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

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。

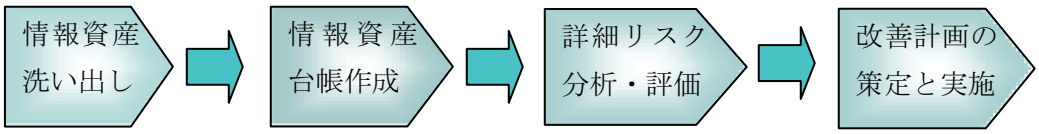
情報資産の洗い出し、情報資産台帳(様式６)の作成については、情報資産の洗い出し対象範囲の決定、情報資産を管理する者の権限及び責任等について解説する。

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、設置型ハードウエア及び移動型ハードウエ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。

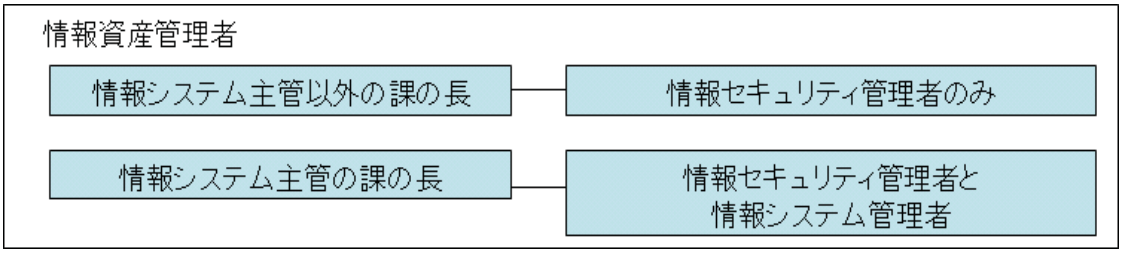
（2） 情報資産管理者の位置づけ

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。

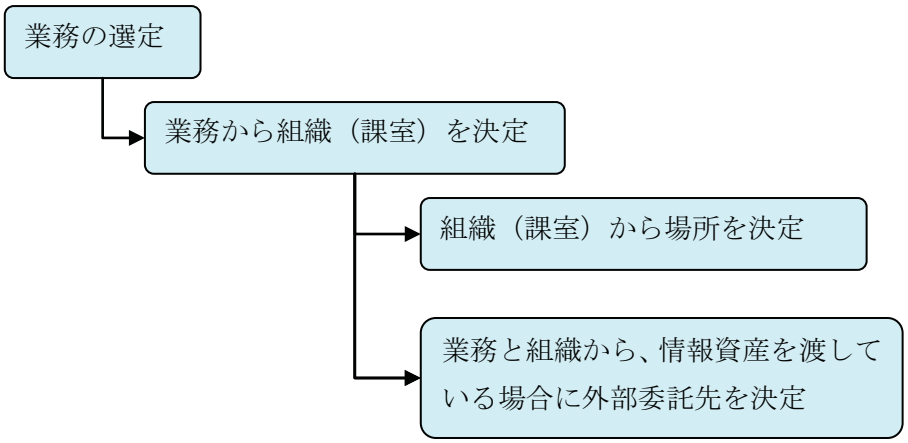
対象範囲を区切らず、全庁で情報資産の洗い出しを行うことが本来あるべき姿である。しかしながら、情報資産の洗い出しは、実施方法の確立段階において試行錯誤も多く、職員の作業負担も大きく、さらに習熟度が低い状況で対象範囲を拡大すると、作業手順や内容面において混乱を招くことも想定される。そのため、最初の取組段階においては、対象範囲を限定してまずは試行的に実施することが、継続的な取組みの観点からは重要である。最初の段階で対象範囲を区切って試験的に行うことは、民間でもよく行われているケースである。

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○○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ＩＳＭＳ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ＩＳＭＳ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で導入されており、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。

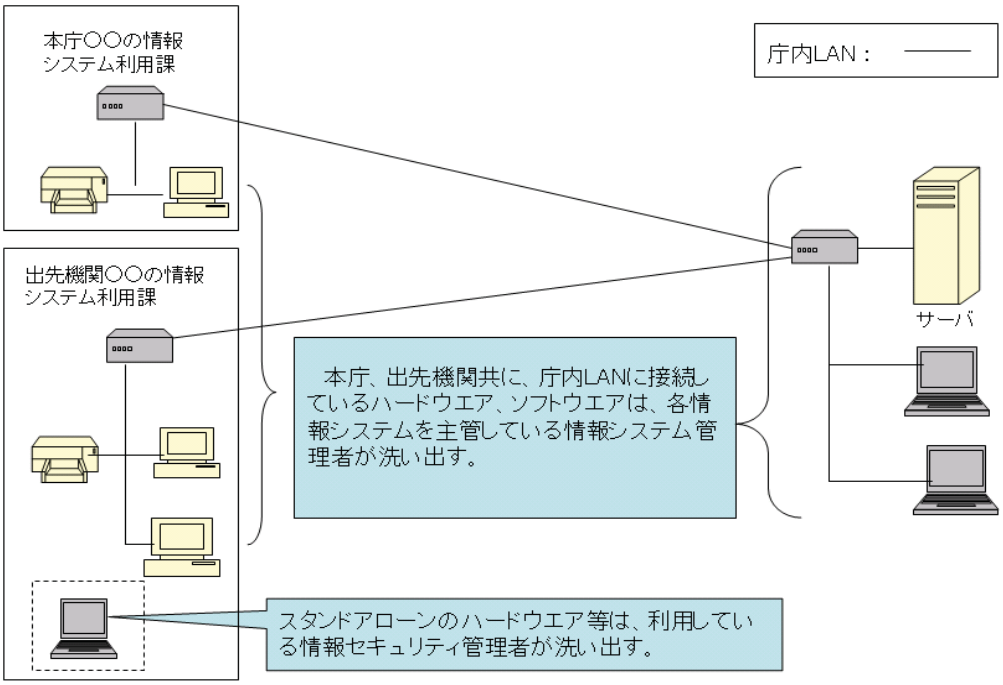
3.2.3　情報資産洗い出し対象の決定

ステップ　（第３章－２）	
＜作業の概要＞ 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。	
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エアは、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エアについては、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エア ・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）

