情報資産のリスク分析に関する検討について

総務省地域力創造グループ
地域情報政策室

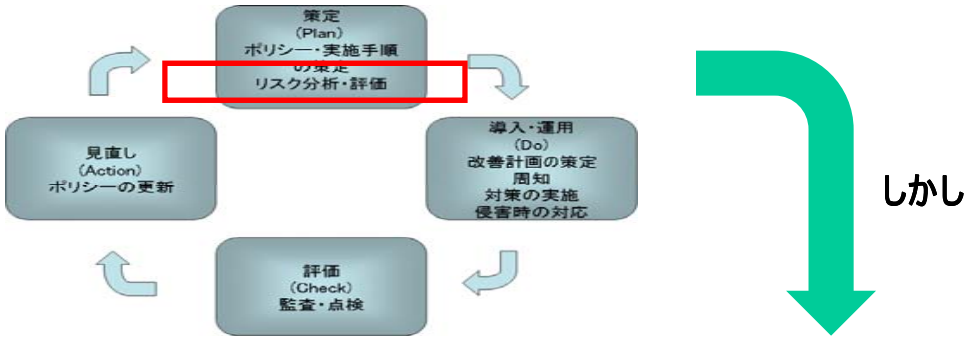
総務省
MIC Ministry of Internal Affairs and Communications

目　次

1　本手引き作成の背景（1/2）

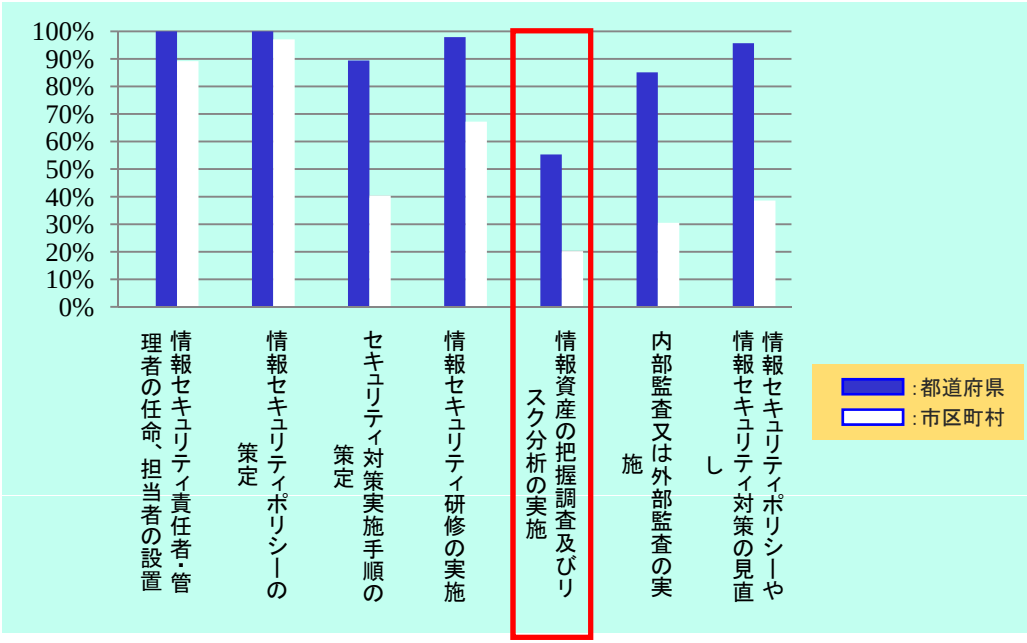
・情報セキュリティ対策のPDCAサイクルの中で、情報資産のリスク分析はプロセス上実施することとされている。
しかしながら、リスク分析はPDCAサイクルの中において実施率が一番低いのが現状である。

情報セキュリティ対策のPDCAサイクル



しかし

☆主な情報セキュリティ対策の実施状況（平成20年4月1日時点）



情報資産管理とセキュリティ事故

○情報資産の持ち出しによる紛失、漏えい等の事故は***情報資産の管理とそのリスク分析の不徹底が原因の1つ***

＜例＞
USBメモリの無断持ち出しによる紛失

管理するUSBメモリの把握（情報資産台帳の作成）及びリスク分析の実施（紛失による情報漏洩の具体的リスクが判明）により、管理対策の徹底が図られ（管理者による持ち出し許可制の実施、特定の場所における厳重な保管等）、事故の未然防止に役立つ。

