DM6-08-071

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

2007 年 11 月

内閣官房情報セキュリティセンター

改訂履歴

改訂日	改訂理由
2006/6/16	初版
2006/9/1	説明補足及び誤記訂正
2007/11/9	政府機関統一基準(第２版)の策定に伴う修正等

本書は、2005 年度に独立行政法人情報処理推進機構に設置された「政府機関における機器等の購入ガイドラインに関する研究会」がとりまとめた「政府機関調達者向けセキュリティ要件活用ガイドブック」（2006 年 3 月）を元に、「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))」（2005 年 12 月 13 日情報セキュリティ政策会議決定）に関連する内容等を内閣官房情報セキュリティセンターにおいて加筆して作成したものである。

また、「政府機関の情報セキュリティ対策のための統一基準(第２版)」（2007 年 6 月 14 日情報セキュリティ政策会議決定）への改訂にあわせて本書も見直し、2007 年 11 月に改訂した。

本書の目的と内容

本書は、府省庁において情報システムの構築又はソフトウェアの開発（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に、「政府機関の情報セキュリティ対策のための統一基準(第２版)」の求める事項に従い、ST 評価・ST 確認等の適切な情報セキュリティ対策を実現するための実施手順を示す解説書である。

1 章では、情報システム及びソフトウェア（以下「情報システム等」という。）のセキュリティ要件、セキュリティ機能及び ST 評価・ST 確認等について、関連する政府機関統一基準の遵守事項及び「業務・システム最適化指針（ガイドライン）」との関係を説明する。

2 章では、調達者が、セキュリティ要件を具体化して調達仕様に含める「セキュリティ要求仕様」を作成し、提案者が作成する「セキュリティ提案仕様」を評価する手順の概要を説明する。また、この手順に関する詳細な解説書である「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」の活用方法を説明する。

3 章では、ST 評価・ST 確認の適用における留意事項を説明する。なお、本書は ST を作成するための解説書ではないことから、ST の作成については、「関連資料等」中の独立行政法人情報処理推進機構が公開している ST 関連資料の記述を参照されたい。

4 章では、情報システムを構成する機器及びソフトウェア製品（以下「機器等」という。）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の取得を調達手続における提案の評価に加える場合の留意事項を説明する。

本書の読者

本書は、次の者を対象とする。

- 府省庁において情報システムの構築等を外部委託により行う調達者

ここでいう調達者には、以下の者を含む。

１） 情報システムセキュリティ責任者： 情報システムにおける情報セキュリティ対策に関する事務を統括する者

２） 情報システムの構築等及びその調達に責任を持つ者

３） 調達を担当する部門の者

なお、省庁対策基準及びこれに基づき策定する各種実施手順においては、「政府機関の情報セキュリティ対策のための統一基準(第２版)」（NISD-K303-071）に基づき、上記１）の情報システムセキュリティ責任者に対して、情報システムの構築等の外部委託において本書で説明する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の実施を求めることとなる。本書では、情報システムに関する調達を適切に行うために、情報システムセキュリティ責任者のほかに、上記２）及び３）の者も読者に想定する。

関連資料等

- 「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」（DM6-07-071）

  内閣官房情報セキュリティセンター、2007 年 11 月

  本関連資料では、府省庁において情報システムの構築等を調達する場合に、適切な情報セキュリティ対策の実現を支援することを目的として、求めるセキュリティ要件を提案者に正確に伝えるとともに、応札において提示される提案仕様を的確に審査するための情報を提供している。

  本書においては、本関連資料を「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」とも記す。

- 「政府機関の情報セキュリティ対策のための統一基準(第２版)」
  （NISD-K303-071）

  内閣官房情報セキュリティセンター、2007 年 6 月 14 日

  以下、「政府機関統一基準」と記す。なお、政府機関統一基準の項目を、統 1.1.2(2) のように、「統」文字と政府機関統一基準の項目番号を示す場合がある。

- 「政府機関の情報セキュリティ対策のための統一基準(第２版) 解説書」
  （NISD-K303-071C）

  内閣官房情報セキュリティセンター、2007 年 6 月 14 日

  以下、「政府機関統一基準解説書」と記す。

- 政府機関統一基準に基づき府省庁において策定する省庁対策基準

- 省庁対策基準に基づき府省庁において策定する各種実施手順

  本書に関係する各種実施手順として、「情報システムにおける情報セキュリティ対策実施規程」「ソフトウェア開発における情報セキュリティ対策実施規程」「機器等の購入における情報セキュリティ対策実施規程」及び「外部委託における情報セキュリティ対策実施規程」又は府省庁で作成するこれらに相当するものがある。

- 「業務・システム最適化指針（ガイドライン）」

  各府省情報化統括責任者(CIO)連絡会議決定、2006 年(平成 18 年)3 月 31 日

  以下、「最適化ガイドライン」とも記す。

- 「ISO/IEC 15408: 2005　Information technology – Security techniques- Evaluation criteria for IT security -- Part 1, 2, 3」

  以下、「ISO/IEC 15408」と記す。

- 「Common Criteria for Information Technology Security Evaluation Version 2.3 -- Part 1, 2, 3」及び
  「Common Criteria for Information Technology Security Evaluation Version 3.1 -- Part 1, 2, 3」

  ISO/IEC 15408 は、Common Criteria for Information Technology Security Evaluation を採用した国際標準で、本資料の Version 2.3 と同等の内容となっ

ている。Common Criteria for Information Technology Security Evaluation を CC とも記す。

- IT セキュリティ評価及び認証制度

  機器等及びシステムにセキュリティ機能が実装されていることを ISO/IEC 15408 に基づき第三者が評価し、認証するための制度である。独立行政法人情報処理推進機構（IPA）が運営している。
  http://www.ipa.go.jp/security/jisec/index.html

