

(別冊) 分析・評価シート
操作マニュアル

平成21年3月

総務省

目次

第1章	本書の利用方法	1
第2章	基本リスク分析・評価	4
2.1	基本リスク分析・評価に関する事前作業	4
2.1.1	リスク分析・評価項目表（様式1）のレイアウト	4
2.1.2	リスク分析・評価項目表（様式1）の見直し作業	7
2.2	基本リスク分析・評価作業	11
2.2.1	基本リスク分析・評価シート（様式2）のレイアウト	11
2.2.2	基本リスク分析・評価の作業内容	11
第3章	詳細リスク分析・評価	15
3.1	情報資産台帳（様式6）の作成	15
3.1.1	情報資産台帳（様式6）のレイアウト	16
3.1.2	情報資産台帳（様式6）作成の作業内容	16
3.2	詳細リスク分析・評価に関する事前作業	28
3.2.1	脅威評価レベル表のレイアウト	28
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	29
3.3	詳細リスク分析・評価作業	33
3.3.1	詳細リスク分析・評価シート（様式8）作成に関する作業内容	33
3.3.2	リスク受容水準の設定とリスク対応の選択	41

第1章 本書の利用方法

本書は、「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（以下、「手引き」という。）」の付属資料である分析・評価シートを利用するための操作マニュアルである。また、利用者の便宜を図るため、一部手引きと内容が重複している箇所もある。

分析・評価シートの構成


分析・評価シートの名称、その用途と手引き及び本書との関係は以下のとおりである。

様式	分析・評価シート名	用途	手引きの対象	本書の対象
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、改善計画を策定する際に使用する。	○	

マーク表示について

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。

マーク表示	内容
 参考	・リスク分析・評価の実施に当たって、利用者の参考となる点を解説している。作業の実施上特に読み飛ばしても構わない。
(入力)	・作業の過程で、様式に入力する項目を表す。
(選択)	・作業の過程で、選択肢から選択する項目を表す。
(転記)	・作業の過程で、他の分析・評価シートから転記する項目を表す。
(文言訂正)	・作業の過程で、必要に応じて内容を訂正する項目を表す。
実施主体	・実際の作業主体の例を表す。

以下のように、本文中で、作業の手順と、それを主体的に実施する組織等を関連付けている。また手引きを参照する目次を記載している。

実施主体	事務局
手引き目次	

基本リスク 分析・評価

第2章 基本リスク分析・評価

本章では、基本リスク分析・評価の作業において使用する分析・評価シートの操作方法について解説する。

本章で解説する作業項目、使用する分析・評価シート（様式）は、以下のとおりである。

作業項目	使用する分析・評価シート（様式）
2.1 基本リスク分析・評価に関する事前作業	・リスク分析・評価項目表（様式1）
2.2 基本リスク分析・評価作業	・基本リスク分析・評価シート（様式2）

2.1 基本リスク分析・評価に関する事前作業

実施主体	事務局
手引き目次	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）

この作業は、「2.2 基本リスク分析・評価作業」を実施する前に、リスク分析・評価項目表（様式1）の用語等を必要に応じて見直す作業である。

2.1.1 リスク分析・評価項目表（様式1）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4分割してある。

赤枠内が作業箇所

(その 1/4)

リスク分析・評価ファイル(基本リスク分析・評価用)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を非表示設定にしている。

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	

リスク分析・評価項目表 (様式 1)

(その 2/4)

リスク分析・評価ファイル(基本リスク分析・評価用)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を非表示設定にしている。

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範囲に関する規定の文書化(抑制)						

リスク分析・評価項目表 (様式 1)

(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、見直しも行っていない。	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。				

リスク分析・評価項目表 (様式 1)

(その 4/4)

リスク分析・評価ファイル(基本リスク分析・評価用)では、すべて列を非表示設定にしている。

文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正	文章訂正
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

リスク分析・評価項目表 (様式 1)

2.1.2 リスク分析・評価項目表（様式1）の見直し作業

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」、「脆弱性評価レベルの例」の記述内容を確認し、必要に応じて以下の見直しを行う。ただし、変更せずに初期設定のまま利用することも可能である。

見直しに関する項目を整理すると、以下のとおりになる。

図表2-1 見直しに関する項目

見直し対象項目	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。

【ステップ1 対策の区分の見直し】

(1) 「対策の区分」の見直し（選択）

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「採用」を各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不要と判断する場合は、「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（入力制御されている）。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。

リスク分析・評価項目表				対策の区分の「採用」は、プルダウンになっている。								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					
1	1	○	i)行政権限の範囲 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					
2	2	○	ii)情報資産の範囲 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情報資産の範囲が定められ、文書化されている。	選択すると注釈が表示される。				採用	採用と不採用 ・初期設定が不採用のとき、採用への変更は禁止 ・初期設定が採用のとき、不採用への変更は可能	不採用	不採用	不採用				
			i)組織体制、権限及び責任 最高情報統括責任者によって、情報セキュリティ対策のための組織体制、権限					採用							採用	

リスク分析・評価項目表（様式1）

(2) 不採用の理由のメモ

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できるように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。

