DM6-06-071

外部委託における情報セキュリティ対策に関する
評価手法の利用の手引

2007 年 11 月

内閣官房情報セキュリティセンター

改訂履歴

改訂日	改訂理由
2006/5/12	初版
2007/11/9	ISMS 適合性評価制度の改訂の反映（資料１） 情報セキュリティ対策ベンチマークの改訂の反映（資料２） 政府機関統一基準(第２版)の策定に伴う修正（資料１、２及び３）

目次

1　本書の目的

本書は、府省庁が情報処理業務を外部委託により行う場合に、委託先の情報セキュリティの確保を目的として各種評価手法を府省庁において利用するための手引書である。

府省庁において情報処理業務を外部委託により行う場合には、府省庁が求める情報セキュリティ水準が委託先において確保される必要がある。このため、府省庁では、情報セキュリティ関係規程の一つとして外部委託についても規程を定めることが想定されている。この規程に従い府省庁としての業務を行うに当たり、情報セキュリティマネジメントシステムに関する適合性評価制度、情報セキュリティ対策ベンチマーク及び情報セキュリティ監査の各評価手法を活用することができる。

本書は、府省庁で情報処理業務の外部委託に責任を持つ情報システムセキュリティ責任者及び調達担当者に対してこれらの制度を適切に利用するための情報を提供し、もって情報処理業務の外部委託における情報セキュリティの確保に資することを目的とする。

2　情報セキュリティ確保の枠組み

情報処理業務を外部委託により行う場合には、以下の枠組みにより情報セキュリティの確保を図ることとなる。

(1) 外部委託の可否の判断
　対象情報処理業務について、これに係る情報システム及び情報に照らして、情報セキュリティ確保の観点から、これを外部委託により行うことの可否を判断すること。

(2) 委託先の選定
　調達において、委託先候補の事業の安定性と情報セキュリティ対策の遂行能力を検討の上、委託先を選定すること。

(3) 実施する情報セキュリティ対策に関する合意
　当該外部委託に係る情報処理業務において委託先が実施すべき情報セキュリティ対策に関して、府省庁及び委託先が合意し、契約に含めること。

(4) 情報セキュリティ対策の実施
　委託先が、当該業務の遂行において、合意した情報セキュリティ対策を実施すること。

(5) 情報セキュリティ対策の履行状況の確認
　委託先における情報セキュリティ対策の履行状況について、府省庁による確認がなされること。

(6) 是正措置
　委託先における情報セキュリティ対策の履行状況の確認の結果、必要であればこれが是正されること。

3　各種制度と利用場面

外部委託において利用できる評価手法として、主に以下の 3 つの制度がある。

- 情報セキュリティマネジメントシステムに関する適合性評価制度
- 情報セキュリティ対策ベンチマーク
- 情報セキュリティ監査

「(2) 委託先の選定」においては、委託先候補が情報セキュリティマネジメントシステムに関する適合性評価制度に基づく認証を取得していること、又は情報セキュリティ対策ベンチマークの結果が求める成熟度に達していることを、選定における評価の要素に含めることができる。また、将来的には、情報セキュリティ監査の結果を選定における評価の要素に含めることも想定される。

「(5) 履行状況の確認」においては、業務における定常的な確認に加えて、委託先における当該情報処理業務を対象にした情報セキュリティ監査が活用できる。

これらの制度はそれぞれの特徴に応じて適切な場面で有効に活用することが重要であることから、本書添付の各資料において利用方法を説明している。

なお、情報セキュリティマネジメントシステムに関する適合性評価制度については、我が国において財団法人日本情報処理開発協会(JIPDEC)が運営している「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」を基に説明することとする。

4　本書の構成

本書は、ISMS 適合性評価制度、情報セキュリティ対策ベンチマーク及び情報セキュリティ監査の各制度については、専門的な知見に基づく説明書の必要性が高いことから、制度を運用しているそれぞれの組織が資料を作成し、これらを内閣官房が取りまとめたものである。内容については経済産業省、特定非営利活動法人日本セキュリティ監査協会 (JASA)、財団法人日本情報処理開発協会及び内閣官房情報セキュリティセンターがタスクフォースを構成して共同で検討し、その成果を各資料に反映している。本書の構成は以下のようになっている。

資料 1
「外部委託における ISMS 適合性評価制度の利用方法」
財団法人 日本情報処理開発協会、2007 年 11 月

資料 2
「外部委託における情報セキュリティ対策ベンチマークの利用方法」
経済産業省、2007 年 11 月

資料 3

「外部委託における情報セキュリティ監査の利用方法」

特定非営利活動法人 日本セキュリティ監査協会、2007 年 11 月

資料１

外部委託における ISMS 適合性評価制度の利用方法

本書は、財団法人日本情報処理開発協会（JIPDEC）により作成されたものである。

改訂履歴

改訂日	改訂理由
2006/5/12	初版
2007/11/9	ISMS 適合性評価制度の改訂の反映 政府機関統一基準(第２版)の策定に伴う修正

目次

1 はじめに

1.1 本書の目的

本書は、各府省庁において情報処理業務を外部委託により行う場合に、調達担当者、情報システムセキュリティ責任者及び課室情報セキュリティ責任者が委託先の選定に ISMS 適合性評価制度を活用するためのガイドである。

本書は、委託先候補における情報セキュリティ対策の履行状況を確認する手段として ISMS 適合性評価制度を利用する場合に、解説書として活用することを目的としたものである。

1.2 適用対象者

各府省庁で情報処理業務の外部委託に係る調達手続を行う調達担当者、当該情報システムの情報システムセキュリティ責任者、及び当該情報処理に係る課室情報セキュリティ責任者

1.3 関連規程

府省庁で策定する「外部委託における情報セキュリティ対策実施規程」又はこれに相当する文書

2 ISMS 適合性評価制度

2.1 ISMS 制度の概要

2.1.1 ISMS 制度の目的

ISMS（Information Security Management System）適合性評価制度（以下、「ISMS 制度」という。）は、国際的に整合性のとれた情報セキュリティマネジメントに対する第三者適合性評価制度である。ISMS 制度は、わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としている。

2.1.2 ISMS 制度の認証基準

認証基準とは、第三者である認証機関が ISMS 制度の認証を希望する事業者の適合性を評価するための基準のことである。ISMS 制度では JIS Q 27001:2006（ISO/IEC 27001:2005）を認証基準として用いている。

2.1.3 ISMS 制度の運用体制

ISMS 制度は、組織が構築した ISMS が JIS Q 27001:2006（ISO/IEC 27001:2005）に適合しているかを審査し登録する「認証機関」、審査員の登録及び審査員になるための研修コースの承認を行う「要員認証機関」、そしてこれらの各機関の業務遂行能

力をみる「認定機関（JIPDEC(財団法人日本情報処理開発協会)/情報マネジメント推進センター)」からなる総合的な仕組みである。

なお、運用体制の詳細については、次の「図　制度のスキーム」を参照されたい。

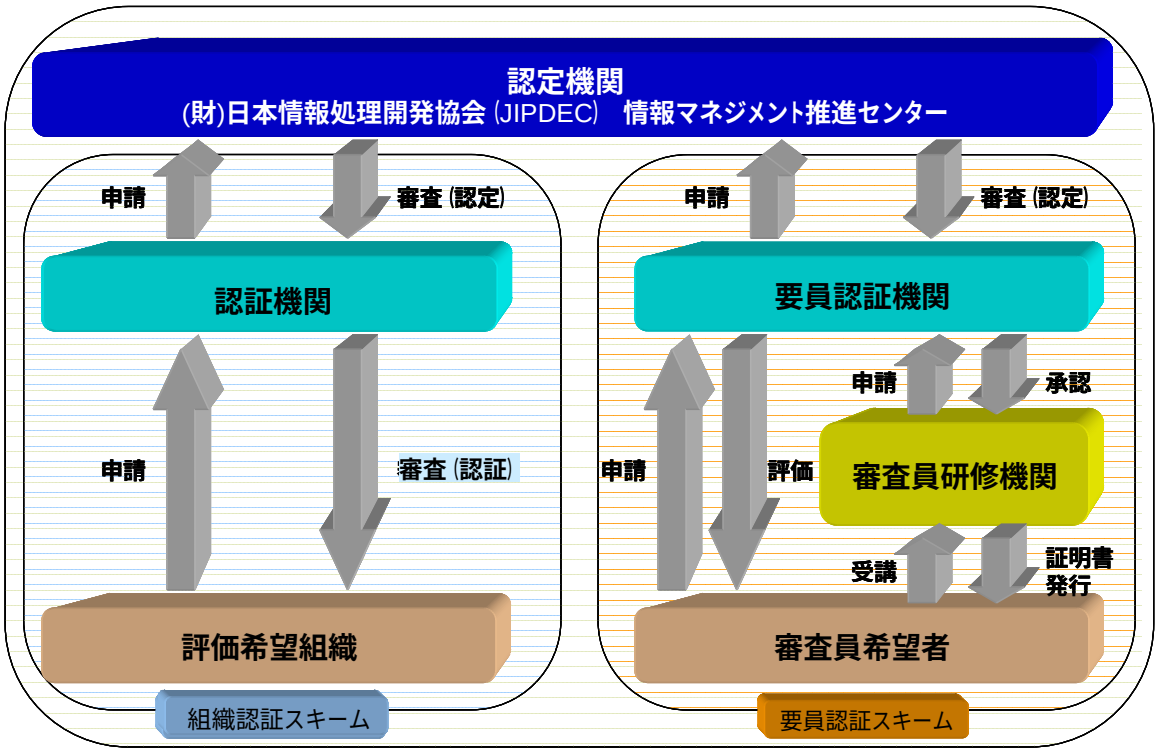


図　制度のスキーム

2.1.4 ISMS 制度に関する情報公開

ISMS 制度の概要や認定された認証機関については、次の URL を参照されたい。

- ISMS 適合性評価制度のホームページ　http://www.isms.jipdec.jp/
- ISMS 認証機関一覧　http://www.isms.jipdec.jp/lst/isr/index.html
- 認証取得事業者一覧　http://www.isms.jipdec.jp/lst/ind/index.html

2.1.5 ISMS 制度に関する問い合わせ先

ISMS 制度に関するお問い合わせにつきましては、電子メールにて財団法人日本情報処理開発協会情報マネジメント推進センター（info@isms.jipdec.jp）まで

- URL；　http://www.isms.jipdec.jp/ask/index.html

2.2　ISMS 制度の活用

各府省庁では委託先の選定に当たり、委託先における事業の安定性に加え、委託す

る業務の種類に応じて必要とされる情報セキュリティ対策の遂行能力が要求する水準に到達していることを確認することが望ましい。一般的に ISMS 認証を取得している企業であれば、情報セキュリティマネジメントに関して一定の水準に到達していることを容易に確認でき、これを第三者の認証機関が客観的に評価・認証していることから、委託先の候補者が ISMS 認証を取得しているか否かを委託先の選定における評価に利用することは、極めて効果的かつ信頼性が高いといえる。

具体的には、ISMS 認証は、「情報セキュリティを確保するための体制の整備」、「取り扱う府省庁の情報の秘密保持等」及び「情報セキュリティが侵害された場合の対処」といった情報セキュリティ対策を客観的に評価する指標として参考にできる。

技術的対策の詳細については、認証を取得している事実のみからすべて充足しているとする根拠とはならないことに留意する必要がある。これについては、委託先が、委託先の ISMS を対象として過去に内部監査又は情報セキュリティ監査を行っていた場合に、必要に応じて、その結果報告書や適用宣言書と呼ばれる対策の採否の一覧の提出を求め、確認することもできる。

3　ISMS 認証の活用方法

委託先の選定に ISMS 認証を活用する際には、次の２点の文書を確認することが有効である。

①登録証

・認証を取得したことを証する登録証

②適用範囲を定義した文書（以下、「適用範囲定義書」と呼ぶ）

・どのような範囲（組織、部門、業務、プロセス、サービス等）で認証を取得したのかを定義した文書。「適用範囲定義書」と呼ばれることが多い。

以下で登録証、適用範囲定義書の見方について解説する。

3.1　登録証

登録証は、ISMS 認証を取得していることを証した文書のことであり、JIPDEC により認定された認証機関より発行される。登録証を確認する際のポイントは次のとおり。なお、登録証の例については、付録１．を参照されたい。

①名称及び所在地

・適用範囲を示す法人名及び部門名の記載から、委託業務に適しているかどうかにつき、ある程度の確認ができる。

・例えば、営業部のみが記載されている場合において、開発業務を委託したいという要求に対してすべて充足している根拠とはならない。

②登録範囲

・登録範囲内の活動（業務プロセスやサービス）の記述から、委託業務に適しているかどうかにつき、ある程度の確認ができる。

・例えば、システムの開発を委託する予定であるが、システムの運用が登録範囲である場合は、委託内容に対してすべて充足している根拠とはならない。

③登録日及び有効期間

・登録日から３年以内であることを確認すること。ただし、３年以内であっても登録を抹消されている可能性もあるため、直近の審査報告書の提出を求めることもあり得る。

④審査登録機関

・記載されている審査登録機関の名称、ロゴマーク及び認定マークにより、認定

されている審査登録機関であることを確認する。

図　認定マーク

3.2　適用範囲定義書

ISMS 認証を取得した事業者は、適用範囲定義書を作成している。適用範囲定義書は、認証を取得している業務やサービス内容を記載しているほか、それを運用している組織やシステム等について組織図やネットワーク構成図を用いて説明している文書である。この文書では、「事業、組織、その所在地、資産及び技術」の各特徴の観点から対象とした組織を説明しているので、委託したい業務プロセスが、それらの中に包含されていることが確認できる。

例えば、委託したい業務と合致していることについて、適用範囲定義書の該当部分を明記し説明することを委託先候補に要求して確認する必要がある。適用範囲定義書の記載例、及び、適用範囲の妥当性の確認の仕方については、付録２．を参照されたい。

また、組織によっては必ずしも適用範囲定義書という名称を用いているわけではないことに留意すること。

適用範囲を確認する際のポイントは次のとおり

①委託業務との合致

・委託を予定している業務が概ね適用範囲と合致していること

付録１．登録証（例）

登録証（例）

株式会社＊＊＊＊＊＊　××部　①

〒***-****
東京都千代田区××××

上記組織が登録範囲に詳述された活動について JIS Q 27001:2006（ISO/IEC 27001:2005）の要求事項に適合した ISMS を実施していることをここに証します。

