基本的な制御を行うために機器に組み込まれたソフトウェア。

²⁰ 分類と分類基準は、ポリシーガイドライン(33頁～34頁)参照。

図表 3-2-1 情報資産の重要度評価基準

分類	分類基準	分類ごとに想定されるリスクの例示	被害の例示
機密性 3	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	<ul style="list-style-type: none"> ・文書、電磁的記録媒体内の電子データ、サーバ等の電子データの中の個人情報情報の漏えい等が想定される。 ・設置型ハードウェア又は移動型ハードウェアについて、不正利用による個人情報情報の漏えい等が想定される。 	<ul style="list-style-type: none"> ・健康診断情報、ケースワーカーによる訪問履歴、税滞納情報、図書館の本貸出履歴、児童・生徒の成績情報・評価情報、職員の人事考課情報等が漏えいした場合
機密性 2	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	<ul style="list-style-type: none"> ・文書、電磁的記録媒体内の電子データ、サーバ等の電子データの中の技術情報、公表前情報の漏えい等が想定される。 ・設置型ハードウェア又は移動型ハードウェアの場合、不正利用による技術情報、公表前情報の漏えい等が想定される。 	<ul style="list-style-type: none"> ・情報システムの脆弱性を含んだ技術情報、公表前の作成中の財政情報、入札公告前に入札情報等が漏えいした場合
機密性 1	機密性 2 又は機密性 3 の情報資産以外の情報資産	<ul style="list-style-type: none"> ・機密性 2 又は機密性 3 以外の情報資産の漏えい等が想定される。 	<ul style="list-style-type: none"> ・公表物、住民票交付申請書の様式等
完全性 2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される、又は行政事務の適確な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報資産	<ul style="list-style-type: none"> ・文書、電磁的記録媒体内の電子データ、サーバ等の電子データの中で、個人情報、公表情報が改ざん等されたことで、住民の権利が侵害される、又は行政事務の適確な遂行に支障を及ぼす場合が想定される。 ・ソフトウェアが改ざん等されたことで、住民の権利が侵害される、又は行政事務の適確な遂行に支障を及ぼす場合が想定される。 ・設置型ハードウェア又は移動型ハードウェアの場合、情報機器の制御内容の設定が改ざん等されたことで、住民の権利が侵害される、又は行政事務の 	<ul style="list-style-type: none"> ・市報、納税通知書、水道料金請求金額、児童・生徒の成績情報・試験結果、ホームページ、情報システムのソースコード等に誤びゅうが生じた場合や改ざんされた場合

		適確な遂行に支障を及ぼす場合が想定される。	
完全性1	完全性2 情報資産以外の情報資産	・完全性2の情報資産以外が情報資産改ざんされた場合が想定される。	・庁内で利用する資料、様式等で誤字等の誤びゅうが発生した場合
可用性2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される、又は行政事務の安定的な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報資産	・情報資産が利用できないことで、住民の権利が侵害される、又は行政事務の安定的な遂行に支障を及ぼす場合が想定される。	・情報システムが緊急停止した場合 ・データベースを誤消去した場合 ・税滞納者管理簿、介護保険業務綴を紛失した場合
可用性1	可用性2の情報資産以外の情報資産	・可用性2の情報資産以外の情報資産が利用できない場合が想定される。	・バックアップデータを誤消去した場合 ・複写された文書を誤裁断した場合

注:滅失・紛失と情報資産の3側面の関係

滅失・紛失は、情報資産の正確性の確保の必要から「完全性」に位置付ける場合があるが、本書では、利用時に文書、電磁的記録媒体等が発見できないことで使用できない状態としていることから、「可用性」に位置づけている。

ウ 明細項目(任意項目)

情報資産台帳(様式6)の明細項目(任意項目)は、以下のとおりである。

任意項目				
収納場所	情報資産の利用範囲	保存期限	個人情報の記録の有無	備考
	市民課職員			6万人の住民記録を扱う端末
	市民課職員			

(ア) 収納場所

情報資産(文書、電磁的記録媒体、移動型ハードウェア、設置型ハードウェア)

の収納場所の登録を行う。以下に例を示す。

図表 3-22 収納場所の入力例

<ul style="list-style-type: none"> ・ロッカー ・机の上 ・机の周辺 ・書庫 ・書棚 ・壁等の側面装着 ・フロア設置 等
--

- ・電子データは、ソフトウェア(又は情報システム)で管理しているため、収納場所の登録は不要とする。
- ・外部委託先の情報資産についても、具体的な収納場所までは特定できないため、不要とする。

(イ) 情報資産の利用範囲

電子データに関するアクセス制限と、文書、電磁的記録媒体、設置型ハードウェア及び移動型ハードウェアに関する利用制限の範囲を明確にするため、情報資産の利用範囲を登録する。情報資産の利用範囲の例としては、以下のよう
なものが挙げられる。

図表 3-23 情報資産の利用範囲の入力例

ヘッダ項目		明細項目	
保管・設置場所	情報資産の種類	個別の情報資産名称	情報資産の利用範囲
総務課執務室	文書	選挙人名簿綴	総務課職員
情報システム課執務室	電磁的記録媒体	ファイルサーバシステムの差分バックアップ(DAT)	情報システム課職員
住民記録システム	電子データ	住民記録データベース	市民課職員
本庁舎 3 階のフロア	設置型ハードウェア	コピー機(2号機)	総務課職員
庁舎内の執務室全部	移動型ハードウェア	情報系システム端末(ノートパソコン)	貸与された職員

(ウ) 保存期限

文書、電磁的記録媒体の保存期限を明確にするために登録を行う。保存期限登録の例としては、以下のようなものが挙げられる。

図表 3-24 保存期限の例

1年(以上)、3年(以上)、5年(以上)、永久、-(定めなし)等

(エ) 個人情報の記録の有無

個人情報が記録されている情報資産かどうかを区別するために登録を行う。データベースや表管理されているものを対象とする。公用車使用申請書、情報システム利用のID登録申請書等に、職員個人の氏名が記載されているようなものは除く。個人情報の記録の有無の例としては、以下のようなものが挙げられる。

図表 3-25 個人情報記録の有無の例

有り(市民情報)、有り(○課職員情報)、無し

(オ) 備考

備考欄の活用方法の例として、以下のようなものが挙げられる。特に、電磁的記録媒体については、1媒体のレーベル面の名称を登録することになるが、重要な情報が複数記録されている場合、備考欄を利用し個人情報の内容を登録することが望ましい。また、住民の個人情報、重要な財産情報(クレジットカード番号、銀行口座番号、固定資産評価額等)、その他の重要な秘密情報(建築許可に係る住居の間取りに関する情報等)などの重要な情報が記録されている場合には、備考欄を利用して情報の内容を記録しておくことが望ましい。これらは、地方公共団体において保有する重要情報を分類し、把握・管理する際に活用することもできる。

図表 3-26 備考欄の活用方法について

活用方法の例	備考の例
情報資産の用途	○○業務で利用する。
電磁的記録媒体のデータ件数の概数登録	○○情報ファイル10万件。
個人情報の項目の登録	氏名、住所、固定資産評価額
管理責任の範囲の明確化	日常の管理は情報システムを利用する課、機

	器・システム設定等の保守は情報システムを 主管する課が管理責任を負う。
外部組織から持ち込んだ情報資 産かどうかの確認	〇〇市(法人)から〇〇業務で利用するた めに持ち込んでいる。

3.2.6 情報資産台帳(様式6)の確認及び情報資産の分類の表示作業の実施

ステップ (第3章-5)	
<p><作業の概要></p> <p>手順1 情報資産管理者は、担当職員等が作成した情報資産台帳(様式6)の内容を確認する。</p> <p>手順2 情報資産管理者は、情報資産台帳(様式6)に登録した文書及び電磁的記録媒体の情報資産の分類の表示を実施する。</p>	
分析・評価シート	情報資産台帳(様式6)
操作マニュアル目次	なし

(1) 情報資産台帳(様式6)の内容確認

手順1	実施主体：情報資産管理者
------------	---------------------

課室の職員等が作業を分担して情報資産台帳(様式6)を作成した場合は、情報資産管理者がその内容を最終的に確認する。

確認すべき事項としては、以下のようなものが考えられる。

- ・情報資産の重要度評価が同じであるはずなのに、異なったものとなっていないか。
- ・保管場所が違っただけで、登録名称が同じであるはずなのに、異なったものとなっていないか。
- ・他の課室が主管している情報資産が登録されていないか。(二重登録)
- ・情報資産の登録に漏れがないか。

(2) 情報資産の分類の表示作業

手順2	実施主体：情報資産管理者
------------	---------------------

情報資産管理者が主導して、情報資産台帳(様式6)に登録した文書及び電磁的記録媒体の機密性の重要度に応じて、情報資産の分類の表示を実施する。表示作業は、事務局から示された方法に従って行う。ただし、電子データについては、情報資産の分類の表示の対象外とする。

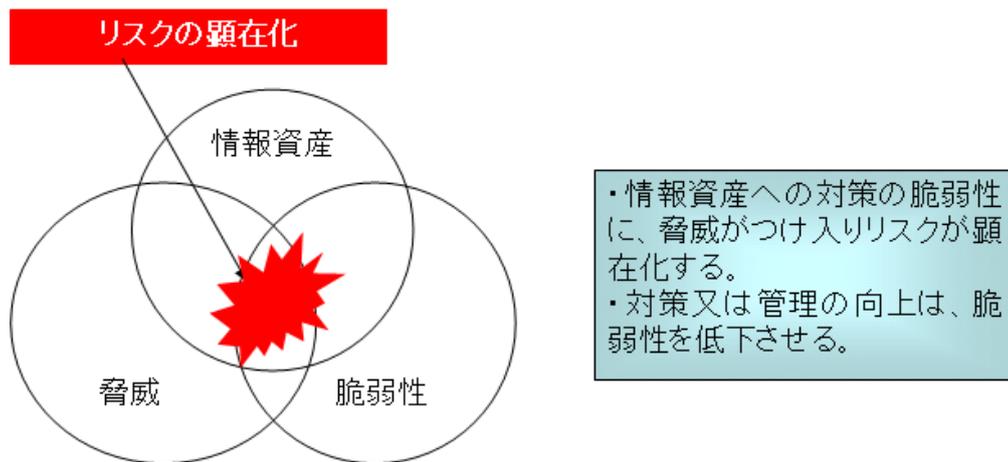
3.3 詳細リスク分析・評価の実施

3.3.1 リスクの3要素

詳細リスク分析・評価とは、リスクの3つの要素である情報資産の重要度、脅威、脆弱性が各々結びつくことで顕在化するリスク状況を分析・評価することである。脅威とは、情報資産に対して害を及ぼす、又は発生する可能性のある事象（不正アクセス、盗難、紛失、故障等）をいう。また、脆弱性とは、情報資産が脅威に対する不備、欠陥がある弱い状態を意味する。