目次

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

1.1.政府機関統一基準における要求事項

政府機関統一基準では、情報システムの構築等において適切なセキュリティ機能が装備されることを目的として、本節に挙げる遵守事項を定めている。構築する情報システムは、開発するソフトウェア、製品として購入するソフトウェア及び製品として購入する機器から構成されることから、情報システムに装備すべきセキュリティ機能は、これらの構成要素において適切に装備することが求められる。

1.1.1.情報システムのセキュリティ要件とセキュリティ機能に関する遵守事項

> 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) (b) 情報システムセキュリティ責任者は、情報システムのセキュリティ要件を決定すること。【基本遵守事項】

本遵守事項では、情報システムの計画・設計を行う際に、情報システムのセキュリティ要件を決定することを情報システムセキュリティ責任者に求めている。

> 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) (c) 情報システムセキュリティ責任者は、情報システムのセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムの構成要素についての対策について定めること。【基本遵守事項】

本遵守事項では、前事項 ((1)(b))で定めた情報システムのセキュリティ要件を満たすために、構成要素であるソフトウェア及び機器における情報セキュリティ対策を定めることを情報システムセキュリティ責任者に求めている。関連文書の「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」では、本遵守事項で求める手順を、組織的に行う方法の例を示している。

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) (f) 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】

本遵守事項では、情報システムの構成要素となる機器及びソフトウェアを選定する際に、要求するセキュリティ機能その他の要求条件を満たす製品に選択肢がある場合、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求めている。製品が求めるセキュリティ機能を持つことは、製品の提供者が示す仕様書や説明により知ることができる。さらに本遵守事項も適用し、セキュリティ要求仕様に対して適切なセキュリティ機能が装備されていることを第三者が確認している製品を選択することにより、セキュリティ機能の確実な装備を担保することができる。

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】

本遵守事項では、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場合には、セキュリティ機能が確実に実装されることを目的として、ISO/IEC

15408 に基づくセキュリティ設計仕様書（セキュリティターゲット、ST）について ST 評価・ST 確認を行うことを求めている。情報システムに重要なセキュリティ要件があるか否かについては、情報システムセキュリティ責任者が判断する。

1.1.2. ソフトウェアの開発におけるセキュリティ要件とセキュリティ機能に関する遵守事項

政府機関統一基準　　6.1.3 ソフトウェア開発
(3) (a) 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が運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果、及び当該ソフトウェアにおいて取り扱う情報の格付けに応じて、セキュリティ機能の必要性の有無を検討し、必要と認めたときは、セキュリティ機能を適切に設計し、設計書に明確に記述すること。【基本遵守事項】

本遵守事項では、ソフトウェアの開発を行う際に、セキュリティ機能を適切に設計し、設計書に明確に記述することを求めている。

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】

本遵守事項では、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、セキュリティ機能が確実に実装されることを目的として、ISO/IEC 15408 に基づくセキュリティ設計仕様書（セキュリティターゲット、ST）について ST 評価・ST 確認を行うことを求めている。そのソフトウェアに重要なセキュリティ要件があるか否かについては、情報システムセキュリティ責任者が判断する。

1.1.3.機器等の購入におけるセキュリティ要件とセキュリティ機能に関する遵守事項

政府機関統一基準　　6.1.1 機器等の購入
(1) (a) 統括情報セキュリティ責任者は、機器等の選定基準を整備すること。【基本遵守事項】

本遵守事項では、統括情報セキュリティ責任者に対して、情報セキュリティの観点から、機器等の選定基準を整備することを求めている。

政府機関統一基準　　6.1.1 機器等の購入
(2) (a) 情報システムセキュリティ責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の候補の選定における判断の一要素として活用すること。【基本遵守事項】

本遵守事項では、情報システムセキュリティ責任者に対して、前記(1) (a)に基づき定められた機器等の選定基準を、機器等の候補の選定において判断の一要素として活用することを求めている。

政府機関統一基準　　6.1.1 機器等の購入
(2) (d) 情報システムセキュリティ責任者は、機器等の購入において、満足すべきセキュリティ要件があり、それを実現するためのセキュリティ機能の要求仕様がある場合であって、総合評価落札方式により購入を行うときには、これについて、IT セキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用すること。【基本遵守事項】

本遵守事項では、機器等の購入において、示された条件の下で、機器等が IT セキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用することを求めている。

1.2.「業務・システム最適化指針（ガイドライン）」における工程

本書では、情報システムの構築等を外部委託により行うことを前提とする。また、情報システムの構築等は、「業務・システム最適化指針（ガイドライン）」（以下「最適化ガイドライン」という）で定められた工程及び仕様書に従うものとする。その工程と作成する主な仕様書を、図 1.1 に示す。