1　本手引き作成の背景（2/2）

・情報資産のリスク分析に関する自治体の現状（リスク分析を実施していない、またはできない主な理由）

情報資産の分類及びリスク分析実施の必要性は認識しているが、**あるべき方法がわからないため**実施には至っていない（A自治体）

情報資産の把握、リスク分析の実施によって達成される課題が不明であることから、**実施する動機が働かない**（C自治体）

情報セキュリティを含む情報政策一般は企画部局が担当することが多いが、地域振興、合併関係事務等が業務時間の大半を占め、**実施することの意義を見出せない業務にあまり労力を割けない**（E自治体）

民間から提供されたリスク分析手法では時間がかかりすぎるため、個々の情報資産のリスク分析は実施していない（B自治体）

リスク分析の実施には、セキュリティ担当部署以外の原課（事業担当課）への協力が不可欠であるが、**そのためのノウハウがつかめない**（D自治体）

情報資産の把握やリスク分析の実施をする際の、**ノウハウが無い（どのような手順や体制でやるか、何から着手すればいいかなど）**（F自治体）

情報セキュリティ対策の水準向上のためのリスク分析・評価の方法論を提供し、情報資産のリスク分析を実施する必要性を認識してもらう必要がある。

２　情報セキュリティ対策におけるリスク分析・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。

リスク分析・評価の実施

情報資産の保護とは、情報資産の機密性、完全性及び可用性を確保することである。

どこまで対策を行う必要があるのかを把握するためには、リスクの状況を組織的に知る必要がある。

リスク分析・評価を行う場合の効果
情報セキュリティの実施状況から現状の情報セキュリティ対策で何が不足しているのか、どこまで行えばよいのかが把握できる。

リスク分析・評価をしない場合の問題
どこまでセキュリティ対策を実施すべきか、またどこに重点を置いて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がある。

＜リスク分析・評価の意義＞

○リスクの高い情報資産が何であるかが明確になる。

○リスクが顕在化した場合の役所及び地域住民等への影響からどのような対策を講ずべきか、また何を優先的に対応する必要があるのかを明確にすることができる。

地方公共団体にとって限りある資源である「人・物・予算」を、どの程度措置するのが適正かどうかを判断する根拠・資料を得ることが可能となる。

３　本手引きのコンセプト（ 1/3）

〇基本リスク分析と詳細リスク分析の２段階のアプローチを採用（手引き４頁参照）

→自治体のセキュリティ対策の現状に応じて、直接情報資産に関わらない組織体制の状況や教育等の現状に係る調査（基本リスク分析）と、情報資産台帳の作成及び情報資産に関するリスク分析（詳細リスク分析）とを選択できるように構成上の工夫をしている。

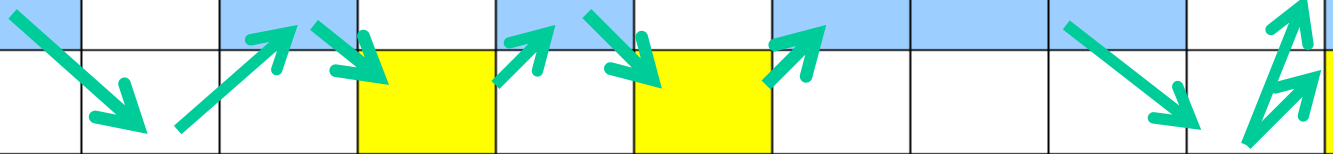
方法	概要
基本リスク分析・評価	規程・規則等の策定、組織体制の確立等の情報セキュリティ対策の現状に係るリスク分析・評価をいう。
詳細リスク分析・評価	情報資産を特定し、当該資産の利用や保管等に関する情報セキュリティ対策の現状に係るリスク分析・評価をいう。

3　本手引きのコンセプト（ 2/3）

○作業手順のステップ化と作業主体の明記

→具体的な作業内容をどの順序で行っていくか明確にするため、作業の手順をステップ化している。また、各ステップ毎に作業の主体を明記することで、自治体内部での作業の展開が分かるように工夫している。

