

外部委託における情報セキュリティ対策実施規程  
雛形

2011 年 4 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
2006/3/10	初版
2006/4/21	各府省庁意見に基づく修正
2006/6/16	<ol style="list-style-type: none"> <li>1. 再委託の可否は、情報セキュリティ責任者が判断すべきことを明示(誤り訂正、7.5)。</li> <li>2. 仮称としていた参照先資料の名称を、確定した名称に変更。  「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」  「情報システムの構築等における ST 評価・ST 確認の実施に関する解説書」</li> <li>3. セキュリティ要求仕様を調達者が提示しセキュリティ機能の実装を求める場合について、調達仕様の記述例(第 部、1. (3))及び契約の記述例(第 部、1. (3))を追加。</li> <li>4. その他</li> </ol>
2007/11/9	政府機関統一基準(第 2 版)の策定に伴う修正等
2008/9/8	政府機関統一基準(第 3 版)の策定に伴う修正等
2011/4/21	政府機関統一管理基準及び政府機関統一技術基準の策定に伴う修正等 <ol style="list-style-type: none"> <li>1. 情報システムの「約款による情報処理サービス」(例えばクラウドサービス等)を利用するうえでのセキュリティ上の配慮事項を追加</li> <li>2. CC 認証の基本遵守への変更に係る修正。</li> <li>3. ST 評価、ST 確認の強化遵守への変更に係る修正。</li> </ol>

## 目次

本雛形の利用方法 .....	5
雛形において想定する前提 .....	5
手直しポイント .....	5
第 部 実施規程雛形 .....	7
1 本書の目的 .....	7
2 本書の対象者 .....	7
3 外部委託の形態 .....	7
3.1 外部委託する業務の分類 .....	7
3.1.1 情報システムの構築等の外部委託 .....	7
3.1.2 情報システムの運用・保守・点検の外部委託 .....	7
3.1.3 情報の加工・処理等の外部委託 .....	8
3.1.4 情報の保存・運搬の外部委託 .....	8
3.2 「約款による情報処理サービス」の利用による外部委託 .....	8
4 外部委託における情報セキュリティ確保に係る手続 .....	10
5 外部委託により情報処理業務を行うことの可否の判断 .....	10
5.1 外部委託の可否の原則 .....	10
5.2 脅威及び対策の検討における留意事項 .....	11
6 調達における手続 .....	13
6.1 委託先の選定基準及び選定手続 .....	13
6.2 国際規格を踏まえた委託先の情報セキュリティ水準の評価 .....	15
6.2.1 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の活用 .....	15
6.2.2 情報セキュリティ対策ベンチマークの活用 .....	15
6.2.3 情報セキュリティ監査の活用 .....	16
6.3 委託先に求める事項の周知 .....	16
6.3.1 委託先に実施させる情報セキュリティ対策の内容の周知 .....	16
6.3.2 情報セキュリティが侵害された場合の対処方法の周知 .....	17
6.3.3 情報セキュリティ対策の履行状況の確認等に関する事項の周知 .....	17
7 契約における手続 .....	18
7.1 外部委託に係る契約における情報セキュリティの考慮 .....	18
7.2 外部委託に係る確認書等における情報セキュリティの考慮 .....	20
7.3 外部委託の継続における注意 .....	20
7.4 外部委託における実施内容の変更に関する注意 .....	20

7.5	再委託に関する制限 .....	20
7.6	「約款による情報処理サービス」の利用による外部委託に関する注意.....	21
8	委託先における情報処理業務実施中の手続.....	23
8.1	取り扱う府省庁の情報の秘密保持等 .....	23
8.2	情報セキュリティ侵害が発生した場合の措置.....	23
8.3	情報セキュリティ対策の履行状況の確認 .....	24
9	納品・検収における手続 .....	24
10	国際規格を踏まえたセキュリティ機能の設計及び実装の評価 .....	24
10.1	情報システムの構築に伴い調達する機器等のセキュリティ機能の評価.....	24
10.2	情報システムの構築等におけるセキュリティ機能の設計及び実装の評価 .....	25
11	本書に関する相談窓口 .....	25
第 部	調達仕様における情報セキュリティ関連事項の記述例.....	26
1	外部委託する業務の分類に基づく事項.....	26
1.1	情報システムの構築等の場合 .....	26
1.2	情報システムの運用・保守・点検の場合 .....	29
1.3	情報の加工・処理等の場合 .....	31
1.4	情報の保存・運搬の場合 .....	33
2	「約款による情報処理サービス」の利用に関する事項.....	34
第 部	契約における情報セキュリティ関連事項の記述例.....	37
1	外部委託する業務の分類に基づく事項.....	37
1.1	情報システムの構築等の場合 .....	37
1.2	情報システムの運用・保守・点検の場合 .....	40
1.3	情報の加工・処理等の場合 .....	41
1.4	情報の保存・運搬の場合 .....	42
2	「約款による情報処理サービス」の利用に関する事項.....	43
付録 1	重要な情報を取り扱う情報処理業務 及び取り扱わない情報処理業務.....	44
1	重要な情報を取り扱う情報処理業務 .....	44
2	重要な情報を取り扱わない情報処理業務 .....	44
付録 2	情報セキュリティ対策等.....	44
付録 3	組織における情報セキュリティ水準の評価に関する制度.....	45

## 本雛形の利用方法

本雛形の第 部は、情報処理業務を外部委託により行う場合に、委託元の業務に適用する規定（仮称「外部委託における情報セキュリティ対策実施規程」）の雛形である。「外部委託における情報セキュリティ対策実施規程 策定手引書」の「2 規定に記載すべき事項」に示す事項の例を、「3 文書構成例」に示す構成で記述したものである。

本雛形の第 部は、情報処理業務を外部委託により行う場合に、調達仕様に記述する情報セキュリティ関連事項の例である。

本雛形の第 部は、情報処理業務を外部委託により行う場合に、契約に記述する情報セキュリティ関連事項の例である。

### 雛形において想定する前提

本雛形は、以下のことを前提としている。

- 本雛形は、統括情報セキュリティ責任者が、府省庁の規定を整備するために利用することを想定している。
- 本雛形を利用して整備した規定は、委託元としての業務を行う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に適用されるものとなる。
- 本雛形では、外部委託により行う次の情報処理業務を典型的なものとして採り上げている。
  - 情報システムの構築
  - ソフトウェアの開発
  - 情報システムの運用
  - 情報システムの保守・点検
  - 情報の加工・処理等
  - 情報の保存・運搬
- 本雛形は、情報処理業務以外の業務を外部委託により行う場合は対象としていない。

### 手直しポイント

「外部委託における情報セキュリティ対策実施規程」を策定するに当たり、以下の点を考慮して手直しをする必要がある。

- 本雛形は、統括情報セキュリティ責任者が、府省庁の規定を整備するために利用することを想定している。
- 府省庁で想定される情報処理業務の種類に応じて、本雛形から該当する記事を選択し、不足する部分及び前提等が異なる部分は追加・修正をする。
- 「外部委託における情報セキュリティ対策実施規程 策定手引書」に記載している様々な解説記事は、本雛形には重複して記載していないことから、策定手引書の「9.3.1 外部委託に係る契約」にある解説記事等を、必要に応じ規程に含めることもできる（例として付録 2 を参照）。また、府省庁において策定手引書を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向けの解説書としてあわせて利用することとする場合には、その解説記事等を当該手引書に含める必要はない。

- 雛形中において/・・・/形式で示す設定値（組織名等）は、各府省庁内の実態、委託する情報処理業務等に合わせて定める。
- 雛形中において【・・・の場合】形式で示す記述は、各府省庁の判断により適宜、選択又は修正して使用する。
- 雛形に記載した 1.2.5.1(1)(a)等の項番は、「政府機関の情報セキュリティ対策のための統一管理基準」(NISD-K304-101) 及び「政府機関の情報セキュリティ対策のための統一技術基準」(NISD-K305-101)の該当する項番である。雛形を利用して策定する規程には、含めなくてよい。

## 第 部 実施規程雛形

### 1 本書の目的

[ 省 ]において情報処理業務を外部委託により行う場合には、委託先における業務の遂行を委託元が直接に指揮命令することがなく、また当該業務に必要な情報を委託元から提供して委託先に取り扱わせるため、情報セキュリティを確保する観点から、委託元としての業務を行う者が委託先による業務の遂行を契約等により適切に管理する必要がある。

本書は、情報処理業務を外部委託により行う場合に、委託元としての業務を行う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遵守すべき事項を定め、もって外部委託により行う情報処理業務の遂行において必要な情報セキュリティ水準を確保することを目的とする。

### 2 本書の対象者

本書は、委託元としての業務を行う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を対象としている。

なお、課室情報セキュリティ責任者は、3.2 項で説明する「約款による情報処理サービス」には無償で利用できるサービスもあることを踏まえ、そのようなサービスを利用する者にも、本規程のうち、「約款による情報処理サービス」について周知及び遵守させる必要がある。

### 3 外部委託の形態

#### 3.1 外部委託する業務の分類

本書においては、外部委託により行う業務を以下のとおりに分類している。なお、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は、これ以外の業務形態についても、本書の内容に準じて委託元としての業務を行うこと。

##### 3.1.1 情報システムの構築等の外部委託

情報システムの構築又はソフトウェアの開発(これらをあわせて「情報システムの構築等」という。)を外部委託により行う場合である。

##### 3.1.2 情報システムの運用・保守・点検の外部委託

情報システムの運用、保守又は点検を外部委託により行う場合であり、運用のみの外部委託、保守・点検の外部委託、運用・保守及び点検をあわせて外部委託する形態等がある。具体的には、次のようなものが想定される。

委託先が、[ 省 ]の庁舎内で、そこに設置された情報システムの運用・保

守・点検を行う。いわゆる「オンサイトサービス」の利用である。

委託先の事業所から回線等を経由して〔 省〕の庁舎内に設置した情報システムに接続し、委託先がその運用・保守・点検を行う。いわゆる「リモートサービス」の利用である。委託先が情報システムの運用を行うリモート運用サービス、情報システムやネットワークの稼働監視を行うリモート監視サービス、及びインターネットを通じた不正アクセスを監視するセキュリティ監視サービス等がある。

委託先の事業所内に〔 省〕の情報システムを設置し、委託先がその運用・保守・点検を行う。いわゆる「データセンター」の利用である。情報システムを構成する資産を〔 省〕が所有する場合と、委託先が所有する場合の両方を含む。

委託先が提供する情報サービスを〔 省〕が利用する。いわゆる「アプリケーションサービスプロバイダ（ASP）」のサービスの利用である。レンタルウェブサーバの利用は、この一例である。