	＜主体その３＞ ･各課室 ＜対象＞ ･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
設置型ハードウエア	＜主体＞ ・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 ＜対象＞ ･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エア
	＜主体＞ ・各課室 ＜対象＞ ･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エア ・ファクシミリ、コピー機等の事務機器
移動型ハードウエア	＜主体＞ ・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 ＜対象＞ ･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エア
	＜主体＞ ・各課室 ＜対象＞ ・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エア ・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エア
外部委託先にある情報資産	＜主体＞ ・情報システム課 ＜対象＞ ･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）	
＜作業の概要＞ 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。 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。 ・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 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。 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。 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。	
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

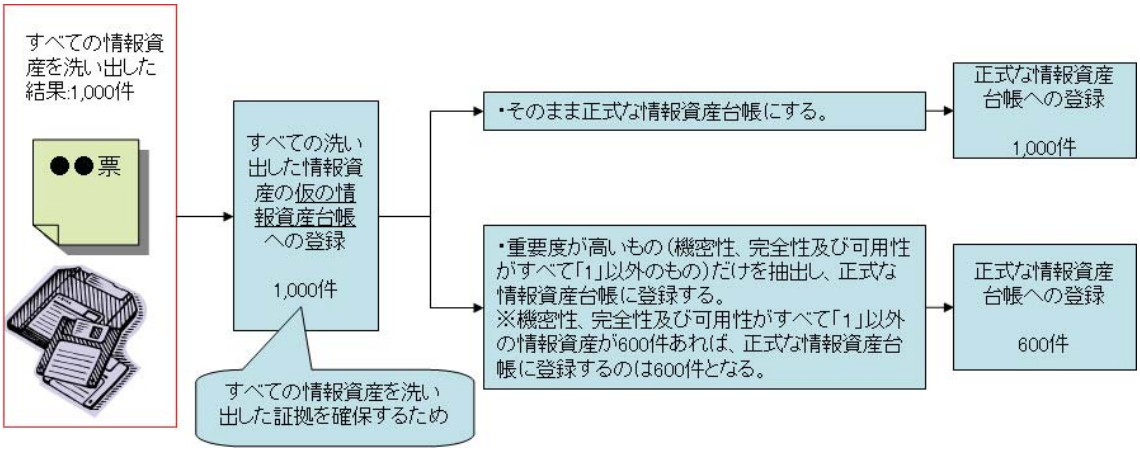
事務局は、情報資産の洗い出しに関する項目を決定する。情報資産の洗い出しに関する項目は、情報資産台帳（様式６）の必須項目を基に設定し、仮の情報資産台帳（様式６）に登録を行う。任意項目の取捨選択については、事務局が、どの程度詳細に情報資産の管理を行うかどうかを検討した上で決定する。なお、仮の情報資産台帳（様式６）に関する項目等は、後述の「3.2.5 情報資産台帳の作成」（63頁）を参照する。

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砕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	・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	・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	・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、職員個人が机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、職員の誰もが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、最も高い機密性に応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、ソフトウエ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	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、以下の手順で進めること。 ・文書、電磁的記録媒体等は、○○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、○○課に連絡し処分方法等を協議する。 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で進めること。 ・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	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。 ・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。 なお、機密区分３以外には特段の表示は不要とする。

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。

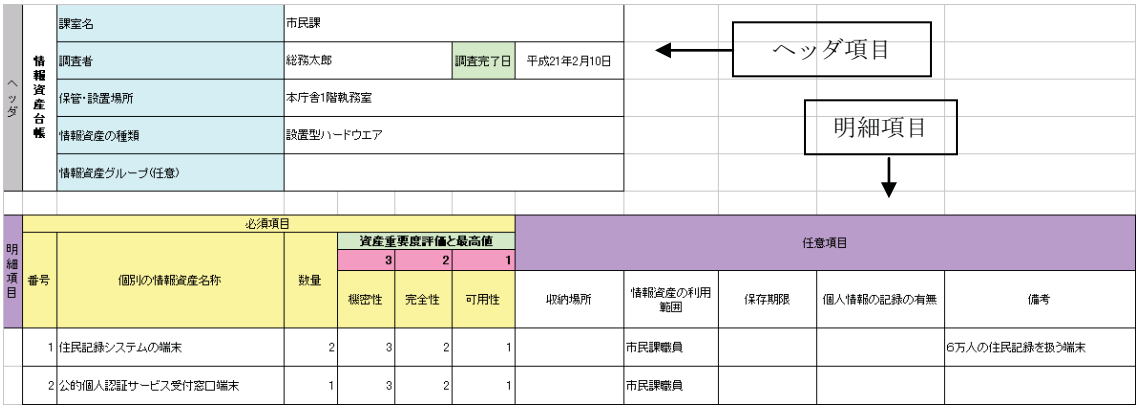
なお、正式な情報資産台帳(様式６)の作成は、仮の情報資産台帳(様式６)に登録されているデータを利用することとなるため、実際の作業上は、情報資産の洗い出しとほぼ同時に正式な情報資産台帳(様式６)の作成も終了していることになる。

3.2.5 情報資産台帳の作成

ステップ （第３章－４）	
＜作業の概要＞ 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。	
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。



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、１×２×５×１０＝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、１×２×５＝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	情報資産台帳	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	設置型ハードウエア		
		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、設置型ハードウエア、移動型ハードウエア）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、設置型ハードウエア、移動型ハードウエアの場合

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、設置型ハードウエア、移動型ハードウエアの保管・設置場所	本庁舎○○課執務室 ○○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、「○○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エ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	・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	「○○会社の執務室」
庁舎外にサーバ等のハードウエアを設置している場合	「○○会社データセンタ」
ＡＳＰ・ＳａａＳを利用している場合	「○○会社の○○ＳａａＳ」
文書や電磁的記録媒体を保管業者に預けている場合	「○○会社の○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　情報資産の種類の選択肢

・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

（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	・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	・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等のソフトウエアの原本 ・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	・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エア ・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 ハードウエア	・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エア ・その他の設置型のハードウエア(封入封緘機等)
移動型 ハードウエア	・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エア ・その他の移動型のハードウエア(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、「○○課用デジタルカメラ」とする。

