DM6-02-081

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

2008 年 9 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、9.3.5 項）。 2. 仮称を記載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. その他
2006/8/4	誤記訂正
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

目次

1　本書の目的

本書は、府省庁において情報処理業務を外部委託により行う際に適用する規定（以下「外部委託における情報セキュリティ対策実施規程」という。）を統括情報セキュリティ責任者が整備するための手引書である。

府省庁においては、「政府機関の情報セキュリティ対策のための統一基準(第３版)」（NISD-K303-072、以下「政府機関統一基準」という。）に基づく省庁対策基準及び関係する規定を整備することが求められている。一方、府省庁の業務を円滑に遂行するためには必要な手順を具体的に示した実施手順を整備することが望まれることから、当該実施手順に従い業務を行えば結果として省庁対策基準も遵守することとなる手順書を策定することが適切である。「外部委託における情報セキュリティ対策実施規程」は、これらの実施手順の一つとして策定し、府省庁の情報処理業務を外部委託により行う場合に適用するものである。

府省庁の情報処理業務の形態には、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・保守・点検、情報の加工・処理及び情報の保存・運搬等がある。これらの情報処理業務を外部委託により行う場合には、当該業務の形態において、府省庁と委託先の業務分担、委託先に取り扱わせる情報、機器の設置場所（庁舎内又は委託先の施設内）、委託先による業務の実施場所（庁舎内又は委託先の施設内）等に関して様々な場合があり、それぞれの場合に応じて適切な情報セキュリティ対策を委託先に実施させるための管理が委託元である府省庁に求められる。

本書は、これらの背景の下で、「外部委託における情報セキュリティ対策実施規程」に含めるべき事項及び記述例を具体的に示し、もって政府機関統一基準及び省庁対策基準への準拠性、業務への適合性等において適切な規定の整備に資することを目的とする。

本書は、情報システムセキュリティ責任者、課室情報セキュリティ責任者及びその他の行政事務従事者が、政府機関統一基準における外部委託に関係する事項の解説書として利用することもできる。

2　規定に記載すべき事項

「外部委託における情報セキュリティ対策実施規程」には、以下の事項を具体化する手順等を記載すること。

2.1　政府機関統一基準（NISD-K303-072）に定める外部委託に係る遵守事項

6.1.2　外部委託　(1) 情報セキュリティ確保のための府省庁内共通の仕組みの整備

6.1.2　外部委託　(2) 委託先に実施させる情報セキュリティ対策の明確化

6.1.2　外部委託　(3) 委託先の選定

6.1.2　外部委託　(4) 外部委託に係る契約
6.1.2　外部委託　(5) 外部委託の実施における手続
6.1.2　外部委託　(6) 外部委託終了時の手続

4.3.1　情報システムのセキュリティ要件　(1) 情報システムの計画
(d)［構築する情報システムに関する ST 評価・ST 確認］
(g)［製品として調達する機器及びソフトウェアに関する IT セキュリティ評価及び認証制度に基づく認証取得］
6.1.3　ソフトウェア開発　(3) ソフトウェアの設計時
(e)［開発するソフトウェアに関する ST 評価・ST 確認］

本書では、上記の遵守事項に基づくもの以外に、府省庁の判断により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に実施を求めることが想定される手順等もあわせて示している。これらは、≪　≫を付して政府機関統一基準の遵守事項を具体化する部分と区別している。

2.2　セキュリティ確保に係るその他の留意事項

政府機関統一基準においては、前節「2.1 政府機関統一基準（NISD-K303-072）に定める外部委託に係る遵守事項」に挙げた遵守事項以外にも、府省庁において情報セキュリティを確保するための遵守事項を定めているところ、情報処理業務を外部委託により行う場合には、これらの遵守事項に基づき府省庁に求められる情報セキュリティ対策と同等水準の対策の実施を委託先に求めることになる。

なお、その内容については、「外部委託における情報セキュリティ対策実施規程」には含めず、委託先に詳細仕様を契約の一部として別途提示し、その実施を求めることが考えられる。例えば、次のような詳細仕様を提示することとなる。

- 情報システムの構築を外部委託する場合に、保護すべき情報のほか、不正アクセス、ウイルス感染等の脅威を示し、これらへの対策を装備することを求める。また、実施内容を明確にするために、実装上の要求事項も提示する。
- 情報システムの運用を外部委託する場合に、保護すべき情報のほか、情報漏えいの脅威を示し、対策を実施することを求める。実施内容を明確にするために、暗号化すべき情報や、取得すべき監査証跡等、運用上の要求事項を具体的に提示することも考えられる。

委託先に提示する詳細仕様の策定においては、内閣官房情報セキュリティセンター中心となって作成する本書以外の策定手引書を活用することが有効である。

3　文書構成例

「外部委託における情報セキュリティ対策実施規程」は、以下の文書構成で作成することが考えられる。

第Ⅰ部 実施規定雛形
1 本書の目的
2 本書の対象者
3 外部委託を行う業務の形態
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
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 調達における手続
7 契約における手続
8 委託先における情報処理業務実施中の手続
9 納品・検収における手続
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
11 本書に関する相談窓口

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Ⅲ部 契約における情報セキュリティ関連事項の記述例

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
付録 2 情報セキュリティ対策等
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

4 策定する上での留意事項

「外部委託における情報セキュリティ対策実施規程」は、以下のことに留意して策定する。

(1) 「外部委託における情報セキュリティ対策実施規程」は、府省庁において外部委託により行う情報処理業務の形態を網羅し、広く適用できる規定とすること。

(2) 外部委託の手続に関する既存の規定等が整備されていれば、「外部委託における情報セキュリティ対策実施規程」を独立した文書として策定することなく、既存の規定等を改定し、本書で求める事項を含めてもよい。

(3) 「外部委託における情報セキュリティ対策実施規程」では、府省庁における実際の調達業務にあわせて、必要に応じて、調達担当者の役割及び調達担当者と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との関係も示すこと。

5 参考資料

「外部委託における情報セキュリティ対策実施規程」の策定に際しては、以下の資料が参考となる。

5.1 政府及び政府関係機関の資料

(1) 『情報システムに係る政府調達の基本指針』
各府省情報化統括責任者（CIO）連絡会議決定、2007 年（平成 19 年）3 月 1 日

http://www.soumu.go.jp/gyoukan/kanri/a_01_f.htm

本参考資料は、情報システムに係る政府調達において、サービス市場における自由で公正な競争を促し、真の競争環境を実現するとともに、調達手続の一層の透明性・公平性の確保を図るため、「重点計画-2006」（平成 18 年 7 月 26 日 IT 戦略本部決定）及び「電子政府推進計画」（平成 18 年 8 月 31 日各府省情報化統括責任者（CIO）連絡会議決定）に基づき策定されたものである。

(2) 『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

本参考資料は、府省庁が情報処理業務を外部委託により行う場合に、情報セキュリティマネジメントシステム適合性評価制度、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を利用するための手引である。これらの制度は、委託先の選定における情報セキュリティ水準の評価、及び委託先における業務実施中に行う情報セキュリティ対策の履行状況の確認に利用できる。

(3) 『情報セキュリティ対策ベンチマーク』
経済産業省、平成 19 年 8 月（改訂）
http://www.meti.go.jp/policy/netsecurity/downloadfiles/070824benchmark.pdf

独立行政法人情報処理推進機構（IPA）
http://www.ipa.go.jp/security/benchmark/index.html

本参考資料は、企業における情報セキュリティの水準を「望まれる水準」（「望まれる水準」は、企業の業態や保有する情報資産等の属性に応じて定められている。）と対比して示すことにより、その改善のために優先的に取り組むべき項目を明確にするための手段を提供するものである。本資料を活用することによって、委託先候補の情報セキュリティ対策への取組状況を把握することが可能となる。なお、上記 IPA のウェブページで、企業が本資料の内容に沿った自己評価を容易に行うことができるツールが利用できる。