例えば、文書、電磁的記録媒体等の情報資産に、ずさんな保管状況、パスワードの未設定等の脆弱性が潜んでいる場合、盗み見、不正アクセス等の脅威が結びつくことで、文書、電磁的記録媒体からの情報漏えい等に対するリスクが顕在化することとなる。

図表3-27 「リスクの3要素とリスクの顕在化」



3.3.2 詳細リスク分析・評価の事前作業(脅威の分析・評価)

ステップ (第3章-6)	
<p><作業の概要></p> <p>手順1 事務局は、脅威評価レベル表(様式7)の脅威の項目設定を見直す。</p> <p>手順2 事務局は、情報資産の機密性、完全性及び可用性の3側面に影響を与える脅威の発生頻度の設定を見直す。</p> <p>手順3 事務局は、リスク分析・評価項目表(様式1)のリスク分析・評価項目と、情報資産の3側面に影響を与える脅威の項目を見直す。</p>	
分析・評価シート	脅威評価レベル表(様式7) リスク分析・評価項目表(様式1)
操作マニュアル目次	3.2.1 脅威評価レベル表のレイアウト 3.2.2 脅威の分析・評価及びリスク分析・評価項目表の見直し作業

3.3.2.1 脅威の分析・評価に関する3つ要素

情報資産に対する脅威を分析・評価するためには、「①脅威の項目設定」、「②脅威の項目ごとの発生頻度」、「③リスク分析・評価項目と、情報資産の3側面(機密性、完全性及び可用性)に脅威がつけ込む発生頻度との関連付け」の3要素について検討する必要がある。

脅威の分析・評価は、詳細リスク分析・評価の一つの工程になるが、詳細リスク分析・評価シート(様式8)に、初回から各課室が脅威を特定すると、同じ執務室内にある情報資産でも、脅威の項目設定に関してバラツキが多く発生することがある。例えば、同じ執務室内において、A課のノートパソコンに対しては不正な持ち出しという脅威が特定され、他方B課のノートパソコンではなりすましによる利用という脅威が特定されることがある。このような脅威の項目設定に関するバラツキが発生すると、この後の作業工程である脆弱性の分析・評価、さらには改善計画まで対応が異なる可能性が大きくなる。

そこで、詳細リスク分析・評価に手馴れていない段階では、事務局が事前に、脅威の項目を統一的に設定する。

3.3.2.2 脅威の分析・評価の実施

(1) 脅威の項目設定

手順1	実施主体：事務局
-----	----------

事務局は、脅威評価レベル表(様式7)に設定されている15の脅威の項目以外に追加すべき脅威があれば追加し、不必要だと考える項目があれば削除する。また、必要に応じて脅威の項目内容を変更する。

脅威評価レベル表(様式7)には、脅威の項目とその発生頻度があらかじめ設定されている。脅威評価レベル表(様式7)に設定された詳細リスク分析・評価を行うための脅威の分類とその種類の例は以下のとおりである。

図表3-28 脅威の分類と種類の例

脅威の分類	脅威の種類の例
偶発的脅威	規則違反 ネットワークからの情報の流出、漏えい又は露呈 情報資産の紛失、置き忘れ又は滅失 誤廃棄、又は消し忘れ ハードウェア・回線(ケーブル)の故障又は損傷 ソフトウェアのバグ、設定ミス又はデータ誤消去
意図的脅威	情報・データの窃取又は不正複写 サーバ・ネットワークへの不正アクセス又は侵入 コンピュータウイルス感染 情報・データの改ざん又は不正消去 端末・電磁的記録媒体の盗難 機器・端末のソフトウェアへの不正設定 重要な情報資産が保管・設置されている室への侵入
環境的脅威	停電、地震、台風、洪水、火事等

脅威評価レベル表のレイアウトは、以下のとおりである。

脅威評価レベル表				
情報資産に与える影響		発生頻度の設定		
脅威の項目	機密性	完全性	可用性	
01 規則違反	2	2	2	空欄は、脅威が発生しても、情報資産に影響を与えないことを意味する。
02 ネットワークからの情報の流出、漏えい又は露呈	2			
03 情報資産の紛失、置き忘れ又は滅失	2	▼	2	発生頻度の設定は、選択肢(1、2、3)から選択する。
04 誤廃棄、又は消し忘れ		1	1	
05 ハードウェア・回線(ケーブル)の故障又は損傷		3	3	16 番に、脅威の項目を追加する場合、同じ行の発生頻度の設定(機密性、完全性、可用性)について選択肢(1、2、3)から選択する。
06 ソフトウェアのバグ、設定ミス又はデータ誤消去	3	3	3	
07 情報・データの窃取又は不正複写	2			
08 サーバ・ネットワークへの不正アクセス又は侵入	2	2	2	
09 コンピュータウイルス感染	3	3	3	
10 情報・データの改ざん又は不正消去		2		
11 端末・電磁的記録媒体の盗難	2		2	
12 機器・端末のソフトウェアへの不正設定	1	1	1	
13 重要な情報資産が保管・設置してある室への侵入			2	
14 停電・雷の災害		3	3	
15 地震・台風・洪水・火事の災害		1	1	
16				
17	16 番以降に追加する。			
18	連番の初期値は変更しない。			
19				
20				
21				
22				
23	脅威の項目を追加する場合に利用するため、空欄としている。 最大 30 項目設定することができる。			
24				
25				
26				
27				
28				
29				
30				

項目の追加、削除及び変更の例を参考までに以下に示す。

図表 3-29 脅威の項目追加例

16 番への追加の例
16 物理的な破壊活動

図表 3-30 脅威の項目削除例

削除前	02 ネットワークからの情報の流出、漏えい又は露呈
削除後	02 ※番号は削除しない。

図表 3-31 脅威の項目変更例

変更前	02 ネットワークからの情報の流出、漏えい又は露呈
変更後	02 ファイル交換ソフトウェアへのウイルス感染によるネットワークからの情報の流出

注：脅威の項目を削除、変更した場合の留意事項

脅威の項目を削除、変更した場合、リスク分析・評価項目表(様式1)のリスク分析・評価項目に関連した脅威の項目を再度選択しないと、発生頻度が未設定の状態(表示は空欄)になる。このために関連付けを再度設定する必要がある。

実施方法は、「図表 3-35 リスク分析・評価項目と脅威の関連付けの選択例」を参考にして行う。

(2) 脅威の項目ごとの発生頻度の設定

手順 2	実施主体：事務局
------	----------

脅威の項目設定後、これまでの経験や組織としての情報セキュリティ対策の状況、情報システムやネットワークの変更、業務変更や組織変更等を考慮した上で、脅威の発生頻度を検討する。本書における脅威の発生頻度の評価レベルは、以下のとおりである。²¹

²¹ I SMS ユーザーズガイド 2006 年 12 月 25 日 財団法人 日本情報処理開発協会 「表 4-11 脅威の判断基準」 25/42 頁

図表 3-3-2 脅威の発生頻度の評価レベルとその考え方

脅威発生頻度評価レベル	1	2	3
脅威の発生頻度の考え方	発生の可能性は極めて低い。	発生の可能性は低い。	発生の可能性は極めて高い。
想定する発生頻度	1年間で1回あるかないか	半年間で1回あるかないか	1か月間で1回以上

情報資産の3側面である機密性、完全性及び可用性の確保に対して、脅威がどのようなものか、また脅威の項目ごとの発生頻度を関連付けることが必要である。

情報資産の3側面につけ入る脅威と発生頻度の設定は、以下のようになる。

図表 3-3-3 情報資産の3側面に対する脅威の発生頻度設定例

情報資産に与える影響 脅威の項目	発生頻度の設定		
	機密性	完全性	可用性
02 ネットワークからの情報の流出、漏えい又は露呈	2		
03 情報資産の紛失、置き忘れ又は滅失	2		2
05 ハードウェア・回線(ケーブル)の故障又は損傷		3	3
06 ソフトウェアのバグ、設定ミス又はデータ誤消去	3	3	3

ここがポイント 空欄の意味と脅威を増やした場合の発生頻度の設定

「図表 3-3-3 情報資産の3側面に対する脅威の発生頻度設定例」において発生頻度の設定の一部が空欄となっているのは、情報資産の機密性、完全性及び可用性に関する脆弱性に、脅威がつけ入ることがない状況を表している。例えば、「ネットワークからの情報流出、漏えい又は露呈」に関しては、機密性には関係するが完全性及び可用性には関係しないため、空欄となっている。

また、脅威評価レベル表(様式7)にあらかじめ登録されている脅威の項目以外の脅威を追加した場合には、機密性、完全性及び可用性の全部か、いずれか1つ以上の発生頻度を設定する必要がある。(「図表 3-3-3 情報資産の3側面に対する脅威の発生頻度設定例」を参照のこと。)

事務局は、あらかじめ設定されている脅威の項目ごとの発生頻度の設定を必要に応じて変更する。

例えば、コンピュータウイルス感染の脅威の発生頻度が減少していると判断した

場合には、以下のとおりとなる。

図表 3-34 情報資産に対する脅威の発生頻度設定の変更例

脅威の項目	機密性	完全性	可用性
(変更前)09 コンピュータウイルス感染	3	3	3
(変更後)09 コンピュータウイルス感染	1	1	1

取組み当初の詳細リスク分析・評価の実施において、各課室が個別に発生頻度の設定を行うと、脅威の項目設定と同様にバラツキが発生することがある。例えば、同じ情報システムの機能を利用している場合や庁舎の同じ階にある課室であっても、脅威の発生頻度が異なることがある。このため、脅威の項目設定と同様に当初は事務局が行い、情報資産管理者の習熟度が上がり、詳細リスク分析・評価の方法と構造を理解した段階で、各課室で行うようにすることが望ましい。今回のリスク分析・評価ファイルは、当該ファイルを「課別」、又は「課別及び設置・保管場所別」等に分離して利用することもできるため、情報資産管理者の習熟度が上がった段階で、各課室に脅威の項目、発生頻度の再設定を行わせることもできる。