・例えば、○○部で利用している○○申請書であれば、「○○部○○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が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、○○データベース、○○プログラムファイル、○○情報、○○課業務関係、○○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　設置型ハードウエア

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　移動型ハードウエア

設置型ハードウエ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、「○○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	・住民票交付綴 ・選挙人名簿管理綴 ・○○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	・オペレーティングシステムのソフトウエア原本（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	・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 ・（ファィルサーバの）○○課フォルダー ・（文書管理システムの）○○課事業計画 ・○○ＳａａＳのデータ
設置型ハードウエア	・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（○○社製）
移動型ハードウエア	・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	・○○システム開発テスト結果綴
	電磁的記録媒体	・○○システム開発のテスト結果（MO）
	設置型ハードウエア	・基幹系システムの開発用端末(デスクトップパソコン)
	移動型ハードウエア	・情報系システムの端末(ノートパソコン)
サーバ室	文書	・○○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) ・○○ソフトウエアＣＤ(原本)
	設置型ハードウエア	・メールサーバ(○○社製) ・ファイルサーバ(○○社製) ・ウイルス監視サーバ(○○社製) ・基幹系システム(○○社製) ・大型レザープリンタ(○○社製) ・レイヤ３スイッチ(○○社製) ・インターネット接続用ルータ(○○社製) ・ファイアウォール機器(○○社製)
	移動型ハードウエア	・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		・オペレーティングシステム(Ｌｉｎｕｘ等) ・メールサーバソフトウエア(Ｓｅｎｄｍａｉｌ等) ・ＤＮＳ[16]ソフトウエア(ＢＩＮＤ[17]等) ・Ｗｅｂサーバソフトウエア(Ａｐａｃｈｅ等) ・ファイルサーバソフトウエア(○○社製) ・○○イントラネットシステム ・○○グループウエア ・○○パスワードファイル ・○○ログファイル メールサーバの送受信内容(※ＩＭＡＰ[18]を利用している場合)
住民記録システム		・住民記録データベース ・○○データベースソフトウエア(○○社製) ・○○オペレーティングシステム(○○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		・国民健康保険データベース ・○○データベースソフトウエア(○○社製) ・○○オペレーティングシステム(○○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		・職員人事情報データベース ・職員給与マスタファイル ・○○データベースソフトウエア(○

[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	・住民票発行綴 ・印鑑証明書発行綴
	電磁的記録媒体	・戸籍情報バックアップ(ＤＡＴ)
	設置型ハードウエア	・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
	移動型ハードウエア	・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	(例:フォルダー単位) ・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		・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		フォルダーの例 ・市民課勤務データ ※　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。

（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：№.１～№.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:№.１～№.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	「○○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	「○○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、○○ソフトウエアの場合は、件数の把握が困難なため、「１」とすることでもよい。

d　設置型ハードウエア

・　入力単位

　「台」

・　入力方法

　同じ業務で使用するハードウエアが１０台ある場合は、「１０台」と入力する。

　ハードウエアで制御装置、磁気ディスク装置等を一体的に構成しているハードウエア群は、「１台」として入力する。

　デスクトップパソコン等で、マウス、キーボート等を接続している場合は、マウス、キーボート等を含め全部で「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エア

【個人情報を保存している機器】

　ハードウエ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　移動型ハードウエア

・ 入力単位

「台」

・ 入力方法

設置型ハードウエ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。設置型ハードウエア及び移動型ハードウエアに関しては､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エア[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] ハードウエ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エア。
[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３－２１　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	・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の漏えい等が想定される。 ・設置型ハードウエア又は移動型ハードウエアについて、不正利用による個人情報の漏えい等が想定される。	・健康診断情報、ケースワーカによる訪問履歴、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	・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。 ・設置型ハードウエア又は移動型ハードウエアの場合、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。	・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、入札公告前の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	・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。	・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	・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。 ・ソフトウエ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。 ・設置型ハードウエア又は移動型ハードウエアの場合、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	・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、移動型ハードウエア、設置型ハードウエア)

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

・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、ソフトウエア(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、設置型ハードウエア及び移動型ハードウエ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	設置型ハードウエア	コピー機(２号機)	総務課職員
庁舎内の執務室全部	移動型ハードウエア	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	○○市(法人)から○○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)	
＜作業の概要＞ 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。 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。	
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。

・保管場所が違うだけで、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。

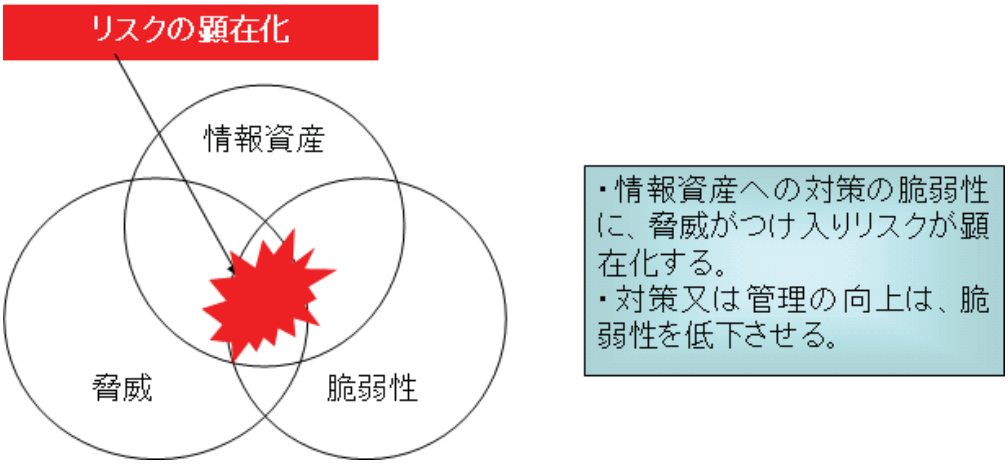
3.3　詳細リスク分析・評価の実施

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）	
＜作業の概要＞ 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。 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。 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。	
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 ハードウエア・回線(ケーブル)の故障又は損傷 ソフトウエアのバグ、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・端末のソフトウエアへの不正設定 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
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ハードウエア・回線(ケーブル)の故障又は損傷		3	3
06ソフトウエアのバグ、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・端末のソフトウエアへの不正設定	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			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			