本参考資料は次の報告書の一部である。
『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』
経済産業省、平成 17 年 3 月
http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html
http://www.meti.go.jp/policy/netsecurity/downloadfiles/sec_gov-report.pdf
（情報セキュリティ対策ベンチマークについては、平成 19 年 8 月改訂）

(4) IT セキュリティ評価及び認証制度に関する資料
独立行政法人情報処理推進機構（IPA）
http://www.ipa.go.jp/security/jisec/index.html

本参考資料は、IT 製品・システムにセキュリティ機能が実装されていることを国際的に合意された規格である ISO/IEC 15408（Common Criteria）に基づき評価し、認証するための制度に関して解説したものである。

(5) 『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、2007 年 11 月
本参考資料は、府省庁が情報システムの構築又はソフトウェアの開発を外部委託により行う場合に、調達仕様において委託先候補に対してセキュリティ要件（当該情報システム又はソフトウェアで実装すべきセキュリティ機能の要求仕様）を提示し、応札におけるセキュリティ機能の提案を評価する方法を説明した資料である。典型的な 3 種類の情報システム例について、セキュリティ要件とセキュリティ機能の例を付録で示している。また、機器等の購入において IT セキュリティ評価及び認証制度及び認証製品リストを利用する際の考慮事項も示している。

(6) 『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

本参考資料は、府省庁が情報システムの構築又はソフトウェアの開発を外部委託により行う場合に、考慮すべき政府機関統一基準の遵守事項を示し、また、上記『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』を利用するための指針を示し、さらに、ST 評価・ST 確認を委託先に求める場合の検討事項を解説した資料である。

(7) 情報セキュリティ監査制度に関する資料
経済産業省
http://www.meti.go.jp/policy/netsecurity/audit.htm

本参考資料は、2002 年 9 月から 2003 年 3 月にかけて行われた「情報セキュリティ監査研究会」（経済産業省が設置。）の成果物である。本資料には、『情報セキュリティ管理基準 Ver1.0』及び『情報セキュリティ監査研究会報告書』（2003 年 3 月 26 日）が含まれている。これらの成果物には、情報セキュリティ監査の在り方、標準的な管理基準、監査基準及び監査を行う主体の在り方等が示されており、これらに基づき、2003 年 4 月から情報セキュリティ監査制度が運営されている。
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

5.2 政府・政府関係機関以外の資料

(1) 情報セキュリティマネジメントシステム適合性評価制度に関する資料
財団法人日本情報処理開発協会（JIPDEC）

http://www.isms.jipdec.jp/isms.html
なお、本制度では、『情報セキュリティマネジメントシステム―要求事項』（JIS Q 27001:2006）を認証基準に採用している。また、『情報セキュリティマネジメントの実践のための規範』（JIS Q 27002:2006）は、管理策についての参考資料である。

6 雛形の利用方法

雛形（別紙１）を参考にして、「外部委託における情報セキュリティ対策実施規程」を効率よく策定することができる。

本書と同じく、雛形においても外部委託により行う業務を「情報システムの構築等」、「情報システムの運用・保守・点検」「情報の加工・処理等」及び「情報の保存・運搬」に類型化している。そのため、これらとは異なる業務を外部委託により行う場合には、適宜、記事を修正、追加又は削除する必要がある。

7 外部委託における情報セキュリティ確保の原則

7.1 適用する規定等

情報処理業務を外部委託により行う場合に、これにかかわる当事者には、府省庁において委託元としての業務を行う者と、当該情報処理業務を行う委託先の事業者がある。

府省庁において委託元としての業務を行う者には、外部委託に関する一般的な手続に加えて、情報セキュリティを確保する観点から、次の規定が適用される。

(1) 「2.1 政府機関統一基準（NISD-K303-072）に定める外部委託に係る遵守事項」に挙げる事項に準拠する省庁対策基準の規定

(2) 本書を参考にして府省庁において策定する「外部委託における情報セキュリティ対策実施規程」

一方、委託先の事業者及びその従業者は政府機関統一基準で定める行政事務従事者には該当せず、省庁対策基準及びこれに基づき整備される規定は適用されないことから、委託先に対しては、一般的な調達、契約手続に加えて、当該業務の遂行において実施すべき情報セキュリティ対策等を調達仕様において提示し、また、委託契約に含めることにより委託先に実施させる必要がある。

7.2 外部委託における情報セキュリティの要件

情報処理業務を外部委託により行う場合には、当該業務の遂行に必要な情報を府省庁から提供して委託先に取り扱わせること、及び情報システムの構築、運用等を委託先が行うことから、次の点において情報セキュリティを確保する必要がある。

(1) 委託先に取り扱わせる情報に関する機密性、完全性、可用性の維持及び利用目的

遵守を含む情報セキュリティ対策が、委託先において行われること。

(2) 情報システムの構築、運用等に必要な情報セキュリティ対策が委託先において行われること。

本書「2.1 政府機関統一基準（NISD-K303-072）に定める外部委託に係る遵守事項」に挙げる事項では、外部委託を行う場合においても、府省庁内において情報処理業務を行う場合と同等の水準の情報セキュリティ対策が行われることを目的として、省庁対策基準及び「外部委託における情報セキュリティ対策実施規程」に含めるべき事項を示している。

7.3 外部委託における情報セキュリティ確保の枠組み

委託先は、自らの情報セキュリティポリシー等に基づき情報セキュリティ対策を行っており、これらは、当然に府省庁に適用する省庁対策基準及び規定とは異なる。このため、以下の枠組みにより外部委託における情報セキュリティの確保を図ることとなる。

(1) 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、当該業務の条件ごとに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) 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) 当該外部委託に係る情報処理業務において実施すべき情報セキュリティ対策に関して、委託元及び委託先が合意すること。

(4) 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) 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、委託元による確認がなされること。

(6) 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。

7.4 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

前節に示した枠組みを実現するために、外部委託に関する手続において、情報セキュリティ確保のために以下の対応が求められる。

(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ことを検討している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。政府機関統一基準の関連する遵守事項については、「9.1 外部委託により情報処理業務を行うことの可否の判断」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、外部委託する情報処理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。政府機関統一基準の関連する遵守事項については、「9.2 調達に関する遵守事項」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。政府機関統一基準の関連する遵守事項については、「9.3 契約に関する遵守事項」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。政府機関統一基準の関連する遵守事項については、「9.4 委託先における情報処理業務実施中の遵守事項」を参照されたい。

(5) 納品・検収における手続

外部委託した情報処理業務の終了時に、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。政府機関統一基準の関連する遵守事項については、「9.5 納品・検収に関する遵守事項」を参照されたい。

7.5 情報セキュリティ対策の分担の明確化

情報処理業務の一部を外部委託により行う場合には、当該業務に関する情報セキュリティ対策を委託先及び府省庁が分担して行うこととなるが、分担の明確化が不十分な場合には、不明確な部分について双方とも自らが行うべきことであると認識せず、結果として当該対策が行われないことが懸念される。このため、委託先及び府省庁のそれぞれで行うべき情報セキュリティ対策の範囲を契約で明確にし、対策を漏れなく実施することが重要である。以下に例を示す。

(1) 府省庁が庁舎内に保有する情報システムの運用を外部委託する場合

情報システムの運用に関する情報セキュリティ対策のうち、外部委託により行う範囲を契約で定め、これを委託先に行わせる。庁舎内のサーバルーム等の安全区域の管理、利用者である行政事務従事者が行う対策は、省庁対策基準及びそれに基づく規定に従い、府省庁において行う。また、公開される脆弱性情報を監視し、サーバのソフトウェアにセキュリティ修正を適用することを含む脆弱性対策を委託先に行わせる場合には、その旨を契約に含める必要がある。