登録範囲　②
データセンタ事業、運用監視事業、運用委託事業にかかわる情報セキュリティマネジメントシステム

登録番号：×××××

初回登録日：2005 年 6 月 1 日
有効期限　：2008 年 5 月 31 日　③

適用宣言書　第 1 版（2005 年 3 月 1 日付）

株式会社○○○○審査機構（ISR○○○）④

審査登録機関のマーク　認定マーク

付録２．適用範囲定義書（例）

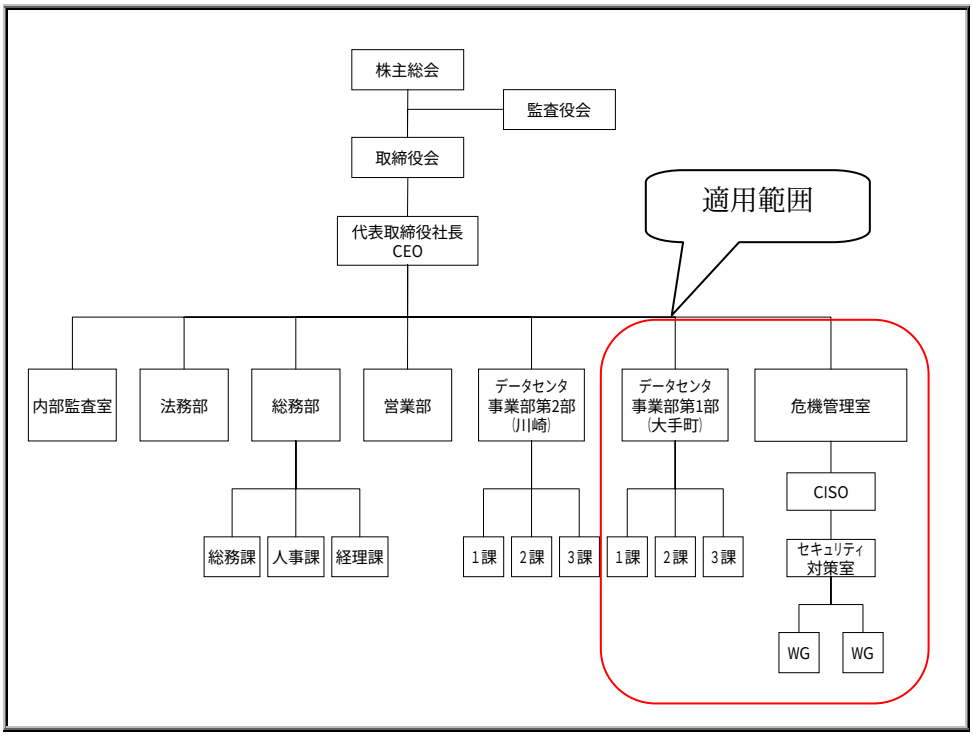
適用範囲定義書（例）

【適用範囲内の主な業務】
データセンタ事業、運用監視事業、運用委託事業

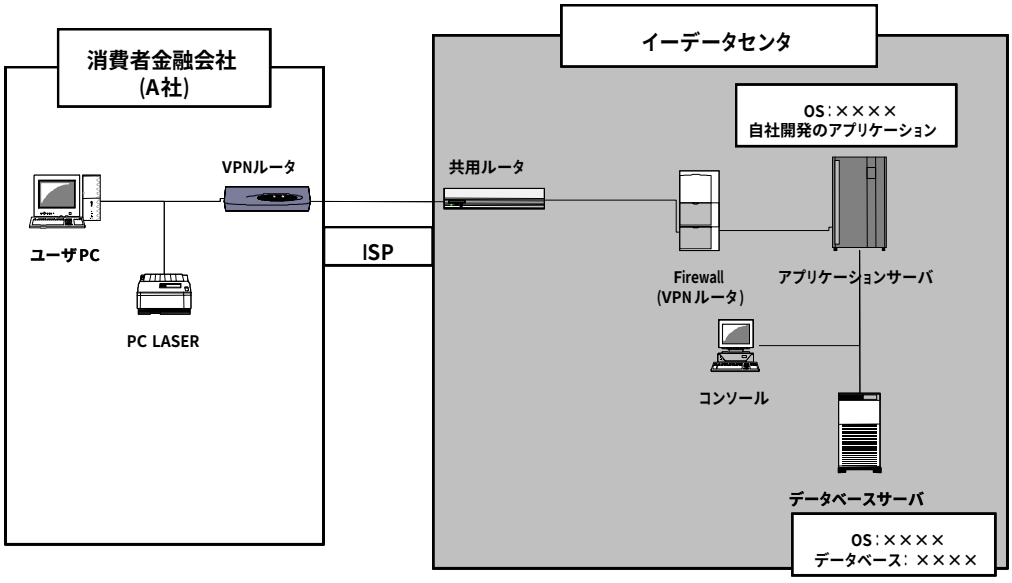
【適用範囲内の要員数】

	従業員 (アルバイトを含む)	派遣社員
大手町事業所	35 名	7 名
全社	150 名	50 名

【組織図】



【適用範囲内のシステム構成】



網掛け部分が認証取得範囲

■適用範囲の妥当性確認（例）

①妥当性を確認できる例

・メルマガサービスの委託を予定している

・委託先候補 A に確認したところ、大手町データセンタでメルマガサービスを提供している

・大手町データセンタのすべての業務において認証を取得している

②妥当性を確認できない例１

・委託先候補では当該業務を川崎データセンタで行う予定である

・大手町データセンタは認証を取得しているが、川崎データセンタは認証を取得していない

③妥当性を確認できない例２

・大手町データセンタで認証を取得している

・適用範囲に含まれない川崎データセンタの設備を用いたメルマガサービスを用いた提案

資料２

外部委託における
情報セキュリティ対策ベンチマークの利用方法

本書は、経済産業省により作成されたものである。

改訂履歴

改訂日	改訂理由
2006/5/12	初版
2007/11/9	情報セキュリティ対策ベンチマークの改訂の反映 政府機関統一基準(第２版)の策定に伴う修正

目次

1　はじめに

1.1　本書の目的

本書は、委託先の情報セキュリティ水準の評価方法又は委託先が適切な情報セキュリティ対策を履行しているかどうかの確認手段として情報セキュリティ対策ベンチマークを利用する場合に、解説書として活用することを目的としたものである。

1.2　適用対象者

各府省庁で実際に情報処理業務を外部委託し、委託先が適切な情報セキュリティ対策を履行しているかどうかを確認する立場にある調達担当者、当該情報システムの情報システムセキュリティ責任者及び当該情報処理業務を担当する課室情報セキュリティ責任者（以降、併せて「調達担当者」という）。

1.3　関連規程

府省庁が策定する「外部委託における情報セキュリティ対策実施規程」又はこれに相当する規程

2　情報セキュリティ対策ベンチマークの概要

2.1　情報セキュリティ対策ベンチマーク策定の背景

企業等の組織においては、情報セキュリティに係る必要な対策や適正と考える水準について、目安となる指標が求められている。このため ISMS 評価基準に基づく評価項目を策定し、個々の評価項目に関する評価の平均的なレベルや改善のための推奨される取組などを提供する目的で策定されたのが、情報セキュリティ対策ベンチマークである。

しかし、組織に求められる情報セキュリティ水準は一様ではなく、組織の業態や保有する情報資産等の属性によって異なると考えられることから、情報セキュリティ対策ベンチマークでは、これらの属性をもとに組織を分類し、それぞれの組織に対して「望まれる水準 」を提示する。情報セキュリティ対策ベンチマークの目的として、情報セキュリティ対策を実施していない、あるいは簡易な対策しか行っていない組織に対し、セルフチェックを通じて情報セキュリティの取組を活性化させることを想定しているが、こういった組織は、中堅・中小企業が中心になると思われる。このため、中堅・中小企業においても適用できるように、可能な限り評価項目の数を抑えている。また、アンケート調査の結果によれば、大企業にも、一部取組が十分でない項目があることが判明していることから、中堅・中小企業のみならず、大企業も本ベンチマークを積極的に活用することが重要である。

なお、組織における情報セキュリティガバナンス[1]の確立という観点からは、経営層自らが情報セキュリティ対策ベンチマークによるセルフチェックを通じて対策の必要性に気づくことが望ましい。このため、経営層向けに平易な言葉を使用するとともに、単に対策を「行っている」／「行っていない」ではなく、対策の取組（成熟度）を評価の基準としている。

2.2　情報セキュリティ対策ベンチマークの概要

情報セキュリティ対策ベンチマークの評価項目は、

1. 情報セキュリティ対策の取組状況を把握するための評価項目（25 項目）
2. 組織プロフィールに関する評価項目（15 項目）

から構成される。このうち外部委託に際しての評価に用いるのは「情報セキュリティ対策の取組状況」だけである。本来の情報セキュリティ対策ベンチマークでは、組織プロフィールに基づき回答組織を分類した上で、該当する組織において「望まれる水準」を設定するが、政府における委託先の選定等にこの「望まれる水準」を用いる

[1] 情報セキュリティガバナンスとは、「社会的責任にも配慮したコーポレートガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義されている（「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」）。内部統制の仕組みを情報セキュリティ対策に適用することで、情報セキュリティ対策の自律的・継続的な推進が効率的に実現できると考えられる。このためには企業の経営層の関与が必要不可欠である。

ことは必ずしも適切ではないため、本書では割愛した。したがって以下では「組織プロフィールに関する評価項目」及び「望まれる水準」に関しては触れない。

(1) 情報セキュリティ対策の取組状況

情報セキュリティ対策の取組状況に関する評価項目は、平成 19 年 8 月の改訂において、ISMS 評価基準 Ver.2.0 の詳細管理策に基づいた評価項目から、その後規格化された JIS Q 27001:2006 の付属書 A の管理目的及び管理策に基づいた評価項目へ見直された。なお、見直しに当たっては、継続性や既存のデータ資産との整合性、平易な言葉の使用と曖昧な表現の排除、企業内の部門単位の利用や公的機関の利用への対応等に配慮した。

評価作業では、各評価項目に関する自社の取組の「成熟度」を確認する。

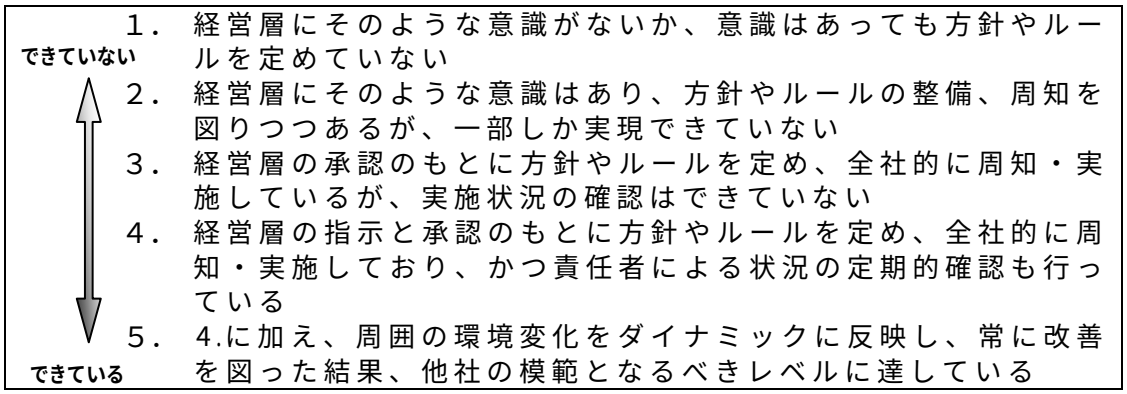


図 1-1　成熟度の構成

評価項目は次の 5 グループで構成され、グループごとに 3～7 項の評価項目が設定されている。

a) 情報セキュリティに対する組織的な取組状況（7 項）
b) 物理的（環境的）セキュリティ上の施策（４項）
c) 通信ネットワーク及び情報システムの運用管理状況（６項）
d) 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況（5 項）
e) 情報セキュリティ上の事故対応状況（3 項）

具体的な評価項目の内容は付録 1 に示す。

なお、ISMS 認証制度の認証取得に至るレベルであれば、成熟度は「成熟度 4」（経営層の指示と承認のもとに方針やルールを定め、全社的に周知･実施しており、かつ責任者による状況の定期的確認も行っている）に達していると考えられる。

また、特定の部門のみ ISMS 認証を取得している場合には、企業全体で考えると「成熟度 3」（経営者の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない）～「成熟度 4」の間に位置するのではないかと考えられる。

2.3 部門単位での算出

全社での回答が困難である場合は、情報セキュリティ対策実施に係る権限が、経営層から部門責任者に対して委任されていることを条件として、委託業務を実施する事業所等の部門単位において情報セキュリティ対策ベンチマークに回答することも可能である。その場合、図 1-1 に示された成熟度の判断に際しては「経営層」を「部門責任者」と読み替える。

部門単位で情報セキュリティ対策ベンチマークを実施する場合、経営者から部門責任者に対して適切な権限が委任されていることを確認しなければならない。

2.4 情報セキュリティ対策ベンチマークと ISMS 認証制度・情報セキュリティ監査との相違点

情報セキュリティ対策ベンチマークは、ISMS 認証制度における認証基準を元に 25 項目に集約した評価項目を採用していることから、基本的には ISMS 認証制度と同様に組織の情報セキュリティへの取組状況について ISMS 認証制度よりも簡便に確認することが可能である。一方で、評価項目が少ないことから、一般には評価の精度が他の手法に比較して低い。また基本的にはセルフチェック（自己申告）による評価であるため、虚偽の情報を受けとる可能性があるなど、結果の信頼性を十分に担保できないことから、外部委託する業務の性質等を勘案し、他の手法を選択した方が良い場合もある。

3　情報セキュリティ対策ベンチマークの適用対象

3.1　委託先の選定

委託先の選定時に情報セキュリティ対策ベンチマークを利用することが考えられる。具体的には、調達仕様書において評価方法として情報セキュリティ対策ベンチマークを明示することにより、委託先の選定基準の一要素として利用することができる。

なお、情報セキュリティ対策ベンチマークは自己評価によるものであり、虚偽の申告が行われる可能性を排除することはできない。したがって、高い信頼性を要求されるような委託先選定には適していない。この場合はISMS認証制度などを主に利用し、情報セキュリティ対策ベンチマークはその補助手段として活用すべきである。

また、ISMS認証制度と併用する場合は、情報セキュリティ対策ベンチマークの要求水準を決定する際にISMS認証取得と同等のレベルになるように配慮する必要がある。詳細は4章にて述べる。

評価対象	調達時における委託先候補の情報セキュリティ対策の水準
実施時期	調達時
関連文書	調達仕様書

3.2　情報セキュリティ対策の履行状況確認

委託先に求める情報セキュリティ対策等を委託中に確認する手段として情報セキュリティ対策ベンチマークを利用することが考えられる。

なお、業務における定常的な確認に加え、委託中の確認に情報セキュリティ対策ベンチマークを用いることができるのは、外部委託に係る業務遂行に際して委託先に実施させる情報セキュリティ対策の内容が、情報セキュリティ対策ベンチマークの対策の取組状況（付録１）で十分に評価できると判断される場合に限定されることに留意する必要がある。情報セキュリティ対策ベンチマークで評価できないと判断される場合は、情報セキュリティ監査などを利用すべきである。

評価対象	委託中における委託先の情報セキュリティ対策の履行状況確認
実施時期	契約時･業務委託中
関連文書	契約書･発注仕様書･SLA

委託先に求める情報セキュリティ対策等を委託中に確認する手段として情報セキュリティ対策ベンチマークを利用する場合、例えば納品時等に情報セキュリティ対策ベンチマーク計測値の申告を契約条件とすることに加え、万が一虚偽や過失に基づく誤った事実を報告し続け、その結果として欠陥を見過ごすこととなって事故が発生した場合の法的措置（契約破棄や損害賠償請求等）を契約書に明記することも考えられる。