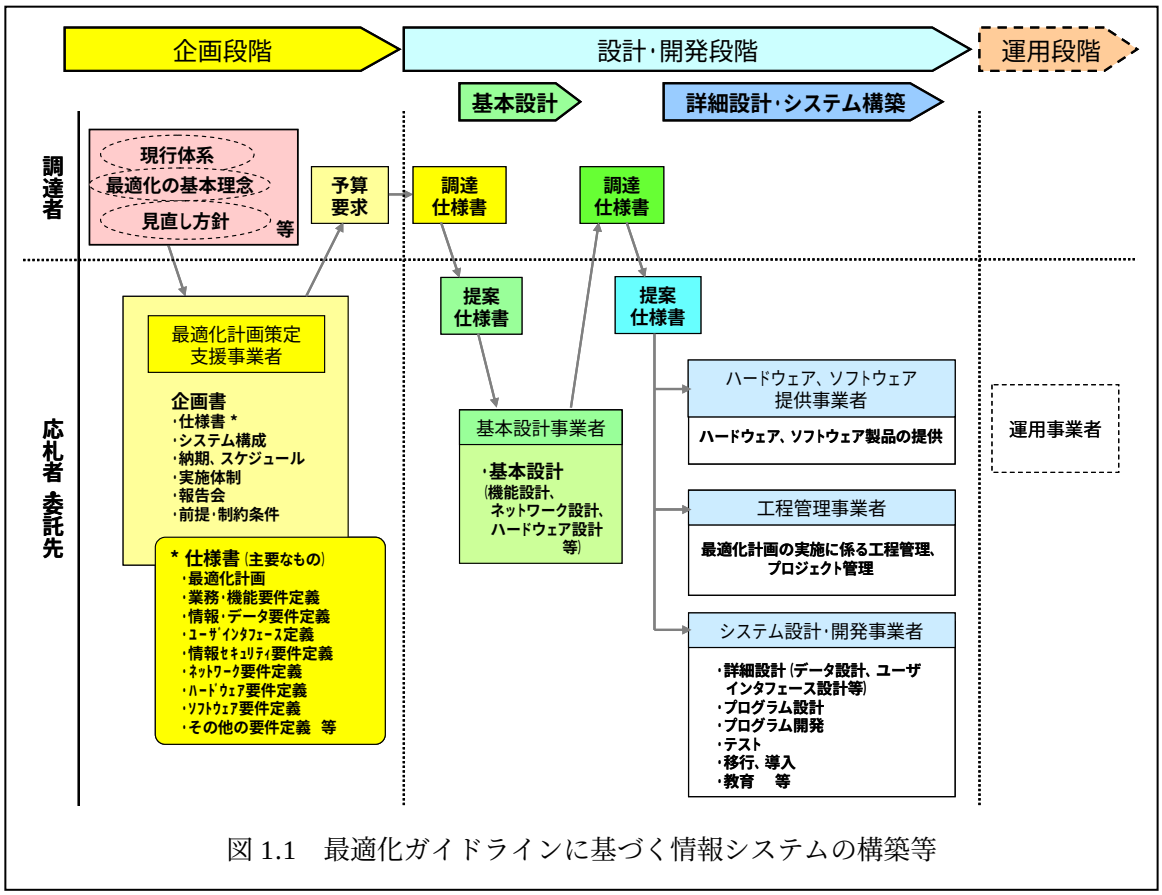

図 1.1　最適化ガイドラインに基づく情報システムの構築等

「最適化ガイドライン」で定める工程に沿って「1.1 政府機関統一基準における要求事項」で求められる事項を行う手順の例を、図 1.2 に示す。

調達者は、「セキュリティ要求仕様」を調達仕様書に含めて提示し、「セキュリティ提案仕様」を提案書に含めて提案させる。この手順については、本書の 2 章と、「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」で説明する。

セキュリティ提案仕様の妥当性について第三者による評価・確認を得る場合には、委託先に ST 評価・ST 確認の手続を行わせ、その結果を提出させる。この手順に関する留意事項については、本書の 3 章で説明する。

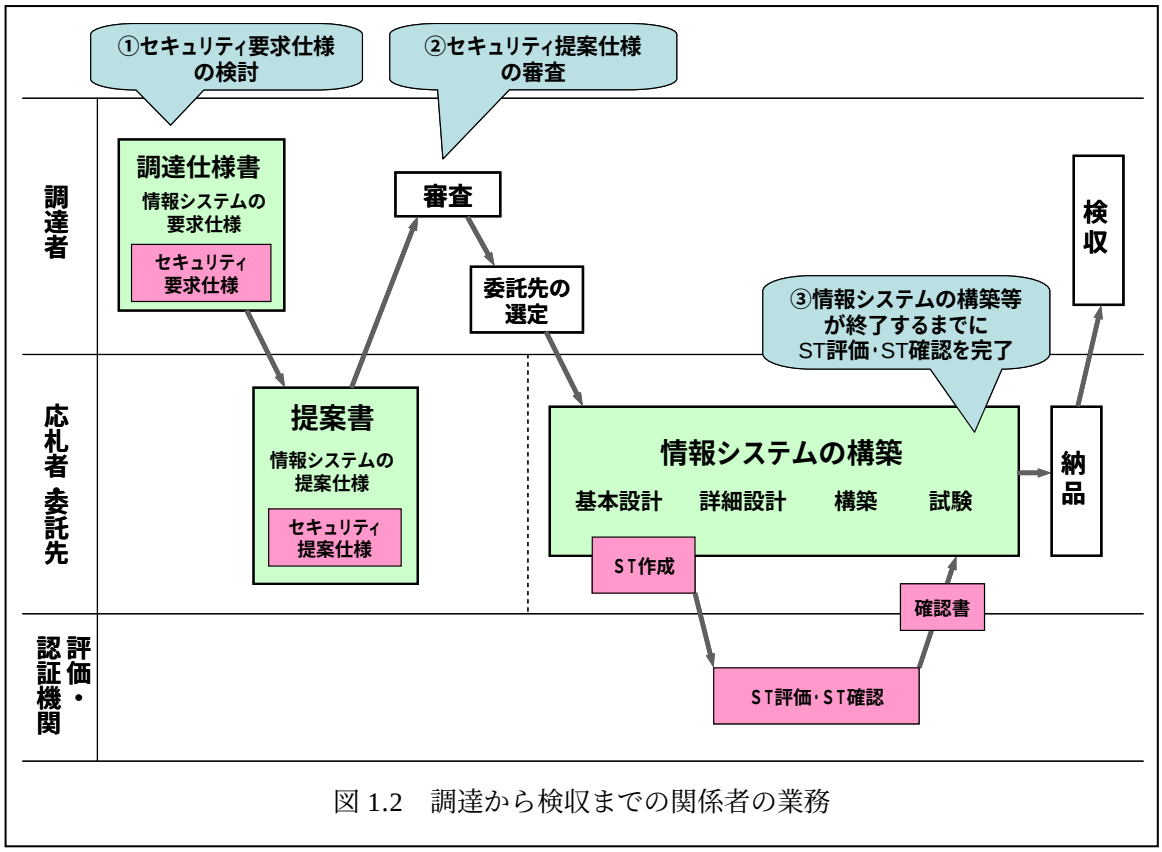

図 1.2　調達から検収までの関係者の業務

2. セキュリティ要件とセキュリティ機能の明確化

府省庁において情報システムの構築等を行う場合には、政府機関統一基準に基づき、情報セキュリティ要件の明確化が求められる。一般的には、情報システムの構築等は外部委託により行うことが多いと想定される。このため、調達者は、調達仕様書の作成段階からセキュリティ要件を検討し、これを応札者に提示し、セキュリティ機能の提案を求める必要がある。本章では、セキュリティ要件の作成方法とセキュリティ機能の提案に関する審査方法の概要を説明し、また、これらを詳しく説明した「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」の活用方法を説明する。