(2) 情報システムのハウジングサービスを利用する場合

情報セキュリティ対策のうち、情報システムを設置するデータセンター等にお

ける安全区域の管理を委託先に求め、情報システムの運用及び利用、それに伴う情報セキュリティ対策は府省庁において行う。この場合には、情報システムの設置場所にかかわらず、省庁対策基準及びこれに基づく規定が当該運用及び利用に適用されるため、このことを関係する行政事務従事者に周知することが重要である。

8 外部委託の形態

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、それぞれに関して実施すべき情報セキュリティ対策等及び整備すべき規定を提示している。[1]

8.1 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、以下「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。その中でも、設計だけ、あるいは設計を除く後続の工程だけを外部委託する場合もある。

当該業務を行う場所には、委託先の事業所内と、府省庁の庁舎内がある。

一般に、情報システムの構築等を外部委託する場合には、次の情報セキュリティ対策等のうち必要なものにつきその実施を契約に基づき委託先に求める。なお、情報セキュリティ対策等の説明は、「9.3.1 外部委託に係る契約」を参照されたい。

(1) 情報セキュリティを確保するための体制の整備
　下記(2)～(9)の情報セキュリティ対策等を実施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
　情報の機密性、完全性、可用性の確保と目的外利用の防止を含む、府省庁が提供する情報の適切な管理

(3) セキュリティ機能の装備
　構築・開発する情報システム等に必要なセキュリティ機能の装備

(4) 脆弱性対策の実施
　構築・開発する情報システム等における脆弱性対策の実施

(5) 外部委託する業務以外の情報の保全
　外部委託する業務で取り扱う情報資産以外の情報資産の保全（庁舎内で情報システムの構築等を行う等、委託先が府省庁の他の情報資産にアクセスし得る環境で業務を行う場合）

[1]「政府機関の情報セキュリティ対策のための統一基準(第３版) 解説書」（NISD-K303-072C）においては、「6.1.2 外部委託」の適用範囲を営業品目の例示により示している。当該例示に挙げている品目は、「ソフトウェア開発」、「情報処理」「賃貸借」及び「調査・研究」である。営業品目とは、調達に関する事業者の参加資格申請手続において各府省庁が共通に適用している「一般競争（指名競争）参加資格申請（物品製造等） 申請の手引き」で定められ、個々の調達案件においても明示されるものである。これに対し、本書では、情報処理業務を外部委託により行う際の情報セキュリティ対策等の相違に着目して、情報処理業務の内容により分類している。

(6) 情報セキュリティが侵害された場合の対処
　情報セキュリティが侵害された場合の指示・連絡体制の策定等

(7) 情報セキュリティ対策の履行状況の確認
　上記(1)～(6)の情報セキュリティ対策の委託先における履行状況の確認

(8) 情報セキュリティ監査の実施
　上記(1)～(6)の情報セキュリティ対策の水準を確保・維持するための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
　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指示・連絡体制の策定等

8.2　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、府省庁の庁舎内で、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「オンサイトサポートサービス」の利用である。

② 委託先の事業所から回線等を経由して府省庁の庁舎内に設置され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」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府省庁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府省庁が所有する場合と、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府省庁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・点検の業務は府省庁が行う。いわゆる「ハウジングサービス」の利用である。

一般に、情報システムの運用・保守・点検を外部委託する場合にも、「8.1 情報システムの構築等の外部委託」に示す(1)、(2)及び(4)～(9)の情報セキュリティ対策等の

実施を、また、「(3) セキュリティ機能の装備」に代えて次の情報セキュリティ対策の実施を契約に基づき委託先に求める。

(3) 運用・保守・点検における情報セキュリティ対策の実施
　当該情報システムにおける情報のバックアップの取得、監査証跡に関する運用操作等の実施

また、委託先に実施を求める情報セキュリティ対策に関して、その水準をサービスレベルとして定める場合がある。なお、情報セキュリティ対策等の説明は、「9.3.1 外部委託に係る契約」を参照されたい。

8.3　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、以下「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。情報の加工・処理等においては、委託先に提供する情報及び加工・処理等により作成され府省庁のものとなる情報について、委託先に適切に管理させる必要がある。

当該業務は、委託先の事業所内で行われることが多いと思料される。

一般に、情報の加工・処理等を外部委託する場合には、次の情報セキュリティ対策等の実施を契約に基づき事業者に求める。なお、情報セキュリティ対策等の説明は、「9.3.1 外部委託に係る契約」を参照されたい。

(1) 情報セキュリティを確保するための体制の整備
　下記(2)～(5)の対策を実施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
　委託元から提供する情報及び作成され府省庁のものとなる情報に係る機密性、完全性、可用性の確保と目的外利用の防止を含む適切な管理

(3) 情報セキュリティが侵害された場合の対処
　情報セキュリティが侵害された場合の指示・連絡体制の策定等

(4) 情報セキュリティ対策の履行状況の確認
　上記(1)～(3)の情報セキュリティ対策の委託先における履行状況の確認

(5) 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
　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指示・連絡体制の策定等

8.4　情報の保存・運搬の外部委託

情報を記録した外部記録媒体の保存又は運搬を外部委託により行う場合である。情報の保存を外部委託により行う例に、災害、故障等に備えて取得する情報システムの運用に係るバックアップの保存及び法令に基づく業務情報の保存を外部委託により

行う場合がある。また、情報の運搬を外部委託により行う例に、情報の保存に伴う運搬その他業務上の必要から行う情報の運搬を外部委託により行う場合がある。

一般に、情報の保存・運搬を外部委託する場合には、取り扱う府省庁の情報の秘密保持等を契約に基づき事業者に求めるが、特に完全性の確保も重要である。その際に、当該事業者は通常は倉庫又は運送に係る事業者であり、情報処理事業者ではないことに留意しつつ、実効性があり実施可能な事項を委託先に求めることとなる。

9　政府機関統一基準（NISD-K303-072）における外部委託に関する遵守事項の解説

9.1　外部委託により情報処理業務を行うことの可否の判断

政府機関統一基準　　6.1.2 外部委託
(1)(a) 統括情報セキュリティ責任者は、外部委託の対象としてよい情報システムの範囲及び委託先によるアクセスを認める情報資産の範囲を判断する基準を整備すること。【基本遵守事項】

情報処理業務を外部委託した場合に、これを行う委託先には府省庁の指揮命令が直接には及ばないことにかんがみ、外部委託の対象としてよい情報システムの範囲及び委託先によるアクセスを認める情報資産の範囲を判断する府省庁の基準を、統括情報セキュリティ責任者が整備すべきことを定めた事項である。当該情報処理業務において求める情報セキュリティ水準が、外部委託により行うのでは確保できないと考えられる場合に該当するか否かを判断する基準を策定することとなる。

「外部委託における情報セキュリティ対策実施規程」では、次のような事項を定めることが考えられる。

(1) 原則の提示
　外部委託の対象としてよい情報システムの範囲及び委託先によるアクセスを認めてよい情報資産の範囲に関する原則を示す。これは、外部委託の対象としてよい情報処理業務の範囲として示すこともできる。
　例えば、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、原則として禁止することが考えられる。

(2) 原則に基づく例示
　上記原則に基づく判断の具体例を示す。外部委託の対象としてはならない情報システム、情報資産又は情報処理業務を列挙する方法がある。あわせて、外部委託の対象としてよい例も列挙することにより、判断の基準を一層明確に示すこともできる。

(3) ≪情報セキュリティ責任者に判断を求める手続≫
　≪上記(1)及び(2)の規定では明確に判断できない場合も想定し、情報システムセキュリティ責任者が、情報セキュリティ責任者に判断を求める手続を示す。≫