4　外部委託における情報セキュリティ対策ベンチマークの利用方法

4.1　委託先の選定

情報セキュリティ対策ベンチマークを委託先選定時に利用する際の簡単なフローを図 4-1 に示す。以下、この流れに沿って説明する。

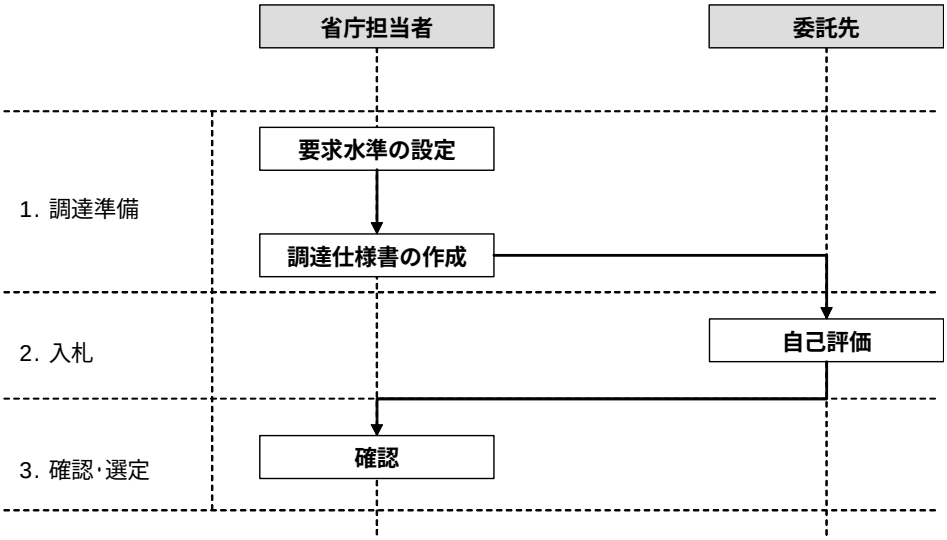


図 4-1 委託先選定時のフロー

4.1.1 要求水準の設定

はじめに、外部委託の対象となる業務の性質に応じて要求水準（情報セキュリティ対策ベンチマークにおける成熟度）を設定する。要求水準を設定する際の基本的な考え方は以下の 2 通りである。

(1) 成熟度 4：経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている

情報セキュリティ対策ベンチマークを利用した自己チェックの結果、成熟度の平均値が 4 以上であることを要求水準として設定する。これは、全社で ISMS 認証取得にいたるレベルとほぼ同等であるとみなすことができる。

(2) 成熟度 3：経営層の承認のもとに方針やルールを定め、全社的に周知・実施している

情報セキュリティ対策ベンチマークを利用した自己チェックの結果、成熟度の平均値が 3 以上であることを要求水準として設定する。

成熟度 3 と 4 のどちらを選択すべきかに関して、委託先に対して一定の情報セ

キュリティ対策の実施を求めるのであれば、基本的には成熟度 3 を求めるのが妥当である。しかし、基本的な対策に加え PDCA サイクルが実施されている事を求める場合は成熟度 4 を求める。

委託先選定時に情報セキュリティ対策ベンチマークと ISMS 認証取得を選択可能とする場合、ISMS 認証と同等のレベルを要求水準とすべきである。具体的には、ISMS 認証取得を条件とする場合に補助的に情報セキュリティ対策ベンチマークを用いるような場合、情報セキュリティ対策ベンチマークについては成熟度 4 を要求する。

なお、各評価項目における最低点を要求水準に加えることもできる。

4.1.2 調達仕様書の作成

情報セキュリティ対策ベンチマークを委託先の選定に活用するためには、要求水準を定めた上で、調達仕様書等に情報セキュリティ対策ベンチマークを利用した自己評価結果を求める旨を明記する必要がある。具体的な記述例を以下に示す。

(1) 成熟度 4 を求める場合

調達仕様書への記述例（１）：

本調達に係る業務を行おうとする事業者は、*[付録 1]* に従い情報セキュリティ対策ベンチマークを利用した自己評価を行い、その評価結果において、全項目に係る平均値（次項 4.1.3(1)参照。）が 4（経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている）に達していることを確認するとともに、*[付録 2]* のとおり確認書を提出すること。[2]

(2) 成熟度 3 を求める場合

調達仕様書への記述例（２）：

本調達に係る業務を行おうとする事業者は、*[付録 1]* に従い情報セキュリティ対策ベンチマークを利用した自己評価を行い、その評価結果において、全項目に係る平均値が 3（経営者の承認のもとに方針やルールを定め、全社的に周知・実施している）に達していることを確認するとともに、*[付録 2]* の通り確認書を提出すること。[3]

[2] 要求水準として各項目に許容されうる最低の成熟度を求める場合は、調達仕様書に「～かつ各評価項目の成熟度が 2 以上であること」などの記述を追加する。
[3] 要求水準として各項目に許容されうる最低の成熟度を求める場合は、調達仕様書に「～かつ各評価項目の成熟度が 2 以上であること」などの記述を追加する。

4.1.3 **自己評価**

委託先候補者は、調達仕様書等に記載された要求水準を満たすことを、情報セキュリティ対策ベンチマークにより確認する。具体的には以下の手順による。なお、直近 6 ヶ月以内に同様の内容について確認した結果がある場合、その結果を充てることができる。

(1) 全項目に係る平均値の算出

情報セキュリティ対策ベンチマークのうち、対策の取組状況（付録１）について 5 段階評価（5 点満点）し、25 項目の総計（125 点満点）を 25 で除することで、全項目に係る平均値を計算する。これらの結果を情報セキュリティ対策ベンチマーク確認書（付録 2）に記載する。

(2) 直近の情報セキュリティ対策ベンチマーク結果の活用

直近の 6 ヶ月以内に、当該事業者より一般に公表された報告書等において、情報セキュリティ対策ベンチマークの結果が公表されている場合は、当該報告書の記載内容が要件を満たすことを確認した上で、当該報告書をもって情報セキュリティ対策ベンチマーク確認書に充てることができる。

(3) 部門単位の適用

全社での回答が困難である場合は、情報セキュリティ対策実施に係る権限が、経営層から部門責任者に対して委任されていることを条件として、委託業務を実施する事業所等の部門単位において情報セキュリティ対策ベンチマークに回答することも可能である。その場合、成熟度の判断に際しては「経営層」を「部門責任者」と読み替えた上で情報セキュリティ対策ベンチマークを実施する。

4.1.4 **確認**

調達担当者は、委託先候補の情報セキュリティ対策の水準が、調達仕様書等に記載された要求水準を満たしていることを情報セキュリティ対策ベンチマークにより確認する。具体的には、委託先候補が提出してきた情報セキュリティ対策ベンチマーク確認書（付録 2）に記載された内容が、以下の条件を満たしていることを確認する。

- 「確認日時」が調達仕様書を公表した日の6ヶ月前の日付から、確認書が提出された日付の間にあること
- 「確認対象」が当該委託を実施する組織と同一又は包含すること
- 確認書が、代表者又は当該委託業務において代表者より権限を委任された者の名で作成されていること（委託先責任者名）
- 「確認に用いた基準」が調達仕様書で求めたものと同一であること
- 全項目の平均値が要求水準で指定された値以上であること

4.2 情報セキュリティ対策の履行状況の確認

情報セキュリティ対策ベンチマークを委託業務中に情報セキュリティ対策の履行状況確認に利用する際の簡単なフローを図 4-2 に示す。以下、この流れに沿って説明する。

なおここで、委託中の管理に情報セキュリティ対策ベンチマークを用いることができるのは、以下の２つの条件が同時に満たされる場合に限定されることに留意しなければならない。

(1) 外部委託に係る業務遂行に際して委託先に実施させる情報セキュリティ対策の内容が、情報セキュリティ対策ベンチマークの対策の取組状況（付録１）で十分に評価できると判断される場合

(2) 情報セキュリティ対策の履行状況の確認において、情報セキュリティ監査を実施せず、自己評価による確認で十分と判断される場合（委託先の選定時においてISMS 取得を条件とした場合は、「十分」と判断される場合に相当しない）

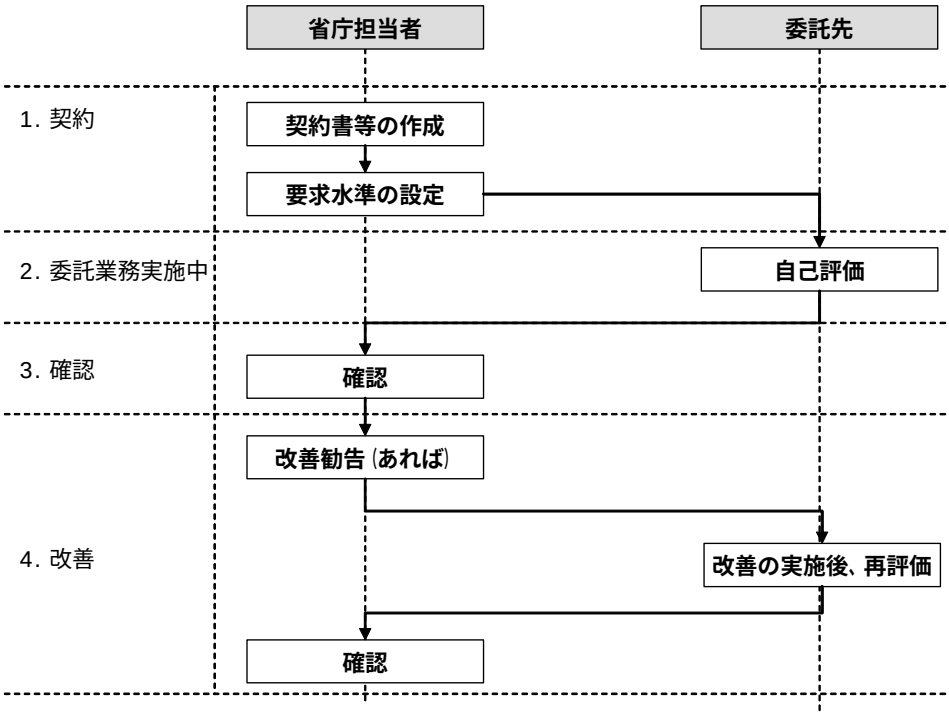


図 4-2 情報セキュリティ対策の履行状況の確認のフロー

4.2.1 契約書等の作成

情報セキュリティ対策ベンチマークを委託中の情報セキュリティ対策の履行状況の確認に活用するためには、契約書等に情報セキュリティ対策ベンチマークを利用した自己評価の実施を求める旨を明記する必要がある。

具体的な記述例を以下に示す。

契約書への記述例：

（自己評価）
第○○条
乙は、甲が提示する方法に基づいて自己評価を実施し、その結果を甲に報告すること。
２　甲は、乙から報告された自己評価の結果が要求水準を満たしていない場合、又は疑義が認められる場合、乙に対して調査を実施し必要と認められる場合には改善勧告を出すことができる。
※甲：府省庁、乙：委託先

SLA への記述例：

（○○条）乙は、甲が別途指定する時期及び様式に従い情報セキュリティ対策に係る自己評価を実施し、その結果を甲に報告する。
（○○条）甲は、自己評価の結果を確認するため乙に対して調査を実施する場合がある。乙はこの調査に協力しなければならない。
※甲：府省庁、乙：委託先

4.2.2 要求水準の設定

外部委託の対象となる業務の性質に応じて要求水準（情報セキュリティ対策ベンチマークにおける成熟度）を設定する。要求水準は基本的に「4.1.1 要求水準の設定」と同様に行う。

ただし、選定時において ISMS 認証の取得又は情報セキュリティ対策ベンチマークの成熟度 4 を求めた場合は、委託中の情報セキュリティ対策についても PDCA サイクルが継続的に実施されていることを確認しなければならないと想定されることから、成熟度 4 を求める。

なお、各評価項目における最低点を要求水準に加えることもできる。

4.2.3 自己評価

委託先は、委託業務中の情報セキュリティ対策の順守状況が要求水準を満たすことを、情報セキュリティ対策ベンチマークにより確認する。具体的な手順は「4.1.3 自己評価」を参照のこと。

4.2.4 確認

調達担当者は、委託先の情報セキュリティ対策順守状況が、要求水準を満たすことを情報セキュリティ対策ベンチマークにより確認する。具体的には、委託先が提出してきた情報セキュリティ対策ベンチマーク確認書（付録 2）に記載された内容が、以下の条件を満たしていることを確認する。

- 「確認日時」が契約書等で規定された期間の間にあること
- 「確認対象」が当該委託を実施する組織と同一又は包含すること

- 確認書が、代表者又は当該委託業務において代表者より権限を委任された者の名で作成されていること（委託先責任者名）
- 「確認に用いた基準」が契約等で求めたものと同一であること
- 全項目の平均値が要求水準以上であること

以上

付録 1．情報セキュリティ対策ベンチマーク

◆注意事項：
全社での回答が困難である場合は、以下の設問に示されている情報セキュリティ対策実施に係る権限が、経営層から部門責任者等に対して委任されていることを条件として、委託業務を実施する事業所等の部門単位において情報セキュリティ対策ベンチマークに回答することも可能である。その場合、各設問において「経営層」を「部門責任者」と読み替えること。
部門単位で情報セキュリティ対策ベンチマークを実施する場合でも、情報セキュリティ対策ベンチマーク確認書は代表者又は当該委託業務において代表者より権限を委任された者の名（例：部門責任者、営業責任者等）で作成しなければならない。これは、情報セキュリティ対策ベンチマークによる確認が適切な権限が委任されている者の下で実施されたこと確認する必要があるためである。

問１　情報セキュリティに対する組織的な取組状況についてうかがいます。

以下の①～⑦のそれぞれの設問について、次の選択肢の中からもっともあてはまる番号を回答欄に記入してください。

1. 経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2. 経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3. 経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4. 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5. ４．に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

① 情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。

ポリシーや規程は、サンプルのコピーではなく、自組織の事業やリスクを鑑みた内容であることが重要です。また、そうしたポリシーや規程を実践するためには、定めた規程類を関係者に十分に周知させると共に、規程類の順守状況を点検し、必要に応じて見直すことが大切です。

② 経営層を含めた情報セキュリティの推進体制やコンプライアンス（法令順守）の推進体制を整備していますか。

推進体制を整備するためには、経営層がリーダシップを発揮すること、各担当者の権限と責任を明文化することなどが重要です。また、法令順守のためには、順守すべき法令を正確かつ網羅的に把握することが必要です。

③　重要な情報資産（情報及び情報システム）を、その重要性のレベルごとに分類し、さらにレベルに応じた表示や取扱をするための方法を定めていますか。

情報資産をその重要性に応じて管理するためには、レベル分け、レベルに応じた表示や取扱方法などの指針及び情報の管理責任者を定める必要があります。

④　重要な情報（たとえば個人データや機密情報など）については、入手、作成、利用、保管、交換、提供、消去、破棄などの一連の業務プロセスごとにきめ細かくセキュリティ上の適切な措置を講じていますか。

適切な措置とは、業務プロセスごとの作業責任者や作業手順の明確化、取扱者の限定、処理の記録や確認などを指します。また、業務プロセスは、手作業で行うか、情報システムに依存するかを問いません。