脅威の項目と発生頻度は、必要に応じて変更する。

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。

発生頻度の設定は、選択肢（1、2、3）から選択する。

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。

16番以降に追加する。

連番の初期値は変更しない。

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。

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エ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] ＩＳＭＳ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３－３２　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、脅威がどのようにつけ入るのか、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３－３３　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	発生頻度の設定		
脅威の項目	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 ハードウエア・回線(ケーブル)の故障又は損傷		3	3
06 ソフトウエアのバグ、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３－３３　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３－３３　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。

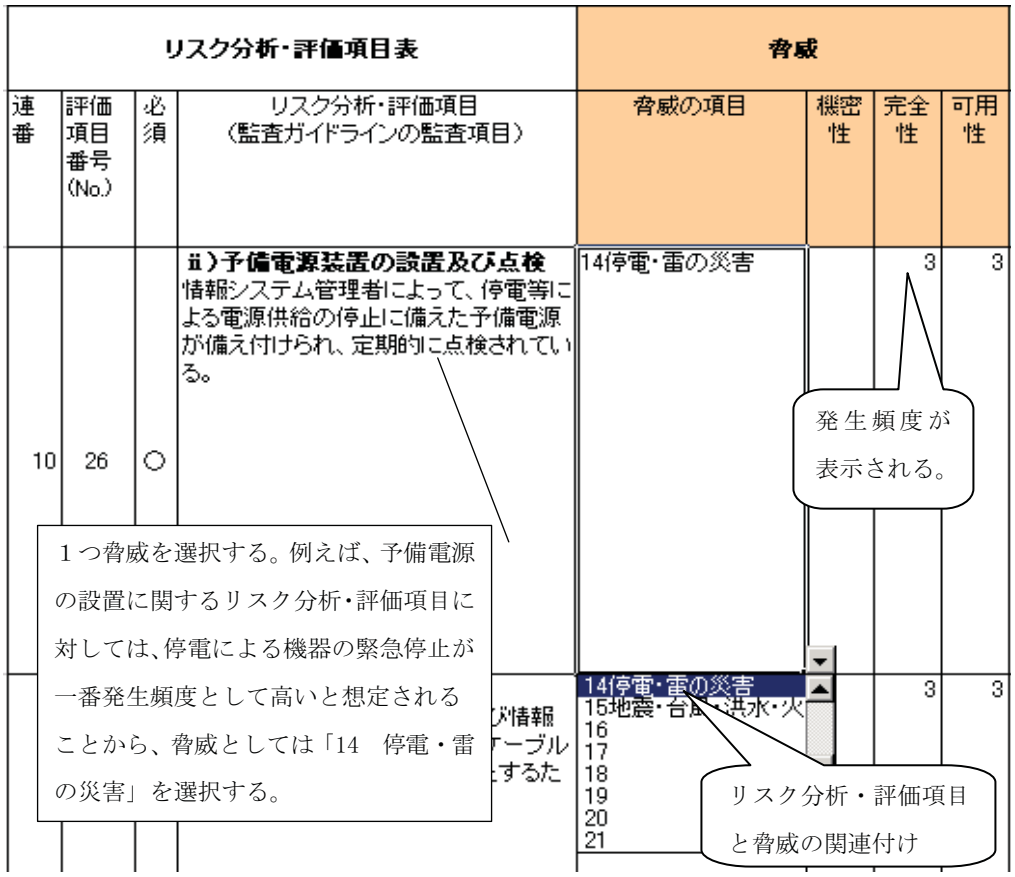
参考　１つの対策で、複数の脅威に対抗する例

・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



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)	
＜作業の概要＞ 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。	
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】、【設置型ハードウエア用対策】、【移動型ハードウエア用対策】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じである。

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

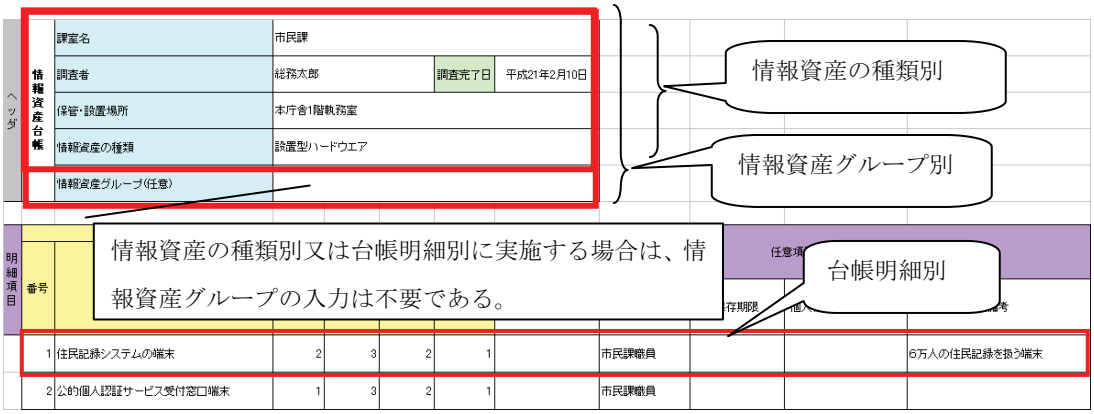
保管・設置場所や情報資産の利用・保管状況により対策が不要な場合には、以下の分析・評価シート上でも、リスク分析・評価項目表（様式１）の対策の区分と同様に、「採用」→「不採用」への変更が直接可能である。

・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。



(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 登録に付き、110 項目の分析・評価ということになり、総評価数は、22,000 回になる。	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	情報資産グループが 28 で、リスク分析・評価項	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 グループに付き、110 項目の分析・評価ということになり、総評価数は、3,080 回になる。 ※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。	精度が高くない。	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 種類に付き、110 項目の分析・評価ということになり、総評価数は、550 回になる。	情報資産の種類別の列の最高値の機密性、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高くない。	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] ＩＳＭＳ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)	
＜作業の概要＞ 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。	
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