委託先の事業所内に〔 省〕の情報システムを設置し、建屋の維持、入退室管理等の物理的管理と通信回線の維持を委託先に行わせ、情報システムのその他の運用・保守・点検の業務は〔 省〕が行う。いわゆる「ハウジングサービス」の利用である。

### 3.1.3 情報の加工・処理等の外部委託

統計処理、集計処理、データエントリー及び媒体変換を含む情報の加工・処理並びに調査・研究（これらをあわせて「情報の加工・処理等」という。）を外部委託により行う場合である。

### 3.1.4 情報の保存・運搬の外部委託

バックアップデータ及び業務情報を含む情報の保存・運搬を外部委託により行う場合である。この場合には、委託先の事業者は、通常は倉庫又は運送に係る事業者である。

## 3.2 「約款による情報処理サービス」の利用による外部委託

約款が用意されており、情報セキュリティに関する事項について利用者による条件選択の余地が限られている情報処理サービス（以下、「約款による情報処理サービス」と言う。）を利用し、外部委託を行う場合である。（利用者に提供される機能など情報セキュリティ以外の契約内容については要求に基づいて用意される又は条件選択や修正ができるものであっても、情報セキュリティに関する事項に条件選択の制限があ



れば、「約款による情報処理サービス」に含む。)例えばクラウドサービス<sup>1</sup>等がこれに該当する。

一般に、外部事業者が提供する「約款による情報処理サービス」を利用する場合には、サービス内容の保証は提供事業者が定める利用規約等の約款の範囲に限られる。したがって、省庁対策基準及び規定で許容されているかどうかを確認のうえ利用を検討することが必要である。具体的には、別紙1の雛形に加え、留意事項とチェックリストをまとめた別紙2の雛形付録を参照するとよい。

「約款による情報処理サービス」の利用に際しては、例えば以下の点に注意する必要がある。

- ・通常の情報処理サービスにより処理された結果生じる著作権等の権利については利用者に帰属することが一般的であるが、「約款による情報処理サービス」では、それらの権利の放棄や移管が利用条件となっている場合がある。
- ・賃貸借・使用貸借部分の所有権はサービス提供者等の事業者側に帰属するため、通常の情報処理サービスの利用終了時におけるデータ削除は、原状回復義務として利用者側の義務となることが想定されるが、「約款による情報処理サービス」では、約款上、データ消去等をサービス利用者側で直接実施できないことがある。
- ・「約款による情報処理サービス」では、利用したデータの削除についてサービス提供者が個別には応じないことや、情報の置き場所が特定の場所に固定されず、海外の法執行機関等による予期せぬアクセスが行われることがある。

なお、サービスの中には無償で利用できるものもあるが、無償で利用する場合でも外部委託に該当するとの認識が必要である。つまり、府省庁外の情報処理サービスを利用する場合には、それが有償で調達手続きを経る場合だけでなく、無償で利用を開始できる場合であっても、本規程を遵守することが求められる。無償で利用する例としては、無償で提供されているメールサービスの利用やアンケート記入及び集計に係るウェブサービスの利用等を挙げることができる。

こうした無償サービスの利用においては、その利用者が調達に従事する行政事務従事者に限られたものではないため、当該留意事項について別紙2の雛形付録に基づき、府省庁内に広く周知する必要がある。

---

<sup>1</sup> クラウドサービスは以下の3つのサービス等の総称である。

1)SaaS：様々なクライアントデバイスから Web ブラウザを通じてネットワーク、サーバ、オペレーティングシステム、ストレージ、アプリケーションの機能（例えば、電子メール等）を利用できるサービス

2)PaaS：利用者が用意するアプリケーションを使用できるようにネットワーク、サーバ、オペレーティングシステム、ストレージ等を提供するサービス

3)IaaS：ネットワークやストレージ等の基本的なコンピュータリソースを提供するサービス

#### 4 外部委託における情報セキュリティ確保に係る手続

情報処理業務を外部委託により行おうとする情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、以下の手続に従うこと。

(1) 外部委託により情報処理業務を行うことの可否の判断

外部委託により行う候補の情報処理業務がある場合に、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。詳細は「5 外部委託により情報処理業務を行うことの可否の判断」を参照されたい。

(2) 調達における手続

調達において示す調達条件、委託先の選定基準、及び、当該業務の実施において委託先に行わせる事項に、情報セキュリティ確保のための事項を含める。詳細は「6 調達における手続」を参照されたい。

(3) 契約における手続

契約において定める委託元及び委託先双方の義務に、情報セキュリティ確保のための事項を含める。詳細は「7 契約における手続」を参照されたい。

(4) 委託先における情報処理業務実施中の手続

外部委託した情報処理業務の実施中に、契約で定めた情報セキュリティ確保のための義務を、委託元及び委託先双方で履行する。詳細は「8 委託先における情報処理業務実施中の手続」を参照されたい。

(5) 納品・検収における手続

外部委託した業務の終了時に、納品に関する検収手続において、契約で定めた情報セキュリティ確保のための義務を委託先が履行したことを確認する。詳細は「9 納品・検収における手続」を参照されたい。

#### 5 外部委託により情報処理業務を行うことの可否の判断

1.2.5.1 (1)(a)

##### 5.1 外部委託の可否の原則

(1) 重要な情報を取り扱う情報処理業務(付録1を参照。)を外部委託により行うことは、情報漏えい等のリスクにかんがみ、これを原則として禁止する。

- 重要な情報とは、これが不適切に取り扱われた場合に、国民の権利利益に重大な損害を与え、あるいは、国民及び国家の安全に重大な懸念が生ずる情報をいう。

(2) 重要な情報を取り扱わない情報処理業務(付録1を参照。)は、外部委託により行うことができる。この場合には、次章以降の規定に従うこと。

(3) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、付録1に掲載されていない情報処理業務を外部委託により行うことを望む場合には、当該情報処理業務及び取り扱う情報について情報セキュリティ責任者に説明し、重

要な情報を取り扱う情報処理業務に該当するか否かの判断を得ること。

- (4) 情報セキュリティ責任者は、(3)項の判断の結果を統括情報セキュリティ責任者に報告し、付録 1 の更新を求めること。統括情報セキュリティ責任者は、必要に応じて付録 1 を更新すること。
- (5) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、重要な情報を取り扱う情報処理業務を外部委託により行うことを特に望む場合には、想定される脅威及び実施可能な対策の有効性に基づくリスク分析を行うこと。その結果リスクが十分に低減できると判断する場合には、情報セキュリティ責任者に判断及びその根拠を報告し、当該情報処理業務を外部委託により行うことにつき許可を求めることができる。情報セキュリティ責任者の許可を得た場合には、指示された対策の実施を条件に、例外として、重要な情報を取り扱う情報処理業務を外部委託により行うことができる。

## 5.2 脅威及び対策の検討における留意事項

情報セキュリティ責任者、情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、前節により情報処理業務が重要な情報を取り扱うものであるか否かを判断又は検討する場合には、以下の事項を考慮すること。

- (1) 当該情報処理業務において、委託先に提供する情報及び委託先によるアクセスを認める情報を洗い出し、重要な情報に該当するか否かを判断すること。
- (2) 委託先による重要な情報の取扱いを不要とするために、外部委託の対象とする情報処理業務の範囲を検討すること。
- (3) 情報システムの構築等を委託先の事業所で行う限りにおいては重要な情報を取り扱わない場合であっても、当該情報システム等の導入作業において、既存の情報システムとの接続作業及び既存の情報システムが稼動している区域での設置作業に伴い、既存の情報システムが保有する重要な情報へのアクセスが可能となる場合があること。
- (4) 情報システムの運用・保守・点検を行う者は、当該業務の遂行に必要なアクセス権を付与されることにより、一般に、当該情報システムで保有するすべての情報にアクセスし得ること。
- (5) 「約款による情報処理サービス」の利用を外部委託として行う場合、サービス内容の利用約款が〔 省 〕の省庁対策基準及び規定を満たしているか確認すること。

「約款による情報処理サービス」を利用する場合、同一サーバ上で他の利用者向けの複数の情報処理を実行しているケースもあり、その場合、セキュリティ対策が十分に実施されていない情報処理の影響を受けること、サーバ資源の利用者ごとの分割が不十分であること、別の利用者に成りすましたことによる情報漏えいが発生すること、サービス提供事業者の従業員が不正を行うこと、それら以外の未知のリスクが発生する可能性があることなどを認識のうえ利用を検討する必要がある。

また、海外の「約款による情報処理サービス」を利用する場合は、想定していないアクセスが許容されてしまう可能性に配慮する必要がある。たとえば、同一サーバを利用している他の利用者が不正をした際に、当該サーバ全体のデータについても海外の捜査機関により差し押さえられて内容を解析されることにより、海

外政府機関が偶然に当該サーバに保存してあった〔 省 〕の情報を把握することなども考えられる。

## 6 調達における手続

### 6.1 委託先の選定基準及び選定手続

1.2.5.1 (1)(b)、1.2.5.1 (3)(a)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先の選定において、委託する情報処理業務の実施に求められる安定性を有すると認められる事業者を選定すること。
- (2) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先に実施を求める情報セキュリティ対策等を調達仕様に含め、委託先候補による提案を評価することにより、適格な事業者を選定すること。求める情報セキュリティ対策等は、表1を目安として情報システムセキュリティ責任者又は課室情報セキュリティ責任者が適切に定めること。

表1．調達仕様において委託先に求める情報セキュリティ対策等

委託する業務の 分類  情報 セキュリティ対策等	情報システムの 構築等	情報システムの運用					情報システムの 保守・点検	情報の加工・ 処理等	情報の保存・ 運搬
		オンサイト サービス	リモート 運用サービス	データ センター	ASP サービス	ハウジング サービス			
(1)情報セキュリティを確保するための体制の整備									
(2)取り扱う府省庁の情報の秘密保持等						物理的 対策			
(3)セキュリティ機能の装備		×	×	×	×	×	×	×	
(4)運用・保守・点検における情報セキュリティ対策の実施	×					×		×	
(5)脆弱性対策の実施						×		×	
(6)情報セキュリティ対策のサービスレベルに関する事項	×							×	
(7)情報セキュリティが侵害された場合の対処									
(8)情報セキュリティ監査の実施									
(9)情報セキュリティ対策の履行が不十分であると思われる場合の対処									
(10)再委託に関する事項 (7.5項)									
(11)国際規格を踏まえた委託先の情報セキュリティ水準の評価(6.2節)									

