DM6-02-061

別紙１：雛形

外部委託における情報セキュリティ対策実施規程

雛形

2006 年 3 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	1. 再請負の可否は、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）。 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」 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Ⅱ部、1.(3)）及び契約の記述例（第Ⅲ部、1.(3)）を追加。 4. その他

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Ⅰ部　実施規程雛形 7
1　本書の目的 7
2　本書の対象者 7
3　外部委託を行う業務の形態 7
3.1　情報システム等の構築・開発の外部委託 7
3.2　情報システムの運用・保守・点検の外部委託 7
3.3　情報の加工・処理の外部委託 8
3.4　情報の保存・運搬の外部委託 8
4　外部委託における情報セキュリティ確保に関係する手続 8
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 9
5.1　外部委託の可否の原則 9
5.2　脅威及び対策の検討における留意事項 10
6　調達における手続 11
6.1　委託先の選定基準及び委託先が具備すべき要件 11
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 12
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 12
6.2.2　情報セキュリティ対策ベンチマークの活用 12
6.2.3　情報セキュリティ監査の活用 13
6.3　委託先に求める事項の周知 13
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 13
6.3.2　情報セキュリティが侵害された場合の対処手順の周知 14
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 14
6.4　委託先の選定における手続の遵守 15
7　契約における手続 15
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 15
7.2　外部委託に係る確認書における情報セキュリティの考慮 16
7.3　外部委託の継続における注意 16
7.4　外部委託における実施内容の変更に関する注意 17

7.5　再請負の原則禁止 17
8　委託先における情報処理業務実施中の手続 18
8.1　取り扱う府省庁の情報の秘密保持等 18
8.2　情報セキュリティ対策の履行状況の確認 18
9　納品・検収における手続 19
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 19
10.1　情報システム等の構築・開発における
セキュリティ機能の設計及び実装の評価 19
10.2　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 19
11　本書に関する相談窓口 20

第Ⅱ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 21
1　情報システム等の構築・開発の場合 21
2　情報システムの運用・保守・点検の場合 24
3　情報の加工・処理の場合 26
4　情報の保存・運搬の場合 27

第Ⅲ部　契約における情報セキュリティ関連事項の記述例 29
1　情報システム等の構築・開発の場合 29
2　情報システムの運用・保守・点検の場合 32
3　情報の加工・処理の場合 33
4　情報の保存・運搬の場合 34

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 36
1　重要な情報を取り扱う情報処理業務 36
2　重要な情報を取り扱わない情報処理業務 36

付録２　情報セキュリティ対策等 36

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 37

本雛形の利用方法

本雛形の第Ⅰ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Ⅱ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Ⅲ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
    - ○ 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。
- 政府機関統一基準の遵守事項を具体化するものではないが、府省庁の判断に

より情報システムセキュリティ責任者に実施を求めることが想定される手順等は、≪　≫を付して明示している。

- 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［6.1.2(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基準(2005 年 12 月版(全体版初版))」(NISD-K303-052) 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Ⅰ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を対象としている。

なお、情報の加工・処理（「3.3 情報の加工・処理の外部委託」を参照。）及び情報の保存・運搬（「3.4 情報の保存・運搬の外部委託」）は、課室情報セキュリティ責任者の責任の下で行う場合がある。これらを外部委託により行う場合には、本書において情報システムセキュリティ責任者に求める事項を、課室情報セキュリティ責任者に求めることとなる。

3　外部委託を行う業務の形態

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　情報システム等の構築・開発の外部委託

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「情報システム等の構築・開発」という。）を外部委託により行う場合である。

3.2　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。

①　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。

② 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動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し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。

③ 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。

④ 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。

⑤ 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。

3.3 情報の加工・処理の外部委託

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・処理を外部委託により行う場合である。

3.4 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。

4 外部委託における情報セキュリティ確保に関係する手続

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

［6.1.2(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及び情報システム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) 情報システム等の構築・開発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。

6　調達における手続

6.1　委託先の選定基準及び委託先が具備すべき要件

6.1.2(1)(b)

(1) 情報システム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	情報システム等の構築・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	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)再請負に関する事項（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択するもの、及び当該対策等の実施を委託先に求めるが委託先の選定後に契約に含めれば足りると判断する場合があるもの）