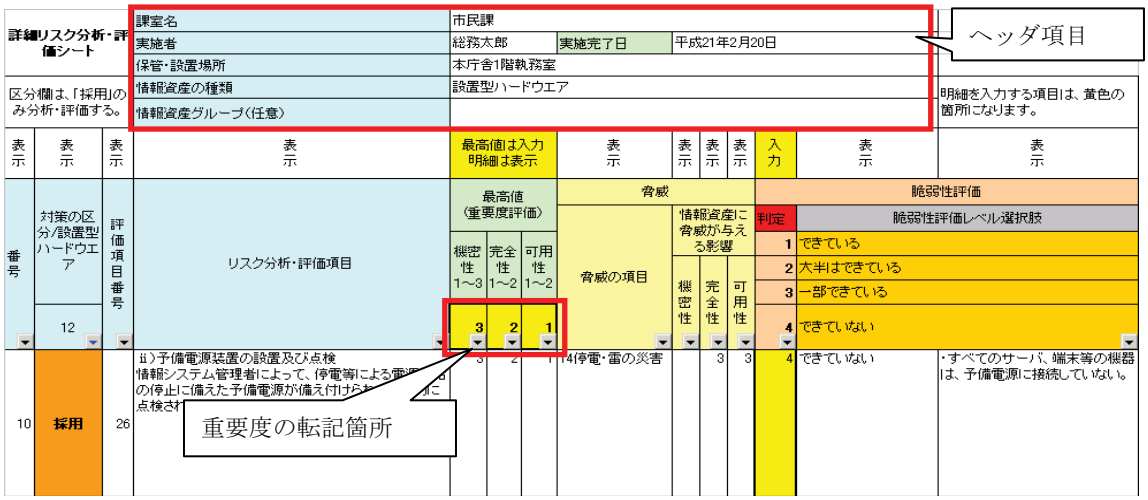
ステップ　（第３章－９）
＜作業の概要＞ 手順１情報資産管理者が主導し、詳細リスク分析・評価シート（様式８）を利用して、事務局から通知された実施単位を基にリスク分析・評価を実施する。 詳細リスク分析・評価の実施の要点は、以下のとおりである。 ・詳細リスク分析・評価シート（様式８）に情報資産台帳（様式６）から転記又は入力する。 ・情報資産台帳単位で機密性、完全性及び可用性の情報資産の重要度（最高値）を転記する。 ・事前に設定したリスク分析・評価項目表（様式１）からの参照情報（脅威の分析・評価結果等が表示）を基に、脆弱性の判定を実施する。また対策の不備や改善案は、「脆弱性状況の登録」欄に必要に応じてメモする。 ・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。 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。 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。 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。 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。 手順６事務局は、リスク対応を選択する。

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

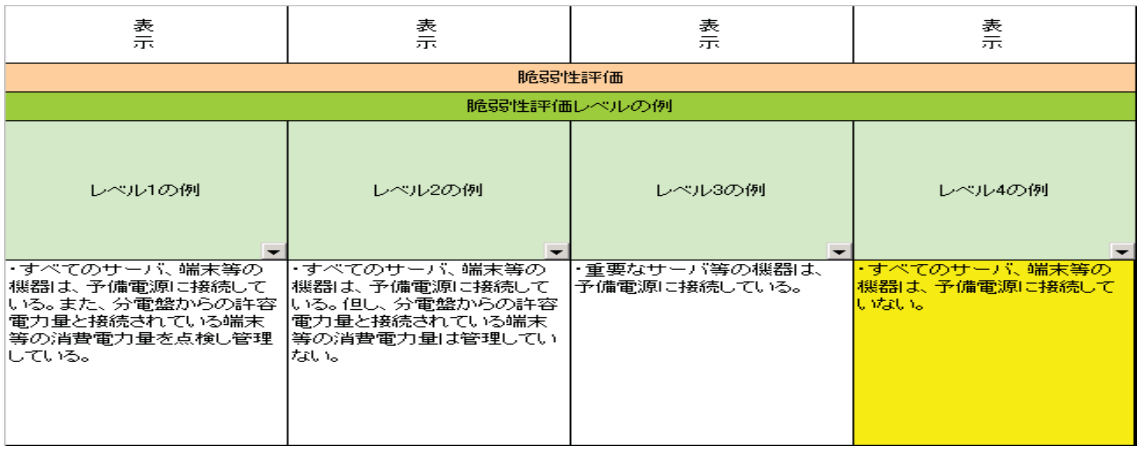
3.3.6.1 詳細リスク分析・評価シート（様式８）のレイアウト

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。

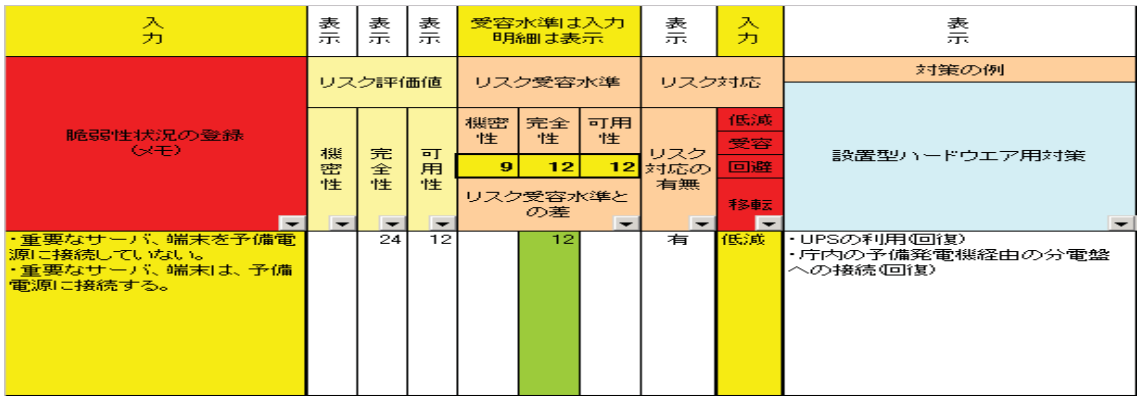
(その 1/3)