：必要                   ：選択（当該対策等の実施を委託先に求めるか否かについて調達ごとに選



	能性がある。
17	準拠法に外国法を指定される場合がある。
18	管轄裁判所に海外の裁判所を指定される場合がある。

## 6.2 国際規格を踏まえた委託先の情報セキュリティ水準の評価

### 1.2.5.1(1)(c)【強化遵守事項】、1.2.5.1(3)(b)【強化遵守事項】

委託先の選定における前節の手續に加えて、選定の厳格性を向上させる場合に、委託先の候補者における情報セキュリティ水準を以下に示す国際規格等を踏まえて評価すること。目的に適した制度を利用する必要がある。

- 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制度

#### 6.2.1 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の活用

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、情報処理業務を外部委託により行う場合であって、委託先候補における情報セキュリティマネジメントに関して客観性の高い評価基準に基づく評価を行う必要があると判断したときは、第三者機関（審査登録機関）による適合性評価に基づく認証の取得有無を、委託先候補の評価の要素として活用すること。

我が国においては、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として、財団法人日本情報処理開発協会（JIPDEC）が「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」を運営している。

本制度の利用方法については、「付録 3 組織における情報セキュリティ水準の評価に関する制度」及び次の資料を参照されたい。

「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」

（内閣官房情報セキュリティセンター、2007年11月）の

資料1「外部委託におけるISMS適合性評価制度の利用方法」（JIPDEC）

- (2) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、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に基づく認証の取得有無を委託先候補の評価の要素として活用する場合には、委託先候補の事業者に対して登録証及び適用範囲定義書の提示を求め、登録範囲及び適用範囲が委託する情報処理業務に合致することを確認すること。

#### 6.2.2 情報セキュリティ対策ベンチマークの活用

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、情報処理業務を外部委託により行う場合であって、委託先候補における情報セキュリティマネジメントの評価を委託先の自己評価により行う必要があると認めるときは、情報セキュリティ対策ベンチマークを委託先候補の評価の要素として活用すること。

本制度の利用方法については、「付録 3 組織における情報セキュリティ水準の評価に関する制度」及び次の資料を参照されたい。

「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」  
(内閣官房情報セキュリティセンター、2007年11月)の  
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)

- (2) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、情報セキュリティ対策ベンチマークを委託先候補の評価の要素として活用する場合には、委託先候補の事業者は、情報セキュリティ対策ベンチマークの結果を提出させ、その内容について以下の点に留意して評価すること。

- ベンチマークの結果は、事業者自身が行ったものであり第三者による確認・認証の結果ではないため、不明確な事項があれば、事業者に質問する等により結果の客観性を高めること。

### 6.2.3 情報セキュリティ監査の活用

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、情報処理業務を外部委託により行う場合であって、委託先候補における情報セキュリティ水準について客観性の高い評価を行う必要があると認めるときは、委託先候補の事業者が過去に実施した情報セキュリティ監査の結果を委託先候補の評価の要素として活用すること。

情報セキュリティ監査については、「情報セキュリティ監査基準」及び「情報セキュリティ管理基準」を含む事項を定めた「情報セキュリティ監査制度」がある。当制度の利用方法については、「付録 3 組織における情報セキュリティ水準の評価に関する制度」及び次の資料を参照されたい。

「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」  
(内閣官房情報セキュリティセンター、2007年11月)の  
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)

- (2) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、情報セキュリティ監査の結果を委託先候補の評価の要素として活用する場合には、委託先候補の事業者は監査報告書を提出させ、監査の対象が委託する情報処理業務に合致することを確認した上で、評価すること。

## 6.3 委託先に求める事項の周知

### 6.3.1 委託先に実施させる情報セキュリティ対策の内容の周知

#### 1.2.5.1 (2)(a)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託に係る業務の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を、調達仕様として委託先候補に周知すること。委託先に実施させる情報セキュリティ対策の範囲は、「6.1 委託先の選定基準及び選定手続」の「表1 調達仕様において委託先に求める情報セキュリティ対策等」の(1)～(7)に示す事項を原則として、外部委託する業務に即して情報システムセキュリティ責任者又は課室情報セキュ



リティ責任者が定めること。

調達仕様の記述例は、「第 部 調達仕様における情報セキュリティ関連事項の記述例」を参照されたい。

### 6.3.2 情報セキュリティが侵害された場合の対処方法の周知

1.2.5.1 (2)(b)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先に請け負わせる業務において情報セキュリティが侵害された場合の対処方法（表 1 (7)）を、調達仕様に記載することにより委託先候補に周知すること。

調達仕様の記述例は、「第 部 調達仕様における情報セキュリティ関連事項の記述例」を参照されたい。

### 6.3.3 情報セキュリティ対策の履行状況の確認等に関する事項の周知

1.2.5.1 (2)(c)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、調達仕様、契約及び確認書等において実施を求める情報セキュリティ対策が委託先において履行されていることを確認するための方法を策定すること。例えば、情報セキュリティ対策項目を定めてその履行状況を委託先から適宜又は定期的に報告させ、対策が履行されていることを確認すること。
- (2) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、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にあたり、必要に応じて、情報セキュリティ監査を行うこと（表 1 (8)）。具体的には、当該業務及び取り扱わせる情報の重要度、当該業務の実施場所、実施期間、委託金額等を考慮し、必要性の判断を行うこと。<sup>2</sup> 以下に例示する場合等には情報セキュリティ監査を適用することが特に望ましい。
  - 国民の安全及び権利保護の観点から情報の機密性・完全性の維持が強く求められる情報処理業務
  - 障害等により国民生活及び産業活動への多大な影響が想定される可用性の要求の高い行政サービスを提供する情報処理業務
  - 政府の信用維持のために可用性及び機密性の確保が求められる情報処理業務
- (3) 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を情報セキュリティ監査により行う場合には、その内容及び方法等を、調達仕様に記載することにより委託先候補に周知すること。
- (4) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先に

---

<sup>2</sup> 情報処理業務を委託先において行う場合には、府省庁内において行う場合と比べ、情報の機密性、完全性、可用性が損なわれるリスクが増大すること、及び当該業務が長期に渡るほど情報セキュリティ上の問題が発生しやすいことに留意し、リスクを評価すること。ただし、実施期間が短い、委託金額が少ない場合等、必ずしも委託先に対する情報セキュリティ監査の活用が合理的でないことがあり得ることに留意し、監査の必要性及び実施可能性を判断すること。

において情報セキュリティ対策の履行が不十分である場合の対処方法(表1(9))を、調達仕様として委託先候補に周知すること。

調達仕様の記述例は、「第 部 調達仕様における情報セキュリティ関連事項の記述例」を参照されたい。

## 7 契約における手続

### 7.1 外部委託に係る契約における情報セキュリティの考慮

1.2.5.1 (4)(a)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先に行わせる情報セキュリティ対策等を契約又はその付属書に含めて明示すること。委託先に行わせる情報セキュリティ対策等の範囲は、表3を原則として、外部委託する業務に即して情報システムセキュリティ責任者又は課室情報セキュリティ責任者が定めること。

表3 契約において委託先に行わせるものとする情報セキュリティ対策等

委託する業務の 分類  情報 セキュリティ対策等	情報システムの構築等	情報システムの運用					情報システムの 保守・点検	情報の加工・処理等	情報の保存・運搬
		オンサイト サービス	リモート 運用サービス	データ センター	ASP サービス	ハウジング サービス			
(1) 情報セキュリティを確保するための体制の整備									
(2) 取り扱う府省庁の情報の秘密保持等						物理的 対策			
(3) セキュリティ機能の装備		×	×	×	×	×	×	×	
(4) 運用・保守・点検における情報セキュリティ対策の実施	×					×	×	×	
(5) 脆弱性対策の実施						×	×	×	
(6) 外部委託する業務以外の情報資産の保全			×	×	×	×	×	×	
(7) 情報セキュリティ対策のサービスレベルに関する事項	×						×	×	
(8) 情報セキュリティが侵害された場合の対処									
(9) 情報セキュリティ対策の履行状況の確認									
(10) 情報セキュリティ監査の実施									
(11) 情報セキュリティ対策の履行が不十分であると思われる場合の対処									
(12) 確認書等に委任する事項								×	
(13) 再委託に関する事項									

：必要           ：選択       ×：非該当又は不必要

：一般にサービスに含まれている本表は一般的な目安を示すものであり、契約に含める事項は案件ごとに判断すること。

契約の記述例は、「第 部 契約における情報セキュリティ関連事項の記述例」を参照されたい。

「情報セキュリティ対策等」の各項目については「付録2 情報セキュリティ対策等」を参照されたい。

## 7.2 外部委託に係る確認書等における情報セキュリティの考慮

### 1.2.5.1 (4)(b)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先に情報処理業務を行わせるに当たり、契約において定めた委託先に行わせる情報セキュリティ対策等に関して、双方の責任の明確化と合意の形成を行い、合意した事項を確認書等として委託先の責任者から提出させ、あるいは、契約の付属書とすること（以降、付属書に記載する事項も含めて契約という。）
- (2) 確認書等又は契約の付属書には、情報セキュリティ対策等を実施する管理体制を含めること。例えば、情報セキュリティ対策等の実施における双方の責任者及び技術担当窓口の者を記載することが考えられる。
- (3) 確認書等又は契約の付属書には、必要に応じて次の事項を含めさせること。
  - 当該情報処理業務に携わる者の特定
  - 契約で求める情報セキュリティ対策の実施に係る具体的な取組内容
- (4) 確認書等は、その内容を契約に含める場合には、省略することができる。

## 7.3 外部委託の継続における注意

### 1.2.5.1 (4)(c)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託契約を継続する場合には、「6.1 委託先の選定基準及び選定手続」に基づきその都度審査するものとし、安易な随意契約の継続をしないこと。外部委託契約の継続には、特に、次の場合を含む。
  - 情報システムの構築において、設計を外部委託により行い、その終了後に当該設計に基づく実装を外部委託により行う場合
  - 情報システムの構築を外部委託により行い、その終了後に当該情報システムの運用、保守又は点検を外部委託により行う場合
  - 情報システムの運用、保守又は点検を外部委託により行い、その後の当該情報システムの運用、保守又は点検も新たな契約の下で外部委託により行う場合

## 7.4 外部委託における実施内容の変更に関する注意

### 1.2.5.1 (4)(d)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約及び確認書等において委託先が行うものと定めた事項の変更を委託先が希望する場合には、情報セキュリティを維持する観点から、契約及び確認書等、並びに委託先の選定において適用した選定基準及び選定手続に基づき、その可否を審査すること。

## 7.5 再委託に関する制限

### 1.2.5.1 (4)(e)

- (1) 再委託による情報処理業務の遂行は、委託先に行わせる場合に比べ、脅威が増大

し、対策は困難になる傾向がある。このため、再委託する必要がない場合には禁止し、再委託する必要がある、かつ再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保される場合には、そのために必要な措置を委託先に担保させること。