【ステップ2 用語の確認及び変更】

リスク分析・評価項目表（様式1）において、「対策の区分」の「管理的対策」又は「人的対策」が「採用」となっている「リスク分析・評価項目」、「対策の例」、「脆弱性評価レベルの例」欄の表現を変更・修正する。

(その1)

①リスク分析・評価項目の内容（用語等）を確認する。

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	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				
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				

対策の区分の「管理的対策」又は「人的対策」が「採用」となっている項目を見直しの対象とする。

リスク分析・評価項目表（様式1）

(その2)

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範囲に関する規定の文書化(抑制)						

②対策の例の「管理的対策」、「人的対策」の表現内容を確認する。

リスク分析・評価項目表（様式1）

(その3)

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				
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おり、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おり、職員等に周知している。但し、見直しは行ってない。	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おり。但し、職員等に周知してない。見直しも行ってない。	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おり。				

③脆弱性評価レベルの例の「管理的対策」、「人的対策」の表現内容を確認する。

リスク分析・評価項目表（様式1）

参考

(例)「情報セキュリティポリシー」を「〇〇管理規程」に置換する場合
 効率的に作業を実施するために、Excel (以下、表計算ソフトウェアと呼ぶ。)の「置換」機能を使用して置換作業を行うことが有効である。詳しい操作方法は以下のとおりである。

- (1) 表計算ソフトウェアのツールバー「編集」を選択し、「置換」をクリックする。
- (2) 検索する文字列に「情報セキュリティポリシー」と入力する。
- (3) 置換後の文字列に「〇〇管理規程」と入力する。
- (4) 「置換」を選択し、「置換対象の文字列」を確認しながら置換する。

The screenshot shows the Microsoft Excel interface with the 'Edit' menu open, highlighting the 'Find and Replace' option (1). The 'Find and Replace' dialog box is open, showing the search text '情報セキュリティポリシー' (2) and the replacement text '〇〇管理規程' (3). The 'Replace' button is highlighted (4). The background shows a table with columns labeled F through P and rows 1 through 5. The table content includes headers like '対策の区分' and '管理の対策', and rows with specific policy details and implementation status (採用/不採用).

リスク分析・評価項目表 (様式1)

2.2 基本リスク分析・評価作業

実施主体	事務局
手引き目次	2.4.2 基本リスク分析・評価シート(様式2)のレイアウト 2.4.3 基本リスク分析・評価の実施

基本リスク分析・評価シート(様式2)を用い、全庁における情報セキュリティに関する対応状況について分析・評価し、課題点の洗い出しや改善のためのメモを残す作業を行う。この作業により、全庁の情報セキュリティの「管理的対策」及び「人的対策」の実施状況を把握することができる。

2.2.1 基本リスク分析・評価シート(様式2)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・評価シート		実施組織	事務局																		
区分欄は、管理的対策又は人的対策が、「採用」のみ分析・評価する。		実施完了日	平成21年1月6日																		
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	表示	表示	表示			
対象の区分		危険性評価												対策の例							
管理	人的	評価項目番号	1	危険性評価レベル4の状態				危険性評価レベル3の状態				危険性評価レベル2の状態				管理	人的				
採用	不採用	1	1	レベル1の例				レベル2の例				レベル3の例				管理	人的				
1		1		1)行政機関の範囲 最高情報責任者によって、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規定され、変更 化されている。				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 ていない。また、見直しを 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。また、見直しを 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。また、見直しを 行っていない。				情報セキュリティポ リシーに適用する行政機 関範囲に関する規定の 変更化が実施されている。	

基本リスク分析・評価シート(様式2)

2.2.2 基本リスク分析・評価の作業内容

基本リスク分析・評価の実施シート(様式2)の作成方法について解説する。

【ステップ1 ヘッダ項目の入力】

ヘッダ項目の入力は、以下のとおりである。

(1) 実施組織(入力)

事務局等の実施する組織名を入力する。

(2) 実施完了日(入力)

基本リスク分析・評価の実施シート(様式2)の作成が完了した年月日を入力する。

ヘッダ	基本リスク分析・評価シート	実施組織	事務局
	区分欄は、管理的対策又は人的対策が、「採用」のみ分析・評価する。	実施完了日	平成21年1月6日
		明細を入力する項目は、黄色の箇所になります。	

基本リスク分析・評価シート(様式2)

【ステップ2 明細項目の入力】

明細項目の入力は、以下のとおりである。

基本リスク分析・評価シート		実施経緯	事務局								
実施完了日		平成21年1月6日									
区分種別、管理対策又は人的対策が、[採用]のみ分析・評価する。		明細を入力する項目は、黄色の箇所になります。									
表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示
対策の区分		「採用」表示の項目のみを対象とする。						脆弱性状況の維持(%)		対策の例	
番号	管理対策	人的対策	脆弱性評価レベル選択肢	脆弱性評価レベルの例				脆弱性状況の維持(%)	管理対策	人的対策	
			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	レベル1の例	レベル2の例	レベル3の例	レベル4の例				
採用	不採用	1 行政機関の範囲 最高情報保護責任者によって、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。	4 できていない	「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。	「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る。職員等に周知されている。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る。但し、職員等に周知していない。見直しも行っていない。	「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る。但し、職員等に周知していない。見直しも行っていない。	「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る。但し、職員等に周知していない。見直しも行っていない。	「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る。但し、職員等に周知していない。見直しも行っていない。	「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る。但し、職員等に周知していない。見直しも行っていない。	