(その 2/3)



(その 3/3)



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、設置型ハードウエア、移動型ハードウエア」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、入力は不要である。

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。

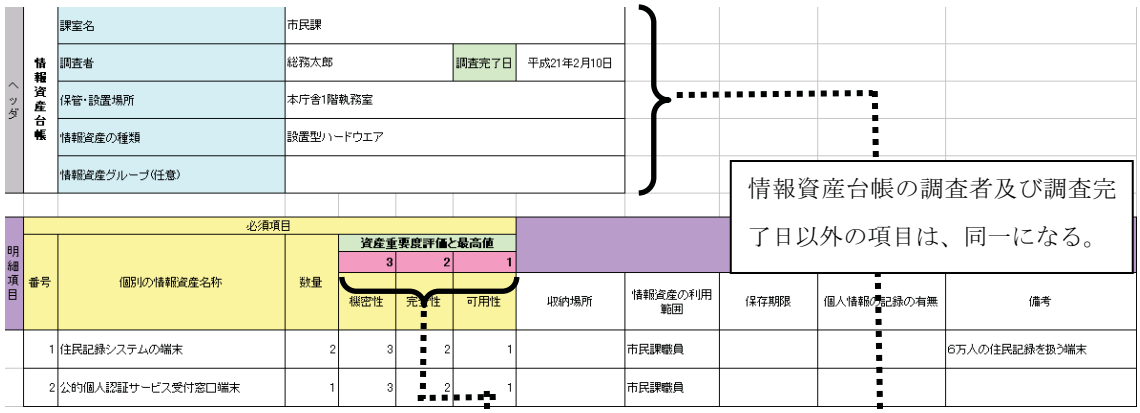
図表３－３７　実施単位を基にした詳細リスク分析・評価シート(様式８)への転記方法

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	情報資産台帳	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	設置型ハードウエア		
		情報資産グループ(任意)			

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。

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 機密性	2 完全性	1 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	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）

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。

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						
	保管・設置場所	本庁舎1階執務室									
区分欄は、「採用」のみ分析・評価する。	情報資産の種類	設置型ハードウエア									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	最高値は入力明細は表示			表示	表示	表示	表示	入力	表示	表示
番号	対策の区分/設置型ハードウエア	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 ～3	完全性 1～2	可用性 1～2	脅威 脅威の項目	情報資産に脅威が与える影響 機密性	完全性	可用性	脆弱性評価 判定	脆弱性評価レベル選択肢	
	12			3	2	1					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	
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	4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

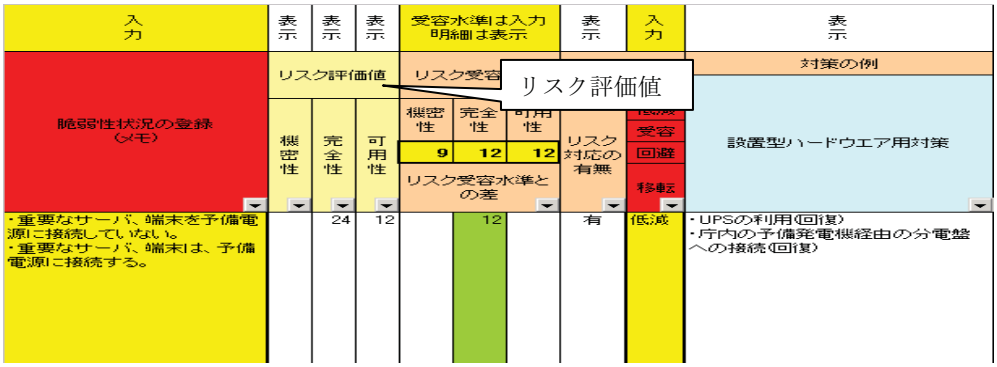
ア リスク評価値の計算方法

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

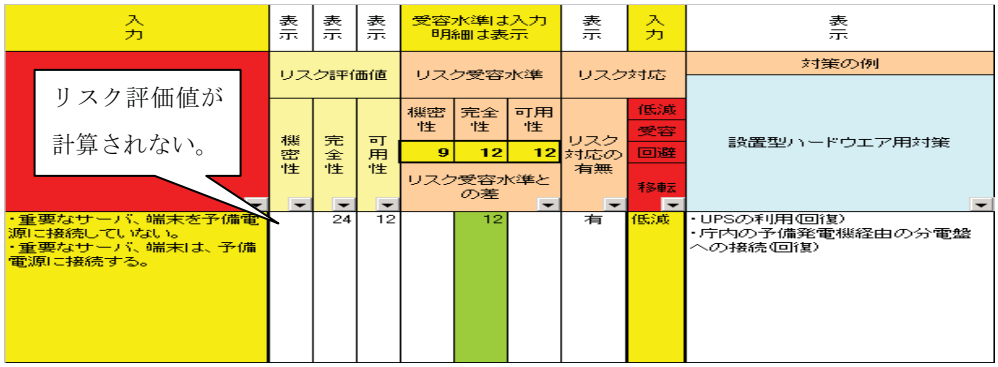


（詳細リスク分析・評価シート）

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



（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「１２」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「１２」以下とした場合、「１２」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

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らない。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	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

リスク受容水準「2」

リスク評価値「3」

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

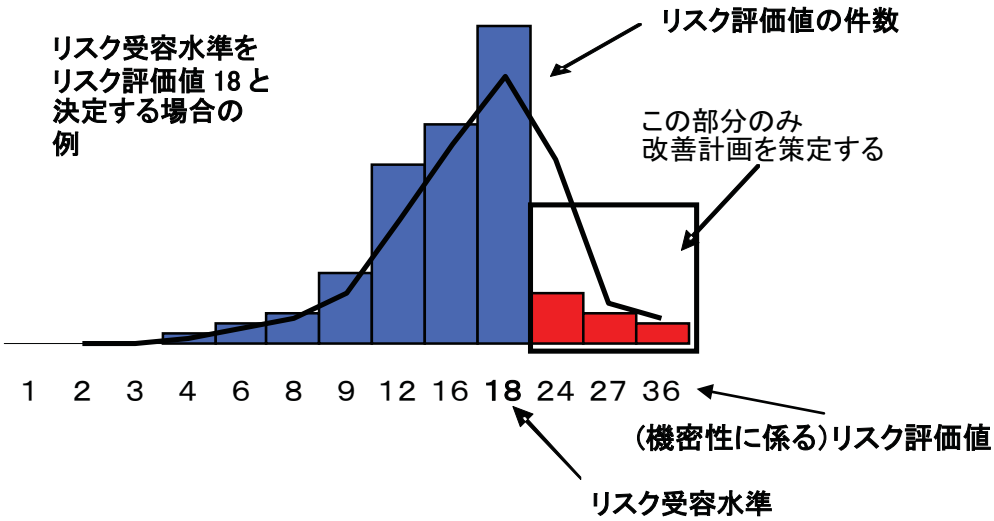
手順３	実施主体：事務局

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、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。