(3) リスク分析・評価項目と脅威の項目との関連付け

手順 3	実施主体：事務局
------	----------

事務局は、リスク分析・評価項目表（様式 1）の各リスク分析・評価項目に対して、脅威の項目を関連付ける。

リスク分析・評価シートでは、リスク分析・評価項目表（様式 1）におけるリスク分析・評価項目に対して、一般的に発生頻度が高いと考えられる脅威の項目をあらかじめ関連付けている。事務局は、自団体の実情に応じて、リスク分析・評価項目に対してあらかじめ設定された脅威の項目と他の脅威の項目を比較し、他の脅威の発生頻度の方が高いと判断した場合は、他の脅威の項目を選択する。

前述したとおり、情報資産に対する脅威は無限に存在するため、はじめの段階では、リスク分析・評価項目に対して、分かりやすく、明確な対策が実施可能な主要な脅威を 1 つ関連付ける。1 つの脅威に 1 つの対策を講ずることでも、様々な脅威に対抗できることが多い。

参考 1つの対策で、複数の脅威に対抗する例

- ・情報漏えいという脅威に対して、持出の許可制という対策を行えば、紛失や盗難の遭遇等に対抗できることになる。
- ・パソコンからの情報漏えいという脅威に対して、オペレーティングシステムのログインパスワードを設定すれば、パソコンを不正に利用できないことで、情報漏えい以外にも、データの改ざん、不正プログラムの意図的導入等に対抗できることになる。
- ・送信データの盗聴という脅威に対して、電子署名の機能を利用することで、盗聴以外にも、データの改ざん(改ざんは防げなくても、検知はできる)、送信者本人のなりすましなどに対抗できることになる。

図表3-35 リスク分析・評価項目と脅威の関連付けの選択例

リスク分析・評価項目表				脅威			
連番	評価項目番号(No.)	必須	リスク分析・評価項目 (監査ガイドラインの監査項目)	脅威の項目	機密性	完全性	可用性
10	26	○	ii) 予備電源装置の設置及び点検 情報システム管理者によって、停電等による電源供給の停止に備えた予備電源が備え付けられ、定期的に点検されている。	14 停電・雷の災害		3	3
				14 停電・雷の災害			
				15 地震・台風・洪水・火		3	3
				16			
				17			
				18			
				19			
				20			
				21			

1つ脅威を選択する。例えば、予備電源の設置に関するリスク分析・評価項目に対しては、停電による機器の緊急停止が一番発生頻度として高いと想定されることから、脅威としては「14 停電・雷の災害」を選択する。

発生頻度が表示される。

リスク分析・評価項目と脅威の関連付け

参考 対策の脆弱性及び情報資産の重要度の変化による脅威への影響

情報セキュリティ対策を強化し、脆弱性が低くなると、脅威の発生頻度が低下することもある。例えば、入室制限を厳格にすると、侵入(脅威)者は減少するこ

とになる。また、入室制限を厳格にしても、室内に保管又は設置している情報資産の重要度が増せば、脅威が高まることもある。これらのことを踏まえて、脅威の評価レベルの設定を見直す必要がある。

3.3.3 詳細リスク分析・評価の事前作業(リスク分析・評価項目表の見直し)

ステップ (第3章-7)	
<p><作業の概要></p> <p>手順 事務局は、リスク分析・評価項目表(様式1)のリスク分析・評価項目、対策の区分、対策の例及び脆弱性評価レベルの例の表現を、必要に応じて見直し、庁内で使用している用語等を踏まえたものに変更する。</p>	
分析・評価シート	リスク分析・評価項目表(様式1)
操作マニュアル目次	3.2.2 脅威の分析・評価及びリスク分析・評価項目表の見直し作業

手順	実施主体：事務局
-----------	----------

事務局は、リスク分析・評価項目表(様式1)の【文書用対策】、【電磁的記録媒体用対策】、【電子データ用対策】、【設置型ハードウェア用対策】、【移動型ハードウェア用対策】の対策の区分の選択を見直し、リスク分析・評価項目、対策の例及び脆弱性評価レベルの例の表現の見直しを行う。

見直しによる変更方法は、「2.3 基本リスク分析・評価の事前作業(リスク分析・評価項目表の見直し)(27頁)において解説したものと同一である。

注：詳細リスク分析・評価に関連する分析・評価シートでの対策の区分の変更
 保管・設置場所や情報資産の利用・保管状況により対策が不要な場合には、以下の分析・評価シート上でも、リスク分析・評価項目表(様式1)の対策の区分と同様に、「採用」→「不採用」への変更が直接可能である。

- ・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)

3.3.4 詳細リスク分析・評価の事前作業(実施単位の決定)

詳細リスク分析・評価は、情報資産台帳(様式6)の項目を基にして実施する。情報資産台帳(様式6)のヘッダ項目又は個別の情報資産名称を軸に、詳細リスク分析・評価を行う。ここでは詳細リスク分析・評価の実施単位として、「台帳明細別」、「情報資産グループ別」、「情報資産の種類別」3例について解説する。

事務局は、以下の解説を踏まえて、詳細リスク分析・評価の実施単位を決定する。

ヘッダ		情報資産台帳		任意項			
課室名	市民課	調査者	総務太郎	調査完了日	平成21年2月10日		
保管・設置場所	本庁舎1階執務室	情報資産の種類	談話型ハードウェア	情報資産グループ(任意)			
明細項目	番号	情報資産の種類別又は台帳明細別を実施する場合は、情報資産グループの入力は不要である。				台帳明細別	
1	住民記録システムの端末	2	3	2	1	市民課職員	6万人の住民記録を扱う端末
2	公的個人認証サービス受付窓口端末	1	3	2	1	市民課職員	

(情報資産台帳)

図表3-36 実施単位の3例について

実施単位	情報資産台帳(様式6)の項目	実施回数例による想定される作業量	詳細リスク分析・評価シート(様式8)の「最高値(重要度評価)」への転記	詳細リスク分析・評価の精度	作業負担
台帳明細別	課室、保管・設置場所、情報資産の種類、個別の情報資産名称	情報資産台帳の個別の情報資産名称の登録数が200でリスク分析・評価項目が110項目(リスク分析・評価項目最大数)であれば、単純には1登録につき、110項目の分析・評価ということになり、 <u>総評価数は、22,000回</u> になる。	明細の機密性、完全性及び可用性の数字を転記する。 明細の機密性、完全性及び可用性の重要度の値を利用するため、きめ細かい評価が可能である。	最も精度が高い	最も作業負担が掛かる。
情報資産	課室、保管・設置場所、情報資産の種類	情報資産グループが28で、リスク分析・評価項目	情報資産のグループ別の列の最高値の機	台帳明細別よりも	台帳明細別ほど、作

グループ別	報資産の種類、情報資産グループ	目が110項目であれば、単純には1グループにつき、110項目の分析・評価ということになり、 <u>総評価数は、3,080回になる。</u> ※グループ数の28は、「図表3-14 情報資産グループの入力例」の掲載件数	密性、完全性及び可用性の数字を転記する。 機密性、完全性及び可用性の重要度の値は、台帳明細別程きめ細かくできない。	精度が低い。	業負担は掛からない。
情報資産の種類別	課室、保管・設置場所、情報資産の種類	情報資産の種類が5で、リスク分析・評価項目が110項目であれば、単純には1種類につき、110項目の分析・評価ということになり、 <u>総評価数は、550回になる。</u>	情報資産の種類別の最高値の機密性、完全性及び可用性の数字を転記する。 機密性、完全性及び可用性の重要度の値は、情報資産グループ別程きめ細かくない。情報資産台帳上では、重要度が最高値になる傾向がある。	情報資産グループ別よりも精度が低い。	情報資産グループ別ほど、作業負担は掛からない。

注:実施回数例について

詳細リスク分析・評価のリスク分析・評価項目別の実施回数例は、一つの課室でも、保管・設置場所数の増減やリスク分析・評価項目に関する情報資産別の対策の組み合わせ数により変動が生じる。

ここがポイント 情報資産グループ別²²の実施単位における重要度の包含について

情報資産の利用・保管等が同質の状況にある場合に、重要度の高い情報資産への対策又は管理の方法・考え方を参考にすれば、重要度の低い情報資産への対策又は管理の程度が分かるようになる。このため、情報資産の重要度に着目して実施する。この考えは、情報資産の種類別の実施単位でも同様である。

²² I SMS ユーザーズガイド 2006年12月25日 財団法人 日本情報処理開発協会 「③ 情報資産のグループ化」 22/42 頁参照。

本書では、最も労力の掛からない「情報資産の種類別」で実施する方法を解説する。
なお、本書の詳細リスク分析・評価の方法は、他の2つの実施単位でも応用することが可能である。

3.3.5 詳細リスク分析・評価の事前作業(情報資産管理者への実施要請)

ステップ (第3章-8)	
<p><作業の概要></p> <p>手順 事務局は、事前作業(脅威の分析・評価、リスク分析・評価項目表の見直し、実施単位の決定)の終了後、詳細リスク分析・評価の実施を情報資産管理者に要請する。</p>	
分析・評価シート	情報資産台帳(様式6)
操作マニュアル目次	なし

手順	実施主体：事務局
----	----------

事務局は、事前作業(脅威の分析・評価、リスク分析・評価項目表の見直し、実施単位の決定)の終了後、各情報資産管理者に対して、実施単位を通知するとともに、各課室で作成した情報資産台帳(様式6)を基にリスク分析・評価を実施するよう要請する。

3.3.6 詳細リスク分析・評価の実施

ステップ (第3章-9)	
<p><作業の概要></p> <p>手順1 情報資産管理者が主導し、詳細リスク分析・評価シート(様式8)を利用して、事務局から通知された実施単位を基にリスク分析・評価を実施する。</p> <p>詳細リスク分析・評価の実施の要点は、以下のとおりである。</p> <ul style="list-style-type: none"> ・ 詳細リスク分析・評価シート(様式8)に情報資産台帳(様式6)から転記又は入力する。 ・ 情報資産台帳単位で機密性、完全性及び可用性の情報資産の重要度(最高値)を転記する。 ・ 事前に設定したリスク分析・評価項目表(様式1)からの参照情報(脅威の分析・評価結果等が表示)を基に、脆弱性の判定を実施する。また対策の不備や改善案は、「脆弱性状況の登録」欄に必要な応じてメモする。 ・ リスクの3要素である情報資産の重要度、脅威の分析・評価、脆弱性の分析・評価を基に、リスク評価値を自動で算出する。 <p>手順2 事務局は、詳細リスク分析・評価シート(様式8)の作成が終了した課室から当該シートを回収し、内容を確認する。</p> <p>手順3 事務局は、リスク受容水準の決定の素案を作成する。</p> <p>手順4 事務局は、リスク受容水準の決定の素案を情報セキュリティ委員会等に諮り、承認を得る。</p> <p>手順5 事務局は、リスク受容水準を詳細リスク分析・評価が終了した当該シートに数値を入力する。</p> <p>手順6 事務局は、リスク対応を選択する。</p>	
分析・評価シート	情報資産台帳(様式6) 詳細リスク分析・評価シート(様式8)
操作マニュアル目次	3.3 詳細リスク分析・評価作業