2.1. セキュリティ要件とセキュリティ機能の明確化の手順

情報システムの構築等を外部委託により行う場合に、セキュリティ要件とセキュリティ機能を明確化する手順を図 2.1 に示す。

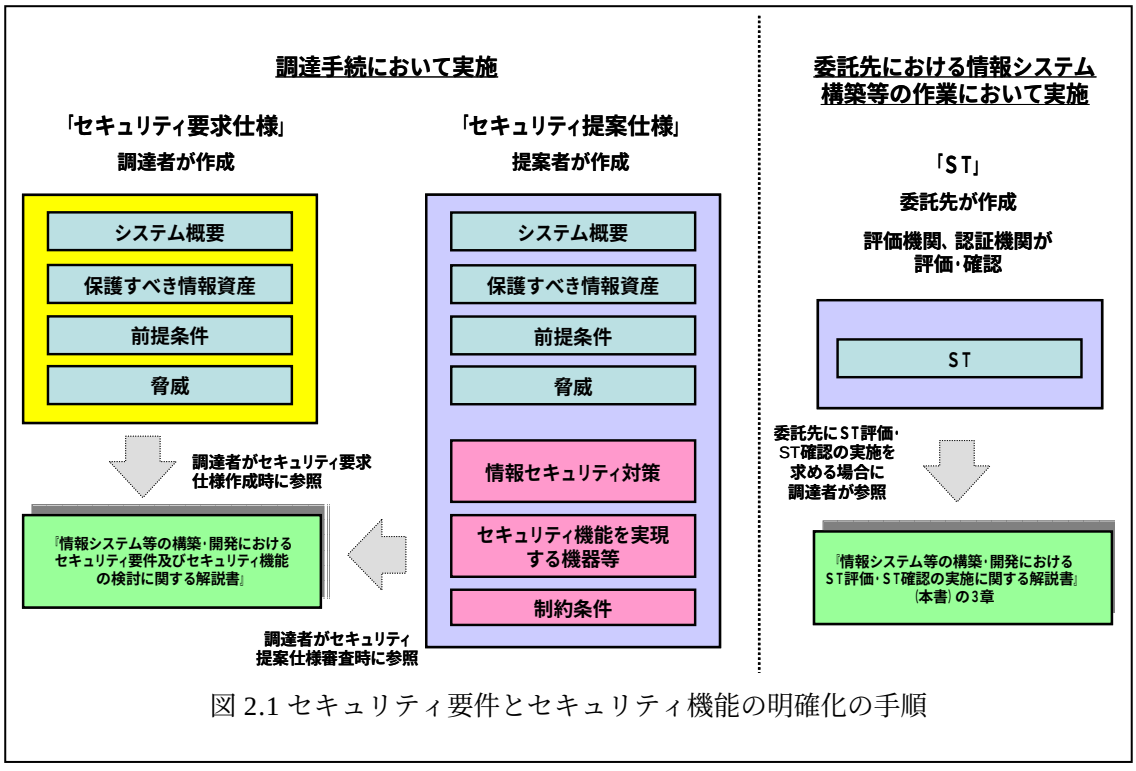

図 2.1 セキュリティ要件とセキュリティ機能の明確化の手順

調達者は、情報システムの構築等において、要求するセキュリティ要件を調達仕様書において明確に示し、セキュリティ機能を含む提案を適切に審査する必要がある。

「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」では、調達仕様に含めて提示するセキュリティ要件を「セキュリティ要求仕様」といい、「システム概要」、「保護すべき情報資産」、「前提条件」及び「脅威」の各項目を含めることとしている。また、応札における提案に応札者が「セキュリティ提案仕様」を含めることを求める。「セキュリティ提案仕様」には、「セキュリティ要求仕様」の各項目に加えて、その情報システム等に装備すべきセキュリティ機能を記した「情報セキュリティ対策」、必要に応じて IT セキュリティ評価及び認証制度に基づく機器等の認証について記した「セキュリティ機能を実現する機器等」、及び前提条件等の変更に関する事項を記した「制約条件」が含まれている。

このため、「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」では、調達者がセキュリティ要求仕様の作成とセキュリティ提案仕様の審査を行うために、セキュリティ要求仕様の作成とセキュリティ提案仕様の審査のポイントをまとめている。また、同書の参考例には、政府機関で使用される代表的な情報システムを例として取り上げてセキュリティ要求仕様の事例とセキュリティ提案仕様の審査例を示しているので、審査する際の参考にすることができる。

情報システムの開発等について委託先を決定し、委託先においてこれを行わせる段階では、セキュリティ機能の設計が適切に行われていることを第三者機関に評価・確認させる「ST 評価・ST 確認」の実施を契約に含めて委託先に行わせることもできる。この場合に実施工程等について調達者が留意すべき事項を、本解説書の 3 章で説明している。