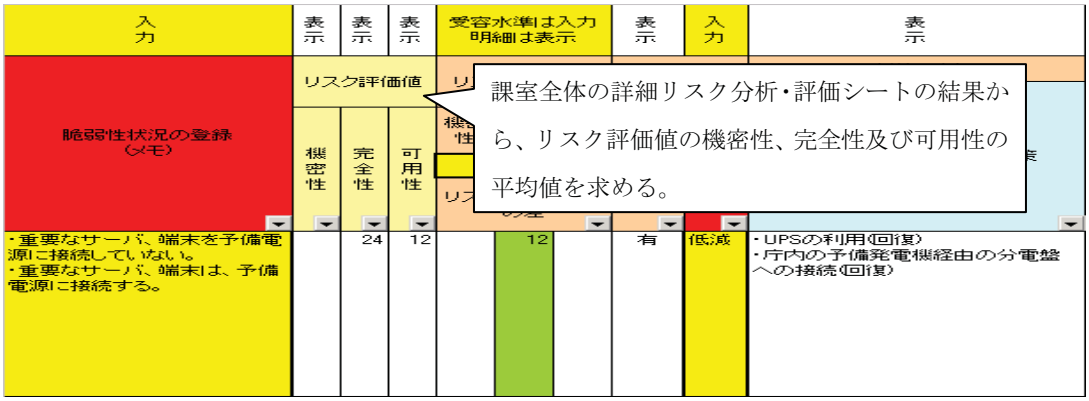
図表３－４５　リスク受容水準の決定に関する考え方の例１



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



(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、表計算ソフトウエアのため、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

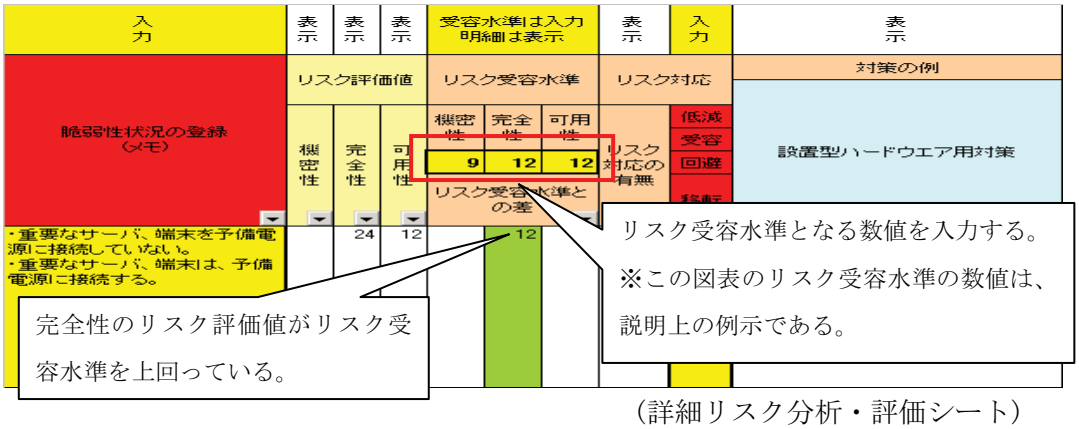
手順５	実施主体：事務局

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



（詳細リスク分析・評価シート）

（７）　残留リスクについて

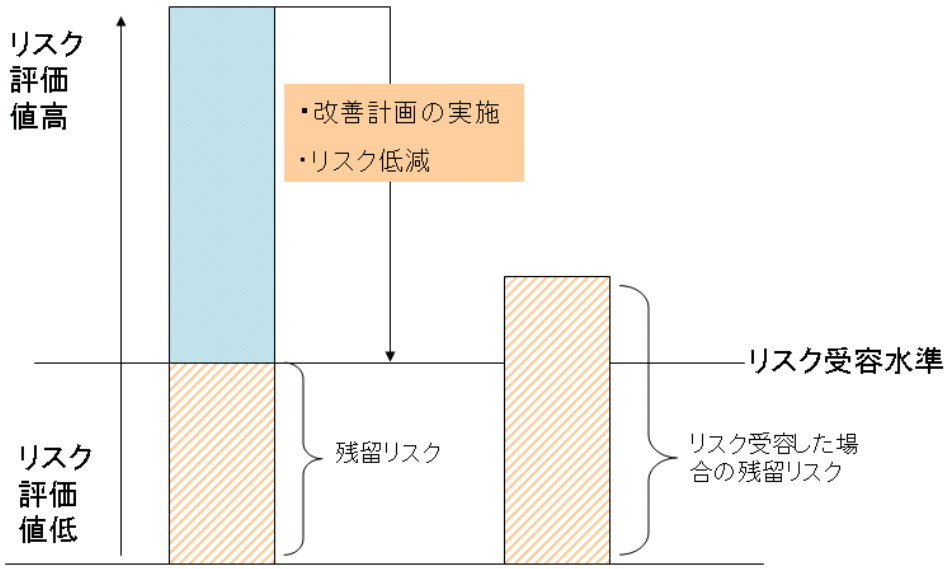
残留リスクとは、リスク受容水準まで脆弱性を改善しても残留するリスクをいう。

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、紛失等を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