⑤　外部の組織に業務や情報システムの運用管理を委託する際の契約書には、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。

セキュリティ上の理由とは、たとえば情報の漏えいや消失、情報あるいは情報システムの誤用などの防止を指します。

⑥　従業者（派遣を含む）に対し、採用、退職の際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にしていますか。

従業者に情報セキュリティについての要求を順守させるためには、従業者の管理責任者を明確にし、従業者が守るべきルールなどを明確にし、それらを周知させておく必要があります。

⑦　経営層や派遣を含む全ての従業者に対し、情報セキュリティに関する自組織の取組や関連規程類について、計画的な教育や指導を実施していますか。

情報セキュリティ教育は、全員に漏れなく定期的に行うことが大切です。セキュリティ対策上の順守事項、禁止事項の徹底とともに、情報セキュリティの脅威と対策についても教育します。

問２　物理的（環境的）セキュリティ上の施策についてうかがいます。

以下の①～④のそれぞれの設問について、次の選択肢の中からもっともあてはまる番号を回答欄に記入してください。

1. 経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2. 経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3. 経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4. 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5. ４．に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

① 特にセキュリティを強化したい建物や区画に対して、必要に応じたセキュリティ対策を実施していますか。

特にセキュリティを強化したい建物や区画については、ゲートや間仕切りを設けるなどして、境界を明確にし、入退館や入退室管理を実施する、あるいは警報装置の設置などを行います。また、荷物の受渡し場所や外部者の作業場所を確保するなど、セキュリティを考慮して物理的に区域を分けるようにします。

② 顧客、ベンダーや、運送業者、清掃業者など、建物に出入りする様々な人々についてセキュリティ上のルールを定め、それを実践していますか。

自組織の建物や事務所には、思ったよりも多くの外来者が出入りしている事があります。そうした外来者に守って頂くべきルールをあらかじめ定めておくことが重要です。

③ 重要な情報機器や配線などは、自然災害や人的災害などに対する安全性に配慮して配置または設置し、適切に保守していますか。

安全性に配慮した配置または設置とは、たとえば、重要なシステムの安全な場所への設置、盗み見の防止や盗聴防止などに配慮した設置、配線類の地下や床下への埋設、浸水、火災、地震などを考慮した配置などを言います。

④ 重要な書類、モバイル PC、記憶媒体などについて適切な管理を行っていますか。

適切な管理とは、たとえば、保管キャビネットの施錠やプリント出力の放置禁止、記憶媒体の粉砕廃棄などを言います。また、重要な書類には、情報システムに関する文書を含みます。

問３　通信ネットワーク及び情報システムの運用管理に関するセキュリティ対策についてうかがいます。

以下の①～⑥のそれぞれの設問について、次の選択肢の中からもっともあてはまる番号を回答欄に記入してください。

1. 経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2. 経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3. 経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4. 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5. ４．に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

① 情報システムの運用に際して、運用環境や運用データに対する適切な保護対策が実施されるよう、十分に配慮していますか。

適切な保護には、開発環境、テスト環境と運用環境の分離、変更管理の実施、開発での本番データの使用制限などが含まれます。

② 情報システムの運用に際して、必要なセキュリティ対策を実施していますか。

必要なセキュリティ対策には、各種手順書の作成、ルールに従った運用、監視、ログの取得と分析などが含まれます。

③ 不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウエアなど）への対策を実施していますか。

不正プログラム対策には、ウイルス対策ソフトの導入や、パターンファイルの更新を適時行うこと、ぜい弱性を解消することなどが含まれます。

④ 導入している情報システムに対して、適切なぜい弱性対策を実施していますか。

適切なぜい弱性対策には、セキュリティを考慮した設定や、パッチ（修正プログラム）の適用、バージョン管理や構成管理、変更管理などが含まれます。

⑤ 通信ネットワークを流れるデータや、公開サーバ上のデータに対して、暗号化などの適切な保護策を実施していますか。

適切な保護策には、VPN の使用や重要な情報の SSL などによる暗号化があります。

⑥　モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策を実施していますか。

モバイル PC や USB メモリなどの記憶媒体の使用場所には、外部のパブリックスペースやリモートオフィス、自宅などを含みます。外部のセキュリティの脅威は内部よりも高いことを考慮して対策を行う必要があります。

問４　情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況**についてうかがいます。**

以下の①～⑤のそれぞれの設問について、次の選択肢の中からもっともあてはまる番号を回答欄に記入してください。

1. 経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2. 経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3. 経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4. 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5. ４．に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

① 情報（データ）や情報システムへのアクセスを制限するために、利用者 ID の管理、利用者の識別と認証を適切に実施していますか。

適切な利用者 ID の管理には、利用者 ID の定期的な見直しによる不要な ID の削除や共用 ID の利用制限、単純なパスワードの設定禁止などがあります。

② 情報（データ）や情報システム、業務アプリケーションなどに対するアクセス権の付与と、アクセス制御を適切に実施していますか。

適切なアクセス権の管理には、アクセスできる情報システムを利用者ごとに限定すること、利用できる機能を制限すること、利用者のアクセス権をレビューすることなどがあります。

③ ネットワークのアクセス制御を適切に実施していますか。

適切なネットワークのアクセス制御には、たとえばネットワークの分割や外部からの接続時の認証などがあります。

④ 業務システムの開発において、必要なセキュリティ要件を定義し、設計や実装に反映させていますか。

自組織での開発、外部委託による開発を問わず、開発の際に必要なセキュリティ対策としては、仕様書にセキュリティ上の要求事項を盛り込むこと、設計や開発に際してぜい弱性を作り込まないように配慮すること、ぜい弱性を残さないための適切なシステム試験を実施することなどがあります。

⑤ ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリ

ティ上の観点からの点検をプロセスごとに実施するなど、適切なプロセス管理を実施していますか。

選定や購入、開発や保守を外部委託している場合は、セキュリティ上の観点からの点検が可能かどうかを回答してください。

問５　情報セキュリティ上の事故対応状況についてうかがいます。

以下の①～③のそれぞれの設問について、次の選択肢の中からもっともあてはまる番号を回答欄に記入してください。

1. 経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2. 経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3. 経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4. 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5. ４．に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

① 万が一システムに障害が発生しても、必要最低限のサービスを維持できるようにするため、情報システムに障害が発生する場合をあらかじめ想定した適切な対策を実施していますか。

適切な対策には、たとえばシステムの二重化、バックアップと運用記録の取得、障害対応手順の明確化、外部委託先とのサービスレベルの合意などがあります。

② 情報セキュリティに関連する事件や事故が発生した際に必要な行動を、適切かつ迅速に実施できるように備えていますか。

事件や事故への備えには、そうした万が一の場合にとるべき行動をあらかじめ検討しておくこと、検討した結果を文書にまとめて関係者に周知しておくこと、緊急の連絡網を整備すると共に、必要な要員や資機材を揃えられるようにあらかじめ手配しておくことなどがあります。

③ 何らかの理由で情報システムが停止した場合でも、必要最小限の業務を継続できるようになっていますか。

万が一、情報システムが停止してしまった場合に備えて、普段は情報システムで行っている業務をたとえば手作業で代替できるように、そうした業務の手順書や様式類をあらかじめ用意しておくこと、またそうした手作業を実施できる場所や資機材を確保しておくこと、さらに手作業で代替できるように要員を訓練しておくことなどが重要です。

以上

付録 2．情報セキュリティ対策ベンチマーク確認書

平成○○年○○月○○日

○○省
○○○殿

[委託先組織名]
[委託先責任者名]

情報セキュリティ対策ベンチマーク確認書

情報セキュリティ対策ベンチマークを実施し、下記の評価結果に相違ないことを確認します。

記

1. 確認日時
　　平成○○年○○月○○日　【実際に確認を行った日時】

2. 確認対象
　　【情報セキュリティ対策ベンチマークの確認を行った範囲について記載（例、当該業務を実施する事業所等の名称）】

3. 情報セキュリティ対策ベンチマーク実施責任者
　　【情報セキュリティ対策ベンチマークによる確認を実施した者。】

4. 確認に用いた基準
　　情報セキュリティ対策ベンチマーク 2007/08 版

5. 確認結果
　　全項目に係る平均値：　　○.○
　　なお、項目ごとの確認結果については別紙に示す。

以上

別紙

情報セキュリティ対策ベンチマーク確認票

			得点
問 1	①	情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。	
	②	経営層を含めた情報セキュリティの推進体制やコンプライアンス（法令順守）の推進体制を整備していますか。	
	③	重要な情報資産（情報及び情報システム）を、その重要性のレベルごとに分類し、さらにレベルに応じた表示や取扱をするための方法を定めていますか。	
	④	重要な情報（たとえば個人データや機密情報など）については、入手、作成、利用、保管、交換、提供、消去、破棄などの一連の業務プロセスごとにきめ細かくセキュリティ上の適切な措置を講じていますか。	
	⑤	外部の組織に業務や情報システムの運用管理を委託する際の契約書には、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。	
	⑥	従業者（派遣を含む）に対し、採用、退職の際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にしていますか。	
	⑦	経営層や派遣を含む全ての従業者に対し、情報セキュリティに関する自組織の取組や関連規程類について、計画的な教育や指導を実施していますか。	
問 2	①	特にセキュリティを強化したい建物や区画に対して、必要に応じたセキュリティ対策を実施していますか。	
	②	顧客、ベンダーや、運送業者、清掃業者など、建物に出入りする様々な人々についてセキュリティ上のルールを定め、それを実践していますか。	
	③	重要な情報機器や配線などは、自然災害や人的災害などに対する安全性に配慮して配置または設置し、適切に保守していますか。	
	④	重要な書類、モバイル PC、記憶媒体などについて適切な管理を行っていますか。	
問 3	①	情報システムの運用に際して、運用環境や運用データに対する適切な保護対策が実施されるよう、十分に配慮していますか。	
	②	情報システムの運用に際して、必要なセキュリティ対策を実施していますか。	
	③	不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウエアなど）への対策を実施していますか。	
	④	導入している情報システムに対して、適切なぜい弱性対策を実施していますか。	
	⑤	通信ネットワークを流れるデータや、公開サーバ上のデータに対して、暗号化などの適切な保護策を実施していますか。	
	⑥	モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策を実施していますか。	
問 4	①	情報（データ）や情報システムへのアクセスを制限するために、利用者 ID の管理、利用者の識別と認証を適切に実施していますか。	
	②	情報（データ）や情報システム、業務アプリケーションなどに対するアクセス権の付与と、アクセス制御を適切に実施していますか。	
	③	ネットワークのアクセス制御を適切に実施していますか。	
	④	業務システムの開発において、必要なセキュリティ要件を定義し、設計や実装に反映させていますか。	
	⑤	ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点からの点検をプロセスごとに実施するなど、適切なプロセス管理を実施していますか。	
問 5	①	万が一システムに障害が発生しても、必要最低限のサービスを維持できるようにするため、情報システムに障害が発生する場合をあらかじめ想定した適切な対策を実施していますか。	
	②	情報セキュリティに関連する事件や事故が発生した際に必要な行動を、適切かつ迅速に実施できるように備えていますか。	
	③	何らかの理由で情報システムが停止した場合でも、必要最小限の業務を継続できるようになっていますか。	
総計		問 1～問5の全 25 問の得点の総計（125 点満点）	
平均		総計を問題数 25 で除したもの	

※本紙に代えて、独立行政法人 情報処理推進機構 (IPA)が提供する情報セキュリティ対策ベンチマークシステム

（https://isec.ipa.go.jp/benchmark-new/member/）の PDF 出力結果を添付しても良い。

資料３

外部委託における
情報セキュリティ監査の利用方法

本書は、特定非営利活動法人日本セキュリティ監査協会(JASA)により作成されたものである。

改定履歴

改訂日	改訂理由
2006/5/12	初版
2007/11/9	政府機関統一基準(第２版)の策定に伴う修正

目次

1 はじめに

1.1 本書の目的

府省庁が外部委託により情報処理を行う場合には、府省庁において策定する規程に従い、委託先に情報セキュリティ対策を確実に行わせるとともに、その履行状況を確認することが必要となる。

本書は、府省庁が委託先における情報セキュリティ対策の履行状況確認手段として、情報セキュリティ監査を利用する場合に解説書として活用することを目的としたものである。

1.2 適用対象者

府省庁において情報処理業務を外部委託する際に、委託先の情報セキュリティ対策の履行状況を確認する立場にある調達担当者、当該情報システムの情報システムセキュリティ責任者及び当該情報処理業務を担当する課室情報セキュリティ責任者

1.3 関連文書

府省庁が策定する「外部委託における情報セキュリティ対策実施規程」又はこれに相当する文書

1.4 本書の改定

本書の内容については予告なく改訂される場合がある。

2 情報セキュリティ監査の概要

2.1 情報セキュリティ監査とシステム監査

情報セキュリティ監査とは、情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況について、基準に従って検証又は評価を行う活動である。

情報セキュリティ監査では、評価の観点として、「現時点において組織が適切な情報セキュリティ対策を講じているか」という点に加え、環境変化に応じた対策を実施するための「情報セキュリティマネジメントが実施されているか」という点もある。また、評価対象は、情報資産のライフサイクルの観点から、情報システムのみならず、情報資産すべてを対象としてマネジメント及び技術的対策の両面から評価を行う。

一方、システム監査は、情報システム全体の構築・運用の最適化を図るために実施することを目的としており、システムの全般的な信頼性、安全性、効率性の向上を目指したものとして位置付けられている。

府省庁の情報資産の取扱いを含む外部委託に当たっては、必要に応じて、その情報資産が適切に取り扱われているかどうか、その管理体制を含めて委託中に情報セキュリティ監査を通して確認することとなる。

2.2 監査形態の分類

情報セキュリティ監査の形態は、いくつかの観点で分類することができる。

2.2.1 監査実施者による分類

情報セキュリティ監査の実施にあたって、その監査実施主体によって第二者監査と第三者監査に分類することができる。

(1) 第二者監査

業務委託契約などにおける発注者と受注者の関係において、発注者が監査主体となり、受注者が被監査対象となる場合。一般に、監査結果は、発注者が受注者の情報セキュリティ管理状況の確認、受注者への改善指導、受注者の選定に利用する。

(2) 第三者監査

業務委託契約などにおける発注者と受注者の関係において、発注者、または、受注者が、独立した第三者に受注者の監査を依頼する場合。独立した第三者が監査主体となり、受注者が被監査対象となる。一般に、監査結果は、被監査対

象（受注者）の利害関係者（発注者、他）が、被監査対象（受注者）の情報セキュリティ管理状況の確認、受注者の選定に利用する。

2.2.2 監査目的による分類

情報セキュリティ監査の実施に当たっては、監査の目的があらかじめ設定されていなければならない。情報セキュリティ監査には、組織体が採用している情報セキュリティ対策の適切性に対して一定の保証を付与することを目的とする監査（保証型の監査という）と、情報セキュリティ対策の改善に役立つ助言を行うことを目的とする監査（助言型の監査という）がある。