3.3.6.1 詳細リスク分析・評価シート(様式8)のレイアウト

レイアウトは、以下のとおりである。表示の都合上3分割している。

(その 1/3)

詳細リスク分析・評価シート		課室名		市民課		実施者		総務太郎		実施完了日		平成21年2月20日		ヘッダ項目	
区分欄は、「採用のみ分析・評価する。」		保管・設置場所		本庁舎1階執務室		情報資産の種類		設置型ハードウェア		情報資産グループ(任意)		明細を入力する項目は、黄色の箇所となります。			
表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示
番号	対策の区分/設置型ハードウェア	評価項目番号	リスク分析・評価項目	最高値は入力 明細は表示	脅威			情報資産に脅威が与える影響		判定	脆弱性評価		脆弱性評価レベル選択枝		
				最高値(重要度評価)	機密性	完全性	可用性	機密性	完全性		可用性	1		2	3
	12			3	2	1									
10	採用	26	ii)予備電源装置の設置及び点検情報システム管理者によって、停電等による電源の停止に備えた予備電源が備え付けられていない点検対象	3	2	1	4	3	3	4	4	できない	すべてのサーバ、端末等の機器は、予備電源に接続していません。		
			重要度の転記箇所												

(その 2/3)

表示	表示	表示	表示
脆弱性評価			
脆弱性評価レベルの例			
レベル1の例	レベル2の例	レベル3の例	レベル4の例
・すべてのサーバ、端末等の機器は、予備電源に接続している。また、分電盤からの許容電力量と接続されている端末等の消費電力量を点検し管理している。	・すべてのサーバ、端末等の機器は、予備電源に接続している。但し、分電盤からの許容電力量と接続されている端末等の消費電力量は管理していない。	・重要なサーバ等の機器は、予備電源に接続している。	・すべてのサーバ、端末等の機器は、予備電源に接続していません。

(その 3/3)

入力	表示	表示	表示	受容水準は入力 明細は表示	表示	入力	表示	
脆弱性状況の登録 (メモ)	リスク評価値			リスク受容水準		リスク対応		対策の例
	機密性	完全性	可用性	機密性	完全性	可用性	リスク対応の有無	設置型ハードウェア用対策
			9	12	12		低減 受容 回避 移転	
			リスク受容水準との差					
・重要なサーバ、端末を予備電源に接続していません。 ・重要なサーバ、端末は、予備電源に接続する。		24	12		12		有	低減
								・UPSの利用(回復) ・庁内の予備発電機経由の分電盤への接続(回復)

3.3.6.2 詳細リスク分析・評価の実施概要

手順 1	実施主体：情報資産管理者
------	--------------

実施手順は、以下のとおりである。

情報資産管理者が主導し、情報資産台帳(様式6)を基に、詳細リスク分析・評価シート(様式8)を作成する。

なお、「番号」、「評価項目番号」、「リスク分析・評価項目」、「脅威」、「脆弱性評価レベルの例」及び「対策の例」は、リスク分析・評価項目表(様式1)の項目と同様である。また、ヘッダ項目の「対策の区分」には、情報資産の種類と「採用」の行数が表示される。

(1) ヘッダ項目の作成

ヘッダ項目について、以下の解説を基にシートに入力(転記)する。

ア 課室名

情報資産台帳(様式6)から転記する。

イ 実施者、実施完了日

詳細リスク分析・評価実施者とリスク分析・評価が完了した年月日を入力する。

ウ 保管・設置場所

情報資産台帳(様式6)から転記する。

エ 情報資産の種類

情報資産台帳(様式6)から転記する。ただし、この項目については、「文書、電磁的記録媒体、電子データ、設置型ハードウェア、移動型ハードウェア」の中から選択する。

オ 情報資産グループ

情報資産台帳(様式6)から転記する。情報資産グループ別に詳細リスク分析・評価を実施しない場合は、入力不要である。

台帳明細別に実施する場合には、詳細リスク分析・評価シート(様式8)に、明細項目を設定していないため、この項目に個別の情報資産名称を転記して利用する。

(2) 情報資産の重要度の転記

シートの最高値(重要度評価)欄へ情報資産台帳に登録された情報資産の重要度を転記する。

情報資産台帳(様式6)の機密性、完全性及び可用性の列における最高値を、詳細リスク分析・評価シート(様式8)の「最高値(重要度評価)」に転記する。これによって、シート明細に「最高値(重要度評価)」が表示される。

図表3-37 実施単位を基にした詳細リスク分析・評価シート(様式8)への転記方法

実施単位	詳細リスク分析・評価シート(様式8)
情報資産の種類別	情報資産台帳(様式6)の「資産重要度評価と最高値」の数字を、詳細リスク分析・評価シート(様式8)の「最高値(重要度評価)」に転記する。
情報資産のグループ別	情報資産台帳(様式6)の「資産重要度評価と最高値」の数字を、詳細リスク分析・評価シート(様式8)の「最高値(重要度評価)」に転記する。
台帳明細別	情報資産台帳(様式6)の明細の機密性、完全性及び可用性の数字を、詳細リスク分析・評価シート(様式8)の「最高値(重要度評価)」に転記する。

参考

情報資産台帳（様式6）と詳細リスク分析・評価シート（様式8）の対応関係

情報資産台帳（様式6）と詳細リスク分析・評価シート（様式8）の対応関係は、以下のとおりである。

ヘッダ	課室名	市民課										
	調査者	総務太郎	調査完了日	平成21年2月10日								
	保管・設置場所	本庁舎1階執務室										
	情報資産の種類	設置型ハードウェア										
	情報資産グループ(任意)											
明細項目	必須項目											
	番号	個別の情報資産名称	数量	資産重要度評価と最高値			収納場所	情報資産の利用範囲	保存期限	個人情報記録の有無	備考	
				機密性	完全性	可用性						
1	住民記録システムの端末	2	3	2	1	市民課職員				6万人の住民記録を扱う端末		
2	2公的個人認証サービス受付窓口端末	1	3	2	1	市民課職員						

情報資産台帳の調査者及び調査完了日以外の項目は、同一になる。

最高値を転記するために入力する。
 なお、台帳明細別の実施単位の場合には、明細の値を入力する。

(情報資産台帳)

詳細リスク分析・評価シート	課室名	市民課										
	実施者	総務太郎	実施完了日	平成21年2月20日								
区分欄は、「採用」のみ分析・評価する。	情報資産の種類	設置型ハードウェア										明細を入力する項目は、黄色の箇所になります。
	情報資産グループ(任意)											
表示	表示	表示	表示	表示	最高値は入力 明細も表示	表示	表示	表示	表示	入力	表示	表示
番号	対策の区分/設置型ハードウェア	評価項目番号	リスク分析・評価項目	最高値(重要度評価)			脅威		脆弱性評価			
				機密性	完全性	可用性	脅威の項目		脆弱性評価レベル選択肢			
	12			3	2	1	機密性	完全性	可用性	判定	脆弱性評価レベル選択肢	
10	採用	26	ii) 予備電源装置の設置及び点検 情報システム管理者によって、停電等による電源供給の停止に備えた予備電源が備え付けられ、定期的に点検されている。	3	2	1	停電・雷の災害	3	3	4	できていない	すべてのサーバ、端末等の機器は、予備電源に接続していない。

明細に重要度を表示

(詳細リスク分析・評価シート)

(3) 明細項目の作成

明細項目について、以下の解説を基に作成等する。

ア 脆弱性評価レベルの判定

リスク分析・評価項目に対する脆弱性評価を実施する。

詳細リスク分析・評価では、レイアウトの対策の区分に「採用」と表示された項目について、「脆弱性評価レベル選択肢」から、情報資産に対する情報セキュリティ対策の状況を基に適当と判断したレベルの値を選択肢から選択する。選択肢における評価レベルとその内容に関しては以下とおりである。

なお、表示される脆弱性評価レベルの例は、情報資産に直結する情報セキュリティ状況を判断する際の参考例である。

※詳細リスク分析・評価シート(様式8)の初期設定の段階で、対策の区分が「採用」となっているものは、前述したとおり「不採用」に変更することもできる。

図表3-38 脆弱性評価レベル選択肢

評価レベル	選択肢の内容
1	できている
2	大半はできている
3	一部できている
4	できていない

参考 外部委託先に情報資産が保管されている場合の留意点

外部委託先に情報資産が保管されている場合、情報資産の保管・管理については、業務委託契約の規定に基づき対処されている。したがって、外部委託先に保管されている情報資産に対してリスク分析・評価を実施する場合は、外部委託先と協議の上、業務委託契約を踏まえて実施する必要がある。実施に当たっては、「リスク分析・評価項目」の中に、業務委託契約等に含まれない項目(契約外の項目等)があることが考えられるため、この場合は、対策の区分の「採用」を「不採用」に変更する。

イ 「脆弱性状況の登録(メモ)」欄に、脆弱性に関する課題や改善のための検討案をメモする。ただし、この作業は任意である。

参考 詳細リスク分析・評価の脆弱性状況の登録の例

・(課題) コンピュータウイルス感染予防のための、ウイルス定義ファイルの更

新をしていない。

- ・(改善案) ウイルス定義ファイルを自動更新する機能を導入する。

課題と改善案の登録に際しては、対策の例を参考にしてもよい。

(4) リスク評価値の表示

ア リスク評価値の計算方法

脆弱性の評価の実施により、詳細リスク分析・評価における3要素である情報資産の重要度、脅威、脆弱性の3要素について、すべて数値によるレベル設定が終了したこととなる。これにより、リスクが顕在化する可能性を意味する情報資産に対するリスク評価値が算出でき、以降でリスク対応により脆弱性の低減等に向けた改善を図ることができる。