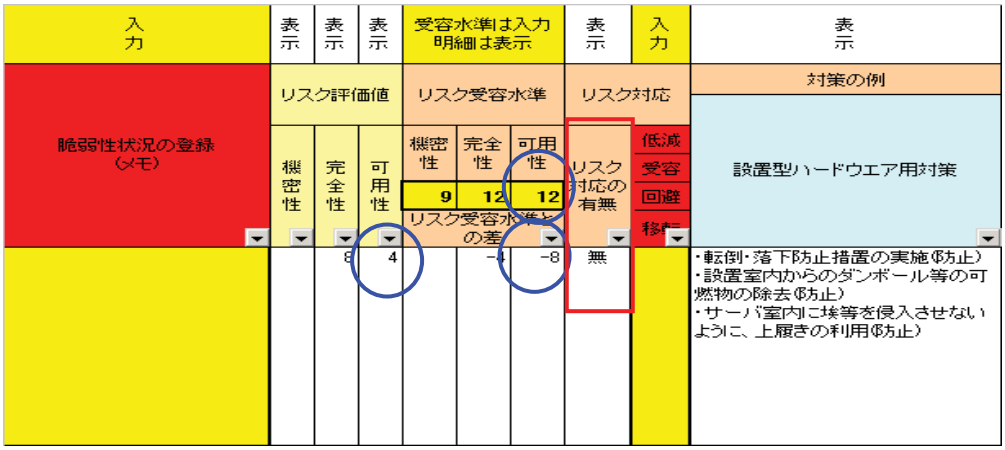
	差分の結果の解釈	リスク対応の有無
機密性、完全性、可用性の内一つでも差分の結果がプラスの場合	リスク対応が必要	リスク対応が必要である。この場合、「リスク対応」欄に「有」が表示される。

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 ※差分がゼロの場合、リスク受容水準との差の欄は、表計算ソフトウエア（ゼロ値非表示設定）の都合上、空欄になる。	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	・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。

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　差分がマイナスの例



（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（個人情報の不要な複写物の廃棄等）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。

ここがポイント 「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と、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）	
＜作業の概要＞ 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。 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。 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。 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。	
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

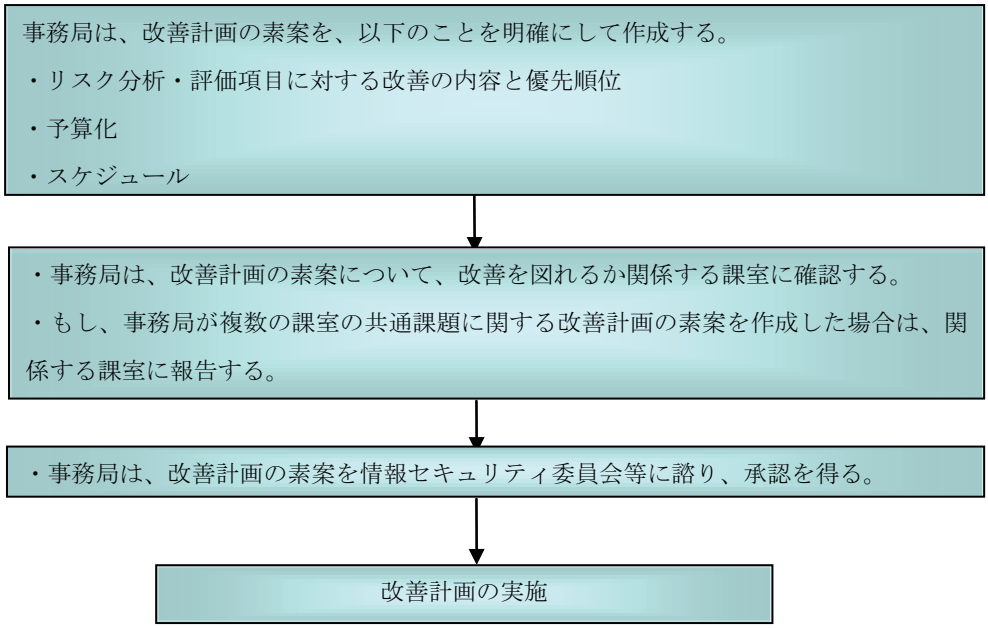
3.4.1　詳細リスク分析・評価に関する改善計画の策定から実施までの流れ

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３－５２　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	設置型ハードウエア							
	情報資産グループ(任意)								
表示	表示	表示	表示	必要に応じて、詳細リスク分析・評価シートから貼り付けて利用する。	入力	入力	入力	入力	入力	入力
番号	対策の区分/設置型ハードウエア	評価項目番号	リスク分析・評価項目	脆弱性状況の登録 (詳細リスク分析・評価シートのメモ)	優先順位 優先度高 優先度低	改善の実施内容 設置型ハードウエア用対策	予算 (単位:千円)	スケジュール 開始日 (YYYY/MM/DD)	スケジュール 終了予定日 (YYYY/MM/DD)	スケジュール 終了日 (YYYY/MM/DD)
12										
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。	・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。	高	重要なサーバ、端末を3月22日(日曜日)に予備電源に接続する工事を行う。	500	平成21年3月3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、設置型ハードウエア、移動型ハードウエ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エ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）設置型ハードウエア用対策

・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）移動型ハードウエア用対策

・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	○○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							
			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	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	○○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	WindowsXPリカバリ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	○○太郎	調査完了日	平成21年1月15日	
	保管・設置場所	情報系システム			
	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	グループウエアのデータ	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(ポリシ、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サーバーで公開
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ソフトウエア(BIND)	1	2	2	2		情報政策課職員		無し	
10	メールソフトウエア(SENDMAIL)	1	2	2	2		情報政策課職員		無し	
11	Webソフトウエア(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	

設置型ハードウエア

情報資産台帳				
	課室名	情報政策課		
	調査者	○○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	設置型ハードウエア		
	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	基幹系システムサーバ	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			

移動型ハードウエア

情報資産台帳					
	課室名	情報政策課			
	調査者	○○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	移動型ハードウエア			
	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							
			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	情報系システムの端末	15	3	2	2	机上	情報政策課職員			
2	基幹系システムの端末	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	貸出用パソコン	4	2	1	1	ロッカー	全職員			