詳細リスク分析・評価		実施ステップ											
		①情報資産洗い出し対象範囲の選定	②対象範囲の承認	③洗い出し時における留意事項の明確化 ④洗い出し項目の明確化、情報資産の抽出等	⑤情報資産台帳の作成 ⑥情報資産台帳の確認等	⑦（狭義の）詳細リスク分析・評価事前作業	⑧（狭義の）詳細リスク分析・評価作業の実施	⑨詳細リスク分析・評価シートの回収と確認	⑩リスク受容水準の決定（入力）	⑪改善計画の策定と提出	⑫改善計画の承認	⑬改善計画の実施
実施主体	事務局											
	課室（管理者）											
	セキュリティ委員会											



３　本手引きのコンセプト（３/３）

〇作業の省力化を図るため、半自動化した作業シートを添付

→リスク分析・評価の作業担当者が効率的に作業可能なものとするため、手引きの各ステップにおいて使用する作業シート（分析・評価シート）をExcelにより作成し、随所に工夫を採り入れ、極力作業の省力化を図っている。

＜工夫の例＞

・プルダウンメニューによる自動選択方式を採用（脆弱性評価値等）

・リスク分析・評価項目毎の脅威の発生頻度等に関して、関連する様式間の自動リンク化（様式１、７及び８等）

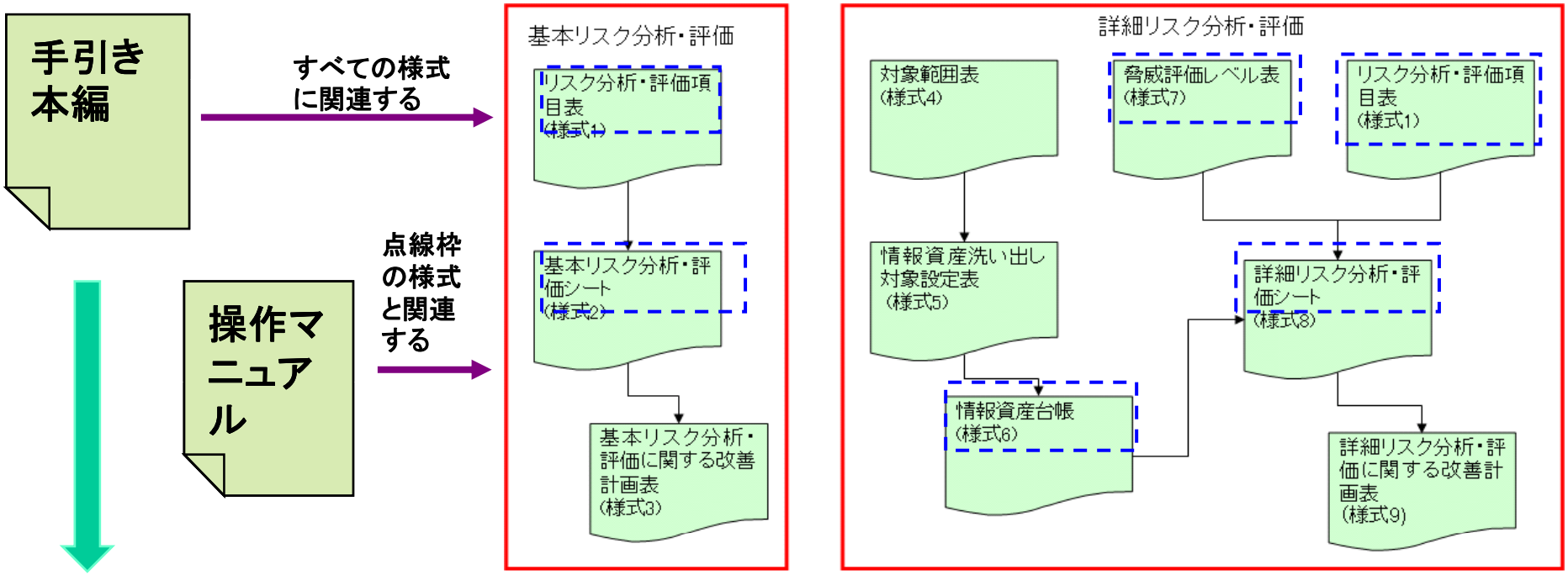
・リスク受容水準と各リスク評価値との差分の自動計算化とリスク対応の有無の自動表示化（様式８）