本書では、リスク評価値を算出する計算を乗算としているが、民間等では加算で行われるケースもある。

リスク評価値=情報資産の重要度評価×脅威の評価レベル×脆弱性の評価レベル

図表3-39 リスク評価値について

入力	表示	表示	表示	受容水準は入力 明細は表示	表示	入力	表示
脆弱性状況の登録 (メモ)	リスク評価値			リスク受容	リスク評価値		対策の例
	機密性	完全性	可用性	機密性 9	完全性 12	可用性 12	設置型ハードウェア用対策
・重要なサーバ、端末を予備電源に接続していない。 ・重要なサーバ、端末は、予備電源に接続する。		24	12	リスク受容水準との差	リスク対応の有無	有	・UPSの利用(回復) ・庁内の予備発電機経由の分電盤への接続(回復)
						低減	

(詳細リスク分析・評価シート)

参考 脅威の発生頻度の設定が空欄の場合のリスク評価値計算について
 脅威の発生頻度の設定がなければ、リスク評価値計算は行わない。下の例では、機密性がそれに当たる。

図表3-40 リスク評価値が計算されない例

入力	表示	表示	表示	受容水準は入力 明細は表示			表示	入力	表示
<div style="border: 2px solid red; padding: 5px; display: inline-block;"> リスク評価値が 計算されない。 </div>	リスク評価値			リスク受容水準			リスク対応		対策の例
	機密性	完全性	可用性	機密性	完全性	可用性	リスク 対応の 有無	低減 受容 回避 移転	設置型ハードウェア用対策
				9	12	12			
	・重要なサーバ、端末を予備電源に接続してはいない。 ・重要なサーバ、端末は、予備電源に接続する。			24	12		12	有	低減

(詳細リスク分析・評価シート)

参考 リスク評価値の考え方

リスク評価値は、リスクが顕在化する可能性を推算したものであり、これによって、情報資産に対する脆弱性の状況を把握し、リスク対応において、改善のための根拠を形成することができる。

イ リスク評価値のマトリックス

リスク評価値は、以下の表に集約できる。

図表3-41 リスク評価値のマトリックス

脅威		1				2				3			
脆弱性		1	2	3	4	1	2	3	4	1	2	3	4
重要度	1	1	2	3	4	2	4	6	8	3	6	9	12
	2	2	4	6	8	4	8	12	16	6	12	18	24
	3	3	6	9	12	6	12	18	24	9	18	27	36

ウ リスク評価値の解釈

リスク評価値が「1」であるということは、その資産価値が最も低く、脅威の発生頻度も最も低く、脆弱性も最も弱い(対策が最も強い)ことを意味する。すなわち、リスクが顕在化する可能性が最も低い、また顕在化しても、資産価値が低いため、影響が小さいことを意味する。

リスク評価値が「36」であるということは、その資産価値も最も高く、脅威の発生頻度も最も高く、脆弱性も最も強い(対策が最も弱い)ことを意味する。すなわち、リスクが顕在化する発生可能性が最も高く、また顕在化すると、資産価値が高いため、影響が大きいことを意味する。

3.3.6.3 課室からの詳細リスク分析・評価シート(様式8)の回収と確認

手順2	実施主体：事務局
-----	----------

関係課室において詳細リスク分析・評価シート(様式8)の作成が終了した後、事務局は、各課室から詳細リスク分析・評価シート(様式8)を回収し、その内容を確認する。

脆弱性の判定に関して、複数の課室で同じ対策が実施されているにも関わらず、1課室だけ脆弱性の判定が異なるといった問題がある。このため、この現象が判定誤りによるものかどうか確認する必要がある。脆弱性の判定誤りとは、例えば以下のようなケースである。

- ・ 複数の課室で同じ情報システムを利用しているが、ある1課室のみパスワード変更等の脆弱性の判定が異なる。
- ・ 書庫を共同で利用しているが、ある1課室のみ入退室管理の脆弱性の判定が異なる。
- ・ 庁内に配備されたノートパソコンにセキュリティワイヤが付けられているが、ある1課室のみ持ち出しに関する脆弱性の判定が異なる。

確認作業を終了した後、リスク受容水準の決定を経て、詳細リスク分析・評価シート(様式8)にリスク受容水準の数値の設定とリスク対応の選択を行う。

3.3.6.4 リスク受容水準の決定と残留リスク

(1) リスク受容水準の考え方

業務において利用し保有する情報資産に対するリスクを完全にゼロとすることは、事実上不可能である。そこで、リスク評価値をある一定の水準まで低減させる対応が必要となってくる。リスク分析・評価の結果算出されたリスク評価値を、ある数値以下に低減させる水準となるのがリスク受容水準である。言い換えれば、情報資産の機密性・完全性・可用性の3つの側面におけるリスク評価値をどの水準までは受容できるかという数値である。リスク受容水準値を超えるリスク評価値を持つ情報資産に対しては、リスクを低減させることが必要であり、何らかの改善計画を策定し実行することになる。

リスク受容水準は、各課室や各情報資産に設定することも可能であるが、課室や情報資産によってリスクの受容水準が異なると、組織全体のセキュリティレベルの均質化が図られずセキュリティ対策にバラツキが生じる可能性がある。このため、リスク受容水準は、情報セキュリティ委員会等で統一的に決定することが必要となる。

本来、高いセキュリティレベルを維持するためには、リスク受容水準は低い(厳しい)ほうが望ましい。しかしながら、初めてリスク分析・評価を行う地方公共団体において、最初からリスク受容水準を低く設定してしまうと、リスク評価値を低減するために多大な労力を要することが予測される。また、情報セキュリティの向上は、一朝一夕に達成できる性質のものではなく、継続的かつ段階的に現状を改善していくことによって達成できるものである。これらのことを踏まえ、当初のリスク受容水準を決定する場合においては、リスク受容水準は比較的高めに設定することが適切である。

(2) リスク評価値用のマトリックスとリスク受容水準の関係

リスク受容水準は、機密性、完全性及び可用性に関して、すべて同じにする場合と、機密性に重点を置き、完全性及び可用性と差を付けた値にする場合などがある。例えば、個人情報の機密性確保に重点対策を講じる場合に、このような差異を設けることが考えられる。

リスク評価値のマトリックスを基にしたリスク受容水準の例を、2つ示す。

ア 機密性、完全性及び可用性のリスク受容水準の値が同一の場合は、以下のとおりである。

図表3-42 リスク受容水準の例1 (機密性、完全性及び可用性を「1 2」とした場合)

機密性

脅威		1				2				3			
脆弱性		1	2	3	4	1	2	3	4	1	2	3	4
重要度	1	1	2	3	4	2	4	6	8	3	6	9	12
	2	2	4	6	8	4	8	12	16	6	12	18	24
	3	3	6	9	12	6	12	18	24	9	18	27	36

完全性

脅威		1				2				3			
脆弱性		1	2	3	4	1	2	3	4	1	2	3	4
重要度	1	1	2	3	4	2	4	6	8	3	6	9	12
	2	2	4	6	8	4	8	12	16	6	12	18	24

可用性

脅威		1				2				3			
脆弱性		1	2	3	4	1	2	3	4	1	2	3	4
重要度	1	1	2	3	4	2	4	6	8	3	6	9	12
	2	2	4	6	8	4	8	12	16	6	12	18	24

: リスク受容水準より高いリスク評価値

機密性、完全性及び可用性のすべてのリスク受容水準を「1 2」以下とした場合、「1 2」までリスクの低減を図る必要があることを意味する。

イ 機密性、完全性及び可用性のリスク受容水準の値が異なる場合で、機密性に重点を置いたリスク受容水準は、以下のとおりである。

図表3-43 リスク受容水準の例2 (機密性を「9」、完全性及び可用性を「12」とした場合)

機密性

音威		1				2				3			
脆弱性		1	2	3	4	1	2	3	4	1	2	3	4
重要度	1	1	2	3	4	2	4	6	8	3	6	9	12
	2	2	4	6	8	4	8	12	16	6	12	18	24
	3	3	6	9	12	6	12	18	24	9	18	27	36

完全性

音威		1				2				3			
脆弱性		1	2	3	4	1	2	3	4	1	2	3	4
重要度	1	1	2	3	4	2	4	6	8	3	6	9	12
	2	2	4	6	8	4	8	12	16	6	12	18	24

可用性

音威		1				2				3			
脆弱性		1	2	3	4	1	2	3	4	1	2	3	4
重要度	1	1	2	3	4	2	4	6	8	3	6	9	12
	2	2	4	6	8	4	8	12	16	6	12	18	24

 :リスク受容水準より高いリスク評価値

機密性のリスク受容水準を「9」以下とし、完全性及び可用性のリスク受容水準を「12」以下とした場合、機密性は「9」、完全性及び可用性は「12」までリスクの低減を図る必要があることを意味する。

(3) リスク受容水準の留意事項

例えば機密性に係るリスク受容水準を「2」とした場合、情報資産の重要度が「3」であれば、脅威の発生頻度が最も低い「1」、脆弱性が最も弱い(対策状況は最も強い)「1」であっても、リスク評価値は「3」となり、これより小さくはない。この場合は、リスク低減について最高の改善を図ったと解釈する。

図表3-44 リスク算定によるリスク受容水準到達の限界

脅威		1				2				3			
脆弱性		1	2	3	4	1	2	3	4	1	2	3	4
重要度	1	1	2	3	4	3	6	9	12	3	6	9	12
	2	2	4	6	8	4	8	12	16	6	12	18	24
	3	3	6	9	12	6	12	18	24	9	18	27	36

リスク受容水準は、リスクが顕在化した場合の組織への影響に対して、当該リスクを受容するか否かの水準になるため、業務への影響、情報セキュリティ対策に係る運用費用、技術的な限界、住民からの事故等の予防に対する安心感等の視点から検討し、決定する。以下において、事務局が素案を作成する場合の2例を紹介し解説する。