- (2) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先が業務の全部又は一部を第三者に再委託により行わせることを認めない場合には、その旨を調達仕様を含めること。
- (3) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先が外部委託を受けた業務の一部を再委託により行うことを望む場合には、再委託の可否及び条件を決定すること。判断基準の例を以下に示す。
  - 再委託することに合理的な理由があると認められる場合にのみ、これを認めることができる。事業者の専門性にかんがみ、当該業務が再委託により技術的に可能となること及び適正な費用で実施可能となることは、合理的な理由として認められ得る。
  - 委託先自体が当該一部の業務を実施する場合に求めるべき水準と同等の情報セキュリティ水準を再委託においても確保させるための情報セキュリティ対策を委託先が再委託先に契約に基づき行わせることを求め、以下の措置を採ること。
    - 当該求めを委託元と委託先の契約において定めること。
    - 再委託先において採る情報セキュリティ対策について委託先から報告させ、これが十分なものであることを確認すること。
    - 委託先が再委託先に情報セキュリティ対策を行わせた結果を委託元が確認する方法を定め、確認すること。

#### 7.6 「約款による情報処理サービス」の利用による外部委託に関する注意

- (1) 外部事業者が提供する「約款による情報処理サービス」を利用する場合には、サービス内容の保証は提供事業者が定める利用規約等の約款の範囲に限られるため、以下の脅威を踏まえて採用の判断を行うこと。

表4 .「約款による情報処理サービス」の利用による外部委託に関する留意事項

	留意事項
1	サービスは約款の範囲でしか提供されない。
2	サービス時間とサポート時間が限られている場合がある。
3	サービスのセキュリティポリシーが開示されないことが多く、省庁対策基準及び規定を満たしているか判断が困難である。
4	サービス提供事業者から提供されるサービスレベルは可用性のみであることが多い。
5	サービス提供事業者は利用者による監査を基本的に受け入れない。
6	バックアップ実施や障害発生時の復旧等の実施内容やタイミングといった、情報システムの運用に関しては約款に記載されていないことが多い。
7	バックアップするデータ形式が他の事業者のサービスに移行できない場合がある。
8	利用者側で情報のバックアップができない場合がある。
9	同一サーバ上で複数の業務(利用者)を実行しているケースがあり、その場合セキュリティ対策が十分に実行されていない業務の影響を受ける可能性がある。

	る。
10	同一サーバ上で複数の利用者が情報処理を実行しているため、別の利用者情報を盗み見し、別の利用者に成りすまして処理を行う可能性がある。
11	サーバ資源の利用者ごとの分割が不適切なことによる情報漏えいが発生する可能性がある。
12	情報の置き場所が特定の場所に固定されず、海外の法執行機関等による予期せぬアクセスが行われうる可能性がある。
13	サービスを有期契約した場合、契約終了後の情報の取り扱い（確実な消去）が不明瞭な場合がある。
14	サービス提供事業者の経営が破たんしたり突然のサービス停止に陥った場合、預けた情報の行方は保証されず、損害賠償も支払われない場合がある。
15	サービス提供事業者の従業員が不正を行う可能性がある。
16	約款の内容はサービス提供者側の都合で利用開始後に一方的に変更される可能性がある。
17	準拠法に外国法を指定される場合がある。
18	管轄裁判所に海外の裁判所を指定される場合がある。

## 8 委託先における情報処理業務実施中の手続

### 8.1 取り扱う府省庁の情報の秘密保持等

1.2.5.1 (5)(a)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託により情報処理業務を行う場合に、委託先に提供する情報を必要最小限の範囲に限定すること。
- (2) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先に情報を提供する場合には、その都度、提供の記録を採ること。
- (3) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先に情報を提供する場合には、安全な受渡方法によりこれを実施すること。
- (4) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、提供した情報が外部委託した業務の終了等により委託先において不要となった場合に、これを返却又は廃棄若しくは抹消させること。委託先に情報を廃棄又は抹消させた場合には、その旨を委託先から書面で報告させること。
- (5) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、提供した情報の返却を受け、若しくは廃棄し又は抹消したことの報告を受けた場合には、その都度、その記録を取ること。
- (6) 委託先における府省庁の情報の取扱規則を策定し、これを遵守させること。本規則には、取り扱う府省庁の情報等に応じて以下に例示する事項等を選択して含めること。
  - 取り扱う情報は外部委託した情報処理業務にのみ使用し、他の目的には使用しないこと。
  - 取り扱う情報は外部委託した情報処理業務を行う者以外には秘密とすること。
  - 取り扱う情報は指定した場所から持ち出さないこと。
  - 取り扱う情報は委託元の許可なく複製しないこと。

### 8.2 情報セキュリティ侵害が発生した場合の措置

1.2.5.1 (5)(b)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先において情報セキュリティが侵害された場合には、「7.1 外部委託に係る契約における情報セキュリティの考慮」に従い契約又は確認書等に含めた情報セキュリティが侵害された場合の対処を行うこと。

### 8.3 情報セキュリティ対策の履行状況の確認

1.2.5.1 (5)(c)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、「7.1 外部委託に係る契約における情報セキュリティの考慮」に従い契約又は確認書等を含めた委託先に実施させる情報セキュリティ対策の履行状況を確認すること。
- (2) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先に実施させる情報セキュリティ対策の履行状況の確認を情報セキュリティ監査により行う旨契約において定めた場合には、定められた内容及び方法に従いこれを実施すること。

## 9 納品・検収における手続

1.2.5.1 (6)(a)

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託の終了時に、委託先が行った情報セキュリティ対策を契約及び確認書等の内容に照らして確認し、その結果を納品検査における合否の判断に加えること。確認する情報セキュリティ対策は、重要性を判断して選択してよい。

## 10 国際規格を踏まえたセキュリティ機能の設計及び実装の評価

### 10.1 情報システムの構築に伴い調達する機器等のセキュリティ機能の評価

1.5.1.1(1)(d)

- (1) 情報システムセキュリティ責任者は、構築する情報システムの構成要素のうち製品として調達する機器及びソフトウェアについて、ITセキュリティ評価及び認証制度に基づく認証取得製品を調達する必要性の有無を検討し、必要があると認められた場合には、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能を定めること。
- (2) 情報システムセキュリティ責任者は、情報システムの構築に係る委託先からの調達に限ることなく当該情報システムの構成要素とする機器及びソフトウェアを調達する場合であって、(1)に従い定めたセキュリティ機能及びその他の要求条件を満たす採用候補製品が複数あり、その中に要求する評価保証レベルに合致するITセキュリティ評価及び認証制度に基づく認証を取得している製品がある場合において、当該製品を情報システムの構成要素として選択すること。
- (3) 情報システムセキュリティ責任者は、情報システムの構築に係る委託先から当該情報システムの構成要素とする機器又はソフトウェアを調達する場合には、委託先の評価・選定基準に、当該機器又はソフトウェアが(1)に定めたセキュリティ機能についてITセキュリティ評価及び認証制度に基づく認証を取得しているか否かを加味すること。

ITセキュリティ評価及び認証制度に基づく認証の取得を製品の選択に利用する場合には、以下の資料もあわせて参照されたい。

- ・「情報システムの構築等におけるセキュリティ要件及びセキュリティ機



能の検討に関する解説書」

内閣官房情報セキュリティセンター、2011年4月

- 「ITセキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」  
経済産業省、2011年4月

## 10.2 情報システムの構築等におけるセキュリティ機能の設計及び実装の評価

### 1.5.1.1(1)(g) 【強化遵守事項】 , 1.5.2.3(1)(a)(ケ)

- (1) 情報システムセキュリティ責任者は、情報システムの構築等を外部委託により行う場合であって、当該構築又は開発について重要なセキュリティ要件があると認めるときには、委託先に、セキュリティ機能の設計についてセキュリティ設計仕様書（ST: Security Target）の評価（以下「ST評価」という。）及び同確認（以下「ST確認」という。）を受けさせること。ただし、情報システム等を更改し、又は構築・開発中に仕様変更が発生した場合であって、重要なセキュリティ要件の変更が軽微であると認めるときは、この限りではない。
- (2) 情報システムセキュリティ責任者は、委託先から、セキュリティ機能の設計に係る ST 評価・ST 確認を受けたことを示す確認書を納品までに提示させること。
- (3) 情報システムセキュリティ責任者は、ST 評価・ST 確認は第三者機関が行うものであること等にかんがみ、委託先の責任によらず確認書が納品までに提出されないおそれがあると考えられる場合には、納品後に当該文書が提出される場合の取扱いを委託先と協議して決定すること。例えば、まず構築した情報システム等の成果物について納品・検収を行い、別途 ST 評価・ST 確認の結果について納品・検収を行う方法がある。

委託先に ST 評価・ST 確認を行わせる場合には、以下の資料もあわせて参照されたい。

- 「情報システムの構築等におけるST評価・ST確認の実施に関する解説書」  
内閣官房情報セキュリティセンター、2007年11月

## 11 本書に関する相談窓口

- (1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、緊急時の対応又は本書の内容を超えた対応が必要な場合には、統括情報セキュリティ責任者に相談し、指示を受けること。
- (2) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、本書の内容について不明な点又は質問がある場合には、統括情報セキュリティ責任者に連絡し、回答を得ること。

## 第 部 調達仕様における情報セキュリティ関連事項の記述例

第 部では、情報処理業務を外部委託により行う場合に、情報セキュリティの観点から調達仕様を含める事項の例を示す。

### 1 外部委託する業務の分類に基づく事項

#### 1.1 情報システムの構築等の場合

##### (1) 情報セキュリティを確保するための体制の整備

- 本調達に係る業務を行う事業者は、当該業務の実施において情報セキュリティを確保するための体制を整備すること。

##### (2) 取り扱う府省庁の情報の秘密保持等

- 本調達に係る業務の実施のために〔 省〕から提供する情報その他当該業務の実施において知り得た情報については、その秘密を保持し、また当該業務の目的以外に利用しないこと。

##### (3) セキュリティ機能の装備

#### 【セキュリティ要求仕様を提示し、応札においてセキュリティ機能の提案を求める場合】

本調達に係る〔情報システム/ソフトウェア〕において取り扱う情報の保護を目的として、〔付属文書(セキュリティ要求仕様)〕に基づき、応札においてセキュリティ機能を提案すること。

#### 【セキュリティ要求仕様を提示し、セキュリティ機能の装備を求める場合】

- 本調達に係る〔情報システム/ソフトウェア〕において取り扱う情報の保護を目的として、〔付属文書(セキュリティ要求仕様)〕に基づきセキュリティ機能を設計し、実装すること。