9.2　調達に関する遵守事項

情報処理業務を外部委託により行うための調達に関して、委託先の選定基準、当該業務の実施において委託先に行わせる事項及びその周知について、政府機関統一基準において遵守事項を定めている。

9.2.1 委託先の選定

政府機関統一基準　　6.1.2 外部委託
(1) (b) 統括情報セキュリティ責任者は、委託先の選定基準及び選定手続を整備すること。【基本遵守事項】

委託先の選定に適用する選定基準及び選定手続の整備を求める事項である。

(1) 委託先の選定基準の整備

整備する委託先の選定基準には、次の事項を含める。

① 事業の安定性

外部委託により情報システムの構築を行い、これを終了した後にも、情報セキュリティを維持するために、当該事業者による保守等が継続して必要な場合がある。また、外部委託によりシステムの運用を行う場合には、予定した期間にわたり、委託先による運用が継続して行われる必要がある。この観点から、将来にわたる事業の安定性について委託先に求める要件を定める。最低限の要件としては、財務状況に関して明白な欠陥が認められる事業者を委託先としないこと等が考えられる。

② 情報セキュリティ対策の遂行能力

「8 外部委託の形態」の各項に示す情報セキュリティ対策の実施を調達仕様に含めることにより、その遂行能力を有することを求める。また、委託先の能力を測るために、以下に示す体制又は実績を有することを選定基準に含めることもできる。

- 情報セキュリティを専門とする部門又は者を有し、外部委託を受けた業務の実施において当該部門又は者の参加が得られること。
- 情報セキュリティ対策の実施又は情報セキュリティ製品の販売等の実績を有すること。

さらに、委託先が情報セキュリティ対策の遂行能力に関して一定の水準にあることを求めるために、その指標として「9.2.2 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」の内容を選定基準に加えることもできる。

(2) 委託先の選定手続の整備

整備する委託先の選定手続には、次の事項を含める。

① 選定基準を調達仕様として提示する。(「9.2.3 委託先に実施させる情報セキュリティ対策等の内容の周知」を参照。)

② 調達仕様として提示した選定基準に基づき委託先を選定する。(「9.2.6 委託

先の選定における手続の遵守」を参照。）

9.2.2 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

政府機関統一基準　　6.1.2 外部委託 (1) (c) 統括情報セキュリティ責任者は、委託先の選定基準策定に当たって、その厳格性向上のために、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方法を整備すること。【強化遵守事項】

委託先の選定基準の策定に当たり、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方法を整備することを求める事項である。

「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方法」としては、以下の制度を活用することが考えられる。

(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（認証機関）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」（平成 19 年 8 月改訂）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/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として提供している。

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認証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、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既に実施した情報セキュリティ監査の結果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外部委託しており、情報セキュリティ監査を実施している場合

② 直近において実施した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

9.2.3 委託先に実施させる情報セキュリティ対策等の内容の周知

政府機関統一基準　　6.1.2 外部委託

(2) (a) 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定め、委託先候補に事前に周知すること。【基本遵守事項】

情報処理業務を外部委託により行う場合に、委託先に実施させる情報セキュリティ対策等の内容を整備し、委託先候補に事前に周知することを求める事項である。

委託先に実施させ、事前に周知する事項としては一般に以下のものが考えられるが、案件ごとに該当する情報セキュリティ対策等を判断する必要がある。各事項の説明は、「9.3.1 外部委託に係る契約」を参照されたい。

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)再請負に関する事項	○	△	△	△	△	△	△	○	△
(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（9.2.2 項）	△	△	△	△	△	△	△	△	△

○：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、又は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、事前に周知する事項は案件ごとに判断すること。

「委託先候補に事前に周知する」方法としては、調達仕様に記載することが想定される。

9.2.4　情報セキュリティが侵害された場合の対処手順の整備と周知

政府機関統一基準　　6.1.2 外部委託
(2) (b) 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を整備し、委託先候補に事前に周知すること。【基本遵守事項】

委託先に行わせる業務において万一情報セキュリティの侵害が発生した場合にも、これに迅速かつ適切に対応するために、対処手順をあらかじめ整備し、これを委託先候補に事前に周知することを求める事項である。

情報セキュリティが侵害される場合は、次の 2 種類に大別される。

(1) 委託先の者がその業務の遂行において情報セキュリティを侵害する場合
情報セキュリティの侵害としては、例えば、次に挙げる事態が考えられる。

① 委託先に受け渡し、又は委託先によるアクセスを認める府省庁の情報の外部への漏えい及び目的外利用

② 委託先の者による府省庁のその他の情報へのアクセス

③ 構築を外部委託する情報システム以外の府省庁の情報システムに対するアクセスや情報セキュリティ侵害

(2) 委託元及び委託先以外の者により情報セキュリティが侵害される場合

例えば、次に挙げる事態が考えられる。

① 運用を外部委託した情報システムに関して、不正アクセス、不正プログラム等による外部からの情報セキュリティ侵害

② データセンター又はハウジングサービスの利用において、安全区域への物理的侵入、通信回線の異常による通信途絶等

情報セキュリティが侵害された場合の対処手順として、委託元と委託先の双方の連絡先、連絡方法及び責任体制をあらかじめ定めておくことが考えられる。

「委託先候補に事前に周知する」方法としては、調達仕様に記載することが想定される。周知する内容は、連絡先、連絡方法及び責任体制の整備を求めること、並びに情報セキュリティが侵害された場合に、速やかにこれを委託元へ報告することを求めることが考えられる。

9.2.5 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周知

政府機関統一基準　　6.1.2 外部委託

(2) (c) 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を確認するための方法及び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を整備し、委託先候補に事前に周知すること。【基本遵守事項】

委託先に行わせる業務において情報セキュリティ対策が確実になされることを目的として、その履行状況を確認するための方法及び履行が不十分である場合の対処方法を整備し、委託先候補に事前に周知することを求める事項である。

履行状況を確認するための方法としては、「9.2.3 委託先に実施させる情報セキュリティ対策等の内容の周知」の表に示す情報セキュリティ対策（表の(1)～(7)）のうち確認する事項を定め、これを適宜又は定期的に報告させることが考えられる。

履行が不十分である場合の対処方法としては、委託先及び委託元が改善について協議を行い、合意した対応を委託先にとらせること等が考えられる。

「委託先候補に事前に周知する」方法としては、調達仕様に記載することが想定される。

9.2.6 委託先の選定における手続の遵守

政府機関統一基準　　6.1.2 外部委託
(3) (a) 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、選定基準及び選定手続に基づき、委託先を選定すること。
【基本遵守事項】

委託先の選定を、(1)(b)に従い統括情報セキュリティ責任者が整備している選定基準及び選定手続に基づき行うことを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に求める事項である。

9.2.7 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に基づく委託先の選定

政府機関統一基準　　6.1.2 外部委託
(3) (b) 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、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方法に従って、委託先の候補者の情報セキュリティ水準を確認し、委託先の選定における一要素として利用すること。
【強化遵守事項】

委託先の情報セキュリティ水準の評価方法を(1)(c)に従い統括情報セキュリティ責任者が整備した場合に、これを委託先の選定基準の一要素として利用することを求める事項である。

(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の利用

委託先の候補者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か否かを、委託先の選定における評価に加味す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認証機関による認証は事業者において構築された情報セキュリティマネジメントシステムについて基準への適合性を評価するものであることから、「9.2.3 委託先に実施させる情報セキュリティ対策等の内容の周知に示す情報セキュリティ対策のうち、「(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」及び「(7) 情報セキュリティが侵害された場合の対処」を客観的に評価する指標として参考にできる。また、「(3) セキュリティ機能の装備」その他の情報セキュリティ対策についても、そ