(4) リスク受容水準の決定の素案作成

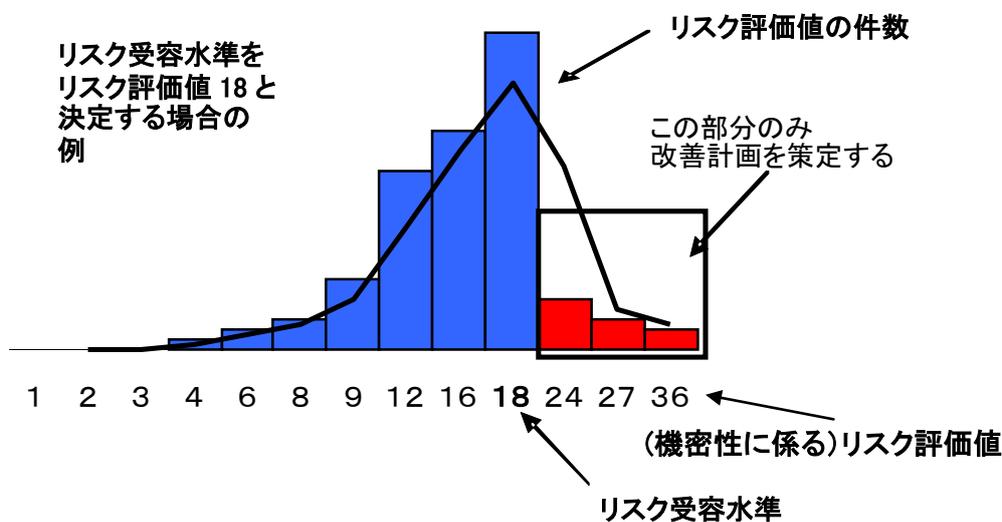
手順3	実施主体：事務局
-----	----------

以下に、初めて詳細リスク分析・評価を実施する際のリスク受容水準の決定の考え方を紹介する。

ア リスク評価値の度数分布状況に基づいて、リスク受容水準を決定する方法

各課室の詳細リスク分析・評価シート(様式8)全体から、機密性、完全性及び可用性のリスク評価値毎の件数の数値分布(度数分布)状況を調べ、一番高い分布を示したリスク評価値をリスク受容水準とする方法である。分布状況の把握には、ヒストグラム等を利用すると視覚的にわかりやすい。

図表 3-45 リスク受容水準の決定に関する考え方の例 1



イ リスク評価値の平均値を基にして、リスク受容水準を決定する方法

各課室の詳細リスク分析・評価シート(様式8)全体から、リスク評価値の機密性、完全性及び可用性の平均値を求めることで、リスク評価値の全体の傾向を知ることができる。この機密性、完全性及び可用性のリスク評価の平均値を基にして、それより低い数値をリスク受容水準とする方法である。例えば、機密性「18」、完全性「16」及び可用性「16」と平均値が算出された場合、これより低い数値を、「図表3-41 リスク評価値のマトリックス」を参考にリスク受容水準とする方法である。

図表 3-46 リスク受容水準の決定に関する考え方の例 2

入力	表示	表示	表示	受容水準は入力 詳細は表示	表示	入力	表示
脆弱性状況の登録 (メモ)	リスク評価値			機密性	完全性	可用性	リスク
	機密性	完全性	可用性	12	有	低	減
・重要なサーバ、端末を予備電源に接続していない。 ・重要なサーバ、端末は、予備電源に接続する。		24	12				・UPSの利用(回復) ・庁内の予備発電機経由の分電盤への接続(回復)

(詳細リスク分析・評価シート)

このように、リスク分析・評価を初めて行う場合は、試行錯誤の要素も多々あり、次年度以降も段階的に改善活動を継続することを考慮した上で、リスク受容水準値を決定することが、現実的に継続可能な無理のない方法である。リスク受容水準を、現状に比べあまり低い数値に設定するとハードルが高くなり、改善に多大な労力を要することになるため注意が必要である。また、次年度(次回)以降については、リスク分析及び改善活動の結果等を踏まえ、リスク受容水準を導き出すことが望まれる。

参考 リスク評価値の活用

分析・評価シートは、表計算ソフトウェアのため、課室全体のリスク分析・評価項目別のリスク評価値の傾向等を知ることができる。他にも、情報資産の種類別・リスク分析・評価項目別のリスク評価値の傾向等、様々な活用方法がある。

(5) リスク受容水準の決定に関する情報セキュリティ委員会等の承認

手順4	実施主体：事務局
-----	----------

事務局で設定したリスク受容水準の数値を、根拠を明確にした上で情報セキュリティ委員会等に諮り、その承認を得る。

(6) リスク受容水準の入力

手順5	実施主体：事務局
-----	----------

事務局は、情報セキュリティ委員会等で承認されたリスク受容水準の数値を、課室の詳細リスク分析・評価シート(様式8)に、1シートごとに入力する。これによって、リスク対応の低減等を行うためのリスク評価値とリスク受容水準との乖離状況を把握できることになる。

数値入力の範囲は、リスク評価値計算の最低値から最高値の範囲で、機密性の場合は「1～36」、完全性及び可用性の場合は「1～24」となる。また、この数値については、「図表3-41 リスク評価値のマトリックス」から選択し入力する。

以下の例では、機密性が9、完全性が12、可用性が12となる場合を示している。

図表3-47 リスク受容水準の設定例

入力	表示	表示	表示	受容水準は入力 明細は表示			表示	入力	表示
脆弱性状況の登録 (ノモ)	リスク評価値			リスク受容水準			リスク対応	対策の例	
	機密性	完全性	可用性	機密性	完全性	可用性	リスク対応の有無	低減 受容 回避 軽減	設置型ハードウェア用対策
・重要なサーバ、端末を予備電源に接続していただく。 ・重要なサーバ、端末は、予備電源に接続する。			24	12	12	9	12	12	

完全性のリスク評価値がリスク受容水準を上回っている。

リスク受容水準となる数値を入力する。
 ※この図表のリスク受容水準の数値は、説明上の例示である。

(詳細リスク分析・評価シート)

(7) 残留リスクについて

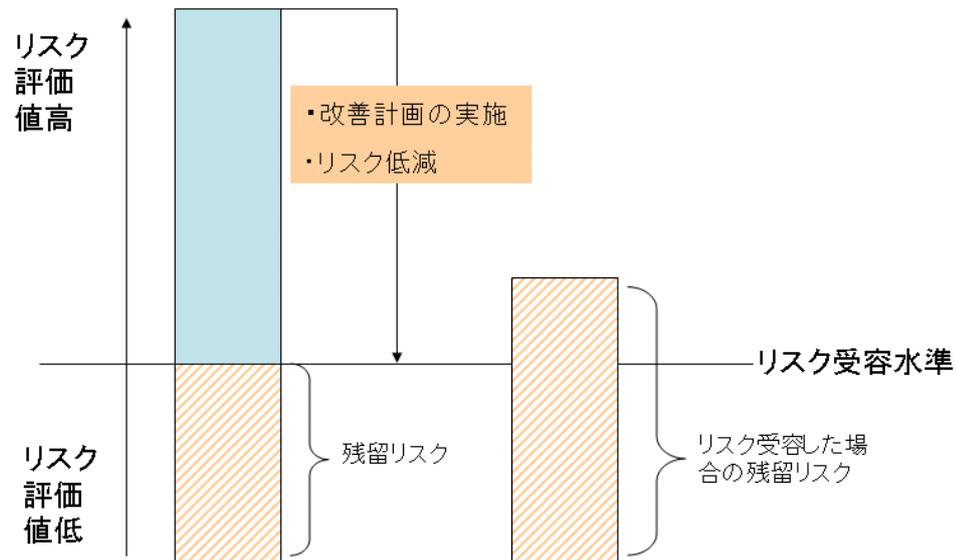
残留リスクとは、リスク受容水準まで脆弱性を改善しても残留するリスクをいう。

リスク受容水準以下の残留リスクであっても、情報資産の価値の変動(公開前情報と公開後情報等)、脅威の傾向(コンピュータウイルス感染の猛威等)、脆弱性の変化(情報システムの効率化のための更改に伴うセキュリティ機能の低下等)により常にリスクは変動するものである。残留リスクは、情報資産の保護状況に伴って、組織的に監視及び注視して行くことが重要である。

参考 ▶ 監視及び注視

ここでいう監視及び注視とは、各職員が情報資産の利用について、紛失等が発生させないように注意することを意味する。

図表 3-48 リスク受容水準と残留リスクについて



図表 3-48にある「リスク受容した場合の残留リスク」とは、予算の確保、技術的困難性等から脆弱性の改善をせず、現状を受け容れてそのまま残留するリスクをいう。例えば、24時間稼働のシステムに監視機能があっても、当面、当該機能を活用するためには、警告発信(アラート)対応をしなければならないが、このためには、24時間での監視体制が必要となる。しかしながら、人も予算も当面確保できない場合、このような監視体制を敷かないことによって生ずる、ホームページ改ざんによる住民等への情報提供が困難になるといったリスクを受容することとなる。この場合、通常の残留リスクよりもリスク値が高くなることから、事後においてリスク軽減対策の最優先の対象とする必要がある。

3.3.6.5 リスク対応の選択

(1) リスク評価値とリスク受容水準の差分について

詳細リスク分析・評価シート(様式8)に、リスク受容水準の数値を入力すると、リスク評価値との差分が表示される。この差分の解釈は、次のとおりである。

図表 3-49 リスク評価値とリスク受容水準の差の解釈

	差分の結果の解釈	リスク対応の有無
機密性、完全性、可用性の内一つでも差分の結果がプラスの場合	リスク対応が必要	リスク対応が必要である。この場合、「リスク対応」欄に「有」が表示される。

<p>機密性、完全性、可用性のすべての差分の結果がマイナスの場合、又は差分がゼロの場合</p> <p>※差分がゼロの場合、リスク受容水準との差の欄は、表計算ソフトウェア（ゼロ値非表示設定）の都合上、空欄になる。</p>	<p>現状でも十分な対策又は管理が取られているため、リスク対応は不要</p>	<p>・リスク対応は不要である。この場合、「リスク対応」欄に「無」が表示される。</p>
---	--	--

注：差分がマイナスの場合

例えば、可用性のリスク評価値が4で、可用性のリスク受容水準が12の場合、リスク評価値計算は、 $4 - 12 = -8$ になる。「図表3-50 差の結果がマイナスの例」の丸印がそれに該当する。また、「図表3-50 差の結果がマイナスの例」のケースでは、リスク評価値がリスク受容水準を上回る機密性に重点を置いた改善を実施することになる。

図表3-50 差がマイナスの例

入力	表示	表示	表示	受容水準は入力 明細は表示	表示	入力	表示
脆弱性状況の登録 (メモ)	リスク評価値	リスク受容水準			リスク対応	対策の例	
	機密性	完全性	可用性	機密性 完全性 可用性 9 12 12 リスク受容水準との差	リスク対応の有無	低減 受容 回避 移行	設置型ハードウェア用対策
		4		-8	無		<ul style="list-style-type: none"> ・転倒・落下防止措置の実施(Ⓔ) ・設置室内からのダンボール等の可燃物の除去(Ⓔ) ・サーバ室内に埃等を侵入させないように、上履きの利用(Ⓔ)

(詳細リスク分析・評価シート)