#### 【セキュリティ機能の概要を提示し、その装備を求める場合】

- 本調達に係る情報システムにおいて以下のセキュリティ機能を具体化し、実装すること。

##### 【情報システムの構築の場合】

本調達に係る情報システムへのアクセスを業務上必要な者に限るための機能

本調達に係る情報システムに対する不正アクセス、ウイルス・不正プログラム感染等、インターネットを経由する攻撃、不正等への対策機能

本調達に係る情報システムにおけるセキュリティ事故及び不正の原因を事後に追跡するための機能

##### 【ソフトウェアの開発の場合】

本調達に係るソフトウェアへのアクセスを業務上必要な者に限るための機能

本調達に係るソフトウェアの不正な利用を防止するために、不正な

入力及び出力を防止する機能

本調達に係るソフトウェアに関連するセキュリティ事故及び不正の原因を事後に追跡するための機能

**【情報システムの構築で、構成ソフトウェアに関して IT セキュリティ**

**評価及び認証制度に基づく認証取得を考慮する場合】**

- 本調達に係る情報システムを構成する 機能を有するソフトウェアについて、取り扱う情報の保護を目的とするセキュリティ機能について、IT セキュリティ評価及び認証制度に基づく認証を取得しているか否かを情報システムに係る提案の評価の要素とする。当該認証を取得している場合は、提案において報告すること。

(評価式は調達ごとに定めることとなるため、本雛形では省略している。)

**【ST 評価・ST 確認を求める場合】**

- 本調達に係る [ 情報システム / ソフトウェア ] において取り扱う情報の保護を目的として、ISO/IEC 15408に基づき必要なセキュリティ機能を設計し、実装すること。当該設計において策定するセキュリティ設計仕様書 ( ST: Security Target ) についてST評価・ST確認を受け、その結果を [ 納品までに / 年 月 日までに ] 提出すること。

(4) 脆弱性対策の実施

**【情報システムの構築の場合】**

- 本調達に係る情報システムの構築における以下の脆弱性対策を提案すること。

構築する情報システムを構成する機器及びソフトウェアの中で、脆弱性対策を実施するものを適切に決定すること。

脆弱性対策を行うとした機器及びソフトウェアについて、公表されている脆弱性情報及び公表される脆弱性情報を把握すること。

把握した脆弱性情報について、対処の要否、可否を判断すること。  
対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を納品時に委託元に報告すること。

**【情報セキュリティが侵害された場合の対処を明示する場合】**

(5) 情報セキュリティが侵害された場合の対処

- 本調達に係る業務の遂行において情報セキュリティが侵害され又はそのおそれがある場合には、速やかに委託元に報告すること。これに該当する場合には、以下の事象を含む。

委託先に提供し、又は委託先によるアクセスを認める [ 省 ] の情報の外部への漏えい及び目的外利用

- 委託先の者による [ 省 ] のその他の情報へのアクセス

(6) 情報セキュリティ対策の履行状況の確認等に関する事項の通知

- 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、委託先に対して以下の報告を求める場合がある。

**【委託先に求める情報セキュリティ対策全般につき報告を求める場合】**

本調達仕様の [ (1) ~ (5) の各項目 ] において求める情報セキュリティ対策の実績

**【委託先に取り扱わせる情報の秘密保持等に係る報告を求める場合】**

- 委託先に取り扱わせる府省庁の情報の秘密保持等に係る管理状況

#### 【情報セキュリティ監査を行う場合】

##### (7) 情報セキュリティ監査の実施

- 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、情報セキュリティ監査の実施内容（監査内容、対象範囲、実施者等）を定めて、それについて予め合意を得たうえで情報セキュリティ監査を行う。委託先は、応札において、情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「監査対応計画書」により提示すること。

#### 【情報セキュリティ対策の履行が不十分な場合の対処を明示する場合】

##### (8) 情報セキュリティ対策の履行が不十分な場合の対処

- 本調達に係る業務の遂行において、委託先における情報セキュリティ対策の履行が不十分である可能性を委託元が認める場合には、委託先の責任者は、委託元の求めに応じこれと協議を行い、合意した対応を採ることとする。

##### (9) 再委託に関する事項

#### 【再委託を禁止する場合】

- 本調達に係る業務は、その全部又は一部を他の事業者にも再委託させてはならない。

#### 【再委託を認める場合】

- 本調達に係る業務の一部を他の事業者にも再委託させる場合には、委託先は、委託元が委託先に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再委託先に行わせること。再委託先に行かせた情報セキュリティ対策及びこれを行かせた結果に関する報告を、委託先に求める場合がある。

#### 【国際規格を踏まえた委託先の情報セキュリティ水準の評価を行う場合】

##### (10) 国際規格を踏まえた委託先の情報セキュリティ水準の評価

#### 【ISMS 認証取得を考慮する場合】

- 本調達に係る業務を行おうとする事業者又はその部門において、情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はこれと同等の認証を取得しているか否かを、提案に関する評価の要素とする。（評価式は調達ごとに定めることとなるため、本雛形では省略している。）

#### 【情報セキュリティ対策ベンチマークの結果を考慮する場合】

- 本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティ対策ベンチマークを実施し、その結果を書式1（本雛形では省略している。）により提示すること。情報セキュリティ対策ベンチマークに基づく平均成熟度が「n」以上であるか否かを、提案に関する評価の要素とする。（情報セキュリティ対策ベンチマークに関する説明を、付録3から引用する。）

#### 【ISMS 認証取得及び情報セキュリティ対策ベンチマークの結果を考慮する場合】

- 本調達に係る業務を行おうとする事業者又はその部門において情報セキ

セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はこれと同等の認証を取得しているか否かを、提案に関する評価の要素とする。（評価式は調達ごとに定めることとなるため、本雛形では省略している。）

- ただし、ISMS認証及びこれと同等の認証を取得していない事業者又はその部門においては、情報セキュリティ対策ベンチマークを実施し、その結果を書式1（本雛形では省略している。）により提出すること。情報セキュリティ対策ベンチマークに基づく平均成熟度が4以上であるか否かを、提案に関する評価の要素とする。

（情報セキュリティ対策ベンチマークに関する説明を、付録3から引用する。）

## 1.2 情報システムの運用・保守・点検の場合

### (1) 情報セキュリティを確保するための体制の整備

- 本調達に係る業務を行う事業者は、当該業務の実施において情報セキュリティを確保するための体制を整備すること。

### (2) 取り扱う府省庁の情報の秘密保持等

- 本調達に係る業務の実施のために〔 省 〕から提供する情報その他当該業務の実施において知り得た情報については、その秘密を保持し、また当該業務の目的以外に利用しないこと。

## 【運用・保守・点検における情報セキュリティ対策の実施を求める場合】

### (3) 運用・保守・点検における情報セキュリティ対策の実施

- 稼働状況の監視、バックアップの取得等、委託先に実施を求める情報セキュリティ対策を具体的に記述する。これらは、委託先に実施を求める運用・保守・点検の業務に含めて記述することも考えられる。

## 【脆弱性対策を外部委託する場合】

### (4) 脆弱性対策の実施

- 本調達に係る情報システムの運用における以下の脆弱性対策を提案すること。

別紙（略）に掲げる機器及びソフトウェアについて、公表される脆弱性情報を常時把握すること。

#### 【対処の要否、可否の判断を委託先にさせる場合】

把握した脆弱性情報について、対処の要否、可否を判断すること。対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を委託元に報告すること。

#### 【対処の要否、可否の判断に委託元も加わる場合】

把握した脆弱性情報について、対処の要否、可否につき委託元と協議し、決定すること。決定した対処又は代替措置を実施すること。

## 【情報セキュリティ対策のサービスレベルに関する事項を求める場合】

#### (5) 情報セキュリティ対策のサービスレベルに関する事項

- (求めるサービスレベルの例に、使用するソフトウェアに関してセキュリティ修正がベンダーから提供された後にこれを適用するまでの期間、インターネット接続に関して外部からの攻撃等の異常を検知してから委託元に報告するまでの時間等がある。情報セキュリティ対策のサービスレベルは、情報システムの運用・保守・点検におけるサービスレベルの一部として記述することも考えられる。)

#### 【情報セキュリティが侵害された場合の扱いを明示する場合】

##### (6) 情報セキュリティが侵害された場合の対処

- 本調達に係る業務の遂行において情報セキュリティが侵害され又はそのおそれがある場合には、速やかに委託元に報告すること。これに該当する場合には、以下の事象を含む。

委託先に提供し、又は委託先によるアクセスを認める [ 省 ] の情報の外部への漏えい及び目的外利用  
委託先の者による [ 省 ] のその他の情報へのアクセス

##### 【情報システムの運用を外部委託する場合】

外部の者による不正アクセス、不正プログラム感染等の情報セキュリティ侵害

##### (7) 情報セキュリティ対策の履行状況の確認等に関する事項の通知

- 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、委託先に対して以下の報告を求める場合がある。

##### 【委託先に求める情報セキュリティ対策全般につき報告を求める場合】

本調達仕様の [ (1) ~ (6) の各項 ] において求める情報セキュリティ対策の実績

##### 【委託先に取り扱わせる情報の秘密保持等に係る報告を求める場合】

委託先に取り扱わせる府省庁の情報の秘密保持等に係る管理状況

#### 【情報セキュリティ監査を行う場合】

##### (8) 情報セキュリティ監査の実施

- 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、情報セキュリティ監査の実施内容（監査内容、対象範囲、実施者等）を定めて、それについて予め合意を得たうえで情報セキュリティ監査を行う。委託先は、応札において、情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「監査対応計画書」等により提示すること。

#### 【情報セキュリティ対策の履行が不十分な場合の対処を明示する場合】

##### (9) 情報セキュリティ対策の履行が不十分な場合の対処

- 本調達に係る業務の遂行において、委託先における情報セキュリティ対策の履行が不十分である可能性を委託元が認める場合には、委託先の責任者は、委託元の求めに応じこれと協議を行い、合意した対応を採ること。

(10)再委託に関する事項

**【再委託を禁止する場合】**

- 本調達に係る業務は、その全部又は一部を他の事業者に再委託させてはならない。

**【再委託を認める場合】**

- 本調達に係る業務の一部を他の事業者に再委託させる場合には、委託先は、委託元が委託先に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再委託先に行わせること。再委託先に行かせた情報セキュリティ対策及びこれを行かせた結果に関する報告を、委託先に求める場合がある。

**【国際規格を踏まえた委託先の情報セキュリティ水準の評価を行う場合】**

(11)国際規格を踏まえた委託先の情報セキュリティ水準の評価

**【ISMS 認証取得を考慮する場合】**

- 本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はこれと同等の認証を取得しているか否かを、提案に関する評価の要素とする。（評価式は調達ごとに定めることとなるため、本雛形では省略している。）