基本リスク分析・評価シート(様式2)

(1) 脆弱性評価レベルの判定(選択)

「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選択肢から行う。選択に当たっては、「脆弱性評価レベルの例」で書か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。

判定	脆弱性評価レベル選択肢		脆弱性評価レベルの例			
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					
			レベル1の例	レベル2の例	レベル3の例	レベル4の例
		「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。	「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る。職員等に周知されている。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る。但し、職員等に周知していない。見直しも行っていない。	「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る。但し、職員等に周知していない。見直しも行っていない。	「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。

① レベル1～4の内容を確認する。

② プルダウンでレベルを選択する。

③ 選択した内容が表示される。

④ 選択したレベルのセルが黄色に変化する。

基本リスク分析・評価シート(様式2)

(2) 脆弱性状況の登録 (入力)

脆弱性評価レベルの値が「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。

表示	入力	表示	表示
		対策の例	
レベル4の例	脆弱性状況の登録 (メモ)	管理的	ここに、現状における課題や改善案を入力する。
・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ない。	・行政機関の範囲の文書化をしていない。 ・行政機関の範囲を情報セキュリティポリシーに記載する。	・情報セキュリティポリシーに適用範囲に関する文書化(抑制)	

基本リスク分析・評価シート(様式2)

参考 基本リスク分析・評価の脆弱性状況のメモの例

- ・(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に際して際は、「対策の例」を参考にしてもよい。

注：画面表示に関する留意事項

基本リスク分析・評価シート(様式2)は、全体で110項目の行があるが、表計算ソフトウェアで、「管理的対策」と「人的対策」が双方とも「不採用」の行については、分析・評価の必要がないため、あらかじめ行を非表示(シート保護機能利用)にしている。このために番号の6と9の間が非表示(表示されない)になっている。

区分	基本リスク分析・評価シート				実施組織	事務所
	表示	表示	表示	表示	実施完了日	平成2
区分欄は、管理的対策又は人的対策が、「採用のみ分析・評価する。					非表示の行がある。 明細「7」、「8」が表示されていない。	
対策の区分	管理的対策		人的対策		リスク分析・評価項目	
番号	40	2				1 2 3 4
6	採用	不採用			i) 情報資産の管理に関わる基準 統括情報セキュリティ責任者及び 情報セキュリティ責任者によって、 情報資産の管理に関わる基準が定められ、文書化されている。	
9	採用	不採用			iii) サーバ障害対策基準 統括情報セキュリティ責任者又は 情報システム管理者によって、 メインサーバに障害が発生した場合の 対策基準及び実施手順が定められ、 文書化されている。	

詳細リスク 分析・評価

第3章 詳細リスク分析・評価

本章では、情報資産の洗い出し、情報資産台帳（様式6）の作成及び情報資産（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）に直接結びついた情報セキュリティ対策状況のリスク分析・評価において使用する分析・評価シート（様式8）の操作について解説する。

本章で行う作業項目及び使用する分析・評価シート（様式）は、以下のとおりである。

作業項目	使用する分析・評価シート（様式）
3.1 情報資産台帳（様式6）の作成	・ 情報資産台帳（様式6）
3.2 詳細リスク分析・評価に関する事前作業	・ リスク分析・評価項目表（様式1） ・ 脅威評価レベル表（様式7）
3.3 詳細リスク分析・評価作業	・ 情報資産台帳（様式6） ・ 詳細リスク分析・評価シート（様式8）

3.1 情報資産台帳（様式6）の作成

実施主体	情報資産管理者
手引き目次	3.2.5 情報資産台帳の作成

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）までの作成を必須とし、情報資産グループ別の作成については任意とする。

3.1.1 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								
	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					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	1					
			秘密性	完全性	可用性						
	1	住民記録システムの端末	2	3	2	1	住民課職員			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け窓口端末	1	3	2	1	市民課職員				

情報資産台帳（様式6）

3.1.2 情報資産台帳（様式6）作成の作業内容

情報資産台帳（様式6）の作成方法について解説する。

【ステップ1 ヘッダ項目の入力】

ヘッダ項目の入力は、以下のとおりである。

ヘッダ	課室名		(1)	市民課		
	調査者		(2)	総務太郎	調査完了日	平成21年2月10日
	保管・設置場所		(3)	本庁舎1階執務室		
	情報資産の種類		(4)	設置型ハードウェア		
	情報資産グループ(任意)		(5)			

情報資産台帳（様式6）

(1) 課室名（必須）（入力）

情報資産を管理している課室名を入力する。

(2) 調査者、調査完了日（必須）（入力）

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を入力する。

(3) 保管・設置場所(必須) (入力)

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。

- ア 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をする。以下に例を示す。

図表3-1 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。

※【ステップ3 任意の明細項目の入力】を参照のこと。

イ 電子データの場合

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、ここでは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3-2 電子データの入力例