以下、参考として、保証型監査と助言型監査の概要を記述する。

(1) 保証型監査

保証型の監査は、監査結果が被監査対象（委託先）の利害関係者（府省庁）に利用されることを想定して実施される監査であり、監査対象たる情報セキュリティのマネジメント又はコントロールが、監査手続を実施した限りにおいて適切である旨（又は不適切である旨）を監査意見として表明する形態の監査をいう。保証型の監査の結論として表明される保証意見は、情報セキュリティ監査人が情報セキュリティ監査制度[*1]において策定されている「情報セキュリティ監査基準」に従って監査手続を行った範囲内での請け合いであって、かつ当該監査手続が慎重な注意のもとで実施されたことを前提に付与される保証である。

[*1]：情報セキュリティ監査制度：
http://www.meti.go.jp/policy/netsecurity/audit.htm

(2) 助言型監査

助言型の監査とは、情報セキュリティのマネジメント又はコントロールの改善を目的として、監査対象の情報セキュリティ対策上の欠陥及び懸念事項等の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を監査意見として表明する形態の監査をいう。助言型の監査の結論として表明される助言意見は、情報セキュリティ対策に対して一定の保証を付与するものではなく、改善を要すると判断した事項を情報セキュリティ監査人の意見として表明するものである。

3 府省庁の外部委託先に対する情報セキュリティ監査の活用

3.1 情報セキュリティ監査の目的

府省庁において業務を外部委託する際に、委託先に対して情報セキュリティ監査を行う目的は

- 委託先の情報セキュリティ管理体制が、府省庁の要求事項を満たしていることを確認するため
- 委託先の情報セキュリティ管理策（コントロール）が、府省庁の要求事項を満たしていることを確認するため

であるが、特に委託先の情報セキュリティ管理策（コントロール）が府省庁の要求事項を満たしていることを確認するには、監査を実施することが最も有効な手段であると思われる。。

以上のような目的を踏まえれば、委託先に対する情報セキュリティ監査は、府省庁自らによる監査か、もしくは保証型の第三者監査（「2.2.2 第三者監査」参照）という実施形態であることが適切である。以下、第三者監査についての記述は、すべて「保証型監査」を前提とする。

3.2 府省庁の外部委託における情報セキュリティ監査の実施形態

府省庁が情報処理業務を外部委託する際、府省庁自らが委託先の情報セキュリティ対策の履行状況を確認する必要がある。よって、その確認手段として情報セキュリティ監査を利用する場合には、原則として、府省庁自らが委託先に対して情報セキュリティ監査を実施することとなる（第二者監査）。

ただし、府省庁内に監査を実施する者が不足している場合又は監査遂行能力が不足している場合等には、府省庁が第三者の監査人を選定し、委託先への監査を依頼することが望ましい（第三者監査）。第三者の監査人を選定するにあたっては、委託先との独立性を有し、かつ監査遂行能力がある者を選択できるよう配慮する必要がある。具体的には、情報セキュリティ監査企業台帳[*1]（経済産業省）に登録されている企業の業務への関与に加え、ＪＡＳＡによる「公認情報セキュリティ監査人資格制度（ＣＡＩＳ）」の資格保有者、「情報セキュリティ監査企業紹介制度」等の活用が考えられる。

[*1]：情報セキュリティ監査企業台帳：
http://www.meti.go.jp/policy/netsecurity/is-kansa/

表 3-1 監査の実施形態

形態		監査実施者	内容
第二者監査	府省庁の担当者による監査	府省庁	・ 府省庁及び委託先合議により作成した情報セキュリティ管理手続[*1]を用いて、府省庁が委託業務実施部門を監査し確認
第三者監査	府省庁が第三者の監査人を選定し、監査を依頼するケース[*2]	外部の専門家（府省庁が監査実施を委託）	・ 府省庁が委託先監査の実施を外部の専門家に委託 ・ 外部の専門家は、府省庁及び委託先合議により作成した情報セキュリティ管理手続[*1]を用いて、委託業務実施部門を監査 ・ 外部専門家の監査結果を府省庁が確認

*1 情報セキュリティ管理手続：
府省庁が外部委託先に要求する情報セキュリティ対策を具体的に記述したもの（詳細は 6.4.2 を参照）。監査では、情報セキュリティ管理手続が機能していることを確認する。

*2 委託先が第三者の監査人を選定し、監査を委託するケースもあり得る。詳細は、「6 第三者監査（保証型監査）の利用」記載する。

府省庁の外部委託における情報セキュリティ監査において実施する第三者監査は、その目的から「保証型監査」となる。

外部委託の調達を行う際には、情報セキュリティ監査を実施する場合には、表 3-1 で示した形態のどの監査を実施するか選択する必要がある。

なお、調達者は、当該業務における情報セキュリティ監査の要否、監査が必要な場合には監査の形態について、調達時に委託先候補に周知しておくことが必要である。

また、各実施形態における作業項目は、以下のとおりである。

表 3-2　情報セキュリティ監査の作業項目と担当

項目	第二者監査	第三者監査（保証型監査）
監査仕様書の作成	府省庁	府省庁
監査対応計画書の作成	委託先	委託先
情報セキュリティ管理手続の策定	府省庁・委託先合議	府省庁・委託先合議（第三者[*1]）
監査計画書の作成	府省庁	第三者
監査の実施	府省庁	第三者
監査報告書の作成	府省庁	第三者
監査報告書の確認	府省庁	府省庁

[*1]：府省庁が第三者に作成委託し、その結果を委託先と協議、合意する形態も有。

4　本書の利用例

4.1 委託先選定基準としての監査の利用

委託先の選定において監査を利用する場合の手順については、「5.委託先の選定における監査の利用」を参照する。

4.2 委託先における情報セキュリティ対策の履行状況確認手段としての監査の利用

4.2.1 第三者監査（保証型監査）の利用

情報セキュリティ対策の履行状況の確認に第三者監査（保証型監査）を利用する場合の手順については、「6．第三者監査（保証型監査）の利用」を参照する。

4.2.2 第二者監査の利用

情報セキュリティ対策の履行状況の確認に第二者監査を利用する場合の手順については、「7.第二者監査の利用」を参照する。

5 委託先の選定における監査の利用

5.1 過去の情報セキュリティ監査の実施結果の利用

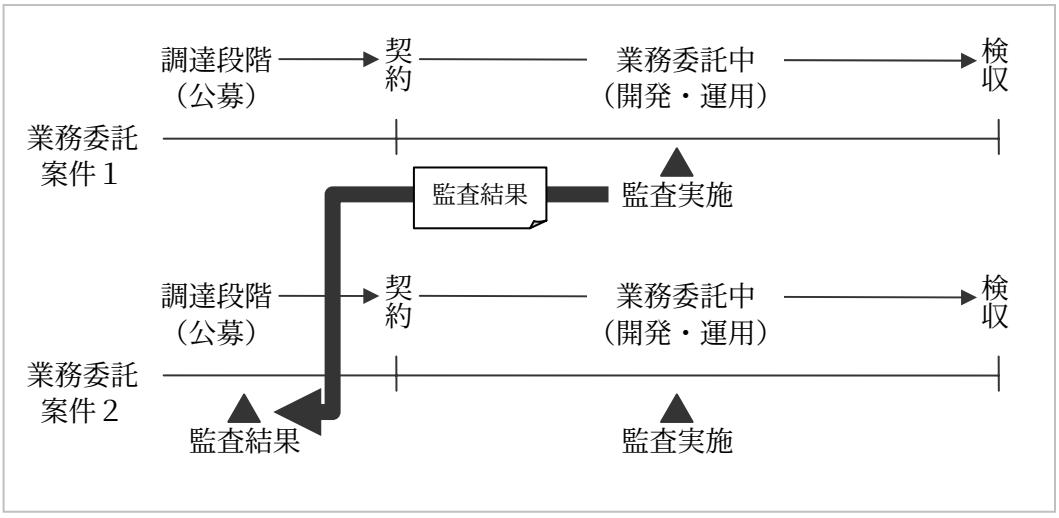
以下のケースにおいては、過去の情報セキュリティ監査の実施結果を委託先選定基準の一要素として活用することも可能である。

- 継続事業である等、直近において、同様の業務を受託しており、監査を実施したことがあるケース
- その他直近において、監査を実施しており、委託元の府省庁と同等のセキュリティレベルにあることが確認できるケース

上記の場合、監査報告書の内容を委託先選定基準の一要素（参考情報）として活用することができる。別案件等での監査結果を調達における選定基準の一つとする場合は、監査対象(場所、組織、業務等)のセキュリティレベルが委託する業務において求めるものと合致することに留意する。

なお、監査報告書の記載例、必要な情報の確認の内容等については、「付録 5：情報セキュリティ監査報告書例」を参照のこと。

図 5-1　情報セキュリティ監査結果を調達時に活用する場合



6 第三者監査（保証型監査）の利用

6.1 調達仕様

府省庁は、所属府省庁で作成されている「外部委託における情報セキュリティ対策実施規程」（又はそれ相当の規程）に従って、外部委託案件で必要となる情報セキュリティ対策を調達仕様に明確に記述する。本章では委託先に対する第三者監査（保証型監査）に係る事項について記載する。

6.2 監査仕様

府省庁は、調達仕様、省庁対策基準[*1]、実施手順[*2]等をベースに監査仕様書を作成する。

業務委託実施中に監査を実施することについて、委託先と事前に合意しておく必要がある。そのため、監査仕様書は調達時に作成し委託先候補に提示しておくことが必要である。監査仕様書は調達仕様の作成と同時に作成する。なお、監査仕様書は調達仕様書の一部（例えば別紙等の形態）としても構わない。

監査仕様書には、以下に示す監査対象業務、監査対象範囲、採用する情報セキュリティ管理手続等を記載する。

また、付録 2：監査仕様書例に情報セキュリティ監査仕様書例を示す。

*1：省庁対策基準：「政府機関の情報セキュリティ対策のための統一基準」（情報セキュリティ政策会議決定）に基づき、各府省庁がそれぞれ策定する情報セキュリティポリシーをいう。

*2：実施手順：省庁対策基準に定められた対策内容を具体的な情報システムや業務においてどのような手順に従って実施していくかについて定めた文書をいう。

6.2.1 監査対象業務

委託業務の種類（調達仕様）に応じた監査の重点項目を記述する。

システム開発業務であれば、技術的対策（IT システムのセキュリティ機能）などが重点項目となる。システム運用業務であれば、物理的環境的セキュリティ対策及び技術的対策（IT システムの運用、識別・認証、アクセス制御の状況）などが重点項目となる。

＜例＞

- 委託先のセキュリティ管理体制、運用環境
- 運用委託システムのセキュリティ機能

6.2.2 監査対象範囲

調達仕様に基づいて、当該監査の対象となる「場所」「組織」「業務」等を定義する。

＜例＞

- 入札･公募データベースシステムの運用委託範囲となる場所、組織、業務。

6.2.3 情報セキュリティ管理手続

委託先に要求する情報セキュリティ対策として、情報セキュリティ管理手続を定義する。情報セキュリティ管理手続は、基本的には、府省庁が定義するものであるが、委託先の情報セキュリティ対策の状況に応じて、府省庁と委託先が合議の上、決定する。合議の場合は、基本的事項のみを調達時に府省庁が作成し、契約後に府省庁、委託先合議の上、詳細を定義する。

＜例＞

- 情報セキュリティ管理基準*、調達仕様、省庁対策基準、実施手順等をベースに、○○業務の調達仕様、及び調達仕様に規定されたセキュリティ要件を基に策定した「情報セキュリティ管理手続」

*：情報セキュリティ管理基準：情報セキュリティ監査制度において策定されている情報セキュリティ対策の実践規範。

6.2.4 監査実施者の条件

【(a) 府省庁が第三者の監査人を選定し、監査を委託する場合】

府省庁が選定した第三者の監査人が監査することを記載する。

【(b)委託先が第三者の監査人を選定し、監査を委託する場合】

監査人の条件について記載する。

＜例＞

- 情報セキュリティ監査について過去２年間の経験を有すること。
- 公認情報セキュリティ監査人資格を持っていること、等

6.3 監査対応計画

「監査対応計画書」とは、府省庁が委託先に提示した「監査仕様書」に対して、委託先が委託業務実施中に監査を受け入れることを表明する文書である。

「監査対応計画書」では「監査仕様書」に対応し、以下に示す監査対象業務、監査対象範囲等を記載する。

なお、付録 3：に監査対応計画書例を示す。

6.3.1 監査対象業務

監査仕様書に準じて、監査の重点項目を記載する。

＜例＞

- 委託先のセキュリティ管理体制、運用環境
- 運用委託システムのセキュリティ機能

6.3.2 監査対象範囲

監査仕様書に基づいて、当該監査の対象となる具体的な「場所」「組織」「業務」を記載する。

＜例＞

- 場所：○○事業所、△△システムセンター
- 組織：△△システム部（××名）
- 業務：□□システムの運用業務

6.3.3 監査実施企業（監査実施者）

【(a)府省庁が第三者の監査人を選択し第三者に依頼する場合)】

委託先が選定した第三者監査人による監査である旨を記述する。

【(b)委託先が第三者の監査人を選定し、監査を委託する場合】

監査仕様書に準じて選定・依頼した監査実施企業を記載する。

＜例＞

- ○○システム株式会社（情報セキュリティ監査企業台帳登録企業）

6.3.4 監査実施時期

監査実施予定時期を記載する。

＜例＞

- ○○年××月中旬*

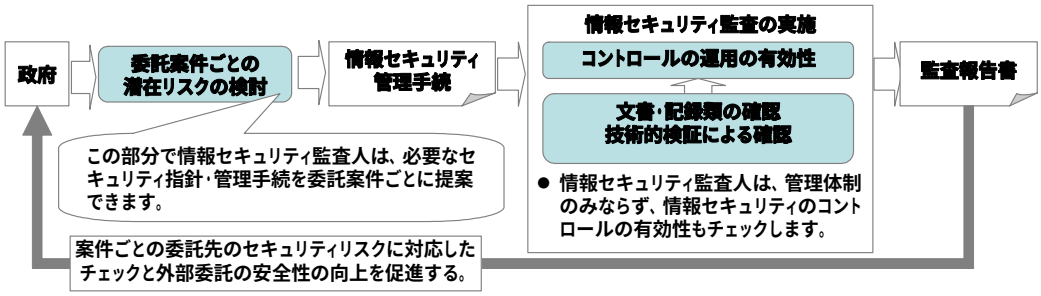
*なお、委託業務実施が長期間にわたり、定期的な監査を行う場合は、その旨の記載も加える。

*原則として１回/年実施。

6.4 監査の手順

委託先と契約後の監査は以下の手順で実施する。

図 6-1　監査の全体像



6.4.1 リスクの検討

基本的には、府省庁が実施するが、委託先の情報セキュリティ対策の履行状況などが不明な場合もあるので、府省庁、委託先合議の上、実施する。合議で実施する場合は、府省庁の主導の下で行う。

- 調達仕様を基に監査対象範囲を決定する。
- 監査対象範囲の重要な情報資産を洗い出す。
- 重要な情報資産（監査対象範囲のシステム／データ）についてリスクを分析する。