のための手順（プロセス）の策定とその実施に関して確認することができる。

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を委託先の選定基準の一要素として利用する場合には、外部委託する情報処理業務が当該認証の登録範囲及び適用範囲に合致することを確認する必要がある。認証においては、事業者が特定する「登録範囲（適用範囲）」と呼ぶ業務の範囲について基準への適合性が評価される。このため、府省庁が外部委託する予定の業務を、認証を取得している範囲において実施する予定であることを確認する。例えば、ある事業者がデータセンターにおける顧客の情報システムの運用に関して認証を取得していても、その認証取得は、当該事業者の別の部門にソフトウェアの開発を外部委託する場合の適合性評価には関係しない。

JIPDEC による ISMS 適合性評価制度の利用方法の詳細については、「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）を参照されたい。

(2) 情報セキュリティ対策ベンチマークの利用

委託先の候補者による情報セキュリティ対策ベンチマークの実施結果を、委託先の選定における評価に加味することが考えられる。

ベンチマークの実施結果は、25 項目の質問ごとに 5 段階評価で表されるが、項目により異なる重み付けをする等、評価方法を委託元で独自に定めることもできる。ただし、この制度は自己評価によるものであり、実施結果を利用する際に、その客観性については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の利用方法の詳細については、「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）を参照されたい。

(3) 情報セキュリティ監査の利用

将来的には、既に実施した情報セキュリティ監査の結果を委託先の選定における評価に加味することが考えられる。

この場合は、監査結果報告書の写を提示させ、これを査閲して、監査対象の範囲及び管理目的が、委託する情報処理業務に合致することを確認する必要がある。

情報セキュリティ監査の利用方法の詳細については、「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）を参照されたい。

9.3 契約に関する遵守事項

情報処理業務の外部委託に関して、契約に含めるべき事項及び委託元の義務を、政府機関統一基準において遵守事項として定めている。

9.3.1 外部委託に係る契約

政府機関統一基準　　6.1.2 外部委託

(4) (a) 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、外部委託を実施する際に、委託先に請け負わせる業務における情報セキュリティ対策、機密保持（情報の目的外利用の禁止を含む。）、情報セキュリティの侵害発生時の対処方法、情報セキュリティ対策の履行状況の確認方法及び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を含む外部委託に伴う契約を取り交わすこと。また、必要に応じて、以下の事項を当該契約に含めること。
(ア)情報セキュリティ監査の受入れ
(イ)サービスレベルの保証
【基本遵守事項】

情報処理業務を外部委託により行わせるに当たり、情報セキュリティ確保のための事項を委託先に確実に行わせるために、これを契約に含めることを求める事項である。契約に含める事項は、調達仕様に記載した事項を含み、これを具体化するものである。

「契約」とは、その形式を契約書に限ることなく、覚書その他契約としての効果を持つものを含む。

契約に含めるべき事項の目安は、次のとおりである。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、外部委託の案件ごとに契約に含める事項とその内容を定める必要がある。

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。

(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を目的として委託先に(2)～(13)の対策を行わせるために、体制を整備し、これを報告することを契約において求める。報告する体制には、情報セキュリティの確保に関する責任者を含めさせること。また、当該責任者は、情報セキュリティの確保について実質的に責任を持つ者であって、委託先の契約者とは異なる場合が多いことに留意すること。

(2) 取り扱う府省庁の情報の秘密保持等

委託元から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について、機密性、完全性、可用性の確保と目的外利用の防止を契約において求める。外部委託する業務を行わせるために情報を提供する場合だけでなく、例えば情報システムの運用の外部委託において府省庁内に持つ情報へのアクセスを認める場合にも本事項を求めること。

外部委託に係る契約において委託元及び委託先の双方に秘密保持を求めることは一般に行われているが、これで十分であるとは限らない。完全性又は可用性の要件があれば、当該要件を契約に含める必要がある。また、情報の目的外利用の禁止も一般的に求められる事項であり、必要性を確認した上で、≪双務的に≫契約に含めること。

これらの目的を達成するために、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。
- 当該情報については、当該外部委託の終了時に、委託元への返却又は廃棄若しくは抹消を確実に行うこと。

(3) セキュリティ機能の装備

情報システムの構築等を外部委託する場合に、当該情報システム等にセキュリティ機能を装備すべきことを契約において求める。セキュリティ機能には、次の例がある。

- 情報システム等の利用に関する主体認証機能、アクセス制御機能及び権限管理機能
- 情報システムに関する証跡管理機能
- 情報の機密性を確保するための暗号化
- 情報システムへの不正アクセスに対抗するネットワーク構成
- 情報システムにおける不正プログラム対策
- 情報システムを構成する機器及びソフトウェアの設定による情報セキュリティ対策の強化
- 情報システムの稼働状態、セキュリティ侵害等を監視するための機能
- 情報システムの可用性を確保するための機器、通信回線等の冗長化

セキュリティ機能の装備を求める場合、次の方法があり、案件ごとに適切な方法を選択することとなる。

① 委託元よりセキュリティ要求仕様を示し、装備すべきセキュリティ機能の設計及び実装を委託先に行わせる。

② セキュリティ要求仕様及び装備すべきセキュリティ機能を委託元で定め、これを委託先に実装させる。

いずれの場合にも、セキュリティ要求仕様及びセキュリティ機能は、情報システムの構築等を行う過程で明確化されていく例が見られるため、委託元及び委託先は、装備すべきセキュリティ機能を調達仕様及び契約又はその付属文書に記述するだけでなく、その内容について必要に応じて協議を行うことが求められる。

委託元から提示するセキュリティ要求仕様の策定方法については、『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、2007 年 11 月）をあわせて参照されたい。なお、この解説書においては、調達時に構築・開発する情報システム又はソフトウェアの仕様が比較的詳細に定まっており、セキュリティ要求仕様もそれに応じて詳細に提示する場合の指針を示している。

セキュリティ機能の装備について客観性の高い評価・確認を行いたい場合には、セキュリティ設計仕様書（ST：Security Target）に関する ST 評価・ST 確認を受けることを委託先求めることもできる（「9.6.1 ST 評価・ST 確認」を参照）。

ST 評価・ST 確認の利用については、『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）をあわせて参照されたい。

(4) 運用・保守・点検における情報セキュリティ対策の実施

情報システムの運用・保守・点検を外部委託する場合に、運用・保守・点検における情報セキュリティ対策の実施をあわせて契約において求める。例えば、運用における情報セキュリティ対策としては、利用者管理（主体認証情報の付与、削除）、情報セキュリティ監視、情報のバックアップの取得、監査証跡に関する運用操作等の実施等がある。

(5) 脆弱性対策の実施

委託先に行わせる脆弱性対策の範囲を明確にし、その実施を契約において求める。

一般に、脆弱性対策は、対象とするソフトウェア、機器等の範囲を定めた上で、次の手順で実施する。

① 公表される脆弱性情報を把握する。[2]
② 公表された脆弱性情報の当該情報システム等への影響を調査・評価する。
③ 当該脆弱性に対するセキュリティパッチの提供有無及びベンダーが提示する対処を把握する。
④ 当該脆弱性への対応方法を定める。
⑤ 当該脆弱性への対応を実施する。

情報システムの構築等の外部委託においては、一般に、上記の各手順を委託先に行わせることになる。ただし、④については、受容するリスクに基づく判断が必要であることから、委託元も判断に加わるか、あるいは、委託先に判断させてその結果を納

[2] 脆弱性情報の把握に当たり、ソフトウェア及びハードウェアの製造・提供元、JPCERT コーディネーションセンター等のセキュリティ関連機関から公表される情報を入手することとなる。