×：非該当又は不必要　　※：一般にサービスに含まれている

本表の区分は一般的な目安であり、調達仕様に記載する事項は案件ごとに判断すること。

「情報セキュリティ対策等」の(1)～(9)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。

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

6.1.2(1)(c), (d)【強化遵守事項】

委託先の選定における前節の手続に加えて、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、2006 年 5 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たときは、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、2006 年 5 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に、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たときは、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、2006 年 5 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に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

6.1.2(2)(a)

(1) 情報システム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委託先が具備すべき要件」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が定めること。

調達仕様の記述例は、「第Ⅱ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手順の周知

6.1.2(2)(b)

(1) 情報システム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手順（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Ⅱ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

6.1.2(2)(c)

(1) 情報システムセキュリティ責任者は、調達仕様、契約及び確認書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評価基準を策定すること。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。[1]　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は、委託先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手順（表１(9)）を、調達仕様として委託先候補に周知すること。

---

[1] 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から、監査の実施可能性も考慮した上で、監査の必要性を判断すること。

調達仕様の記述例は、「第Ⅱ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。

6.4　委託先の選定における手続の遵守

6.1.2(3)(a)

(1) 情報システムセキュリティ責任者は、「6.1 委託先の選定基準及び委託先が具備すべき要件」の定めに従い委託先を選定すること。

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

6.1.2(4)(a)

(1) 情報システム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２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が定めること。

表２　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	情報システム等の構築・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	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) 確認書に委任する事項	△	△	△	△	△	△	△	△	×
(13) 再請負に関する事項	○	△	△	△	△	△	△	○	△

○：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Ⅲ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における情報セキュリティの考慮

6.1.2(4)(b)

(1) 情報システムセキュリティ責任者は、委託先に情報処理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者を記載することが考えられる。

(3) 確認書又は契約の付属書には、必要に応じて次の事項を含めること。

- 委託先が実施する情報セキュリティ対策等の具体的な取組内容
- 当該外部委託に係る業務を行う者の特定とそれ以外の者による当該業務の禁止

(4) 確認書及び契約の付属書は、契約に加えて取り交わす必要がない場合には、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

6.1.2(4)(c)

(1) 情報システム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委託先が具備すべき要件」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

6.1.2(4)(d)

(1) 情報システムセキュリティ責任者は、契約及び確認書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、並びに委託先の選定において適用した選定手続、選定基準及び委託先が具備すべき要件に基づき、その可否を審査すること。

7.5 再請負の原則禁止

6.1.2(4)(e)

(1) 再請負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、情報システム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全部又は一部を第三者に再請負により行わせることを原則として禁止すること。

(2) 情報システム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請負により行わせることを認めない場合には、その旨を調達仕様に含めること。

(3) 情報システム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請負により行うことを望む場合には、再請負の可否及び条件を検討し、情報セキュリティ責任者の判断を得ること。判断基準の例を以下に示す。

- 再請負を行う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、当該業務が再請負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請負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請負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。
    - 再請負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。
    - 委託先が再請負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。

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

6.1.2(4)(f)

(1) 情報システムセキュリティ責任者は、外部委託により情報処理を行う場合に、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は、委託先に要機密情報を提供する場合には、その移送における情報漏洩対策を施すこと。情報漏洩対策として、書面の不要部分のマスキング、媒体中の情報を暗号化した上での郵送、暗号化通信等、安全な方法を採ること。

(4) 情報システム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、消去又は廃棄させること。委託先において情報を消去又は廃棄した場合には、その旨を委託先から報告させること。

(5) 情報システムセキュリティ責任者は、提供した情報の返却を受け、若しくは消去又は廃棄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　情報セキュリティ対策の履行状況の確認

(1) 情報システム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に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

6.1.2(5)(a)

(1) 情報システム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 情報システム等の構築・開発におけるセキュリティ機能の設計及び実装の評価

4.3.1(1)(d), 6.1.3(3)(e)

(1) 情報システムセキュリティ責任者は、情報システム等の構築・開発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する場合であって、重要なセキュリティ要件の変更が軽微であると認めたときは、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、まず情報システムの構築又はソフトウェアの開発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、2006年6月

10.2 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

4.3.1(1)(f)【強化遵守事項】

(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に重要なセキュリティ要件があると認める場合には、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るときには、その中から当該セキュリティ機能に関して IT セキュリティ評価及び認証制度に基づく認証を取得している製品を選択すること。