2.2. セキュリティ要求仕様作成における「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」の活用例

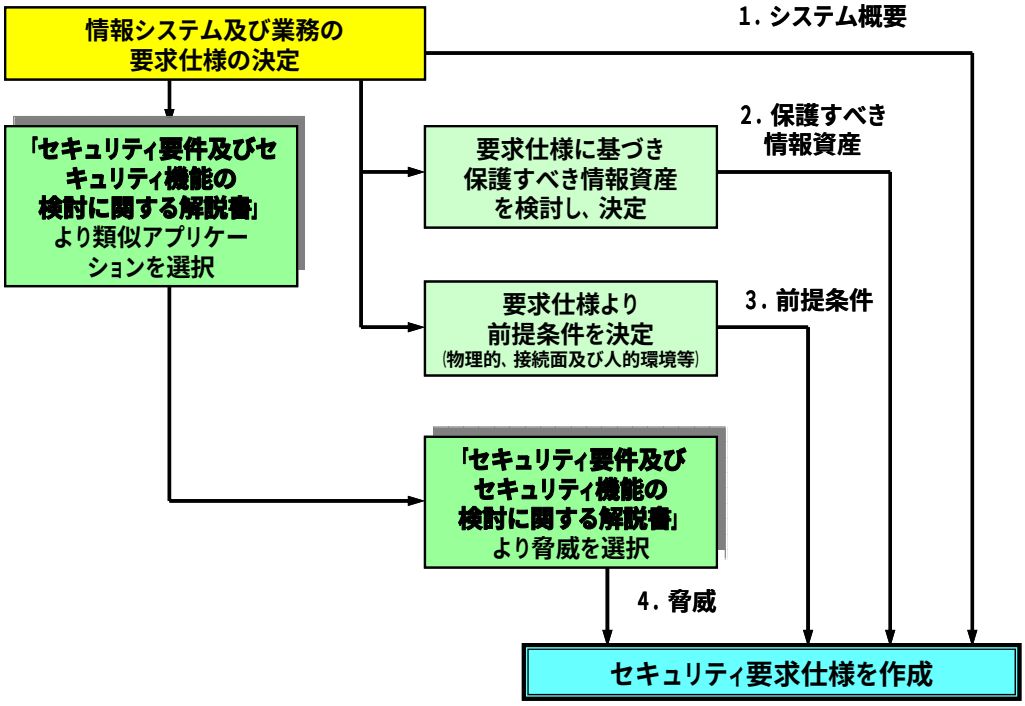

図 2.2　「セキュリティ要件及びセキュリティ機能の検討に関する解説書」を活用したセキュリティ要求仕様の作成

図 2.2 に「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」を活用したセキュリティ要求仕様作成の業務の流れを示す。

「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」には情報システムにおけるセキュリティ要求仕様の例が示されており、構築する情報システムに類似している例を参考に、保護すべき情報資産、前提条件及び脅威を含めたセキュリティ要求仕様を作成することができる。

2.3.セキュリティ提案仕様の審査の際の「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」の活用例

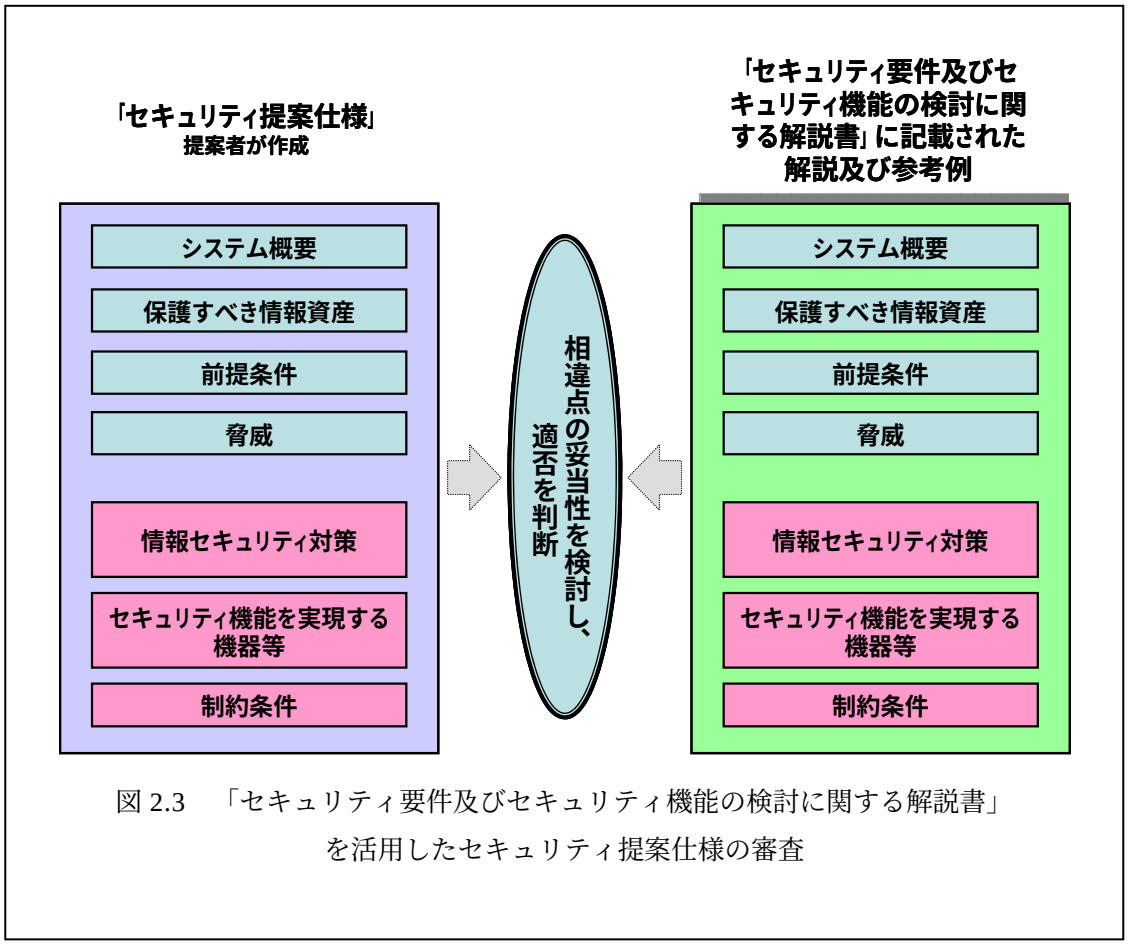

図 2.3　「セキュリティ要件及びセキュリティ機能の検討に関する解説書」を活用したセキュリティ提案仕様の審査

図 2.3 に「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」を活用したセキュリティ提案仕様審査の業務の流れを示す。