品・検収時に報告させることで足りるとするかを定めておく必要がある。

情報システムの運用・保守・点検の外部委託においては、脆弱性対策の実施を外部委託する業務に含めるか否かを明確にする必要がある。外部委託する業務に含める場合には、上記の各手順を定常的に委託先に行わせる。ただし、④について委託元も判断に加わるかどうかの選択があることは、情報システムの構築等の場合と同様である。脆弱性対策の実施を外部委託する業務に含めない場合には、これを委託元が自ら行うか、別の事業者に外部委託して行わせることになる。

(6) 外部委託する業務以外の情報資産の保全

委託先に庁舎内で業務を行わせる等、委託先が府省庁の他の情報資産にアクセスし得る環境で業務を行わせる場合に、当該他の情報資産へのアクセスの禁止及びその保全は委託先が当然守るべき事項である。そこで、委託先による当該他の情報資産へのアクセスの禁止及び保全を契約において明示的に求めることも考えられる。

(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

外部委託する業務に関して確保すべき情報セキュリティ対策のサービスレベルを、契約において求めることもできる。

一般に、サービスレベルは継続的な業務である情報システムの運用・保守・点検に関する管理指標であり、情報セキュリティ対策のサービスレベルについても同様である。指標として、次の例がある。

① 当該情報システムの稼働率等、可用性に関する目標

② 脆弱性情報に関して、その公表から対応策の決定及び実施までの期間の目標

情報セキュリティ対策のサービスレベルは、情報システム全体に関するサービスレベルを設定する場合に、その一部として委託先と合意し、設定することが考えられる。

(8) 情報セキュリティが侵害された場合の対処

「情報セキュリティが侵害された場合」を具体的に示し、これに該当する場合には速やかに委託元へ報告することを契約において求める。また、不正アクセス、サービス不能攻撃、不正プログラムの感染等、短時間で被害が拡大する情報セキュリティ侵害については、緊急時対策を委託先に行わせること、あるいは委託元及び委託先が共同で行うことも考えられる。これらの前提として、報告の体制及び連絡方法も契約において定める。

「情報セキュリティが侵害された場合」の具体例は、次のとおりである。

① 情報システムの構築等の場合

- 委託先に提供した情報の漏えい及び目的外利用

- 外部委託した業務以外の情報への委託先によるアクセス

② 情報システムの運用・保守・点検の場合

- 委託先に提供した情報の漏えい及び目的外利用
- 外部委託した業務以外の情報への委託先によるアクセス
- 委託元、委託先又は外部の者による情報システムからの情報漏えい及び目的外利用
- 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

③ 情報の加工・処理等の場合

- 委託先に提供した情報の漏えい及び目的外利用
- 委託先で作成した情報の漏えい及び目的外利用

④ 情報の保存・運搬の場合

- 委託先に取り扱わせた情報の漏えい及び毀損

(9) 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（上記(1)～(8)の各事項。）の履行状況の確認について、その内容及び方法を契約において定める。

確認の方法としては、外部委託する案件によらず、業務における定常的な確認を実施する必要がある。また、これに加え、委託する情報処理業務及び取り扱わせる情報の重要性等を踏まえ、必要に応じて情報セキュリティ監査を実施することとなる。

① 業務における定常的な確認

外部委託する案件毎に、業務の実施状況について定例的に報告を受ける機会を活用する等により、あらかじめ定めた時期又は頻度で、契約において実施を求めた情報セキュリティ対策の履行状況を報告させるとともに、課題への対処について十分に協議する。この場合、契約の内容を具体化した確認事項をあらかじめ委託元において策定する等により、実務に即して履行状況を確認し、対応を協議することとなる。例えば、以下の方法がある。

- 情報システムの構築を外部委託する場合には、通常の業務管理として、定例的に、又は工程ごとに、進捗管理、品質管理等を目的として委託先から業務報告をさせるだけでなく、情報セキュリティ対策についても、契約で履行を求めた事項の実施状況を具体的に報告させる。例えば、委託先との間での情報の受渡し・返却の実績及び受け渡した情報の管理状況を確認する。また、情報システムの設計及び実装のそれぞれの工程において、業務仕様等の設計及び実装について確認を行うだけでなく、情報セキュリティ

機能の設計及び実装についても、要求仕様を満足する根拠等を含めて具体的に報告を受ける。

- 情報システムの運用及び保守をオンサイトサービスとして委託先に行わせる場合には、通常、運用・保守の実績と課題に関して定例報告を行わせることとなるが、この場において、情報セキュリティ対策についても、契約で求めた事項を報告させる。例えば、当該期間における脆弱性対策（セキュリティ修正の適用、代替策の適用等）の実績を報告させる。

② 情報セキュリティ監査による確認

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当たり、必要に応じて、委託先が情報セキュリティ監査を受け入れることを契約に含め、情報セキュリティ監査を行うこと。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[3]。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

以上を踏まえ、統括情報セキュリティ責任者は、情報セキュリティ監査の必要性を判断するための指針又は例示等を規程に含めること。

なお、短期間又は小規模な情報処理業務の外部委託であって情報セキュリティに関する懸念が少ないと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判断する場合には、「9.5 納品・検収に関する遵守事項」に従い外部委託終了時の確認は行うが、外部委託する情報処理業務の実施中の確認は不要とすることも考えられる。また、情報の保存・運搬を外部委託により行う場合には、必要に応じて、業務の実態に即して情報セキュリティ対策の履行状況の確認を行うこととなる。

(10)情報セキュリティ監査の実施

委託先の情報セキュリティ対策の履行状況について、業務における定常的な確認に加えて情報セキュリティ監査により確認する場合には、実施する情報セキュリティ監

[3] 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、情報セキュリティ監査の必要性及び実施可能性を考慮し、実施について判断すること。

査の目的、対象範囲（上記(1)～(8)のうちで対象とする事項）、管理基準、実施主体等について、委託先と協議の上で契約において具体的に定めなければならない。これらの要求仕様は、調達の段階において、調達仕様に「監査仕様書」を添付する等により委託先候補に対して提示し、委託先候補が「監査対応計画書」等により確認したものである。

監査の実施に当たっては、契約の範囲内で、委託先との間で合意した手続に従い確認していくこととなる。

なお、管理基準については、一般的な情報セキュリティ管理策の典型として、「情報セキュリティ監査制度」で定める情報セキュリティ管理基準（経済産業省告示）を利用することも考えられる。

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

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

情報セキュリティ監査の実施手順については、「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）を参照されたい。

(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

「(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」の結果、又は情報セキュリティ事故の発生等を契機として、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認識した場合には、委託元及び委託先が協議した上で必要な是正措置を採らせること等を契約において求めることが考えられる。

(12)確認書等に委任する事項

「9.3.2 外部委託に係る確認書等」に記述する確認書等を委託先から受領する予定がある場合には、確認書等に委任する事項を契約に明記しておくこと。確認書等に記述する内容に関して別途協議を行う際に、その根拠についてあらかじめ合意しておくためである。

(13)再請負に関する事項

委託先が情報処理業務を他の事業者に行わせる再請負に関する事項を、契約において定める。その内容は、例えば次のとおりである。ただし、委託先がその請負内容の全部又は一部を第三者に再請負させることは原則として禁止されることに留意すること（「9.3.5 再請負の原則禁止」を参照されたい。）。

① 再請負を禁止する場合は、その旨

② 再請負を認める場合は、以下の事項

- 再請負を認める条件及び許可手続
- 再請負を許可した場合に委託先に求める事項
  - ○ 再請負先における情報セキュリティ対策水準を確保するために委託先に求める施策
  - ○ 当該施策の実施状況に関する委託元への報告

9.3.2 外部委託に係る確認書等

政府機関統一基準　　6.1.2 外部委託

(4) (b) 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、外部委託に係る契約者双方の責任の明確化と合意の形成を行い、委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書等を提出させること。また、必要に応じて、以下の事項を当該確認書等に含めさせること。

