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

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）	
＜作業の概要＞ 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。 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。	
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]

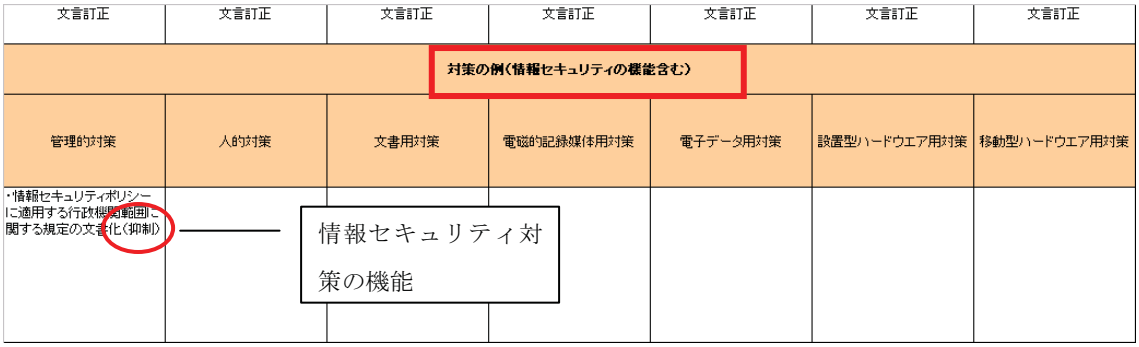
基本リスク分析・評価シート（様式２）では、脅威及び対策の区分の文書用対策から移動型ハードウエア用対策まで列の非表示設定

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	設置型ハードウエア用対策	移動型ハードウエア用対策
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エア用対策まで列の非表示設定



(その 3/4)

(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

（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

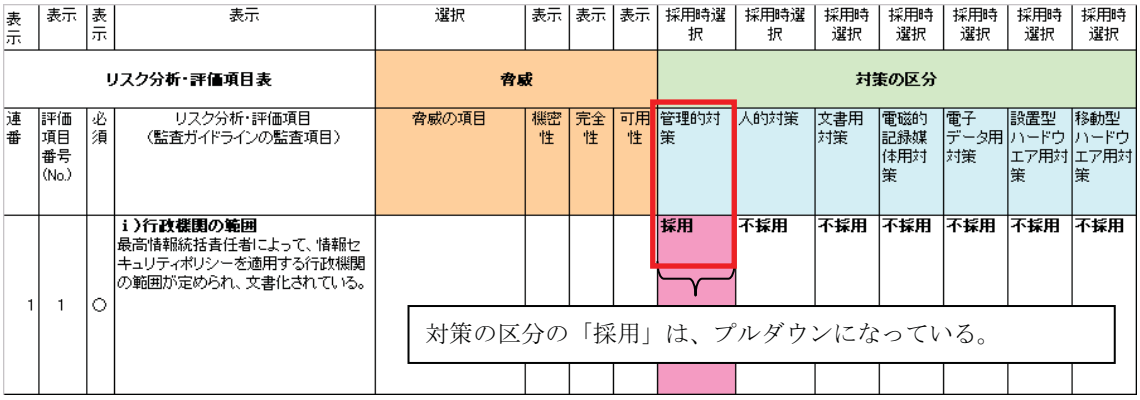
ア 対策の区分の見直しと当該区分「不採用」時の対応

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。



（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、設置型ハードウエア、移動型ハードウエア」に関連する対策の内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、設置型ハードウエア、移動型ハードウエア」に関連する対策の内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
１１２ iii）認証用ＩＣカード等の放置禁止 認証用ＩＣ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ＩＣ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、「○○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ＩＤ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エアの常駐等
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エアの導入により、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)といった複合的効果が得られる。

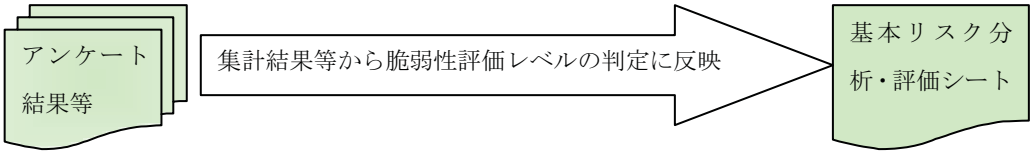
2.4　基本リスク分析・評価の実施

ステップ　（第２章－２）	
＜作業の概要＞ 手順事務局は、基本リスク分析・評価の実施方法を検討の上決定し、基本リスク分析・評価シート（様式２）を利用して、基本リスク分析・評価を実施する。	
分析・評価シート	基本リスク分析・評価シート(様式２)
操作マニュアル目次	2.2 基本リスク分析・評価作業