・脆弱性の評価の例示をあらかじめ設定し、脆弱性評価を行う際の判断材料を提供（様式２、８）

・「脅威」の項目をあらかじめ登録（１５項目）し、各リスク分析・評価項目と最も関係すると思われる「脅威」の項目をあらかじめ関連付け（様式７）

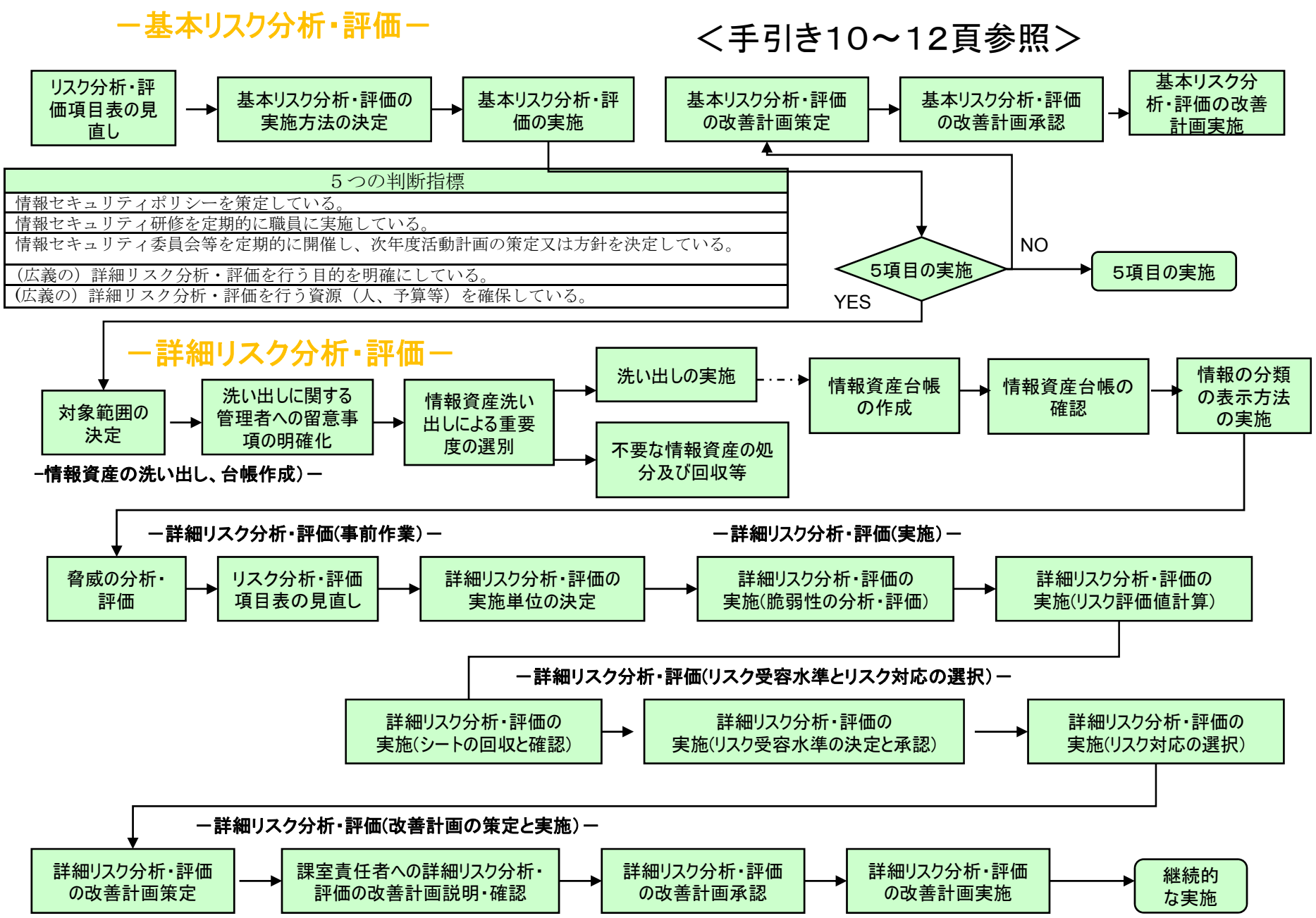
4　本手引きの構成と手引き本編の章立て

・手引きは、リスク分析・評価の方法論を解説した手引き本編に、リスク分析・評価の作業で使用するシート等の付属資料(分析・評価シート)及び分析・評価シートの利用方法を解説した操作マニュアルから構成（手引き本編6頁～8頁参照）。