(ア)当該委託業務に携わる者の特定

(イ)遵守すべき情報セキュリティ対策を実現するために、当該者が実施する具体的な取組内容

【基本遵守事項】

委託先に情報処理業務を行わせる場合には、委託元及び委託先双方の責任を契約において定める。加えて、その履行において求める事項は、契約の下で双方が協議を行い、これを具体化する。具体化した事項は、確認書等として委託先の責任者から提出させ、あるいは、契約書の付属書とする。例えば、以下の例が考えられる。

(1) 委託先において当該業務を行う体制及び者
委託元から提供する情報を取り扱う者を明らかにする目的で、当該業務を行う体制及び者を確認書等に記載して報告させる。

(2) 委託先における情報の管理
委託元から提供する情報を委託先において管理する方法を確認書等に記載して報告させる。当該業務を行う者以外の者に当該情報にアクセスをさせないための施策、及び当該業務を行う者が目的外に当該情報を使用しないための施策に関して報告を求めることが考えられる。

(3) 構築する情報システムに装備すべきセキュリティ機能
情報システムにおいて装備すべきセキュリティ機能については、その要求事項を調達仕様で示すとともに契約で定めるが、機能の詳細及び実装方法については、委託先が提示した当該情報システムの構成製品及び構築技術に応じて委託先及び委託元が協議をして合意し、その結果を記載した確認書等又は契約の付属書を作成することが考えられる。

なお、政府機関統一基準の本事項で求める内容が契約に含まれていると判断される

場合には、確認書等は省略してよい。

9.3.3 外部委託の継続における注意

政府機関統一基準　　6.1.2 外部委託

(4) (c) 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、外部委託契約の継続に関しては、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。【基本遵守事項】

政府機関統一基準「6.1.2 外部委託」の (3) (a) において、整備されている選定基準及び選定手続に基づき委託先を選定すること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に求めている。この求めが、外部委託による情報処理業務の実施を終了し、後続の業務も外部委託により行う場合にも、当然に適用されることを確認している事項である。

外部委託契約の継続には、例えば次のような場合がある。

(1) 情報システムの構築のうち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

(2) 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

(3) 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

これらの場合に、情報セキュリティの要件としても、その都度委託先を審査し、安易な随意契約の継続は避けなければならない。

9.3.4 外部委託における実施内容の変更に関する注意

政府機関統一基準　　6.1.2 外部委託

(4) (d) 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、委託先の提供するサービス（情報セキュリティ基本方針、実施手順、管理策の維持及び改善を含む。）の変更に関しては、選定基準及び選定手続に基づき、その是非を審査すること。【基本遵守事項】

情報処理業務を外部委託により行うに当たり、提供するサービス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、その是非を審査すること

を求める事項である。

委託先の提供するサービスとは、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である。委託先がその変更を希望する場合には、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、変更の是非を審査する必要がある。

9.3.5 再請負の原則禁止

政府機関統一基準　　6.1.2 外部委託

(4) (e) 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、委託先がその請負内容の全部又は一部を第三者に再請負させることを禁止すること。ただし、委託先からの申請を受け、再請負させ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措置が担保されると判断する場合は、その限りでない。
【基本遵守事項】

外部委託した業務の全部又は一部を他の事業者に再請負により行わせることは、委託元の管理が直接には及ばない状況において情報処理業務を行わせることであり、委託先に情報処理業務を行わせる場合に比べ脅威が増大する一方で対策は困難になる傾向があることにかんがみ、再請負を原則として禁止する事項である。

ただし、再請負させ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措置が担保されると判断する場合には、再請負により業務を行わせることができる。「情報セキュリティが十分に確保される」とは、再請負により業務を行わせるときの情報セキュリティ水準が、委託先が行う場合の水準と同等であることをいう。このためには、委託先に求めるものと同等の水準の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、委託元と委託先の契約において定める必要がある。

委託先が再請負により情報処理業務を行うことを特に望む場合には、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、情報処理業務の内容を具体的に検討して再請負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。

(1) 再請負を行うことに合理的な理由が認められること

情報処理業務の一部を再請負により行うことについて合理的な理由が認められること。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実施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。

(2) 同等の情報セキュリティ水準が確保できること

再請負において情報セキュリティを確保するための措置につき委託先に説明を求

め、当該措置が情報処理業務及び取り扱わせる情報にかんがみ実効性のあるものと認められること。

なお、再請負先に行わせる内容に応じて、委託先自体が実施する場合に求めるべき水準と同等の水準の情報セキュリティ対策が再請負先の事業者において確保できることが、再請負を認める条件となる。

9.4 委託先における情報処理業務実施中の遵守事項

委託先における情報処理業務の実施中の委託元の遵守事項を、政府機関統一基準で定めている。

9.4.1 提供する情報の取扱い

> 政府機関統一基準　　6.1.2 外部委託
> (5) (a) 行政事務従事者は、委託先に要保護情報又は重要な設計書を提供する場合、提供する情報を必要最小限とし、以下の措置を講ずること。
> (ア)委託先に情報を提供する場合は、安全な受渡方法によりこれを実施し、提供した記録を取得すること。
> (イ)外部委託の業務終了等により提供した情報が委託先において不要になった場合には、これを確実に返却させ、又は廃棄させ、若しくは抹消させること。
> 【基本遵守事項】

委託先に提供する府省庁の情報について、漏えい防止のための措置を採ることを府省庁の行政事務従事者に求める事項である。

情報処理業務を外部委託により行う場合であって、当該業務に関する文書及び情報、情報システムに関する仕様書及び試験用データその他要保護情報を委託先に提供するときは、当該提供を安全な方法により行い、その記録を残すべきこと、及び外部委託により行う業務の終了時には当該情報を確実に返却又は廃棄、若しくは抹消させることが必要である。このうち、委託先において当該情報を廃棄又は抹消させる場合には、これが確実に行われたことを確認するために、委託先の責任者に廃棄又は抹消したことの報告を書面で提出させる。

なお、政府機関統一基準において、外部委託に限らず一般的な情報の提供に関する項に「3.2.5 情報の提供」がある。この項では、機密性２情報及び機密性３情報を府省庁外の者に提供する場合には、それぞれ課室情報セキュリティ責任者に届け出ること及び課室情報セキュリティ責任者の許可を得ることを求めている。≪外部委託において委託先に情報を提供する場合には、当該委託に関して責任を持つ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への届出・許可手続を経た上で、

その後の情報の返却又は廃棄若しくは抹消を確認することも含めて、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本事項（6.1.2 (5)(a)）に従い情報の提供に係る管理を行う。≫

9.4.2　情報セキュリティ侵害が発生した場合の措置

政府機関統一基準　　6.1.2 外部委託
(5) (b) 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、請け負わせた業務の実施において情報セキュリティの侵害が発生した場合に、定められた対処方法に従い、委託先に必要な措置を講じさせること。
【基本遵守事項】

委託先における情報処理業務の実施中に情報セキュリティ侵害が発生した場合に、「9.3.1 外部委託に係る契約」の「(8) 情報セキュリティが侵害された場合の対処」に従い、委託先に必要な措置を講じさせることを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に求める事項である。

9.4.3　情報セキュリティ対策の履行状況の確認

政府機関統一基準　　6.1.2 外部委託
(5) (c) 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、定められた方法に従い、委託先における情報セキュリティ対策の履行状況を確認すること。
【基本遵守事項】

委託先における情報処理業務の実施中に、「9.3.1 外部委託に係る契約」の「(9) 情報セキュリティ対策の履行状況の確認」に従い、(1)～(8)の情報セキュリティ対策の履行状況を契約で定めた内容及び方法により確認する。確認の方法として、契約で合意した「(10) 情報セキュリティ監査の実施」に従う監査を含める場合もある。そして、履行状況の確認の結果に基づき、必要に応じ、「(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」を実施する。