「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」にはセキュリティ提案仕様の審査のポイントが情報システム等の例とともに記述されており、類似システムの例を参照して審査を行うことができる。調達者は、セキュリティ提案仕様で提案されている脅威に対する情報セキュリティ対策の妥当性を検討し、また、セキュリティ要求仕様で提示した「保護すべき情報資産」、「前提条件」及び「脅威」について、セキュリティ提案仕様において変更を提案している場合及び制約条件を提示している場合には、その妥当性も検討する。

3. ST 評価・ST 確認の実施手順

本章では、情報システムの構築等において、ST 評価・ST 確認を行う場合の手順を説明する。

ST 評価・ST 確認は、IT セキュリティ評価及び認証制度において定められている確認手続である。ST 評価・ST 確認では、情報システム、開発するソフトウェア及び機器等のセキュリティ設計仕様書（セキュリティターゲット、ST）が ISO/IEC 15408 に適合していることを、第三者である評価機関が評価し、評価結果を確認機関（IT セキュリティ評価及び認証制度の運用元である独立行政法人 情報処理推進機構）が確認する。本書の 2 章で説明したセキュリティ要件とセキュリティ機能の明確化が情報システム、開発するソフトウェア及び機器等の設計において適切に行われていることが、ST 評価・ST 確認を実施することにより客観的に確認できる。

なお、政府機関統一基準では、重要なセキュリティ要件がある情報システムの構築及びソフトウェアの開発において、ST を作成し、ST 評価・ST 確認を取得することを求めている[1]。一般的には、情報システムの構築及びソフトウェアの開発は外部委託により行うことが多いと想定されることから、調達者は、調達仕様及び契約において委託先に対して ST 評価・ST 確認の実施を求め、その条件を示す。

[1] 政府機関統一基準では、セキュリティ機能の装備を第三者による評価に基づき調達者が確認する方法として、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提案の評価に加味する方法と、ST 評価・ST 確認の実施を求める方法がある。製品として調達する機器等（ソフトウェア製品及び機器）には、前者を適用する（統 4.3.1(1)(f)、6.1.1(2)(d)）。情報システムの構築及びソフトウェアの開発については、個別の仕様に基づき構築・開発を行うことにかんがみ、後者を適用する（統 4.3.1(1)(d)、6.1.3(3)(e)）。なお、適用条件等の詳細は、「1.1 政府機関統一基準における要求事項」を参照されたい。