**【情報セキュリティ対策ベンチマークの結果を考慮する場合】**

- 本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティ対策ベンチマークを実施し、その結果を書式1（本雛形では省略している。）により提出すること。情報セキュリティ対策ベンチマークに基づく平均成熟度が $n$ 以上であるか否かを、提案に関する評価の要素とする。（情報セキュリティ対策ベンチマークに関する説明を、付録3から引用する。）

**【ISMS 認証取得及び情報セキュリティ対策ベンチマークの結果を考慮する場合】**

- 本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はこれと同等の認証を取得しているか否かを、提案に関する評価の要素とする。（評価式は調達ごとに定めることとなるため、本雛形では省略している。）
- ただし、ISMS認証及びこれと同等の認証を取得していない事業者又はその部門においては、情報セキュリティ対策ベンチマークを実施し、その結果を書式1（本雛形では省略している。）により提出すること。情報セキュリティ対策ベンチマークに基づく平均成熟度が4以上であるか否かを、提案に関する評価の要素とする。（情報セキュリティ対策ベンチマークに関する説明を、付録3から引用する。）

1.3 情報の加工・処理等の場合

(1) 情報セキュリティを確保するための体制の整備

- 本調達に係る業務を行う事業者は、当該業務の実施において情報セキュリティを確保するための体制を整備すること。

(2) 取り扱う府省庁の情報の秘密保持等

- 本調達に係る業務の実施のために〔 省 〕から提供する情報その他当該業務の実施において知り得た情報については、その秘密を保持し、また当該業務の目的以外に利用しないこと。

**【情報セキュリティが侵害された場合の対処を明示する場合】**

(3) 情報セキュリティが侵害された場合の対処

- 本調達に係る業務の遂行において委託先に提供し、又は委託先によるアクセスを認める情報について外部への漏えい、目的外利用等、情報セキュリティ侵害が起き又はそのおそれがある場合には、速やかにこれを委託元に報告すること。

(4) 情報セキュリティ対策の履行状況の確認等に関する事項の通知

- 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、委託先に対して以下の報告を求める場合がある。

**【委託先に求める情報セキュリティ対策全般につき報告を求める場合】**

本調達仕様の〔(1)～(3)の各項〕において求める情報セキュリティ対策の実績

**【委託先に取り扱わせる情報の秘密保持等に係る報告を求める場合】**

委託先に取り扱わせる府省庁の情報の秘密保持等に係る管理状況

**【情報セキュリティ監査を行う場合】**

(5) 情報セキュリティ監査の実施

本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、情報セキュリティ監査の実施内容（監査内容、対象範囲、実施者等）を定めて、それについて予め合意を得たうえで情報セキュリティ監査を行う。委託先は、応札において、情報セキュリティ監査を受け入れる部門、場所、時期等を「監査対応計画書」等により提示すること。

**【情報セキュリティ対策の履行が不十分な場合の対処を明示する場合】**

(6) 情報セキュリティ対策の履行が不十分な場合の対処

- 本調達に係る業務の遂行において、委託先における情報セキュリティ対策の履行が不十分である可能性を委託元が認める場合には、委託先の責任者は、委託元の求めに応じこれと協議を行い、合意した対応を採ること。

(7) 再委託に関する事項

**【再委託を禁止する場合】**

- 本調達に係る業務は、その全部又は一部を他の事業者にも再委託させてはならない。

**【再委託を認める場合】**

- 本調達に係る業務の一部を他の事業者にも再委託させる場合には、委託先は、委託元が委託先に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再委託先に行わせること。再委託先に行かせた情



報セキュリティ対策及びこれを行わせた結果に関する報告を、委託先に求める場合がある。

**【ISMS 認証取得等を委託先の選定において考慮する場合】**

(8) 国際規格を踏まえた委託先の情報セキュリティ水準の評価

- **【ISMS認証取得を考慮する場合】**  
「1 情報システムの構築等の場合」と同じ。
- **【情報セキュリティ対策ベンチマークの結果を求める場合】**  
「1 情報システムの構築等の場合」と同じ。
- **【ISMS認証取得及び情報セキュリティ対策ベンチマークの結果を考慮する場合】**  
「1 情報システムの構築等の場合」と同じ。

1.4 情報の保存・運搬の場合

(1) 取り扱う府省庁の情報の秘密保持等

- 本調達において [保存/運搬] を委託する [ 省 ] の情報について、その漏洩及び毀損を防止するための十分な安全管理を行うこと。

**【情報の保存に関して委託先の情報セキュリティ監査を行う場合】**

(2) 情報セキュリティ監査の実施

- 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、添付「情報セキュリティ監査仕様書」に示す仕様に基づき情報セキュリティ監査を行う。委託先は、応札において、情報セキュリティ監査を受け入れる部門、場所、時期等を「監査対応計画書」等により提示すること。(情報セキュリティ監査仕様書において、監査内容、対象範囲、実施者等を提示する。)

**【情報の保存に関して ISMS 認証取得等を委託先の選定において考慮する場合】**

(3) 国際規格を踏まえた委託先の情報セキュリティ水準の評価

- **【ISMS認証取得を考慮する場合】**  
「1 情報システムの構築等の場合」と同じ。
- **【情報セキュリティ対策ベンチマークの結果を考慮する場合】**  
「1 情報システムの構築等の場合」と同じ。
- **【ISMS認証取得及び情報セキュリティ対策ベンチマークの結果を考慮する場合】**  
「1 情報システムの構築等の場合」と同じ。

(情報の保存・運搬を外部委託により行う場合には、物品を安全に保存・運搬すること自体が委託先の提供するサービスの内容であることに留意して調達仕様に記載する事項を定める必要がある。

以下の各事項は、適切なサービスを利用すれば実質的に達成されるものであり、通常は調達仕様に含まれない。

- 情報セキュリティを確保するための体制の整備

- 情報セキュリティが侵害された場合の対処
- 情報セキュリティ対策の履行状況が不十分であると思われる場合の対処)

## 2 「約款による情報処理サービス」の利用に関する事項

- (1) 情報セキュリティを確保するための体制及び機能の整備
- 本調達に係る情報サービスを提供する事業者は、当該情報サービスの実施において情報セキュリティを確保するための体制を整備すること。
- (2) 取り扱う府省庁の情報の秘密保持等
- 本調達に係る業務のために〔 省 〕から提供する情報その他当該業務の実施において知り得た情報については、その秘密を保持し、また当該業務の目的以外に利用しないこと。

### 【情報セキュリティ機能について開示を求める場合】

- (3) セキュリティ機能の整備
- 本調達に係る情報サービスを提供する事業者は、当該情報サービスにおいて装備している情報セキュリティ対策を記した約款を提供すること。約款への記載が不可能な場合は、別の手立てで委託元に情報セキュリティ対策を示すこと。

### 【情報セキュリティが侵害された場合の対処を明示する場合】

- (4) 情報セキュリティが侵害された場合の対処
- 本調達に係る業務の遂行において情報セキュリティが侵害され、又はそのおそれがある場合には速やかに委託元に報告すること。これに該当する場合には、以下の事象を含む。

〔 省 〕の情報の外部への漏えい及び目的外利用  
サービス提供事業者による〔 省 〕の情報への不適切なアクセス

- (5) 情報セキュリティ対策の履行状況の確認等に関する事項の通知
- 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために委託元から報告を求められた場合は、速やかに提供を行うこと。

本調達仕様の〔(1)～(3)の各項〕において求める情報セキュリティ対策の実績  
サービス提供事業者に取り扱わせる府省庁の情報の秘密保持等に係る管理状況

### 【情報セキュリティ監査を行う場合】

- (6) 情報セキュリティ監査の実績
- 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は情報セキュリティ監査の実施内容（監査内容、対象範囲、実施者等）を定めて、それについて予め合意を得たうえで情報セキュリティ監査を行う。  
サービス提供事業者は応札において、情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「監査対応計画書」等により提示すること。監査を受け入れることができない場合は、内部監査報告書等、委託元の監査に代わるものを提示すること。

**【情報セキュリティ対策の履行が不十分な場合の対処を明示する場合】**

(7) 情報セキュリティ対策の履行が不十分な場合の対処

- 本調達に係る業務の遂行において、以下の表5に記載された留意事項への対策が約款に記載されていること。約款に記載されている対策が不十分である可能性を委託元が認める場合には、委託先の責任者は、委託元の求めに応じこれと協議を行い、合意した対応を採ること。

表5 . 「約款による情報処理サービス」の利用による外部委託に関する留意事項

	留意事項
1	サービスは約款の範囲でしか提供されない。
2	サービス時間とサポート時間が限られている場合がある。
3	サービスのセキュリティポリシーが開示されないことが多く、省庁対策基準及び規定を満たしているか判断が困難である。
4	サービス提供事業者から提供されるサービスレベルは可用性のみであることが多い。
5	サービス提供事業者は利用者による監査を基本的に受け入れない。
6	バックアップ実施や障害発生時の復旧等の実施内容やタイミングといった、情報システムの運用に関しては約款に記載されていないことが多い。
7	バックアップするデータ形式が他の事業者のサービスに移行できない場合がある。
8	利用者側で情報のバックアップができない場合がある。
9	同一サーバ上で複数の業務(利用者)を実行しているケースがあり、その場合セキュリティ対策が十分に実行されていない業務の影響を受ける可能性がある。
10	同一サーバ上で複数の利用者が情報処理を実行しているため、別の利用者情報を盗み見し、別の利用者に成りすまして処理を行う可能性がある。
11	サーバ資源の利用者ごとの分割が不適切なことによる情報漏えいが発生する可能性がある。
12	情報の置き場所が特定の場所に固定されず、海外の法執行機関等による予期せぬアクセスが行われうる場合がある。
13	サービスを有期契約した場合、契約終了後の情報の取り扱い(確実な消去)が不明瞭な場合がある。
14	サービス提供事業者の経営が破たんしたり突然のサービス停止に陥った場合、預けた情報の行方は保証されず、損害賠償も支払われない場合がある。
15	サービス提供事業者の従業員が不正を行う可能性がある。
16	約款の内容はサービス提供者側の都合で利用開始後に一方的に変更される可能性がある。
17	準拠法に外国法を指定される場合がある。
18	管轄裁判所に海外の裁判所を指定される場合がある。

(8) 再委託に関する事項

**【再委託を禁止する場合】**

- 本調達に係る業務は、その全部又は一部を他の事業者に再委託させてはな

らない。

**【再委託を認める場合】**

- 本調達に係る業務の一部を他の事業者に再委託させる場合には、委託先は、委託元が委託先に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再委託先に行わせること。再委託先に行かせた情報セキュリティ対策及びこれを行かせた結果に関する報告を、委託先に求める場合がある。