情報資産	保管・設置場所の例
電子データの保管・設置場所	・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

	<ul style="list-style-type: none"> ・国民健康保険システム ・土木工事積算システム
--	--

ウ 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 3-3 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」

(4) 情報資産の種類(必須) (選択)

以下の情報資産の種類から選択する。

図表 3-4 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

(5) 情報資産グループ(任意) (入力)

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 3-5 情報資産グループの入力例

情報資産の種類	情報資産グループ
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 ・ 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 ・ 団体で開発・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)

【ステップ2 必須の明細項目の入力】

明細項目への入力は、以下のとおりである。

明細項目	(1)	(2)	必須項目	(4)		
	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
		入力した値(重要度)の最高値が表示される。		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

情報資産台帳（様式6）

(1) 番号（入力）

情報資産の区別ができるように算用数字を入力する。

(2) 個別の情報資産名称（入力）

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。

ア 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に当たっては、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、課室の上部組織である部等単位で情報資産の名称を統一することも重要である。

参考 情報資産名称の登録方法の例示

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」と表記する。
- ・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」と表記する。

イ 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。

ウ 電磁的記録媒体の格納情報について

電磁的記録媒体の格納情報については、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。また、1媒体に複数のファイルが記録されている場合においても、レーベル面等の名称を登録する。

エ 電子データの登録について

電子データは、その性質上、登録単位をどの程度きめ細かく登録するのかが非常に難しいため、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。

オ 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。

カ 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。

キ 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」等と登録する。

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 3-6 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

	<ul style="list-style-type: none"> ・(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

(3) 数量(入力)

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数量の最低単位は「1」とする。

ア 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、紛失時の検出が遅れる可能性がある。

イ 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、紛失時等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3-7 備考欄の活用例

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）」

ウ 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3-8 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ダ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」とすることもよい。

エ 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」と入力する。

オ 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。

(4) 資産重要度評価と最高値（選択）

手引きの「情報資産の重要度評価基準」を参考にして入力する。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、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。

図表3-9 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

【ステップ3 任意の明細項目の入力】

明細項目への入力は、以下のとおりである。

任意項目				
(1)	(2)	(3)	(4)	(5)
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			

情報資産台帳（様式6）

(1) 収納場所（入力）

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）を対象に収納場所の登録を行う。以下に例を示す。

図表 3-10 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。

(2) 情報資産の利用範囲 (入力)

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 3-11 情報資産の利用範囲入力例

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

※情報システム課等の名称は、手引き「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」を参照のこと。

(3) 保存期限 (入力)

文書、電磁的記録媒体の保存期限を入力する。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 3-12 保存期限の例

1年(以上)、3年(以上)、5年(以上)、永年、－(定めなし)等

(4) 個人情報の記録の有無 (入力)

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。ただし、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 3-13 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

(5) 備考 (入力)

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。

図表 3-14 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パソコン、電磁的記録媒体であるかどうかの確認	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 詳細リスク分析・評価に関する事前作業

実施主体	事務局
手引き目次	3.3.2 詳細リスク分析・評価の事前作業(脅威の分析・評価) 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)

詳細リスク分析・評価における、以下の事前作業について解説する。この作業の実施は任意とする。

3.2.1 脅威評価レベル表のレイアウト

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			
脅威の項目 (脅威の内容)と発生頻度の設定 (数値)は、必要に応じて変更可能である。	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
01 規則違反	2	2	2
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
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
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			
19	連番の初期値は変更しない。		
20			
21			
22	脅威設定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。		
23			
24			
25			
26			
27			
28			
29			
30			

空欄は、脅威が発生した場合でも、情報資産の重要度に影響を与えないことを意味する。

プルダウンで値の変更が可能。

発生頻度の設定は、選択肢(1、2、3)から選択する。

脅威評価レベル表 (様式7)

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

【ステップ1 脅威の分析・評価】

リスク分析・評価項目表（様式1）における脅威の項目及び発生頻度は、あらかじめ脅威評価レベル表（様式7）において、一般的な脅威として設定している内容を参照している。脅威の内容や発生頻度を変更する必要がある場合は、脅威評価レベル表（様式7）の内容を変更する。

(1) 脅威の項目（文言訂正）

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。

(2) 発生頻度（選択）

発生頻度は、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等を踏まえ、必要に応じて、発生頻度の設定を訂正（変更）する。

図表3-15 脅威の項目と発生頻度設定の変更例

(03 情報資産の紛失、置き忘れ又は滅失を変更する例)

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
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

↓

脅威の項目の文言訂正（置き忘れ→盗難）及び発生頻度の設定数値（機密性2→3、可用性2→1）を変更

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
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、盗難又は滅失	3		1

脅威評価レベル表（様式7）

(3) リスク分析・評価項目と脅威の項目の設定変更 (選択)

脅威評価レベル表 (様式7) で、脅威の項目を見直した場合 (項目の追加、変更、削除) や発生頻度を変更した場合には、リスク分析・評価項目表 (様式1) の脅威の項目と発生頻度は、自動的に変更されないため、該当する脅威の項目を変更する必要がある。