リスクの検討については、「6.5 リスクの識別」及び「付録 1：リスク分析資料例」を参照のこと。

6.4.2 情報セキュリティ管理手続の作成

情報セキュリティ管理手続は、基本的には、府省庁が定義するものであるが、委託先の情報セキュリティ対策の状況に応じて、府省庁と委託先が合議の上、決定する。

- 情報セキュリティ管理基準、調達仕様、省庁対策基準、実施手順などをベースに、具体的な情報セキュリティ対策を記述した「情報セキュリティ管理手続」を策定する。
- 情報セキュリティ管理手続は、契約で定めた委託先に要求する情報セキュリティ対策を、監査ができる程度に具体化したセキュリティ対策に関する記述となる。

(1) 必要項目の抽出

- リスク分析の結果に基づき、調達仕様、省庁対策基準、実施手順などと「情報セキュリティ管理基準」を参照し、委託する情報処理業務の重要度を勘案した上で、必要とされる項目の情報セキュリティ管理手続を策定する。
- 情報セキュリティ管理手続の策定に当たっては、「6.6 調達仕様と情報セキュリティ管理基準のコントロール項目との対応」も参照のこと。

(2) 追加項目の抽出

- 「調達仕様に固有の要件（※１）」から、情報セキュリティの観点で「委託業務に固有の必要項目（※２）」を抽出する。
  - （※１）調達仕様に固有の要件
    - 例えば、委託するサーバの運用業務で 24 時間 365 日の運用を求めることなど。
  - （※２）委託業務に固有の必要項目
    - 例えば、サーバを二重化やホットスタンバイにすることなど。具体的には、調達仕様、省庁対策基準、実施手順などと「情報セキュリティ管理基準」から項目を抽出した後、調達仕様に従って、監査対象範囲にとって特に必要と考えられる項目を追加する。例えば、監査対象範囲内において非常に重要な情報資産が存在し、脅威の発生頻度が高く、発生しうる被害が大きなものとなる場合、通常の情報セキュリティ対策に加えて、厳重な対策を追加することが想定される。
- 項目を追加する際は、他の項目での表現の抽象度を参照しつつ、表現を検討する。

(3) 文言の修正

府省庁と委託先が合議の上、最終的な情報セキュリティ管理手続の詳細を決定する。

- 抽出した必要項目と追加項目から、情報セキュリティ管理手続を作成する。
- 抽出された必要項目と追加項目の整合性をとるように、文言の修正や項目の分離・統合を行う。

6.4.3 監査計画書の作成

監査計画書は、監査人（府省庁、第三者）が委託先と調整[*1]の上、作成する。

監査の基本的な方針を監査基本計画書として文書化し、その基本方針に則った監査手続の実施計画を監査実施計画書として文書化する。

*1 委託先と調整：

監査人が第三者の場合は、府省庁、委託先、監査人の三者間で調整する。

表 6-1 監査計画書

	監査基本計画書	監査実施計画書
概要	監査の基本的な方針として計画	個別の監査についての詳細な計画
内容	・ 監査対象とする範囲 ・ 監査対象とする期間又は期日 ・ 監査対象とする段階（例えば運用段階） ・ 監査対象に係る監査目標 ・ 監査業務の管理体制 ・ 他の専門職の利用の必要性と範囲	・ 監査手続の実施時期 ・ 監査手続の実施場所 ・ 監査手続の実施担当者及びその割当て ・ 実施すべき監査手続の概要 必要に応じて以下を含める。 －監査要点 －実施すべき監査手続の種類 －監査手続実施の時期 －試査の範囲 ・ 監査手続の進捗管理手段又は体制

- 付録 4：に情報セキュリティ監査計画書例を示す。

6.4.4 情報セキュリティ監査の実施

監査人は、情報セキュリティ監査を実施する。

- 監査計画書に基づいて監査を実施する。
- 監査人は、管理体制のみならず、情報セキュリティのコントロールの有効性もチェックする。
- 監査証拠を収集し、評価する。
- 監査調書を作成する。

6.4.5 監査報告書の作成

監査人は、監査結果を報告書としてまとめる。

監査報告書は、以下の事項を満たしていることが確認できる内容とする。

- 監査人の意見表明により、委託先における情報システム及びそれらの情報システムが処理するデータの管理状況、利用状況、取扱状況が、「情報セキュリティ管理手続」を満たしている。
- 当初予定された監査対象範囲をカバーしており、かつ監査目標が達成されていること。

付録 5：に情報セキュリティ監査報告書例を示す。

6.4.6 監査報告会の実施

府省庁、委託先、監査人は、監査報告会を実施する。

【(a)府省庁が第三者の監査人を選定し、監査を委託する場合】

- 監査結果について、報告会又は確認会を実施し、監査内容について府省庁に報告する。
- 府省庁は、委託先のセキュリティ管理体制の妥当性を判断する。

【(b)委託先が第三者の監査人を選定し、監査を委託する場合】

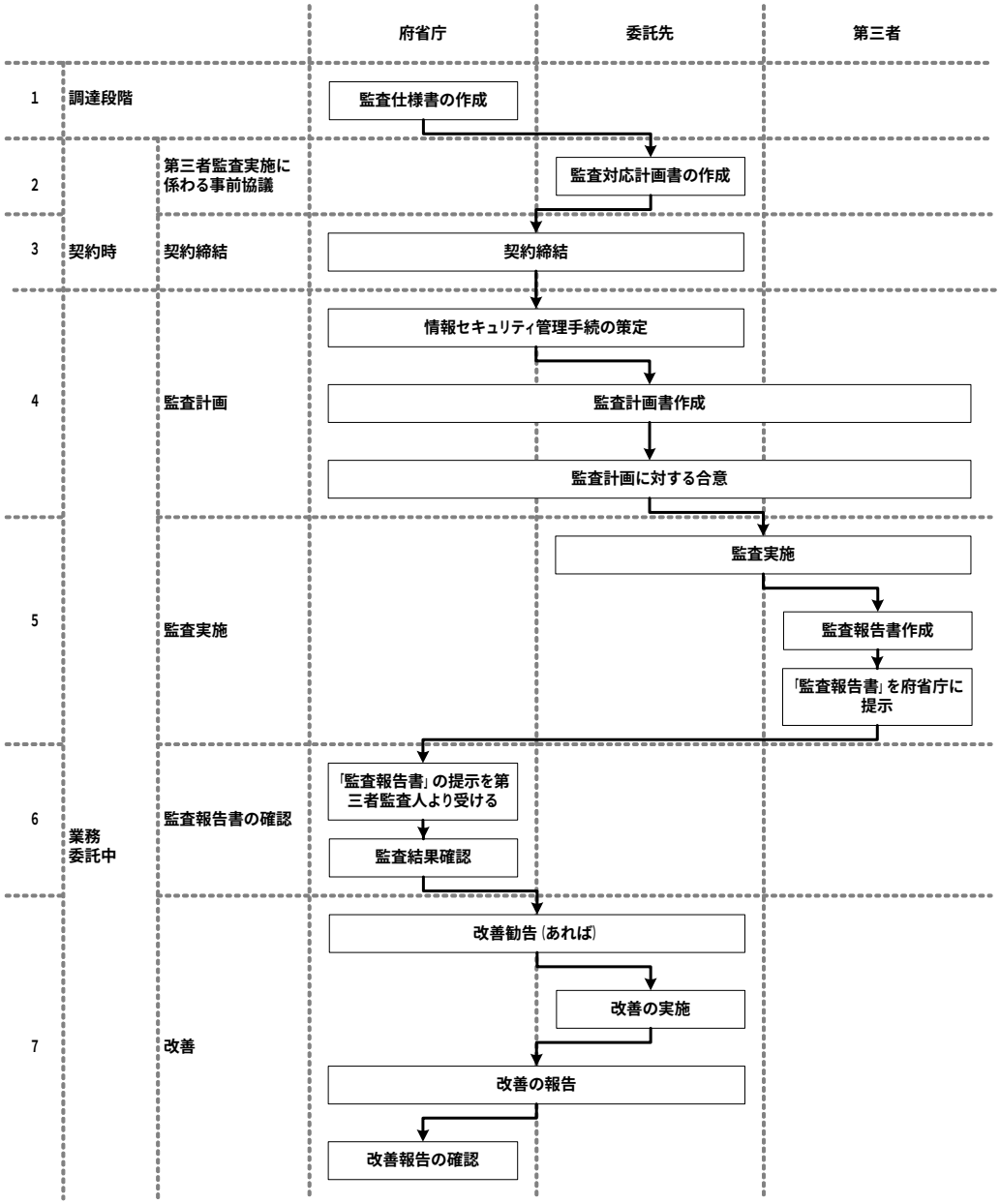
- 監査結果について、報告会又は確認会を実施し、監査内容について被監査対象である委託先に報告する。
- 委託先は、府省庁に監査結果を報告する。
- 府省庁は、委託先からの報告を受けて、委託先のセキュリティ管理体制の妥当性を判断する。

6.4.7 監査フロー

前節までで示した監査の全体の流れを、
(a)府省庁が第三者の監査人を選定し、監査を委託する場合
(b)委託先が第三者の監査人を選定し、監査を委託する場合
それぞれについて以下に示す。

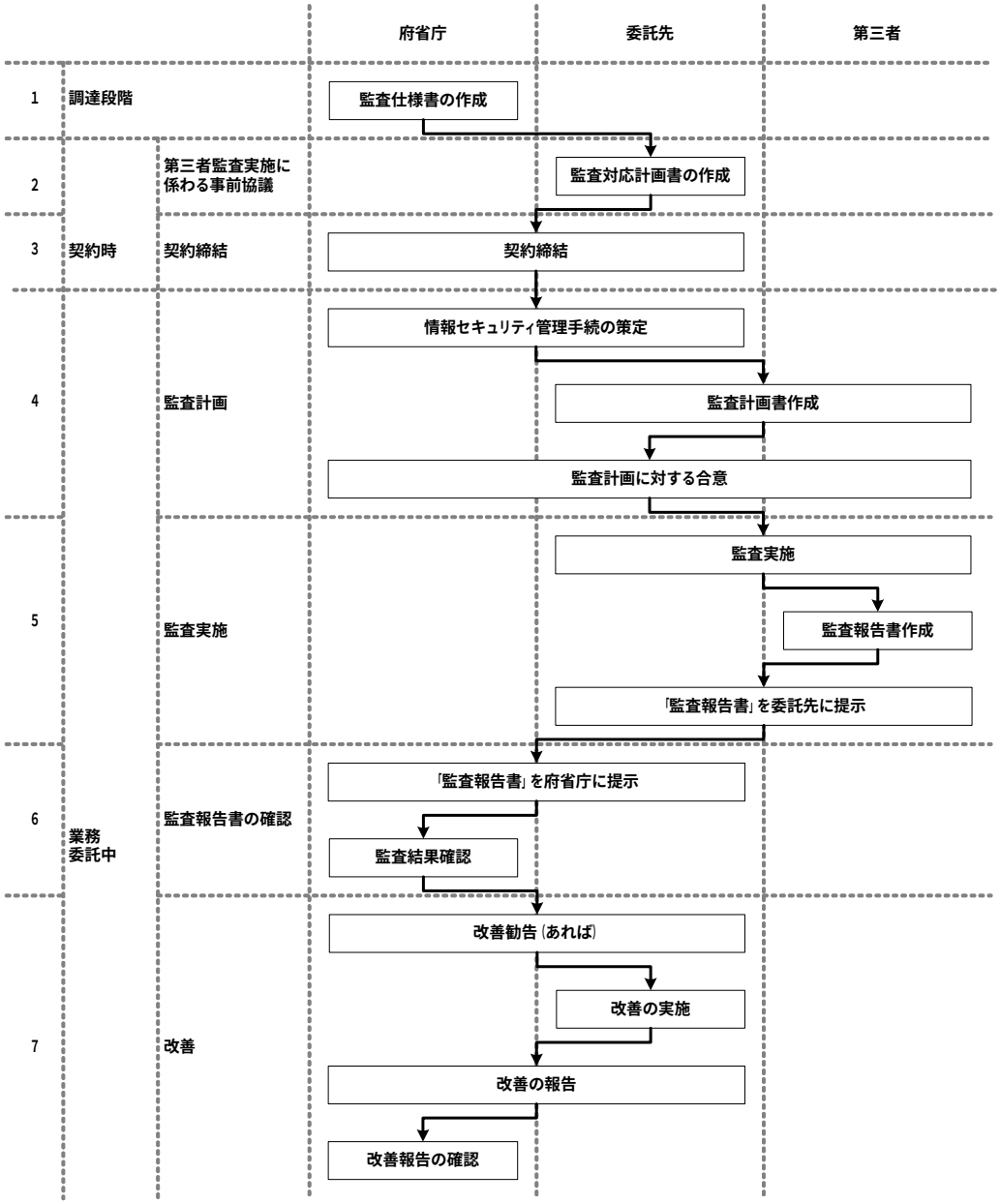
【(a)府省庁が第三者の監査人を選定し、監査を委託する場合】

図 6-2　監査フロー（a）



【(b)委託先が第三者の監査人を選定し、監査を委託する場合】

図 6-3　監査フロー（b）



6.5 リスクの識別

監査では、委託先において情報資産に対するリスクのマネジメントが効果的に実施されているか判断することが重要である。委託先において重要な情報資産（監査対象範囲のシステム／データ）の機密性、完全性、可用性が損なわれるリスクを検討する。なお、リスクの識別は、情報セキュリティ管理手続作成の前段階として、府省庁、委託先合議により実施する。また、府省庁において外部委託の対象となる業務についてのリスクの識別が既になされている場合は、その内容をもとに検討することも可能である。

6.5.1 監査対象範囲の決定

府省庁は、委託先と合議の上、外部委託する業務内容をかんがみて、監査対象範囲を決定する。

6.5.2 情報資産の洗い出し

府省庁は、委託先と合議の上、監査対象となる情報資産を洗い出す。

(1) 監査対象データ棚卸表の作成

監査対象データの棚卸しのため、監査対象範囲となったシステムや業務ごとに、そのシステムや業務が処理しているデータを棚卸表にまとめる。棚卸表には機密性、完全性、可用性の観点から情報の価値区分を記入する。既に情報処理の委託業務において取り扱うデータが棚卸されている場合は、その台帳を利用することもできる。

「監査対象データ棚卸表」及び表に記入する情報の価値区分については「付録１：リスク分析資料例」の(a)及び(b)の表を参照のこと。

6.5.3 重要な情報資産（監査対象範囲のシステム／データ）に係るリスク分析

府省庁は、委託先と合議の上、情報資産価値、脅威の発生確率および脆弱性の３つの要素からリスクの大きさを評価する。

(1) 情報資産価値の評価

監査の対象となるデータの情報資産価値の評価については、「6.5.2(1)監査対象データ棚卸表の作成」において実施済みである。

(2) 脅威の評価

「監査対象データ棚卸表」重要な情報資産に係る脅威の発生確率を評価する。

まず、監査対象のデータ及びシステムに対する脅威を洗い出す。脅威の例については「付録１：リスク分析資料例」の(c)を参照のこと。

次に、府省庁は、委託先と合議の上、監査対象範囲で洗い出した脅威それぞれについて、その脅威が発生するレベル（発生確率・発生頻度など）を評価・設定する。

脅威が発生するレベルを評価・設定する際には、調達者の過去の経験、社会的な動向、委託先での事件・事故の発生状況等を勘案して定義する。一般的な過去の事件・事故の例や監査結果等も入手可能であれば参考にする。