**【国際規格を踏まえた委託先の情報セキュリティ水準の評価を行う場合】**

(9) 国際規格を踏まえた委託先の情報セキュリティ水準の評価

**【ISMS 認証取得を考慮する場合】**

- 本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はこれと同等の認証を取得しているか否かを、提案に関する評価の要素とする。（評価式は調達ごとに定めることとなるため、本雛形では省略している。）

**【情報セキュリティ対策ベンチマークの結果を考慮する場合】**

- 本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティ対策ベンチマークを実施し、その結果を書式1（本雛形では省略している。）により提出すること。情報セキュリティ対策ベンチマークに基づく平均成熟度が「n」以上であるか否かを、提案に関する評価の要素とする。（情報セキュリティ対策ベンチマークに関する説明を、付録3から引用する。）

**【ISMS 認証取得及び情報セキュリティ対策ベンチマークの結果を考慮する場合】**

- 本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はこれと同等の認証を取得しているか否かを、提案に関する評価の要素とする。（評価式は調達ごとに定めることとなるため、本雛形では省略している。）
- ただし、ISMS認証及びこれと同等の認証を取得していない事業者又はその部門においては、情報セキュリティ対策ベンチマークを実施し、その結果を書式1（本雛形では省略している。）により提出すること。情報セキュリティ対策ベンチマークに基づく平均成熟度が4以上であるか否かを、提案に関する評価の要素とする。（情報セキュリティ対策ベンチマークに関する説明を、付録3から引用する。）

## 第 部 契約における情報セキュリティ関連事項の記述例

第 部では、情報処理業務を外部委託により行う場合に、情報セキュリティの観点から契約に含める事項の例を示す。

### 1 外部委託する業務の分類に基づく事項

#### 1.1 情報システムの構築等の場合

##### (1) 情報セキュリティを確保するための体制の整備

###### 【情報セキュリティの確保のために体制を整備する場合】

- [乙]は、本契約に係る業務の実施における情報セキュリティ確保のための体制を整備し、[甲]に報告するものとする。

###### 【外部委託を受けた業務を実施する体制を

###### 情報セキュリティ確保の体制ともする場合】

- [乙]は、第 条に基づき整備する実施体制において、情報セキュリティの確保に努めるものとする。
- [乙]は、本契約に係る業務の実施体制を整備し、[甲]に報告するものとする。

(当該体制については、委託元、委託先の両方で協議し、合意した結果を別途確認書等として取り交わすこととなる。)

##### (2) 取り扱う府省庁の情報の秘密保持等

契約における通常秘密保持条項が該当する。以下の内容が含まれていることを確認し、必要に応じ記述を加えること。

- [乙]は、本契約に係る業務に関して [甲] から提供された情報その他知り得た情報を実施体制に定めた者以外の者には秘密とし、また、当該業務の遂行以外の目的に使用しないこと。
- [乙]は、本契約に係る業務に関して [甲] から提供された情報を、当該業務の終了時に委託元に返却するか、消去又は廃棄してその旨を書面で報告すること。
- [乙]は、本契約に係る業務に関して委託元から提供、貸与等された情報その他知り得た情報を当該業務の終了後においても他者に漏えいしないこと。
- [乙]は、本契約に係る業務に関して [甲] から提供された情報その他アクセスを認められた府省庁の情報を、別途定める規則に従い取り扱うこと。  
(別途定める規則には、取り扱う府省庁の情報等に応じて、以下に例を示す事項等を選択して含めること。  
取り扱う情報は外部委託した情報処理業務にのみ使用し、他の目的には使用しないこと。  
取り扱う情報は外部委託した情報処理業務を行う者以外には秘密とすること。  
取り扱う情報を指定した場所から持ち出さないこと。  
当該情報を委託元の許可なく複製しないこと。  
当該情報は、当該委託の終了時に、委託元への返却若しくは消去又は廃棄を確実に行うこと。)

### (3) セキュリティ機能の装備

#### 【情報システムの構築の場合】

##### 【調達において提示したセキュリティ要求仕様と提案を受けたセキュリティ機能を付属文書で示し、当該セキュリティ機能の装備を求める場合】

- [乙]は、[付属文書(セキュリティ要求仕様及びセキュリティ機能)]に示すセキュリティ機能を構築する情報システムに装備すること。  
(本雛形では、付属文書は省略している。)

##### 【調達において提示したセキュリティ要求仕様を付属文書で示し、必要なセキュリティ機能を設計した上でその装備を求める場合】

- [乙]は、[付属文書(セキュリティ要求仕様)]に示すセキュリティ要求仕様に基づき、必要なセキュリティ機能を設計し、装備すること。  
(本雛形では、付属文書は省略している。)

##### 【契約でセキュリティ機能の概要を提示する場合】

- [乙]は、構築する情報システムに以下のセキュリティ機能を持たせること。
  - 構築する情報システムへのアクセスを業務上必要な者に限るための機能
  - 構築する情報システムに対する不正アクセス、ウイルス・不正プログラム感染等、インターネットを経由する攻撃、不正等への対策機能
  - 構築する情報システムにおけるセキュリティ事故及び不正の原因を事後に追跡するための機能

#### 【ソフトウェアの開発の場合】

##### 【調達において提示したセキュリティ要求仕様と提案を受けたセキュリティ機能を付属文書で示し、当該セキュリティ機能の装備を求める場合】

- [乙]は、[付属文書(セキュリティ要求仕様及びセキュリティ機能)]に示すセキュリティ機能を開発するソフトウェアに装備すること。  
(本雛形では、付属文書は省略している。)

##### 【調達において提示したセキュリティ要求仕様を付属文書で示し、必要なセキュリティ機能を設計した上でその装備を求める場合】

- [乙]は、[付属文書(セキュリティ要求仕様)]に示すセキュリティ要求仕様に基づき、必要なセキュリティ機能を設計し、装備すること。  
(本雛形では、付属文書は省略している。)

##### 【契約でセキュリティ機能の概要を提示する場合】

- [乙]は、開発する情報システムに以下のセキュリティ機能を持たせること。
  - 開発するソフトウェアへのアクセスを業務上必要な者に限るための機能
  - 開発するソフトウェアに対する不正アクセス、ウイルス・不正プログラム感染等、インターネットを経由する攻撃、不正等への対策機能
  - 開発するソフトウェアにおけるセキュリティ事故及び不正の原因を

## 事後に追跡するための機能

### 【ST 評価・ST 確認を求める場合】

#### (4) セキュリティ機能の設計に関する確認

##### 【ST 評価・ST 確認の結果を納品時に提出する場合】

- [乙]は、[構築する情報システム/開発するソフトウェア]に関して、取り扱う情報の保護を目的として、ISO/IEC 15408に基づき必要なセキュリティ機能を設計及び実装すること。当該設計において策定するセキュリティ設計仕様書(ST: Security Target)についてST評価・ST確認を受け、その結果を納品までに[甲]に提出すること。

##### 【ST 評価・ST 確認の結果を納品後に提出する場合】

- [乙]は、[構築する情報システム/開発するソフトウェア]に関して、取り扱う情報の保護を目的として、ISO/IEC 15408に基づき必要なセキュリティ機能を設計及び実装すること。当該設計において策定するセキュリティ設計仕様書(ST: Security Target)についてST評価・ST確認を受け、その結果を 年 月 日までに[甲]に提出すること。ST評価・ST確認を受けるために納品物に追加・変更が必要となった場合には、当該追加・変更は[乙]の責任においてこれを行うものとする。

### 【情報システムの構築の場合】

#### (5) 脆弱性対策の実施

- [乙]は、構築する情報システムに関して次の脆弱性対策を実施すること。  
構築する情報システムを構成する機器及びソフトウェアの中で、脆弱性対策を実施するものを適切に決定すること。  
脆弱性対策を行うとした機器及びソフトウェアについて、公表されている脆弱性情報及び公表される脆弱性情報を把握すること。  
把握した脆弱性情報について、対処の要否、可否を判断すること。  
対処したのに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を納品時に[甲]に報告すること。

### 【外部委託する業務以外の情報資産の保全を明示する場合】

#### (6) 外部委託する業務以外の情報資産の保全

- (略)

#### (7) 情報セキュリティが侵害された場合の対処

- [乙]は、本調達に係る業務の遂行において情報セキュリティが侵害され又はそのおそれがある場合には、これを速やかに[甲]に報告すること。これに該当する場合には、以下の事象を含む。  
[乙]に提供し、又は[乙]によるアクセスを認める[甲]の情報の外部への漏えい及び目的外利用  
[乙]の者による[甲]のその他の情報へのアクセス

#### (8) 情報セキュリティ対策の履行状況の確認

- (定期的に報告を求める等、情報セキュリティ対策の履行状況の確認として行う事項及び方法を列挙する。)

### 【情報セキュリティ監査を行う場合】

#### (9) 情報セキュリティ監査を行う事項及び方法

- (情報セキュリティ監査に関して、調達及び応札において確認した事項及び方法を記述する。)

(10)情報セキュリティ対策の履行が不十分であると思われる場合の対処

- [乙]による情報セキュリティ対策の履行が不十分である可能性を[甲]が認める場合には、[乙]の責任者は、[甲]の求めに応じこれと協議を行い、合意した対応を採るものとする

**【確認書等を求める場合】**

(11)確認書等に委任する事項

- (略)

(12)再委託に関する事項

**【再委託を禁止する場合】**

- [乙]は、本契約に係る業務を再委託により第三者に行わせないこと。

**【再委託を認める場合】**

- [乙]は、[甲]が[乙]に求める情報セキュリティ対策と同水準の情報セキュリティ対策を再委託先に行わせること。
- [乙]は、再委託先に行かせた情報セキュリティ対策及びその結果を[適宜確認し、/監査し、][甲]に報告すること。

1.2 情報システムの運用・保守・点検の場合

(1) 情報セキュリティを確保するための体制の整備

「1 情報システムの構築等の場合」と同じ。

(2) 取り扱う府省庁の情報の秘密保持等

「1 情報システムの構築等の場合」と同じ。

(3) 運用・保守・点検における情報セキュリティ対策の実施

- (略)

**【脆弱性対策を委託する場合】**

(4) 脆弱性対策の実施

- [乙]は、情報システムの[運用/保守/点検]のにおいて、次の脆弱性対策を実施すること。  
 別途定める脆弱性対策を行うものとする機器及びソフトウェアについて、公表されている脆弱性情報及び公表される脆弱性情報を把握すること。  
 把握した脆弱性情報について、対処の要否、可否を[[甲]と協議し、]判断すること。対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を随時に[甲]に報告すること。

**【外部委託する業務以外の情報資産の保全を明示する場合】**

(5) 外部委託する業務以外の情報資産の保全

- (略)