章	目次	概要
第1章	総則	・本書の目的、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	詳細リスク分析・評価	・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。 ・(狭義の)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。

5　本手引きを基にしたリスク分析・評価の作業フロー



６　本手引きの内容上の主要なポイント

（１）本手引きが対象とする情報資産の種類とその例（手引き21頁参照）

・本手引きが対象とする情報資産の種類は、直接的に対策が行える主要なものに限定する。

図表１－７　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フラッシュメモリ、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(電子文書、ソフトウエア、組織で運用している情報システムのソースコード等を含む。)
設置型ハードウエア ※床置き、机上、ラック等に設置等して使用する資産	サーバ、デスクトップパソコン、ルータ、スイッチ、プリンタ、ファクシミリ、コピー機、スキャナー等
移動型ハードウエア ※持ち出しができるように製造された資産	ノートパソコン、携帯電話、デジタルカメラ、ICレコーダ等

※「人」、「組織の評判、イメージ」等については、基本リスク分析の対象であることや直接対策を行うことが困難であるため、詳細リスク分析の対象となる情報資産から除いている。

６　本手引きの内容上の主要なポイント

（2）リスク分析・評価項目について（手引き21頁参照）

・情報資産のリスク分析・評価をするに当たって必要となるリスク項目については、情報セキュリティ対策のPDCAサイクル及び関連ガイドラインとの整合性確保の観点から、監査ガイドライン（H19.7総務省）の必須監査項目を利用した。
・項目数は、重点的な分析・評価を可能とするべく必須項目の１１０項目した。
・これにより、PDCAサイクル上の後続プロセスである評価（C）における監査の実施に引き継げるようにしている。

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	文言訂正
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	設置型ハードウエア用対策	移動型ハードウエア用対策	管理的対策
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。	30使用不可				採用	不採用	不採用	不採用	不採用	不採用	不採用	・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	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。	30使用不可				採用	不採用	不採用	不採用	不採用	不採用	不採用	・情報セキュリティポリシーに適用する情報資産範囲に関する規定の文書化（抑制）
3	3	○	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、権限及び責任が定められ、文書化されている。	30使用不可				採用	不採用	不採用	不採用	不採用	不採用	不採用	・情報セキュリティポリシー等に組織体制、権限及び責任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）

６　本手引きの内容上の主要なポイント

（３）詳細リスク分析の対象範囲の決定について（手引き51頁参照）

情報資産台帳の作成、リスク分析の実施の実施対象業務の決定について、参考となる考え方を解説。

＜取組の初期段階＞
情報セキュリティを担当する**情報システム課等に限定**し試行的に実施する。

→情報資産の洗い出し、情報資産台帳作成等のノウハウの取得

範囲の拡大

＜2回目以降（その1）＞
住民情報を扱う業務（住民課等）、住民の資産情報等を扱う業務（税務課等）を対象範囲に含める。

→リスクが顕在化した場合の影響を考慮し、情報資産管理の面から重要な個人情報を取り扱う業務を対象とする

範囲の拡大

＜2回目以降（その2）＞
業務の情報システム依存度の高い住民関係業務（住民課）、税務業務（税務課）等を優先的な対象範囲とする。

→情報漏洩が発生した場合の被害の大きさから、システム依存度の高い業務を対象とする。

範囲の拡大

＜3回目以降＞
その他の業務に対象範囲を拡大する。
（予算・決算業務（財政課）、観光業務（観光経済課等）、環境保全業務（環境生活課）等）
→相対的に個人情報を取り扱う場面が少ない業務、システム依存度の低い業務に対象範囲を拡大する。