(変更前の画面)

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)		機密性	完全性	可用性
25	75	○	iii) 外部職員等が場合は、情報セキュリティ管理者による許可を得ている。	03 情報資産の紛失、置き忘れ又は滅失			

注: 数値が消えて空欄になる。 (脅威の項目列)

注: 脅威の項目及び発生頻度は、自動的に変更されない。 (iii) 外部職員等が場合は、情報セキュリティ管理者による許可を得ている。 (リスク分析・評価項目列)

リスク分析・評価項目表 (様式1)

(変更中の画面)

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
25	75	○	iii) 外部での情報処理業務の制限 脅威の項目を選択し直す。許可を得ている。	03 情報資産の紛失、置き忘れ又は滅失			
			iv) 私物パソコンの使用制限 職員等が外部で情報処理作業を行う際に私物パソコンを用いる場合、情報セキュリティ管理者による許可を得ている。また、機密性の高い情報資産の私物パソコンによる情報処理作業は行われていない。	01 規則違反 02 ネットワークからの情報の流出 03 情報資産の紛失、盗難又は 04 誤廃棄、又は消し忘れ 05 ハードウェア・回線(ケーブル)の 06 ソフトウェアのバグ、設定ミス又 07 情報・データの窃取又は不正 08 サーバ・ネットワークへの不正	2		

注: 脅威の項目を選択し直す。 (iii) 外部での情報処理業務の制限 (リスク分析・評価項目列)

リスク分析・評価項目表 (様式1)

(変更後の画面)

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
25	75	<input type="radio"/>	ii)外部での情報処理業務の制限 職員等が外部で情報処理作業を行う場合は、情報セキュリティ管理者による許可を得ている。	03情報資産の紛失、盗難又は滅失	3		1

リスク分析・評価項目表 (様式1)

(4) リスク分析・評価項目と脅威の項目の見直し (選択)

上記の作業とは別に、リスク分析・評価項目表 (様式1) の個別の「リスク分析・評価項目」に対してあらかじめ設定されている脅威と他の脅威の項目を比較し、他の脅威の発生頻度のほうが高いと判断した場合は、他の脅威の項目を選択し直す。

図表3-16 リスク分析・評価項目と脅威との関連付け変更の例

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
14	40	<input type="radio"/>	ii)記憶装置の情報消去 情報システム管理者によって、廃棄又はリース返却する機器内部の記憶装置からすべての情報が消去され、復元が	04誤廃棄、又は消し忘れ			

一つ脅威を選択する。例えば、「記憶装置の情報消去」に関するリスク分析・評価項目に対する脅威として「04誤廃棄、又は消し忘れ」より「07情報・データの窃取又は不正複製」の発生頻度の方が高いと想定する場合は、「07」の脅威を選択し直す。

04誤廃棄、又は消し忘れ
05ハードウェア・回線(ケーブル)の故障又は損傷
06ソフトウェアのバグ、設定ミス又はデータ誤り
07情報・データの窃取又は不正複製
08サーバ・ネットワークへの不正アクセス又は不正利用
09コンピュータウイルス感染
10情報・データの改ざん又は不正消去
11端末・電磁的記録媒体の盗難

リスク分析・評価項目表 (様式1)

【ステップ2 リスク分析・評価項目表（様式1）の見直し作業】

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。ここでの選択は、【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5つである。

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
23	72	○	Ⅱ) 情報資産等の業務以外の目的での使用禁止 職員等による業務以外の目的での情報資産の持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスは行われていない。	02 ネットワークからの情報の流出、漏えい又は露呈	2			不採用	不採用	不採用	不採用	採用	不採用	採用
			Ⅱ) 情報資産等の外部持出制限 職員等がパソコン等の端末、記録媒体	03 情報資産の紛失、置き忘れ又は滅失	2		2	不採用	不採用	採用 不採用	採用	不採用	採用	

リスク分析・評価項目表（様式1）

対策の区分の「採用」は、プルダウンになっている。

不採用の理由のメモの作成と「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」の表現内容の変更については、基本リスク分析・評価と同様の作業となるため、本書「2.1 基本リスク分析・評価に関する事前作業」（4頁）を参照する。