3.1. ST 評価・ST 確認を実施する工程

ST 評価・ST 確認を委託先に行わせる場合に、ST を作成し、ST 評価・ST 確認を受ける工程を図 3.1 に示す。

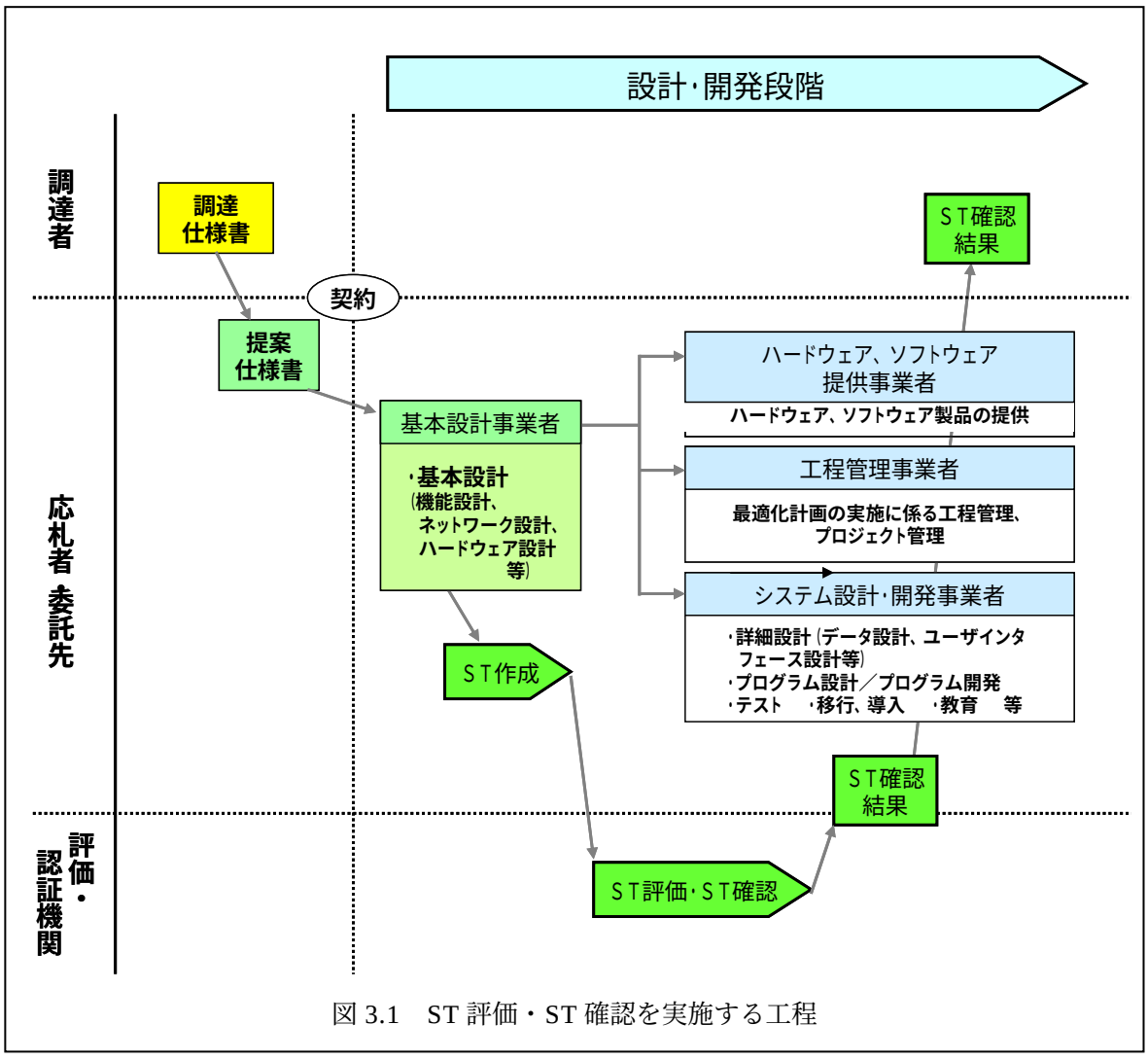

図 3.1　ST 評価・ST 確認を実施する工程

ST は、一般に、設計工程で作成する。図 3.1 では、基本設計において情報システム又はソフトウェアの機能を設計するものと想定している。ST は、業務仕様やそれを実現する情報システム等の機能を設計する一環で、情報セキュリティの側面に関する機能を設計することにより作成する仕様書であり、詳細設計やコーディングに先立ち確定し、早期に ST 評価の申請をすべきである。政府機関統一基準解説書では、このことを「(ST 評価・ST 確認

の）申請行為は設計段階のうちに行われることが通常の手順である。」（政府機関統一基準解説書 4.3.1(1)(d)及び 6.1.3(3)(e)の解説）と記述している。

また、ST 評価・ST 確認を受ける過程では、評価機関による評価において装備すべきセキュリティ機能を追加・変更等すべきであるとの指摘を受ける可能性がある。ST 評価・ST 確認が完了し、ST 確認書が交付されて初めて情報システム等に装備するセキュリティ機能が最終的に確定することから、情報システムの構築等において手戻りを避ける観点からも、ST 評価・ST 確認は早期に終了することが重要である。情報システムの構築等を外部委託する場合には、納品を受けるまでに委託先において ST 評価・ST 確認を終了させ、ST 確認書を提示させることを原則とする。政府機関統一基準解説書では、「開発が終了するまでにセキュリティ設計仕様書について、ST 評価・ST 確認済みになっている必要がある」（政府機関統一基準解説書 4.3.1(1)(d)及び 6.1.3(3)(e)）としている[2]。

以上のことから、ST 評価・ST 確認を委託先に行わせる場合には、調達仕様に以下の事項を記載する必要がある。

- 当該調達において、構築する情報システム（又は開発するソフトウェア）のセキュリティ機能設計に関して ST 評価・ST 確認を受けること。
- ST 評価・ST 確認は当該委託業務が終了するまでに終え、取得した ST 確認書を納品までに提示すること。

これらの事項は、契約にも含めること。

[2] 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委託先が第三者機関による 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調達者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、設計の完了から検収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調達者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。

3.2. 基本設計と詳細設計以降とをそれぞれ別に調達する場合の ST 評価・ST 確認の実施について

情報システムの構築等において、基本設計、詳細設計以降等、工程により調達を分ける場合がある。この場合には、調達者は、全体の設計・開発の工程を考慮して ST 評価・ST 確認を行わせる工程を決め、ST 評価・ST 確認の取得時期を指示する必要がある。

セキュリティ機能の設計は情報システム等の機能を設計する一環で行うことから、一般的には、ST 評価・ST 確認を、機能設計を含む基本設計を担当する事業者に行わせる場合が多いと想定される。この場合には、詳細設計を開始した後にその要求仕様が変更されることを避けるために、詳細設計の開始までに基本設計を担当する事業者が ST 評価・ST 確認を終えることが望まれる。(図 3.2 参照)