2.4.1　基本リスク分析・評価の実施方法の検討

事務局は、基本リスク分析・評価の実施に当たって、基本リスク分析・評価シート（様式２）を利用し、(自ら)セルフチェックを実施する。リスク分析・評価項目の内容により事務局だけでは調査しきれない場合は、リスク分析・評価項目を参考にして、全庁又は関係課室へのアンケート、あるいは関係課室へのヒアリングなどの方法により情報収集を行い、これらの結果を基本リスク分析・評価シート（様式２）に反映させる方法も考えられる。

図表２－４　基本リスク分析・評価の実施方法の例



2.4.2　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。

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いますか。

・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れていない。

ハ　引き出し等に一部は入れていない。

ニ　引き出し等に入れていない。

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）×１	12
ロ	4	8	（4+8）×２	24
ハ	7	2	（7+2）×３	27
ニ	6	1	（6+1）×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	設置型ハードウエア用対策	移動型ハードウエア用対策
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	設置型ハードウエア用対策	移動型ハードウエア用対策
・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(対策の例)

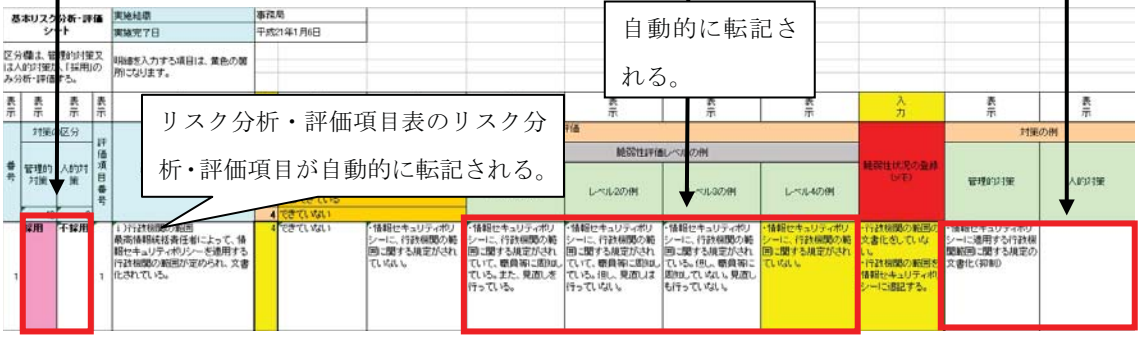
自動的に転記される。

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。

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。

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。



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）	
＜作業の概要＞ 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。 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。 手順３事務局は、改善計画に基づき、改善を実施する。	
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

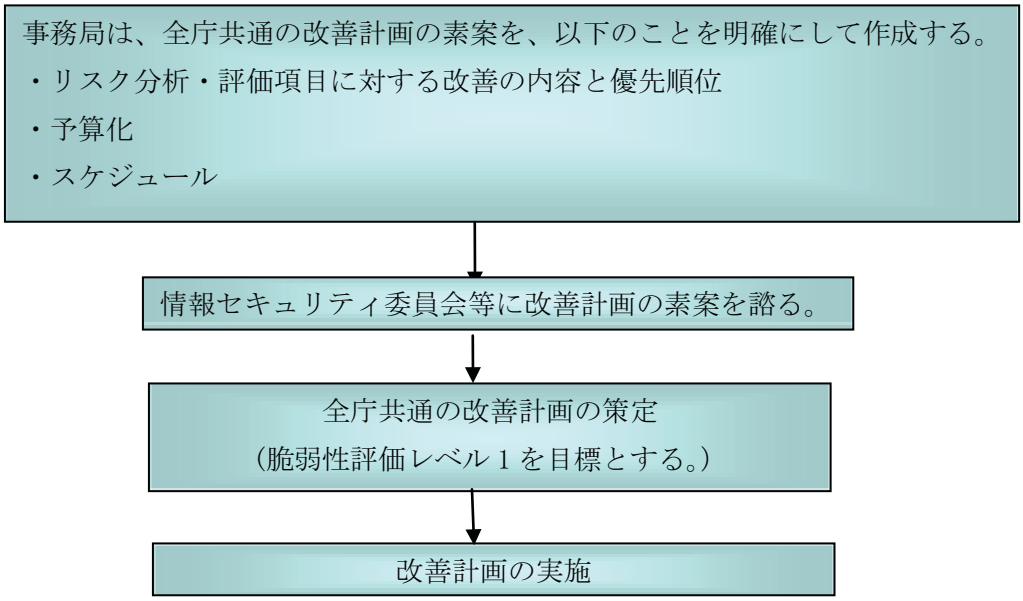
2.5.1　基本リスク分析・評価に関する改善計画の策定から実施までの流れ

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、以下のようになる。（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対して、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
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・評価シートのメモ）	優先順位	改善の実施内容		予算	スケジュール		
	管理的対策	人的対策				優先度高 優先度低	管理的対策	人的対策	(単位：千円)	開始日 (YYYY/MM/DD)	終了予定日 (YYYY/MM/DD)	終了日 (YYYY/MM/DD)
	42	3										
1	採用	不採用	1	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追記する。	高	情報セキュリティポリシーを改正して、庁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　ヘッダ項目の作成

（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。