3.3 詳細リスク分析・評価作業

3.3.1 詳細リスク分析・評価シート（様式8）作成に関する作業内容

詳細リスク分析・評価作業において使用する詳細リスク分析・評価シート（様式8）の操作方法について解説する。

実施主体	情報資産管理者
手引き目次	3.3.6 詳細リスク分析・評価の実施

【ステップ1 シートのコピー】

詳細リスク分析・評価を行う前に、情報資産の種類別等の詳細リスク分析・評価を行う実施単位毎に、詳細リスク分析・評価シート(様式8)をコピーする必要がある。

<「詳細リスク分析・評価シート」の初期画面>

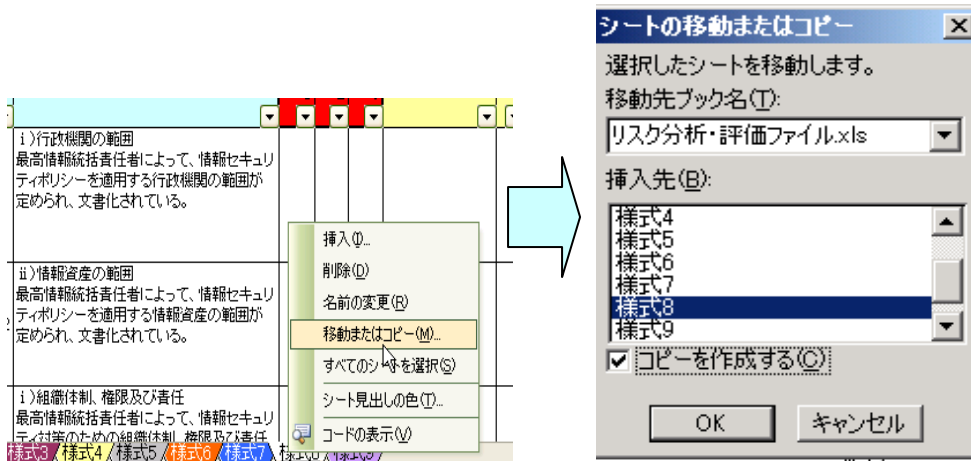
詳細リスク分析・評価シート		調査名	市民課	実施完了日		平成21年2月20日							
実施者		情報資産の種類	総務本部長	実施場所		本庁舎1階執務室							
区分欄は、「採用」のみ分析・評価する。		情報資産グループ(任意)			明細を入力する項目は、黄色の箇所になります。								
表示	表示	表示	表示		最高値は入力 明細は表示	表示	表示	表示	入力	表示	表示		
番号	対象の区分	評価項目番号	最高値 (重要度評価)			脅威			脆弱性評価				
			機密性 1~3	完全性 1~2	可用性 1~2	情報資産に 脅威が与える 影響			脆弱性評価レベル選択結果				
リスク分析・評価項目			機密性	完全性	可用性	脅威の項目	機密性	完全性	可用性	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
1		1	3	2	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。													
2		2											
ii)情報資産の範囲 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情報資産の範囲が定められ、文書化されている。													

詳細リスク分析・評価シート（様式8）

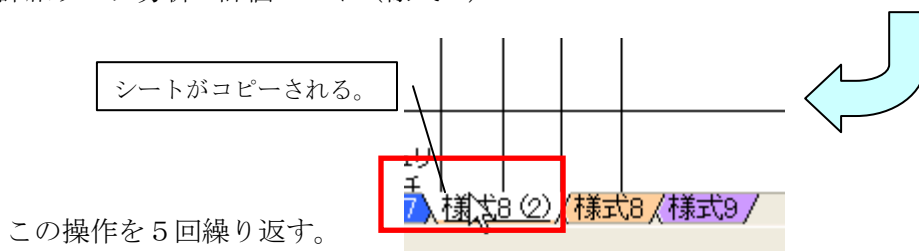
(1) 作業を開始する前に、「様式8」を同じブックの中に、「情報資産の種類」又は「情報資産グループ」の数量分コピーする。(新規のブックを作成する場合は、他のシートとの参照関係を維持するため、分析・評価ファイル単位でコピーする必要がある)

(例) 1 課室で1 保管・設置場所の場合、「情報資産の種類」毎に詳細リスク分析・評価を行う場合

「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5シートを作成する必要がある。



詳細リスク分析・評価シート（様式8）



- (2) 「情報資産の種類」を選択し、「対策の区分」の「採用」のみを表示させる。
 ア 「情報資産の種類」を選択する。

ヘッダ		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		情報資産グループ(任意)		設置型ハードウェア		(ア)		脆弱性評価		脆弱性評価		脆弱性評価		
表示		表示		表示		表示		表示		表示		表示		表示		
明細項目	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)	機密性	完全性	可用性	脅威の項目	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	脆弱性評価	脆弱性評価	
	12				最高値	3	2	1			1	1	1	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。	脅威							2	2	2	2	2
				ii) 情報資産の範囲								3	3	3	3	3
												4	4	4	4	4

詳細リスク分析・評価シート (様式 8)

- イ 表計算ソフトウェアの機能で、「オートフィルタ」をクリックし、「対策の区分」の「採用」を選択する。
 「対策の区分」には「採用」のみが表示される。

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		情報資産グループ(任意)		設置型ハードウェア		脆弱性評価		脆弱性評価		脆弱性評価		
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(重要度評価)	機密性	完全性	可用性	脅威の項目	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	脆弱性評価	
	採用	12		最高値	3	2	1			4	4	4	4	
			8	ii) 機器の取付け 情報システム管理者によって、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度等の影響を可能な限り排除した場所に設置し、容易に取外せないように固定するなどの対策が講じられている。	脅威							4	4	4
			10	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。								4	4	4
			20									4	4	4

詳細リスク分析・評価シート (様式 8)

- (3) 「情報資産の種類」等の実施単位毎に、上記の操作を繰り返し作業する。

【ステップ2 ヘッダ項目の操作】

ヘッダ項目の操作は、以下のとおりである。

(画面レイアウト)

拡大 詳細リスク分析・評価シート (様式8)