(2) リスク対応の選択

手順6	実施主体：事務局
-----	----------

事務局は、回収した課室の詳細分析・評価シート(様式8)に、リスク対応の選択を選択肢から行う。

リスク対応は、「低減」、「受容」、「回避」、「移転」の4つの選択がある。「図表3-50 差分がマイナスの例」にあるように、「リスク対応（リスク対応の有無）」欄に「有」（差分がプラスの場合）が表示された場合に、リスク対応の選択を、選択肢から行う。

図表3-51 リスク対応の選択肢

選択肢	内容	改善計画との関係
低減	リスクのある状態から改善を図り、リスクの顕在化の発生可能性を低減する。	・リスク評価値がリスク受容水準より高い値（差がプラスの場合）を示している状態で、当該受容水準まで、リスクを下げるための改善を図ることである。この場合は、改善計画を策定する。
受容	低減、回避、移転もせずに、リスクの現状を受け容れる。	・リスク評価値がリスク受容水準より高い値（差がプラスの場合）を示している状態に対して、現状を認識した上で特段の対応を取らないことである。この場合は、改善計画を策定しない。
回避	特定業務の停止や危険な利用機能を使用不可とし、リスクの顕在化の原因をなくしてしまう。	・業務で利用・保有している情報資産に対して、リスクが顕在化した場合の影響が大きい場合、又は情報資産洗い出し時点で、情報システムを廃止することが決定していた場合等、情報資産を使用又は保有しないことの改善計画を策定する。 ・情報資産の洗い出し時点における不要な情報資産の処分（個人情報等の不要な複製物の廃棄等）もリスクの回避策になるが、本書では、情報資産台帳に登録が行われるものに対する対応策のことを指しているため、リスク対応として取り扱わない。
移転	情報資産にリスクが顕在化した場合に備えて保険を掛ける、又は業務や情報システムをアウトソーシングするなどして、リスクが顕在化した場合の被害を受ける影響を極小化する。	・保険を掛ける、又は業務や情報システムをアウトソーシングする場合の改善計画を策定する。

ここポイント 「移転」と「回避」

詳細リスク分析・評価シート(様式8)では、「移転」も「回避」も選択できるようにしているが、民間等のISMSの取組みでもこれらの選択肢を選ぶケースはごく少数である。

参考 「受容」を選択した場合の脆弱性状況の登録の例

リスク対応について「受容」を選択した場合、「脆弱性状況の登録」欄に、「受容」を選択した理由を記載しておくことが望ましい。例えば、サーバ室における物理的対策の実施に関してリスクの「受容」を選択した場合は、「サーバ室の施設設備の老朽化により、物理的セキュリティ対策を全面的に行わなければならないが、費用負担が大きく、当面予算の確保ができないため、リスクを受容する。」などの記載をしておく、後日リスク状況の見直しをする際に役立つ。

3.4 詳細リスク分析・評価に関する改善計画の策定と実施

ステップ (第3章-10)	
<p><作業の概要></p> <p>手順1 事務局は、詳細リスク分析・評価に関する改善計画表(様式9)を利用し、改善計画の素案を作成する。</p> <p>手順2 事務局は、関係する課室と協議し、改善計画の内容が実施可能かどうか確認する。もし、複数の課室の共通課題に関する改善計画の素案を策定した場合には、関係する課室に報告する。</p> <p>手順3 事務局は、改善計画の素案を取りまとめ、情報セキュリティ委員会等に諮り、承認を得る。</p> <p>手順4 情報資産管理者又は事務局は、改善計画に基づき実施する。</p>	
分析・評価シート	詳細リスク分析・評価に関する改善計画表(様式9)
操作マニュアル目次	なし

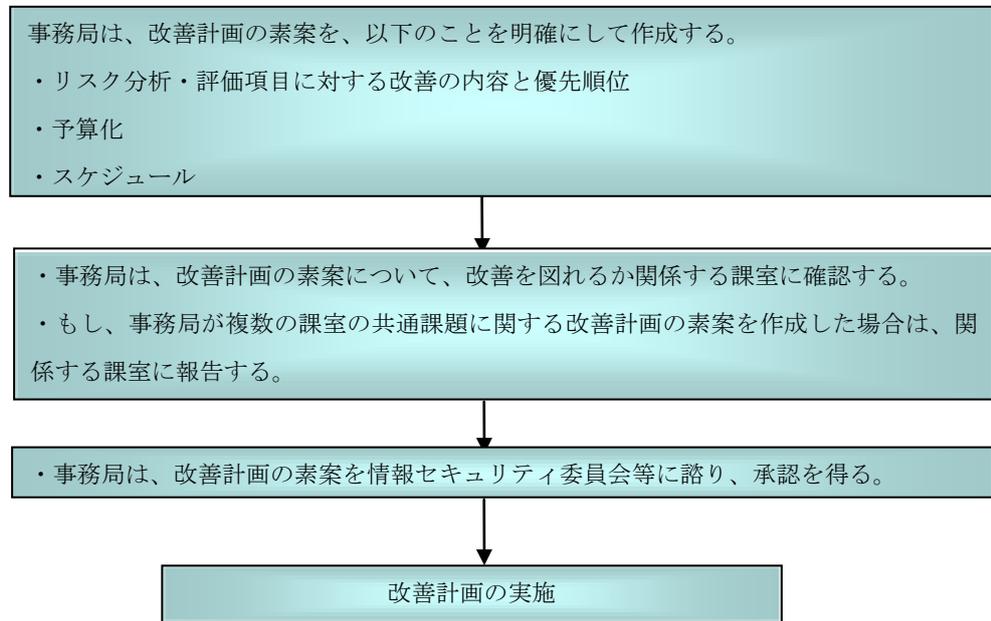
3.4.1 詳細リスク分析・評価に関する改善計画の策定から実施までの流れ

事務局は、課室から回収した詳細リスク分析・評価の結果を基に、リスク対応で「低減」、「回避」又は「移転」を選択したリスク分析・評価項目について、改善計画を策定する。計画の策定に当たっては、詳細リスク分析・評価に関する改善計画表(様式9)を利用し、対策の緊急性、経済性、有効性を検討した上で、リスク分析・評価項目のリスク対応の「低減」、「回避」又は「移転」を選択した場合について、当該脆弱性に対する改善内容、優先順位、実施のスケジュール等を決定する。また、対策の実施に当たって予算化をしなければならないものもあることから、予算化作業を行う。

事務局は、関係する課室に確認が終了した改善計画の素案について、情報セキュリティ委員会に諮り、承認を得る。

詳細リスク分析・評価シート(様式8)の「脆弱性状況の登録」に必要なメモが取られている場合は、当該情報を参考とし、改善計画の策定に役立てる。

図表 3-5-2 詳細リスク分析・評価結果を基にした改善計画策定から実施までのフロー図



3.4.2 詳細リスク分析・評価に関する改善計画表の作成

(1) 詳細リスク分析・評価に関する改善計画表(様式9)のレイアウト

レイアウトは、以下のとおりである。

詳細リスク分析・評価に関する改善計画表		課室名	市民課	作成日	平成21年2月26日				
		情報セキュリティ委員会 承認日	平成21年3月2日						
		保管・設置場所	本庁舎1階執務室						
		情報資産の種類	設置型ハードウェア						
		情報資産グループ(任意)							
表示	表示	表示	表示	入力	入力	入力	入力	入力	入力
番号	対策の区分/設置型ハードウェア	評価項目番号	リスク分析・評価項目	優先順位	改善の実施内容	予算	スケジュール		
				優先度高			開始日 (YYYY/MM/DD)	終了予定日 (YYYY/MM/DD)	終了日 (YYYY/MM/DD)
				優先度低		(単位:千円)			
10	採用	26	ii)予備電源装置の設置及び点検 情報システム管理者によって、停電等による電源供給の停止に備えた予備電源が備え付けられ、定期的に点検されている。	高	・重要なサーバ、端末を予備電源に接続してしまふ。 ・重要なサーバ、端末は、予備電源に接続する。	500	平成21年3月8日	平成21年3月22日	

(2) 詳細リスク分析・評価に関する改善計画の素案の作成

手順 1	実施主体：事務局
------	----------

事務局は、詳細リスク分析・評価に関する改善計画表(様式9)を利用し、

関係課室の改善計画の素案を作成する。

ア ヘッダ項目の作成

(ア) 課室名

課室名を入力する。

(イ) 作成日

改善計画を作成した年月日を入力する。

(ウ) 承認日

情報セキュリティ委員会等が改善計画を承認した年月日を入力する。

(エ) 保管・設置場所

詳細リスク分析・評価から転記する。

(オ) 情報資産の種類

文書、電磁的記録媒体、電子データ、設置型ハードウェア、移動型ハードウェアから選択し入力する。

(カ) 情報資産グループ

情報資産グループ別に詳細リスク分析・評価を実施している場合は、詳細リスク分析・評価シート（様式8）から転記する。

※他の単位で詳細リスク分析・評価を実施している場合は、転記不要である。

イ 明細項目の作成(ただし、番号、対策の区分、評価項目番号、リスク分析・評価項目は、リスク分析・評価項目表(様式1)と同じ内容が表示されているため、入力は不要)

※詳細リスク分析・評価に関する改善計画表(様式9)の初期設定の段階で、対策の区分が「採用」の場合は、前述の「不採用」に変更することもできる。詳細リスク分析・評価シート(様式8)で「採用」→「不採用」に変更した場合、当該シートに対応する詳細リスク分析・評価に関する改善計画表(様式9)の同じリスク分析・評価項目を「不採用」に直接変更する。

(ア) 脆弱性状況の登録

詳細リスク分析・評価シート(様式8)の「脆弱性状況の登録(メモ)」に入力した内容を、必要に応じて参考情報として転記する。

(イ) 優先順位

選択肢:緊急性、経済性、有効性の観点から、優先順位(高又は低)を決定する。緊急性、経済性、有効性の観点は、「図表2-8 改善計画の優先順位の考え方」(43頁)を参照すること。

(ウ) 改善の実施内容

現状の脆弱性を改善するための具体的な実施内容を作成する。詳細な計画とする場合は、別紙として作成する。

<リスク低減に関する実施内容の例>

(a) 文書用対策

- ・情報資産台帳に文書名称を登録する。
- ・情報システム仕様書は、鍵のかかるキャビネットに整理して保管する。

(b) 電磁的記録媒体用対策

- ・電磁的記録媒体を外部から持ち込む場合は、ウイルス感染のチェックを必ず実施する。
- ・電磁的記録媒体を課室の外部に持ち出す場合は、電磁的記録媒体管理簿に必要事項を記入する。