(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、2006年6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Ⅱ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Ⅱ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に含める事項の例を示す。

1　情報システム等の構築・開発の場合

(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

【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。

【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。）

(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］*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、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、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) 再請負に関する事項

【再請負を禁止する場合】

- 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請負により行わせてはならない。

【再請負を認める場合】

- 本調達に係る業務の一部を他の事業者に再請負により行わせる場合には、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請負先に行わせること。再請負先に行わ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。

【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。）

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、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、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)再請負に関する事項

【再請負を禁止する場合】

- 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請負により行わせてはならない。

【再請負を認める場合】

- 本調達に係る業務の一部を他の事業者に再請負により行わせる場合には、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請負先に行わせること。再請負先に行わ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。

【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。）

3　情報の加工・処理の場合

(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、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) 再請負に関する事項

【再請負を禁止する場合】

- 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請負により行わせてはならない。

【再請負を認める場合】

- 本調達に係る業務の一部を他の事業者に再請負により行わせる場合には、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請負先に行わせること。再請負先に行わ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 情報システム等の構築・開発の場合」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 情報システム等の構築・開発の場合」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 情報システム等の構築・開発の場合」と同じ。

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 情報システム等の構築・開発の場合」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 情報システム等の構築・開発の場合」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 情報システム等の構築・開発の場合」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めない。

- 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）

第Ⅲ部　契約における情報セキュリティ関連事項の記述例

第Ⅲ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　情報システム等の構築・開発の場合

(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、第〇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、委託先の両者で協議し、合意した結果を別途確認書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

契約における通常の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 *［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）

【サービスレベルを契約で定める場合】

(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

- （略）

(8) 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

(9) 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】

(10)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。）

(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

- *［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

【確認書を求める場合】

(12)確認書に委任する事項

- （略）

(13)再請負に関する事項

【再請負を禁止する場合】

- *［乙］*は、本契約に係る業務を再請負により第三者に行わせないこと。

【再請負を認める場合】

- *［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請負先に行わせること。
- *［乙］*は、再請負先に行わ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。

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 情報システム等の構築・開発の場合」と同じ。

(2) 取り扱う府省庁の情報の秘密保持等

「1 情報システム等の構築・開発の場合」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）

(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。
  - ① *［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
  - ② *［乙］*の者による*［甲］*のその他の情報へのアクセス
  - ③ *［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
  - ④ 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
  - ⑤ 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
  - ⑥ 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④、⑤及び⑥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

【確認書を求める場合】

(11)確認書に委任する事項

- （略）

3 情報の加工・処理の場合

(1) 情報セキュリティを確保するための体制の整備

「1 情報システム等の構築・開発の場合」と同じ。

(2) 取り扱う府省庁の情報の秘密保持等

「1 情報システム等の構築・開発の場合」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

【確認書を求める場合】

(7) 確認書に委任する事項

- （略）

(8) 再請負に関する事項

【再請負を禁止する場合】

- *［乙］*は、本契約に係る業務を再請負により第三者に行わせないこと。

【再請負を認める場合】

- *［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請負先に行わせること。

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）

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。

⑴ 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/

⑵ 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、企業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。

http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html

http://www.meti.go.jp/policy/netsecurity/downloadfiles/1_benchmark.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/

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 管理基準	認証基準：ISO/IEC 27001:2005 管理策：ISO/IEC 17799:2005 (ISO/IEC 27001 付属書 A と共通) 2006 年 5 月に、これらの国内規格として 認証基準：JIS Q 27001:2006 管理策：JIS Q 27002:2006 (JIS Q 27001 付属書 A と共通) が発行される予定。 JIPDEC による『ISMS 適合性評価制度においては認証基準は「ISMS 認証基準 Ver.2.0」、管理策は ISO/IEC 17799:2000 であるが、今後、JIS Q 27001:2006 及び JIS Q 27002 に移行する予定である。	「情報セキュリティ対策ベンチマーク評価項目」 「ISMS 認証基準 Ver.2.0」の詳細管理策（JIS X 5080:2002 (ISO/IEC 17799:2000)）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、任意性は実質的にない。	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は、現状では限定的。また、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。

① 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

② 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) に基づくものであり、この点は、ISMS適合性評価制度の「ISMS 認証基準 Ver2.0」と同様である。

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