脅威ごとに発生レベルを評価・設定する例は、「付録１：リスク分析資料例」の(d)及び（e）を参照のこと。

(3) 脆弱性の評価

府省庁は、委託先と合議の上、脅威に対抗するための対策の実施状況を評価する。これまでの委託先において把握されているコントロール策の実施状況に係る資料や自己点検結果等も参考にすることもできる。

対策の実施状況に係る情報が事前に入手できない場合は、それぞれの対策が適切に実施されているか、リスク分析のために調査を実施することが理想的である。ただし、本来、監査を実施するための前提作業であるリスク分析作業に過大な負荷をとられるのを避けるため、全ての対策が一定レベルで実施されており、脆弱性は全ての範囲において一定であるとみなす方法もある。

(4) リスクの評価

府省庁は、委託先と合議の上、情報資産価値、脅威、及び脆弱性の３つの要素からリスクを評価する。

脆弱性をパラメーターとして固定し、情報資産価値と脅威からリスクの大小を評価する例は、「付録１：リスク分析資料例」の(f)及び（g）を参照のこと。

「脅威の発生確率」と「情報資産価値」のそれぞれの値の組み合わせによって、リスクを算出する。 「脅威の発生確率」、「情報資産価値」がそれぞれ高くなれば、リスクもより大きくなる。

リスクの評価結果に応じて適切なコントロール策が実施されているか、監査において確認する。

6.6 調達仕様と情報セキュリティ管理基準のコントロール項目との対応

情報セキュリティ監査では、前節までで示したように対象となる委託業務に対して、「6.5 リスクの識別」で示される手順により、識別したリスクに応じて情報セキュリティ管理基準をベースとして情報セキュリティ管理手続を策定し、策定された情報セキュリティ管理手続が委託先において機能していることを確認するために監査を行うことになる。

また、府省庁が外部委託する場合に、一般的に委託先において実施が必要であり調達仕様書で要求することが想定される情報セキュリティ対策として以下が挙げられる。

(1)情報セキュリティを確保するための体制の整備
(2)委託先が取り扱う府省庁の情報の秘密保持等
(3)運用・保守・点検における情報セキュリティ対策の実施
(4)脆弱性対策の実施
(5)情報セキュリティが侵害された場合の対処

これら対策が委託業務実施中に委託先において確実に履行されていることの確認も情報セキュリティ監査の役割となる。次表に、上記で示した(1)～(5)と情報セキュリティ管理基準の項目との関連を示す。次表で「○」が記載されている情報セキュリティ管理基準項目は、(1)～(5)のセキュリティ対策と関連性が強い項目である。「○」のついた情報セキュリティ管理基準項目から情報セキュリティ管理手続を策定する際には、調達仕様で要求した情報セキュリティ管理手続の確認も考慮することが必要である。

表 6-2　外部委託に係る契約内容と管理基準の項目（コントロール）との対応

情報セキュリティ管理基準の大項目 ＼ 委託先に実施させる情報セキュリティ対策	1 セキュリティ基本方針	2 組織のセキュリティ	3 資産の分類及び管理	4 人的セキュリティ	5 物理的及び環境的セキュリティ	6 通信及び運用管理	7 アクセス制御	8 システムの開発及び保守	9 事業継続管理	10 適合性
(1)情報セキュリティを確保するための体制の整備（委託先で(2)～(5)の対策を確実に行うための体制の整備）	○	○								
(2)取り扱う府省庁の情報の秘密保持等			○	○	○	○	○			○
(3)運用・保守・点検における情報セキュリティ対策の実施			○	○	○	○	○			○
(4)脆弱性対策の実施			○	○		○ 特に 6.1		○ 特に 8.5		○
(5)情報セキュリティが侵害された場合の対処			○	○		○ 特に 6.1			○	○

■＜ (1)の体制が確保されているという前提＞

表中の数字（“6.1”“8.5”）は、情報セキュリティ管理基準の中項目を示すものであり、内容は以下の通り

6.1　運用手順及び責任

8.5　開発及び支援過程におけるセキュリティ

6.7 監査結果の評価と対応

6.7.1 監査結果の評価

府省庁の調達担当者は、監査結果を受領した後にその結果を評価する。標準的な評価基準を定めることは難しいが、委託先と情報セキュリティ管理手続作成にあたって調整を行う際に、妥当であると判断できる基準を合意しておくこともできる。

6.7.2 対応

(1) 委託先の情報セキュリティ対策の履行状況が、妥当と判断できる場合

引き続き、業務委託を継続する。

(2) 委託先の情報セキュリティ対策の履行状況が、妥当と判断できない場合

問題点の改善を委託先に要求する。ただし、委託内容によっては、問題点の修正が委託業務期間を超えて実施される場合もある（情報システムの大幅改修など)。そのような場合に備えて、あらかじめ SLA などを締結し、妥当と判断できない場合のペナルティ条項を契約に盛り込むこともできる。

6.8 その他関連文書

6.8.1 監査調書

監査調書は、監査業務の実施記録として、監査証拠や関連資料をまとめたものである。チェックシートや報告書を作成する際の根拠となる情報として活用されるとともに、監査業務の品質管理にも役立つ。また、監査人が、正当な注意を払った上で監査業務を遂行したことの証左となる場合もあり、必要な情報を正確に漏れなく記録することが必要である。

監査調書の形態については、特に定めはない。

6.8.2 契約書の条文

委託先が監査を受け入れることを契約書に明記する。

契約書への反映については、「付録 6：契約への反映」を参照。

7 第二者監査の利用

7.1 調達仕様

府省庁は、所属省庁で作成されている「外部委託における情報セキュリティ対策実施規程」（又はそれ相当の規定）に従って、外部委託案件で必要となる情報セキュリティ対策を調達仕様に明確に記述する。本章では委託先に対する第二者監査（府省庁による監査）に係る事項について記載する。

7.2 監査仕様

府省庁は、調達仕様、政府機関統一基準、省庁対策基準、実施手順等をベースに監査仕様書を作成する。

業務委託中に第二者監査を実施することについて、委託先と事前に合意しておく必要がある。そのため、監査仕様書は調達時に作成し委託先候補に提示しておくことが必要である。監査仕様書は調達仕様の作成と同時に作成する。なお、監査仕様書は調達仕様書の一部（例えば別紙等の形態）としても構わない。

監査仕様書では、監査対象業務、監査対象範囲、情報セキュリティ管理手続等を記載する。

7.3 監査対応計画

「監査対応計画書」とは、府省庁が委託先に提示した「監査仕様書」に対して、委託先が委託業務実施中に監査を受け入れることを表明する文書である。

「監査対応計画書」では、「監査仕様書」に対応し、監査対象業務、監査対象範囲等を記載する。

7.4 第二者監査の手順（全体の流れ）

7.4.1 リスクの検討

【6.4.1 リスクの検討】を参照。

7.4.2 情報セキュリティ管理手続の作成

【6.4.2 情報セキュリティ管理手続の作成】を参照。

7.4.3 監査計画書の作成

【6.4.3 監査計画書の作成】を参照。

7.4.4 情報セキュリティ監査の実施

【6.4.4 情報セキュリティ監査の実施】を参照。

7.4.5 監査報告書の作成

【6.4.5 監査報告書の作成】を参照。

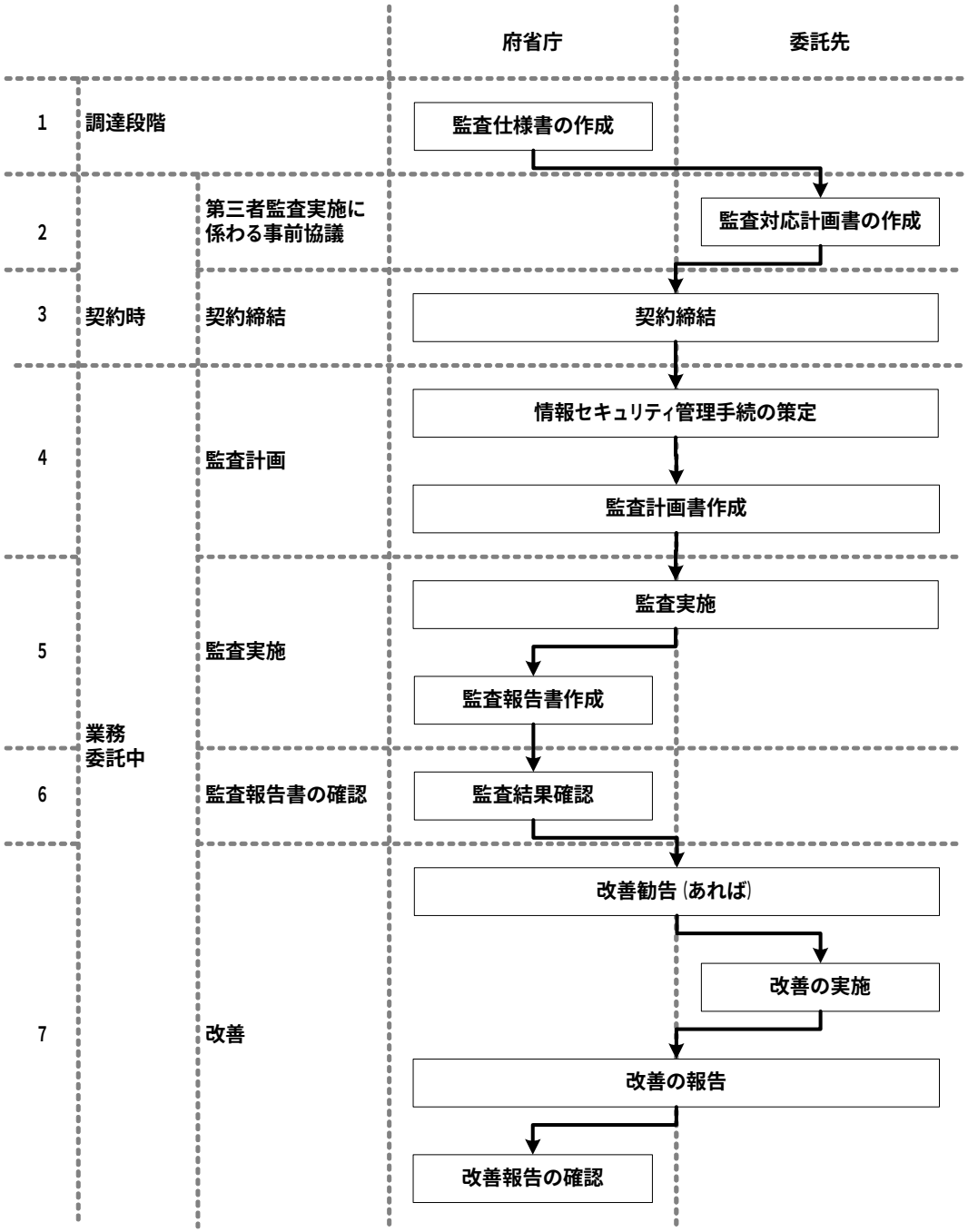
7.4.6 監査報告会の実施

- 監査結果について、報告会又は確認会を実施し、監査内容について、委託先に通知する。
- 委託先のセキュリティ管理体制の妥当性を判断する。

7.4.7 業務委託中の監査フロー

業務委託中の監査の場合、監査の流れは以下のようになる。

図 7-1 第二者監査フロー



7.5 リスクの識別

【6.5 リスクの識別】を参照。

7.6 調達仕様と情報セキュリティ管理基準のコントロール項目との対応

【6.6 調達仕様と情報セキュリティ管理基準のコントロール項目との対応】を参照。

7.7 監査結果の評価と対応

【6.7 監査結果の評価と対応】を参照。

7.8 その他関連文書

【6.8 その他の関連文書】を参照。

付録1：リスク分析資料例

(a) 情報資産価値の定義

機密性区分による情報資産価値

機密性区分	価値	定義
機密性３	3	（府省庁の規程等に準ずる）
機密性２	2	（府省庁の規程等に準ずる）
機密性１	1	（府省庁の規程等に準ずる）

完全性区分による情報資産価値

完全性区分	価値	定義
完全性２	2	（府省庁の規程等に準ずる）
完全性１	1	（府省庁の規程等に準ずる）

可用性区分による情報資産価値

可用性区分	価値	定義
可用性２	2	（府省庁の規程等に準ずる）
可用性１	1	（府省庁の規程等に準ずる）

(b) 監査対象データ棚卸表

システム名（業務名）	分類名	情報資産区分			利用者		情報資産管理者
		機密性	完全性	可用性	部署	人数	
○○省□□業務システム	△△データ	3	2	2	管理部	5 名	管理部長
	××データ	2	1	1	運用部	2 名	運用部長
	□□データ	2	2	2	ｻｰﾋﾞｽ部	20 名	サービス部長
○○省××システム	・・・	・	・	・	・・・	・名	・・・
・・・	・・・	・	・	・	・・・	・名	・・・

１．システム名（業務名）

委託先の情報処理に係るシステム又は業務の名称

２．分類名

委託先の情報処理に係るシステム又は業務が取り扱うデータの分類

３．情報資産区分

機密性、完全性、可用性のそれぞれの観点での情報資産区分

４．利用者

当該データの利用者の部署名とその人数

５．情報資産管理者

当該データの管理者

(c) 想定される脅威の洗い出し

脅威		概要	機密性	完全性	可用性
データに対する脅威	情報漏えい	開示範囲を超えて情報が公開されてしまう。 アクセス権の不適切な設定により情報が漏えいする	●	－	－
	情報改ざん	故意又は過失によって、情報の内容が不適切に変更される	－	●	－
	情報消去	故意又は過失によって、情報が消去される	－	－	●
システムに対する脅威	サービス停止	DoS 攻撃によるサービスの停止 ハードウェアの故障や操作ミスにより機器が停止することによるサービスの停止	－	－	●
	不正アクセス	機器が目的外に利用される 他人の ID を不正に用いての機器の利用 機器のセキュリティホールを利用してユーザ権限を不正に奪取する	●	●	●
	悪意あるソフトウェア	ウイルス／ワームへの感染 スパイウェア／トロイの木馬が仕込まれる	●	●	●

(d) 脅威の発生頻度の定義

評価段階	評価内容
3	発生する可能性や誘発要因の頻度が高い。 誰もが脅威を認識しており、実際に発生している 年に数回（月又は四半期に１回以上）の発生が予想される。一般的な不注意により発生する。 （例）発生する可能性が高い（１年に何度も）　など
2	発生する可能性や誘発要因の頻度が中程度である。 脅威の発生の可能性があるが、今のところあまり起きていない 年に１～２回程度の発生が予想される。特定の状況下でのみ発生する。 （例）発生する可能性が中程度（年に１～２回程度）　など
1	発生する可能性や誘発要因の頻度が低い。 脅威の発生の可能性はほとんどない １年に１回あるかないかである。発生はあまり考えられない。 （例）発生する可能性が低い（数年に１回程度）　など