9.5　納品・検収に関する遵守事項

委託先における情報処理業務を終了し検収を行う際の遵守事項を、政府機関統一基準で定めている。

政府機関統一基準　　6.1.2 外部委託

(6) (a) 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、委託先に請け負わせた業務において行われた情報セキュリティ対策を確認し、その結果を納品検査における確認の判断に加えること。

【基本遵守事項】

委託先に行わせた情報処理業務の終了時に、契約及び確認書等において委託先に求めた情報セキュリティ対策の実施について確認し、その結果を納品検査における判断に加えることを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に求める事項である。求めた情報セキュリティ対策が適切に行われていれば、この点においては当該業務が契約に適合して行われたものと判断できる。確認する情報セキュリティ対策としては、「9.3.1 外部委託に係る契約」及び「9.3.2 外部委託に係る確認書等」で挙げた対策があり、重要性を判断して選択することができる。

確認を行うために委託先による報告が必要であれば、当該報告を求めることもあらかじめ契約で定めておく。

以下に挙げる対策は、外部委託の終了時に確認する必要性が高いものと考えられる。

(1) 情報システムの構築等におけるセキュリティ機能の装備及び脆弱性対策

情報システムの構築等を外部委託した場合には、当該業務において情報セキュリティ対策が適切に行われていることがその後の運用における情報セキュリティを確保する前提となる。例えば、契約において求めたセキュリティ機能が装備されていなければ、これが当該情報システムの運用において情報セキュリティ侵害を許す環境となり得る。

また、契約において求めた脆弱性対策が行われていなければ、これが当該情報システムの運用において不正侵入等の情報セキュリティ侵害を受ける原因の一つとなり得る。委託先が行った脆弱性対策を確認するために、委託先には、契約及び確認書等において脆弱性対策を実施することとしたソフトウェア製品及び機器等に関して次の事項を文書で提示させる必要がある。

① 動作条件・動作環境・機能選択等を定めるために選択、付与等をしたパラメータの値（情報セキュリティに関連する本情報は、構築・開発した情報システムの構成説明文書等に含めることも考えられる。）

② 公開されている脆弱性情報

③ 脆弱性情報への対処（セキュリティ修正の適用、代替策・回避策の適用、対策実施せず、等）

④　脆弱性情報への対処に関して、安全性、注意事項等の説明

情報システムの構築等の委託先とは別の事業者に、当該情報システムの運用を外部委託する場合がある。この場合には、情報システムの構築等におけるセキュリティ機能の装備及び脆弱性対策に関して受領した報告を、運用を外部委託する事業者への説明に使用することができる。

(2) 情報システムの運用・保守・点検における脆弱性対策

情報システムの運用、保守又は点検を脆弱性対策の実施を含めて外部委託した場合に、当該外部委託の期間に委託先が行った脆弱性対策の実績を報告させることが考えられる。

(3) 再請負を認めた場合に委託先が行った措置

再請負を認めた場合に、再請負先における情報セキュリティ水準を確保するために契約において委託先に求めた措置について、その実績を報告させることが考えられる。報告の内容は、例えば、委託先が再請負先に実施を求めた情報セキュリティ対策と、再請負先における当該対策の実施状況とすることが想定される。

9.6 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

9.6.1 ST 評価・ST 確認

政府機関統一基準において、情報システムの構築及びソフトウェアの開発に関して「セキュリティ設計仕様書の ST 評価・ST 確認」を求める次の二つの事項がある。

> 政府機関統一基準　　4.3.1 情報システムのセキュリティ要件
> (1) (d) 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た場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価・ST 確認を受けること。ただし、情報システムを更改し、又は構築中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書におい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、この限りでない。【基本遵守事項】

> 政府機関統一基準　　6.1.3 ソフトウェア開発
> (3) (e) 情報システムセキュリティ責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価・ST 確認を受けること。ただし、当該ソフトウェアを要素として含む情報システムについてセキュリティ設計仕様書の ST 評価・ST 確認を受ける場合、又はソフトウェアを更改し、若しくは開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書におい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、この限りでない。
> 【基本遵守事項】

情報システムの構築及びソフトウェアの開発において、当該情報システム又はソフトウェアに重要なセキュリティ要件がある場合には、ISO/IEC 15408 に基づきセキュリティ設計仕様書を策定し、その ST 評価・ST 確認を受けることを求める事項である。本事項は、府省庁が自ら情報システムの構築又はソフトウェアの開発を行う場合には、府省庁が第三者機関に依頼して ST 評価・ST 確認を受けることを想定している。

外部委託により情報システムの構築又はソフトウェアの開発を行う場合には、通常は ST 評価・ST 確認を受ける業務もあわせて外部委託することとなることから、委託元及び委託先に以下の対応が求められる。

(1) 委託元は、外部委託により行う情報システムの構築又はソフトウェアの開発において ST 評価・ST 確認を受けることを求める要求仕様を明確かつ適切に定め、調達仕様においてこれを委託先候補に提示すること。

(2) 委託先は、提示された要求仕様に関して ST 評価・ST 確認を受けること。

(3) 委託先は、ST 評価・ST 確認を受けたことを示す確認書を、納品までに委託元に提示すること。

(4) 構築した情報システム又は開発したソフトウェアの納品までに第三者機関による ST 評価・ST 確認を受け、その確認書を提示することができないと見込まれる場合には、納品における ST 評価・ST 確認の扱いについて委託元及び委託先があらかじめ協議し、合意した内容を契約に含める必要がある。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。なお、これに該当する場合としては、設計の完了から納品までの期間が短い場合が挙げられる。また、ST 評価は第三者機関が行うため、これに要する期間を委託元及び委託先において確実には予測できない点にも留意する必要がある。

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）

9.6.2 製品に関する IT セキュリティ評価及び認証制度と外部委託の関係

政府機関統一基準において、情報システムの構築に関連して機器及びソフトウェアに対して「IT セキュリティ評価及び認証制度に基づく認証取得」を求める次の事項がある。

> 政府機関統一基準　　4.3.1 情報システムのセキュリティ要件
> (1) (g) 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については、重要なセキュリティ要件があると認めた場合には、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、当該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場合であって、その中に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がある場合には、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。【強化遵守事項】

構築する情報システムの構成要素として調達する機器及びソフトウェアの選択に当たり、採用候補製品が複数ある場合に、ISO/IEC 15408 に基づく 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を情報システムセキュリティ責任者に求める事項である。

本事項に基づき、外部委託により情報システムの構築を行う場合には、委託元に以下の対応が求められる。

(1) 機器及びソフトウェアに要求するセキュリティ機能の決定

委託元は、外部委託により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、情報システムを構成する、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) 機器及びソフトウェアの選択

情報システムの構築の委託先にかかわらずに情報システムを構成する機器及びソフトウェアを選定することができる場合であって、前項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情報システムの構成要素として選択すること。

(3) ≪委託先の選定における機器及びソフトウェアの評価の考慮

情報システムの構築の委託先を選定することにより、製品として調達する機器及びソフトウェアが定まる場合には、本事項に従い製品の選択を行うことができない。この場合には、情報システムの構成要素として提案される機器又はソフトウェアが 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委託先の選定基準の要素として加味することとし、調達仕様において当該選定基準を委託先候補に提示することが考えられる。なお、構築する情報システムの種類及び提示する仕様の具体性によっては、構成要素とする機器及びソフトウェアの種類が調達の時点では必ずしも確定していないことも考えられる。この場合には、本認証取得を評価の要素として加味することは適切でない。また、当該情報システムの設計を完了していれば、その構成要素とこれらに求めるセキュリティ要件が明確にされていると考えられるため、その後の情報システムの実装を外部委託により行う場合に本項の委託先の選定基準が適用できると考えられる。≫

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ことについては、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、2007年11月）