(c) 電子データ用対策

- ・ウイルス感染を監視するため、コンピュータウイルス対策ソフトウェアとパターンファイルを、常に最新のバージョンに更新する機能を導入する。

(d) 設置型ハードウェア用対策

- ・サーバ等の地震対策として、ラックの固定措置を講ずる。

(e) 移動型ハードウェア用対策

- ・職員が利用しているノートパソコンを庁舎外に持ち出す場合は、BIOSパスワードを設定していることを確認する。未設定の場合は、持出を禁止する。

(エ) 予算

改善計画を作成する上で、情報システム改修や物品購入等の予算措置が必要になる場合に予想される必要経費を入力する。本書では、千円単位としているが、各地方公共団体において、入力する金額単位を修正することとしてもよい。

(オ) 開始日と終了予定日並びに終了日

改善計画の実施開始年月日と終了予定年月日を入力する。また、改善が終了した際に終了年月日を入力する。

3.4.3 詳細リスク分析・評価に関する改善計画の確認、承認及び実施

(1) 課室への確認

手順 2	実施主体：事務局
------	----------

事務局は、課室と協議し、改善計画の内容が実施可能かどうか確認する。複数の課室で同じ脆弱性の状態が検出された場合は、これらの課題を事務局が

まとめて改善を行うことを、関係する課室に報告する。

(2) 課室の改善計画の素案に関する情報セキュリティ委員会等の承認

手順3	実施主体：事務局
-----	----------

事務局は、改善計画の素案を取りまとめ、情報セキュリティ委員会等に諮り、その承認を得る。庁内横断的な情報セキュリティに係る意思決定組織である情報セキュリティ委員会等の承認を得ることにより、円滑に改善計画を実施することができるようになると考えられる。

(3) 課室の改善計画の実施

手順4	実施主体：情報資産管理者又は事務局
-----	-------------------

情報資産管理者は、課室の改善計画を実施する。また、複数の課室で同じ脆弱性の状態が検出された場合には、事務局が改善計画を実施する。

改善計画の進捗状況は、監査等で確認し、情報セキュリティ委員会等に、定期的に報告していくことが望ましい。

付録 1 : 情報資産台帳サンプル

以下に、情報資産の種類別の情報資産台帳のサンプルを示す。

文書											
情報資産台帳	課室名	情報政策課									
	調査者	〇〇太郎	調査完了日	平成21年1月15日							
	保管・設置場所	情報政策課執務室									
	情報資産の種類	文書									
	情報資産グループ(任意)										
必須項目					任意項目						
番号	個別の情報資産名称	数量	資産重要度評価と最高値			収納場所	情報資産の利用範囲	保存期限	個人情報の記録の有無	備考	
			3	2	2						
			機密性	完全性	可用性						
1	告知放送機器等設置申請書綴	48	3	2	2	キャビネット	情報政策課職員	永年	有り(市民情報)		
2	文書保存管理簿	1	1	1	1	キャビネット	情報政策課職員	1年	無し		
3	情報系システム委託等契約書	1	1	1	1	キャビネット	情報政策課職員	5年	無し		
4	実施計画(策定資料)	1	1	1	1	キャビネット	情報政策課職員	5年	無し		
5	介護支援システム調達	1	2	1	1	キャビネット	情報政策課職員	5年	無し		
6	ネットワーク改修資料	1	1	1	1	キャビネット	情報政策課職員	5年	無し		
7	光ケーブル配線資料	1	1	1	1	キャビネット	情報政策課職員	5年	無し		
8	地域安心安全情報共有システム	1	2	1	1	キャビネット	情報政策課職員	5年	無し		
9	人事給与システム調達(資料)	1	2	1	1	キャビネット	情報政策課職員	5年	無し		
10	情報政策課契約書綴	1	2	2	2	キャビネット	情報政策課職員	5年	無し		
11	情報関係リース契約綴	1	2	1	1	キャビネット	情報政策課・出納室職員、監査委員	10年	無し		
12	公式ホームページ見直し関係	1	1	1	1	キャビネット	情報政策課職員	3年	無し		
13	ブレードシステム概要デザインシート	1	2	2	2	キャビネット	情報政策課職員・システム導入業者	永年	無し		

電磁的記録媒体

情報資産台帳	課室名	情報政策課									
	調査者	〇〇太郎	調査完了日	平成21年1月15日							
	保管・設置場所	電算室									
	情報資産の種類	電磁的記録媒体									
情報資産グループ(任意)											
必須項目						任意項目					
番号	個別の情報資産名称	数量	資産重要度評価と最高値			収納場所	情報資産の利用範囲	保存期限	個人情報の記録の有無	備考	
			3	2	2						
			機密性	完全性	可用性						
1	クライアント管理システムシステムディスクCD	1	2	1	1	左キャビネット	情報政策課職員	-	無し		
2	システムリカバリ用ディスクイメージHDD	2	2	1	1	左キャビネット	情報政策課職員	-	無し		
3	ファイルサーバー定期バックアップ(DAT)	5	3	2	2	左キャビネット	情報政策課職員	5年	有り(市民情報)	個人情報を含む庁内ファイルサーバーのバックアップデータのため。	
4	メールバックアップ(DAT)	5	2	2	1	左キャビネット	情報政策課職員	1年	有り(職員情報)	個人情報を含む庁内メールサーバーのバックアップデータのため。	
5	MS-Access2002CD	4	1	1	1	右キャビネット	情報政策課職員	-	無し		
6	MS-OfficeXP PersonalCD	7	1	1	1	右キャビネット	情報政策課職員	-	無し		
7	MS-OfficeXP ProCD	6	1	1	1	右キャビネット	情報政策課職員	-	無し		
8	MS-OfficeXP PersonalCD	4	1	1	1	右キャビネット	情報政策課職員	-	無し		
9	MS-Office2000PersonalCD	18	1	1	1	右キャビネット	情報政策課職員	-	無し		
10	MS-Office2000ProCD	3	1	1	1	右キャビネット	情報政策課職員	-	無し		
11	MS-Office2003 PersonalCD	2	1	1	1	右キャビネット	情報政策課職員	-	無し		
12	MS-Office2003 ProCD	1	1	1	1	右キャビネット	情報政策課職員	-	無し		
13	WindowsXPLIカバリCD	33	1	1	1	右キャビネット	情報政策課職員	-	無し		

電子データ

情報資産台帳	課室名	情報政策課								
	調査者	〇〇太郎	調査完了日	平成21年1月15日						
	保管・設置場所	情報システム								
	情報資産の種類	電子データ								
情報資産グループ(任意)										
必須項目					任意項目					
番号	個別の情報資産名称	数量	資産重要度評価と最高値			収納場所	情報資産の利用範囲	保存期限	個人情報の記録の有無	備考
			3	2	2					
			機密性	完全性	可用性					
1	メールサーバのデータ	1	3	2	2		全職員		有り(職員情報)	
2	グループウェアのデータ	1	2	2	2		全職員		無し	
3	ホームページ管理システムのデータ	1	1	2	2		情報政策課職員		無し	
4	Firewall VPN(ボジス、共有鍵)	1	2	1	1		情報政策課職員		無し	
5	条例DB	1	1	1	1		全職員		無し	庁内LAN~外部WEBサーバで公開
6	AntiVirus管理DB	1	1	1	1		情報政策課職員		無し	
7	WindowsUpdate(Wsus)	1	1	1	1		情報政策課職員		無し	
8	ルータ、Firewall、スイッチ構成ファイル	1	2	2	1		情報政策課職員		無し	
9	DNSソフトウェア(BIND)	1	2	2	2		情報政策課職員		無し	
10	メールソフトウェア(SENDMAIL)	1	2	2	2		情報政策課職員		無し	
11	Webソフトウェア(Apache)	1	2	2	2		情報政策課職員		無し	
12	庁内情報系ファイルサーバの課割当全体	1	3	2	2		情報政策課職員		無し	

設置型ハードウェア

情報資産台帳	課室名	情報政策課								
	調査者	〇〇太郎	調査完了日	平成21年1月15日						
	保管・設置場所	電算室								
	情報資産の種類	設置型ハードウェア								
	情報資産グループ(任意)									
必須項目										
番号	個別の情報資産名称	数量	資産重要度評価と最高値			任意項目				
			3	2	2					
			機密性	完全性	可用性	収納場所	情報資産の利用範囲	保存期限	個人情報の記録の有無	備考
1	基幹システムサーバ	3	3	2	2	ラック	情報政策課職員			
2	ファイルサーバ	1	3	2	2	ラック	情報政策課職員			
3	メールサーバ	1	3	2	2	ラック	情報政策課職員			
4	Webサーバ	1	3	2	2	ラック	情報政策課職員			
5	DNSサーバ	1	3	2	2	ラック	情報政策課職員			
6	例規サーバ	1	2	2	2	ラック	情報政策課職員			
7	財務会計システムサーバ	1	3	2	2	ラック	情報政策課職員			
8	WSUSサーバ	1	2	2	2	ラック	情報政策課職員			
9	情報・庁内LAN系管理者用監視用の端末	1	2	2	1	ラック	情報政策課職員			
10	ADSL(VPN)ルータ	2	3	2	2	ラック	情報政策課職員			
11	ISDNルータ	1	3	2	2	ラック	情報政策課職員			
12	プリンタ	2	1	1	2	床置き	情報政策課職員			

移動型ハードウェア

情報資産台帳	課室名	情報政策課								
	調査者	〇〇太郎	調査完了日	平成21年1月15日						
	保管・設置場所	情報政策課執務室								
	情報資産の種類	移動型ハードウェア								
	情報資産グループ(任意)									
必須項目						任意項目				
番号	個別の情報資産名称	数量	資産重要度評価と最高値			収納場所	情報資産の利用範囲	保存期限	個人情報の記録の有無	備考
			3	2	2					
			機密性	完全性	可用性					
1	情報システムの端末	15	3	2	2	机上	情報政策課職員			
2	基幹システムの端末	5	3	2	2	机上	情報政策課職員			
3	情報政策課デジタルカメラ	1	1	1	1	ロッカー	情報政策課職員			SDメモリーカードは別途保管
4	情報政策課ビデオカメラ	1	1	1	1	ロッカー	情報政策課職員			テープは別途保管
5	複合機(プリンタ、FAXコピー)	1	1	1	2	床置き	情報政策課職員			
6	貸出用モバイルプリンタ	1	1	1	1	ロッカー	全職員			
7	貸出用ハンコン	4	2	1	1	ロッカー	全職員			