(e) 脅威ごとの発生頻度の設定

想定する脅威	機密性	完全性	可用性	脅威のレベルの考え方
情報の漏えい等	3	－	－	情報の漏えいや情報資産の盗難は高い危険があると考える
情報改ざん	－	2	－	情報資産の改ざんは中程度と考える
情報消去	－	－	2	情報資産の消去は中程度の危険があると考える
サービス停止	－	－	2	サービスの停止による情報資産の利用不可は、中程度の危険があると考える
不正アクセス	2	2	2	不正アクセスは、高い危険があると考える
ウイルス感染	3	3	3	ウイルス感染は、かなりの頻度でおこっている

(f) リスク評価表

		脅威の発生確率		
		3	2	1
情報資産価値	3	リスク大	リスク大	リスク中
	2	リスク大	リスク中	リスク小
	1	リスク中	リスク小	リスク小

(g) リスク検討結果

システム名（業務名）	データ			脅威			リスク (*4)
	名称	資産価値(*1)		名称	発生確率		
					個別 (*2)	全体 (*3)	
○○システム		機密性	3	不正アクセス	2	3	大
				ウイルス感染	3		
		完全性	2	不正アクセス	2	3	大
				ウイルス感染	3		
		可用性	2	サービス停止	2	3	大
				不正アクセス	2		
				ウイルス感染	3		
	△△データ	機密性	3	情報漏えい	3	3	大
		完全性	2	情報改ざん	2	2	中
		可用性	2	情報消去	2	2	中
	××データ	機密性	2	情報漏えい	2	2	中
		完全性	1	情報改ざん	1	1	小
		可用性	1	情報消去	1	1	小
・・・	・・・	・・・	・	・・・	・	・	・

＊1．資産価値

「(a)情報資産価値の定義」及び「(b)監査対象データ棚卸表から資産価値」をもとめて記入。（対象となるデータの中で、最も価値の高いものの資産価値をシステム全体の価値とする。）

＊2．個別

「(e)脅威ごとの発生頻度の設定」からそれぞれの脅威個別について発生確率をもとめて記入

＊3．全体

脅威個別の発生確率のうち、最も高いものの値を記入

＊4．リスク

*1 と*3 から(f)リスク評価表を使ってリスクを算出

付録2：監査仕様書例

(a) 府省庁が第三者の監査人を選定し、監査を依頼するケース

平成○○年○○月○○日

［委託先組織名］
［委託先代表者名］

［○○省所属名］
［○○省調達担当者氏名］

情報セキュリティ監査仕様書

今回委託仕様において発注する委託業務については､○○省の基準､実施手順等により、委託先において情報セキュリティ監査を受けることが必要であり、以下の監査仕様に基づいて、受託仕様に加えて監査対応計画書を作成下さい。当監査は、調達仕様に記載し、契約で求める情報セキュリティ対策の履行状況を確認すること目的としています。

委託先として発注が決定する場合には、運用委託開始後、○○省の指定する第三者による情報セキュリティ監査を受けていただきます。

なお、監査実施に係る費用は、○○省の負担とします。

１．監査対象業務

- ○○省××業務システムの運用業務

２．監査対象範囲

- 入札・公募データベースシステムの運用委託範囲となる場所、組織、業務

３．情報セキュリティ管理手続

- 情報セキュリティ管理基準、調達仕様、○○省基準、実施手順、○○業務の調達仕様、監査目的及びリスク分析結果を踏まえて策定する情報セキュリティ管理手続

４．監査実施企業（監査実施者）の条件

- ○○省が指定する第三者が監査人となること

(b) 委託先が第三者の監査人を選定し、監査を委託するケース

平成〇〇年〇〇月〇〇日

［委託先組織名］
［委託先代表者名］

［〇〇省所属名］
［〇〇省調達担当者氏名］

情報セキュリティ監査仕様書

今回委託仕様において発注する委託業務については､〇〇省の基準､実施手順等により、委託先において情報セキュリティ監査を受けることが必要であり、以下の監査仕様に基づいて、受託仕様に加えて監査対応計画書を作成下さい。当監査は、調達仕様に記載し、契約で求める情報セキュリティ対策の履行状況を確認すること目的としています。

委託先として発注が決定する場合には、運用委託開始後、本監査仕様書に基づき委託先で選定する第三者による情報セキュリティ監査を実施し監査報告書の提出をお願いします。なお、監査実施に係る費用は、委託先の負担とします。（又は、「なお、監査実施に係る費用は、〇〇省の負担とします。」）

１．監査対象業務

- 委託先のセキュリティ管理体制、運用環境
- 運用委託システムのセキュリティ機能

２．監査対象範囲

- 入札・公募データベースシステムの運用委託範囲となる場所、組織、業務

３．情報セキュリティ管理手続

- 「情報セキュリティ管理基準」、〇〇省基準、実施手順等をベースに、〇〇業務の調達仕様、監査目的及びリスク分析結果を踏まえて策定する情報セキュリティ管理手続

４．監査実施企業（監査実施者）の条件

- 情報セキュリティ監査企業台帳への登録企業であること
- NPO日本セキュリティ監査協会に所属する企業であること
- 監査チームリーダは、公認情報セキュリティ主任監査人の資格登録者であること
- 監査人のうち2名以上は公認情報セキュリティ監査人（補も含む）の資格登録者であること

付録3：監査対応計画書例

(a) 府省庁が第三者の監査人を選定し、監査を依頼するケース

平成〇〇年〇〇月〇〇日

［〇〇省所属名］
［〇〇省調達担当者名］

［委託先所属組織名］
［委託先代表者氏名］

監査対応計画書

監査仕様に基づき、以下の監査対応計画を作成しておりますので、ご査収のほどお願い致します。

１．監査対象業務

- 委託先のセキュリティ管理体制、運用環境
- 運用委託システムのセキュリティ機能

２．監査対象範囲

- 場所：東京都〇〇区〇〇町
- 組織：データベース運用管理部
- 業務：入札公募データベースシステムの運用業務

３．監査実施企業（監査実施者）

- 〇〇〇〇株式会社
  （委託先が選定した監査人）

４．監査実施時期

- 平成xx年x月ごろを予定

(b) 委託先が第三者の監査人を選定し、監査を委託するケース

平成〇〇年〇〇月〇〇日

［〇〇省所属名］
［〇〇省調達担当者名］

［委託先所属組織名］
［委託先代表者氏名］

監査対応計画書

監査仕様に基づき、以下の監査対応計画を作成しておりますので、ご査収のほどお願い致します。

１．監査対象業務

- 委託先のセキュリティ管理体制、運用環境
- 運用委託システムのセキュリティ機能

２．監査対象範囲

- 場所：東京都〇〇区〇〇町
- 組織：データベース運用管理部
- 業務：入札公募データベースシステムの運用業務

３．監査実施企業（監査実施者）

- 〇〇〇〇株式会社
  情報セキュリティ監査企業台帳登録企業、NPO日本セキュリティ監査協会会員
  公認情報セキュリティ主任監査人３名、公認情報セキュリティ監査人５名、情報セキュリティ監査人補５名から監査チームを編成（監査チームリーダは公認情報セキュリティ主任監査人にて実施）

４．監査実施時期

- 平成xx年x月ごろを予定

付録4：情報セキュリティ監査計画書例

(a) 監査基本計画書

平成○○年○○月○○日
［監査人所属組織名］
［監査人代表者氏名］

監査基本計画書

監査の目的	□□省から委託する○○業務に関して、委託先に契約で求める情報セキュリティ対策の履行状況を確認する。
監査対象の組織	□□省から委託する○○業務を行う委託先の部門
監査基準	情報セキュリティ監査基準
情報セキュリティ対策の基準	府省庁の要求に基づき、府省庁と委託先で策定し合意した「情報セキュリティ管理手続」
監査対象とする範囲	○○業務に係る情報システム及びそれらの情報システムが処理する電子データの管理状況、取扱い状況と、主な IT セキュリティマネジメント状況
監査対象とする期間 又は期日	２００ｘ年ｘ月ｘ日～２００ｘ年ｘ月ｘ日
監査対象とする段階	運用段階にある情報システム
監査対象にかかわる監査目標	情報セキュリティ管理手続に対する準拠性
監査体制	＜資料１＞を参照
監査業務の管理体制	＜資料２＞を参照
他の専門職の利用と範囲	＜資料３＞を参照
監査スケジュールの概要	＜資料４＞を参照

＜資料１＞　　監査体制

役　割	氏　名	所持資格等
監査チーム リーダー	○○ ○○	公認情報セキュリティ主任監査人
監査チーム サブリーダー	○○ ○○	公認情報セキュリティ監査人
監査人	○○ ○○	公認情報セキュリティ監査人補
監査人	○○ ○○	

＜資料２＞　　監査業務の管理体制

以下の取組みにより、監査品質の向上を図る。

フェーズ	監査チーム内において実施	対象部署への協力の依頼
監査前	監査チェックシートのレビュー 監査チーム勉強会の実施	事前ヒアリングへの協力 事前閲覧が必要な資料の提示
監査時	監査人の適切な配置 監査記録の整備 監査結果のレビューの実施	実査への協力
監査後	監査結果報告ミーティング	

上記の品質向上取組をレビューするため、監査チームから独立した品質管理者を以下のとおり定める。

品質管理者氏名	所属・役職	所持資格等
○○ ○○	××事業部	公認情報セキュリティ監査人

＜資料３＞　　他の専門職の利用の必要性と範囲

監査チームのサポートのため、以下の後方支援チームを編成する。

後方支援チーム氏名	所属・役職	サポート範囲
○○ ○○	法務部	法務領域
○○ ○○	情報システム部	技術的監査領域

＜資料４＞　　監査スケジュールの概要

主な監査業務	実施時期	備　考
対象データ棚卸し リスク分析	２００ｘ年ｘ月	
監査計画策定	２００ｘ年ｘ月	
実査	２００ｘ年ｘ月	監査実施計画書に基づいて実施
報告書作成	２００ｘ年ｘ月	

(b) 監査実施計画書

平成○○年○○月○○日
［監査人所属組織名］
［監査人代表者氏名］

監査実施計画書

監査の目的	□□省から委託する○○業務に関して、委託先に契約で求める情報セキュリティ対策の履行状況が、情報セキュリティ管理手続に合致していることを確認すること。
監査対象の組織	○○株式会社： ○○部 ○○株式会社： ××部
監査基準	情報セキュリティ監査基準
情報セキュリティ対策の基準	府省庁の要求に基づき、府省庁と委託先で合意の下に策定した「情報セキュリティ管理手続」
監査対象とする範囲	○○業務に係る情報システム及びそれらの情報システムが処理する電子データの管理状況、取扱い状況と、主な IT セキュリティマネジメント状況
監査手続の実施時期	２００ｘ年ｘ月ｘ日～ｘ日 各部署の監査日時については、資料１を参照
監査手続の実施場所	視察： サーバ室 再実行： 各端末の設置場所
監査人氏名	チーフ監査人 ○○ ○○ サブチーフ監査人 ○○ ○○ 監査人 ○○ ○○ 監査人 ○○ ○○ 各部署の担当については、資料１を参照
監査対象とする期間 又は期日	２００ｘ年ｘ月ｘ日～２００ｘ年ｘ月ｘ日
監査の重点項目	情報セキュリティにかかわる以下の領域を重点的に監査 ・ 物理的環境的セキュリティ ・ 通信及び運用管理 ・ アクセス管理

＜資料１＞　　監査スケジュール・主な監査ポイント・担当一覧

監査日時	監査対象部署	主な監査ポイント	技法	担当
XX/XX（月） XX:XX-XX:XX	○○部	セキュリティ基本方針 セキュリティ内部監査及び教育 資産の分類及び管理 従業員との秘密保持契約 セキュリティ事故・事件への対応 重要な施設の管理 重要な媒体の管理 アクセス管理 ＩＤ・パスワード管理 その他情報システム安全対策 外部委託管理 コンプライアンス・個人情報保護　等	閲覧 〃 〃 〃 閲覧 視察 ヒアリング 再実行 ヒアリング 視察 閲覧 ヒアリング	
XX/XX（月） XX:XX-XX:XX	××部	セキュリティ基本方針及び投資計画 セキュリティ教育 資産の分類及び管理 セキュリティ事故・事件への対応 電子商取引の運営管理 アクセス管理 ＩＤ・パスワード管理 コンプライアンス・個人情報保護　等	ヒアリング 〃 〃 〃 〃 再実行 ヒアリング 〃	
XX/XX（月） XX:XX-XX:XX	△△部	セキュリティ基本方針及び投資計画 セキュリティ教育 資産の分類及び管理 セキュリティ事故・事件への対応 重要な施設の管理 重要な媒体の管理 アクセス管理 ＩＤ・パスワード管理 コンピュータウイルス対策 バックアップ管理 オペレーション管理 取り外し可能な媒体の管理 電子商取引の運営管理 電子メール管理 コンプライアンス・個人情報保護　等	ヒアリング 〃 〃 〃 視察 〃 再実施 ヒアリング 閲覧 〃 〃 〃 ヒアリング 〃 〃	

付録5：情報セキュリティ監査報告書例

（第三者監査（保証型）の場合の例）

平成○○年○○月○○日

［報告先組織名］
［報告先代表者名］

［監査人所属組織名］
［監査人代表者氏名］

情報セキュリティ監査結果報告書

当社は、○○省が運用を委託し、貴社が運用している XXXX システムについて、貴社が、○○省と貴社の経営者の間で定めた情報セキュリティに係る管理手続（以下「情報セキュリティ管理手続」という。）を平成×年×月×日から平成×年×月×日までの期間において履行していることを確認するために、情報セキュリティ監査を実施した。

情報セキュリティ管理手続に基づいて、平成×年×月×日から平成×年×月×日までの期間において、○○システムのセキュリティ対策が機能していることについての責任は、貴社の経営者にある。

この情報セキュリティ監査は、「情報セキュリティ監査基準」に準拠して実施した。ただし、当社は貴社の情報セキュリティ管理手続の十分性については意見を表明しない。

当社が追加的手続を実施した場合には、貴社の経営者に報告したであろうその他の発見事項があったかもしれない。

（確認した情報セキュリティ管理手続とその結果は、ここ又は別紙に記載する。）

この報告書は、○○省のための情報利用を意図したものであり、他の第三者の利用を意図したものでなく、また、他の第三者はこの報告書を利用してはならない。

以上

－別紙－

確認した情報セキュリティ管理手続とその結果

監査領域	情報セキュリティ管理手続	結果	発見事項
通信及び運用管理	サーバルームへの可搬媒体の持込み・持出しは記録すること。	× 実施しているとは認められない	CD-R などの媒体をサーバ室へ持ち込むことが必要な業務が行われているが、サーバ室への入室の際、外部媒体の持込み・持出しの管理が行われていない。
：	可搬媒体を処分する際は、粉砕等の物理的破壊を実施すること。	○ 実施していると認められる。	－
：	：	：	：
：		：	：

－以上－

付録6：契約への反映

(a) 府省庁が第三者の監査人を選定し、監査を依頼するケース

（監査）

第●条

乙は、甲が提示する監査仕様書に基づく甲が選定する監査人による情報セキュリティ監査を受け入れること。

※甲：府省庁、乙：委託先

(b) 委託先が第三者の監査人を選定し、監査を委託するケース

（監査）

第●条

乙は、甲が提示する監査仕様書に基づき、乙が選定する外部監査人による情報セキュリティ監査を実施し、その結果を甲に報告すること。

※甲：府省庁、乙：委託先