### 【情報セキュリティ対策のサービスレベルに関する事項を定める場合】

#### (6) 情報セキュリティ対策のサービスレベルに関する事項

- (略)

#### (7) 情報セキュリティが侵害された場合の対処

- [乙]は、本調達に係る業務の遂行において情報セキュリティが侵害され又はそのおそれがある場合には、これを速やかに[甲]に報告すること。これに該当する場合には、以下の事象を含む。
  - [乙]に提供し、又は[乙]によるアクセスを認める[甲]の情報の外部への漏えい及び目的外利用
  - [乙]の者による[甲]のその他の情報へのアクセス
  - [甲]の者、[乙]の者又は外部の者による当該情報システムからの情報漏えい及び情報の目的外利用
  - 当該情報システムへの不正アクセスによる情報漏えい、サービス停止、情報の改ざん
  - 当該情報システムへのサービス不能攻撃によるサービス停止
  - 当該情報システムにおける不正プログラムの感染による情報漏えい、サービス停止、情報の改ざん
- [甲]及び[乙]は、上記、及びその他被害が短時間に拡大する情報セキュリティ侵害については、別途定める緊急時対策を実施すること。(別途定める緊急時対策は、契約の付属文書とすることが想定される。本雛形では省略している。)

#### (8) 情報セキュリティ対策の履行状況の確認

- (定期的に報告を求める等、情報セキュリティ対策の履行状況の確認として行う事項及び方法を列挙する。)

### 【情報セキュリティ監査を行う場合】

#### (9) 情報セキュリティ監査を行う事項及び方法

- (情報セキュリティ監査に関して、調達及び応札において確認した事項及び方法を記述する。)

#### (10) 情報セキュリティ対策の履行が不十分であると思われる場合の対処

- [乙]による情報セキュリティ対策の履行が不十分である可能性を[甲]が認める場合には、[乙]の責任者は、[甲]の求めに応じこれと協議を行い、合意した対応を採るものとする

### 【確認書等を求める場合】

#### (11) 確認書等に委任する事項

- (略)

## 1.3 情報の加工・処理等の場合

#### (1) 情報セキュリティを確保するための体制の整備

「1 情報システムの構築等の場合」と同じ。

#### (2) 取り扱う府省庁の情報の秘密保持等

「1 情報システムの構築等の場合」と同じ。

(3) 情報セキュリティが侵害された場合の対処

- [乙]は、本調達に係る業務の遂行において [乙] に提供し、又は [乙] によるアクセスを認める [甲] の情報の外部への漏えい若しくは目的外利用が認められ又はそのおそれがある場合には、これを速やかに [甲] に報告すること。

(4) 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の履行状況の確認として行う事項及び方法を列挙する。)

**【情報セキュリティ監査を行う場合】**

(5) 情報セキュリティ監査を行う事項及び方法

- (情報セキュリティ監査に関して、調達及び応札において確認した事項及び方法を記述する。)

(6) 情報セキュリティ対策の履行が不十分であると思われる場合の対処

- [乙] による情報セキュリティ対策の履行が不十分である可能性を [甲] が認める場合には、[乙] の責任者は、[甲] の求めに応じこれと協議を行い、合意した対応を採るものとする

**【確認書等を求める場合】**

(7) 確認書等に委任する事項

- (略)

(8) 再委託に関する事項

**【再委託を禁止する場合】**

- [乙] は、本契約に係る業務を再委託により第三者に行わせないこと。

**【再委託を認める場合】**

- [乙] は、[甲] が [乙] に求める情報セキュリティ対策と同水準の情報セキュリティ対策を再委託先に行わせること。

1.4 情報の保存・運搬の場合

(1) 取り扱う府省庁の情報の秘密保持等

- [乙] は、本調達に係る業務の遂行において [甲] が [保存/運搬] を委託する情報について、その漏洩及び毀損を防止するための十分な安全管理を行うこと。

**【情報セキュリティ監査を行う場合】**

(2) 情報セキュリティ監査を行う事項及び方法

- (情報セキュリティ監査に関して、調達及び応札において確認した事項及び方法を記述する。)

(情報の保存・運搬を外部委託により行う場合には、物品を安全に保存・運搬すること自体が委託先の提供するサービスの内容であることに留意して契約に記載する事項を定める必要がある。以下の各事項については、利用するサービスの契約に実質的に含まれる場合には個々に記載する必要は

ない。

- 情報セキュリティを確保するための体制の整備
- 情報セキュリティが侵害された場合の対処
- 情報セキュリティ対策の履行状況が不十分であると思われる場合の対処)

## 2 「約款による情報処理サービス」の利用に関する事項

「約款による情報処理サービス」においては契約内容が規定のものとして用意されており、利用ごとに交渉や修正ができないことが一般的であるため、「6.1(3)「約款による情報処理サービス」の利用におけるサービス選定の留意事項」に示した脅威についてリスクを評価・検討した上で委託先を選定すること。

## 付録 1 重要な情報を取り扱う情報処理業務

### 及び取り扱わない情報処理業務

#### 1 重要な情報を取り扱う情報処理業務

以下の情報処理業務は重要な情報を取り扱うものであり、原則として外部委託の対象としてはならない。

- (1) ×××システムの構築及び運用
- (2) システムの構築に伴う導入  
(既存システムとの接続確認及びシステムの設置において既存の xxx システムに保有する重要な情報へアクセスすることが可能となるため)
- (3) システムの運用
- (4) 情報の統計処理

#### 2 重要な情報を取り扱わない情報処理業務

以下の情報処理業務は重要な情報を取り扱わないものであり、外部委託の対象としてよい。

- (1) システムの構築（既存システムとの接続確認及びシステムの設置を除く）
- (2) システムの構築及び運用
- (3) 情報の統計処理

## 付録 2 情報セキュリティ対策等

〔「策定手引書」の「9.3.1 外部委託に係る契約」にある情報セキュリティ対策等の説明記事を引用することができる。本雛形では省略している。〕

### 付録3 組織における情報セキュリティ水準の評価に関する制度

組織における情報セキュリティ水準の評価に活用できる制度に、「情報セキュリティマネジメントシステムに関する評価制度」、「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制度」がある。

#### (1) 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

委託先における情報セキュリティマネジメントシステムに関して、第三者機関（審査登録機関）による適合性評価に基づく認証を取得していることを委託先の選定の要素に含めることができる。

我が国においては、財団法人日本情報処理開発協会（JIPDEC）が「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」を運営している。

<http://www.isms.jipdec.jp/isms.html>

#### (2) 情報セキュリティ対策ベンチマーク

情報セキュリティ対策ベンチマークは、事業者が自らの情報セキュリティ対策を評価するための制度であり、評価項目は、対策の取組状況を把握するための評価項目（25項目）と、組織プロフィールに関する評価項目（15項目）からなる。本制度に基づく評価結果を委託先の選定の要素に含めることができる。

本制度は、経済産業省が「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」の「参考資料 情報セキュリティ対策ベンチマーク」として公表している。（平成19年8月改訂）

[http://www.meti.go.jp/policy/netsecurity/sec\\_gov-TopPage.html](http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html)

<http://www.meti.go.jp/policy/netsecurity/downloadfiles/070824benchmark.pdf>

また、これを独立行政法人情報処理推進機構（IPA）が、ウェブページ上で使える自動化ツールにして提供している。

<http://www.ipa.go.jp/security/benchmark/index.html>

以上の制度の特徴は、以下の表のとおりである。

これらの両制度の特徴を踏まえ、委託先の情報セキュリティ水準の評価方法を定める。例えば、JIPDECによる「ISMS適合性評価制度」等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の認証取得を評価の要素に含め、認証を取得していない事業者については情報セキュリティ対策ベンチマークの結果を評価の要素に含めることが考えられる。

	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
概要	組織における情報セキュリティマネジメントに関する評価・認証制度	組織における情報セキュリティマネジメントに関する自己評価のための仕組み
認証基準及び管理策	認証基準：JIS Q 27001:2006 (ISO/IEC 27001:2005) 管理策：JIS Q 27002:2006 (ISO/IEC 17799:2005)	「情報セキュリティ対策ベンチマーク評価項目」 JIS Q 27001:2006 の付属書 A の管理目的及び管理策に基づき 25 項目に集約
評価対象の範囲	業務・事業所等、事業者が評価対象の範囲を定める。	事業者全体を対象とすることを想定しているが、業務・事業所等、事業者が範囲を定めて利用することもできる。
評価項目の選択	管理策に基づきリスク評価を実施して評価項目を選択するため、任意性は実質的でない。	定められた一般的に求められる項目
評価の継続性	内部監査及びマネジメントレビューを年 1 回以上実施する。また、認証登録の継続のため、年 1 回以上のサーベイランス（維持審査）及び 3 年ごとの更新審査を受ける。	(評価の継続性を確保する仕組みは定めていない。)
評価の信頼性	認定機関により認定された審査登録機関により客観的な評価・認証が行われるため、信頼性は高い。	自己評価であるため、評価の客観性、信頼性は高くない。
確認できる事項	情報セキュリティマネジメントの維持・改善の第三者機関による評価結果が確認できる。	情報セキュリティマネジメントの維持・改善の自己評価結果が確認できる。望ましい水準と現在の水準を比較することもできる。
適用性・費用等	情報セキュリティマネジメントシステムに関する認証取得には、費用及び時間を要する。	自己評価であるため簡便に実施でき、費用及び時間について負担が小さい。
委託先の選定における利用手順	委託先候補があらかじめ取得している認証を、登録証及び適用範囲定義書の確認を通じて評価する。	調達手続において情報セキュリティ対策ベンチマークを実施し、その結果を提出することを委託先候補に求める。

### (3) 情報セキュリティ監査

将来的に、以下の場合には、上記の制度に替えて情報セキュリティ監査を利用することも考えられる。

継続業務である等、直近において同様の情報処理業務を委託しており、情報セキュリティ監査を実施している場合

直近において、第三者による情報セキュリティ監査等の手段により、委託元と同等の情報セキュリティ水準にあることが確認できる場合

情報セキュリティ監査は、「情報セキュリティ監査制度」に基づき行うことができる。本制度で定めている「情報セキュリティ管理基準」(経済産業省告示)は ISO/IEC 17799:2000 (JIS X 5080:2002) に基づくものである。

<http://www.meti.go.jp/policy/netsecurity/audit.htm>

なお、監査主体を選定する際の参考に資するよう、任意登録制の「情報セキュリティ監査企業台帳」が整備されている。

<http://www.meti.go.jp/policy/netsecurity/is-kansa/index.html>

また、本制度については、特定非営利活動法人日本情報セキュリティ監査協会（JASA）が普及促進に係る活動を行っている。

<http://www.jasa.jp/index.html>