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	
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)				脆弱性評価		脆弱性評価レベル選択肢					
表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示	表示
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	脆弱性(重要度評価)	脅威の項目	脆弱性	完全性	可用性	判定	脆弱性評価	脆弱性評価レベル選択肢	
12	20	ii)機器の取付け 情報システム管理者によって、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度等の影響を可能な限り排除した場所に設置し、容易に取外せないよう固定するなどの対策が講じられている。	3 2 1	15地震・台風・洪水・火事の災害	1	1	1	4	4	設置型ハードウェアの重要な機器は、転倒防止措置及び埃対策をしていない。またダンボール等も、散乱した状態になっている。	

詳細リスク分析・評価シート (様式8)

脆弱性評価		脆弱性評価レベルの例		脆弱性状況の登録(7)		脆弱性		脆弱性		脆弱性	
レベル1の例	レベル2の例	レベル3の例	レベル4の例	脆弱性	完全性	可用性	脆弱性	完全性	可用性	脆弱性	完全性
設置型ハードウェアの重要な機器は、転倒防止措置及び埃対策を施している。ダンボール等が、室内に散乱してはいない。また、設置室内の物理的セキュリティを定期的に点検している。	設置型ハードウェアの重要な機器は、転倒防止措置及び埃対策を施している。ダンボール等が、室内に散乱してはいない。また、設置室内の物理的セキュリティを定期的に点検している。	設置型ハードウェアの重要な機器は、転倒防止措置及び埃対策を施している。ダンボール等が、室内に散乱してはいない。また、設置室内の物理的セキュリティを定期的に点検している。	設置型ハードウェアの重要な機器は、転倒防止措置及び埃対策を施している。ダンボール等が、室内に散乱してはいない。また、設置室内の物理的セキュリティを定期的に点検している。	脆弱性	完全性	可用性	脆弱性	完全性	可用性	脆弱性	完全性
9	12	12	12	8	4	4	8	4	4	4	4

詳細リスク分析・評価シート (様式8)

(1) 脆弱性評価レベルの判定 (選択)

詳細リスク分析・評価シート (様式8) の「対策の区分/情報資産の種類」が「採用」となっている項目について、「脆弱性評価レベルの例」を参考にして、適当と判断する判定値を「脆弱性評価レベル選択肢」から選択する。これによって選択した「レベルの例」の箇所が黄色に表示される。もし対策が不要の場合には、詳細リスク分析・評価シート (様式8) の対策の区分を「採用」→「不採用」に変更できる。

なお、あらかじめ設定した「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。

(その1)

入力したレベルの色が変化する。

脆弱性評価		脆弱性評価				
判定	脆弱性評価レベル選択肢	脆弱性評価レベルの例				
1	できている。	レベル1の例	レベル2の例	レベル3の例	レベル4の例	
2	大半までできている。					
3	一部できている。					
4	できていない。					
5	一部できていない。	「脆弱性評価レベルの例」を参考に判定を行い、レベル値を選択する。	・設置型ハードウェアの重要な機器は、転倒防止措置及び対策を施している。ダンボール等が、室内に散乱していない。また、設置室内の物理的セキュリティを定期的に点検している。	・設置型ハードウェアの重要な機器は、転倒防止措置及び対策を施している。ダンボール等が、室内に散乱していない。但し、設置室内の物理的セキュリティは定期的に点検していない。	・設置型ハードウェアの重要な機器は、転倒防止措置及び対策を施している。但し、ダンボール等は、散乱した状態になっている。	・設置型ハードウェアの重要な機器は、転倒防止措置及び対策を施していない。またダンボール等も、散乱した状態になっている。

詳細リスク分析・評価シート (様式8)

(その2)

「リスク評価値」、 「リスク受容水準との差」、 「リスク対応の有無」 が表示される。

表示		表示		表示		表示		表示		表示		
レベル3の例		レベル4の例		(メモ)		リスク評価値		リスク受容水準		リスク対応		
・設置型ハードウェアの重要な機器は、転倒防止措置及び対策を施している。但し、ダンボール等は、散乱した状態になっている。		・設置型ハードウェアの重要な機器は、転倒防止措置及び対策を施していない。またダンボール等も、散乱した状態になっている。				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
						9	12	12	9	12	12	低減 受容 回避 移転
						リスク受容水準との差		リスク受容水準との差		リスク受容水準との差		
						8	4	-4	-8	無	無	・転倒・落下防止措置の実施(※防) ・設置室内からのダンボール等の可燃物の除去(※防) ・サー(室内)に埃等を侵入させないように、上履きの利用(※防)

詳細リスク分析・評価シート (様式8)

注:詳細リスク分析・評価シート(様式8)上で、「採用」→「不採用」に変更した場合

表計算ソフトウェアの関数機能で、リスク分析・評価項目表(様式1)の対策の区分を参照し、情報資産の種類別に「採用」が表示される仕組みにしている。このためシートで「採用」→「不採用」に「入力規則」の機能を利用し変更した場合は、関数設定が消去されてしまうことに注意する必要がある。

「採用」の状態

C20		※ =IF(\$F\$4=" 文書",様式1\K12,IF(\$F\$4=" 電磁的記録媒体",様式1\L12,IF(\$F\$4=" 電子データ",様式1\M12,IF(\$F\$4=" 設置型ハードウェア",様式1\N12,IF(\$F\$4=" 移動型ハードウェア",様式1\O12,""))))																						
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P									
1	ヘッダ	詳細リスク分析・評価シート			課室名	市民課																		
2					実施者	総務太郎		実施完了日	平成21年2月20日															
3					保管・設置場所	階執務室																		
4		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																		
5					情報資産グループ(任意)																			
6		表示	表示	表示	最高値は入力 明細は表示			表示	表示	表示	表示	入力	表示											
7	明細項目	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												
8						12	20	ii)機器の取付け 情報システム管理者によって、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度等の影響を可能な限り排除した場所に設置し、容易に取外せないように固定するなどの対策が講じられている。	3	2	1	15地震・台風・洪水・火事の災害	1	1	4	できていない	脆弱性評価レベル選択							
9																		機密性 1~3	完全性 1~2	可用性 1~2	脅威の項目	情報資産に脅威が与える影響	判定	脆弱性評価レベル選択
10																							1	できている
11																							2	大半はできている
12								3	一部できている															
20													4	できていない										

詳細リスク分析・評価シート(様式8)

「不採用」の状態

C20		※ 不採用																						
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P									
1	ヘッダ	詳細リスク分析・評価シート			課室名	市民課																		
2					実施者	総務太郎		実施完了日	平成21年2月20日															
3					保管・設置場所	階執務室																		
4		区分欄は、「採用」のみ分析・評価する。			情報資産の種類	ハードウェア																		
5					情報資産グループ(任意)																			
6		表示	表示	表示	最高値は入力 明細は表示			表示	表示	表示	表示	入力	表示											
7	明細項目	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												
8						11	20	ii)機器の取付け 情報システム管理者によって、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度等の影響を可能な限り排除した場所に設置し、容易に取外せないように固定するなどの対策が講じられている。	3	2	1	15地震・台風・洪水・火事の災害	1	1	4	できていない	脆弱性評価レベル選択							
9																		機密性 1~3	完全性 1~2	可用性 1~2	脅威の項目	情報資産に脅威が与える影響	判定	脆弱性評価レベル選択
10																							1	できている
11																							2	大半はできている
12								3	一部できている															
20													4	できていない										

詳細リスク分析・評価シート(様式8)

(2) 脆弱性状況の登録（入力）

脆弱性評価を行った際に、個別の課室等における課題の把握や改善のために役立つと思われる事項があれば、今後の改善計画作成に役立てるため、必要に応じてメモする。ただし、この作業は任意である。

図表 3-17 脆弱性状況の登録例

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	リスク 対応の 有無	低減 受容 回避 移転	ここにメモする。	
				9	12	12				
リスク受容水準との差				有						
<ul style="list-style-type: none"> 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		12			有	低減	<ul style="list-style-type: none"> 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（様式8）

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。

3.3.2 リスク受容水準の設定とリスク対応の選択

実施主体	事務局
手引き目次	3.3.6.4 リスク受容水準の決定と残留リスク 3.3.6.5 リスク対応の選択

【ステップ1 リスク受容水準の設定】

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。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「1～3
6」、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3-19 リスク評価値のマトリックス」から選択し入力する。リスク受容水準の決
定方法は、手引きの「3.3.6.4 リスク受容水準の決定と残留リスク」を参照する。

図表3-18 リスク受容水準の入力例

リスク評価値			リスク受容水準			リスク対応
機密性	完全性	可用性	機密性	完全性	可用性	
			9	12	12	低減 受容 回避 移転
			リスク受容水準との差			リスク対応の有無

リスク受容水準を入力する。

詳細リスク分析・評価シート（様式8）

図表3-19 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

【ステップ2 リスク対応の選択】

「リスク受容水準との差」がプラスの値の場合、「リスク対応」の4つの選択肢から、
取るべき対応を選択する。

リスク対応は、「低減」、「受容」、「回避」、「移転」の4つである。

図表 3-20 リスク対応の選択肢

選択肢	内容
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。
受容	低減、回避、移転もせずに、リスクの現状を受け容れる。
回避	特定業務の停止や危険な利用機能を使用不可にし、リスクの顕在化の原因をなくしてしまう。
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、また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。

図表 3-21 リスク対応の選択例

入力	表示	表示	表示	受容水準は入力 明細は表示	表示	入力	
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		リスク対応の選択肢 「低減、受容、回避、 移転」から入力する。
	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	
・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	有	低減	設置型ハードウェア対策 ・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（様式8）

- ・リスク対応の有無に関して、リスク評価値とリスク受容水準との差のいずれかが1以上の場合（リスク評価値－リスク受容水準＞0の場合）は「有」、その他の場合は「無」又は「空欄」が表示される。
- ・「無」は、「対策の区分」が「採用」において、リスク評価値がリスク受容水準以下であることを示す。
- ・「空欄」は、詳細リスク分析・評価シート（様式8）上で、「採用」→「不採用」に変更した場合であることを示す。