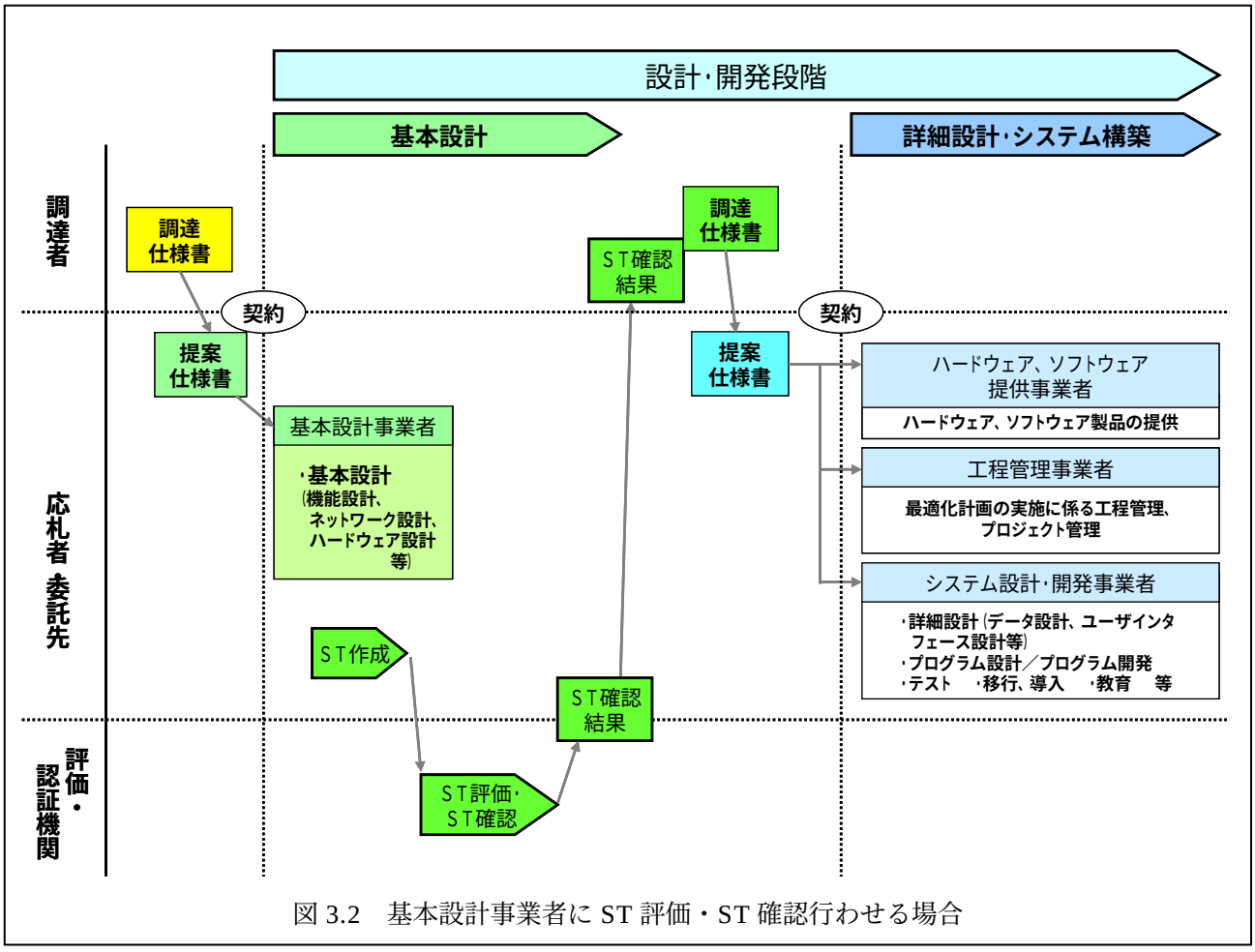

図 3.2 基本設計事業者に ST 評価・ST 確認行わせる場合

このため、この場合は、基本設計に関する調達仕様書に、ST 評価・ST 確認に関して以下の事項を記載する必要がある。

- 当該調達において、設計する情報システム（又はソフトウェア）のセキュリティ機能設計に関して ST 評価・ST 確認を受けること。
- ST 確認書を X 年 A 月 B 日までに提示すること[3]。

これらの事項は、契約にも含める。

[3] この場合にも、前節の脚注と同様に、ST 評価は第三者機関が行い、これに要する期間を調達者及び委託先において確実には予測できないため、必要に応じて、この点を考慮した契約等とすることが考えられる。

3.3. 重要なセキュリティ要件の変更と ST 評価・ST 確認の有効性

3.3.1. 情報システムの構築等における重要なセキュリティ要件の変更

情報システムの構築等において ST 評価・ST 確認を終えた後に、前提としていた重要なセキュリティ要件が変更された場合には、変更された要件に基づく情報システム等に対しては、ST 評価・ST 確認の結果は無効となる。

セキュリティ要件の変更は、調達者が委託先に提示した要件や前提が変更となった場合に起こり得る。例えば、情報システムを設置する物理的環境や業務仕様の変更等、調達仕様の様々な側面がセキュリティ要件の変更につながる。2 章で示した手順では、「セキュリティ要求仕様」の変更が、セキュリティ要件の変更になり得る。このため、実施した ST 評価・ST 確認を無効としないためにも、調達仕様において要求仕様を明確に提示すること、また、契約後にも委託先との間で情報システム等の仕様に関して不明確な事項を残さないことが重要である。

ただし、重要なセキュリティ要件の変更が軽微であると情報システムセキュリティ責任者が判断するときには、ST 評価・ST 確認の結果を引き続き有効なものとして調達側で扱うことができる[4]。「重要なセキュリティ要件の変更が軽微である」かどうかの判断においては、その変更に伴う情報セキュリティ上のリスクの増大について慎重に評価する。

3.3.2. 情報システム等の更改における重要なセキュリティ要件の変更

ST 評価・ST 確認を実施した情報システム等を更改するとき又は開発中に仕様変更が発生したときに、重要なセキュリティ要件を変更した場合には、更改等した情報システム等に対して、ST 評価・ST 確認の結果は無効である。必要があれば、更改等した情報システム等において、ST 評価・ST 確認をあらためて受けることになる。

[4] 政府機関統一基準 4.3.1(1)(d)及び 6.1.3(3)(e)のただし書きを参照されたい。

ただし、重要なセキュリティ要件の変更が軽微であると情報システムセキュリティ責任者が判断するときには、前項の場合と同様に、ST 評価・ST 確認の結果を引き続き有効なものとして調達側で扱うことができる。

3.4. ST 評価・ST 確認における評価保証レベル(EAL)の扱い

ST 評価・ST 確認においては、ST 及び機能仕様書のみを評価する。ST には評価保証レベル（EAL: Evaluation Assurance Level）を含む「TOE セキュリティ保証要件」も記述するが、これらは評価の対象には含まれない[5]。このため、調達者は、情報システムの構築等について ST 評価・ST 確認の実施を求める場合に、調達仕様においてこれらを指定する必要はない。

なお、情報システムの構築等においては、作成すると考えられる開発資料の範囲にかんがみ、EAL は 1 又は 2 とすることが通常のこととして想定される。

[5] 評価保証レベル（EAL）及び TOE セキュリティ保証要件は、IT セキュリティ評価及び認証制度における認証において評価の対象となる。その内容については、「4.1認証に関する確認事項」を参照されたい。

4. 認証製品の活用について

政府機関統一基準には、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た機器等の活用に関する遵守事項がある（4.3.1(1)(f) 及び 6.1.1(2)(d)、1 章を参照）。本章では、認証取得を調達における評価に含める際のポイントを説明する。

4.1. 認証に関する確認事項

以下に製品の認証に関する確認のポイントを示す。

（1） 認証されたセキュリティ機能の確認

調達者は、認証取得を製品の評価に活用する場合は、当該製品において想定する脅威への対策として求めるセキュリティ機能を明確にし、他方では、認証された機器等の認証されたセキュリティ機能を十分に理解する必要がある。認証されたセキュリティ機能が求めるセキュリティ機能と異なる場合には、期待する認証を取得した製品には該当しない。認証されたセキュリティ機能は、認証報告書又はセキュリティ設計仕様書で確認することができる。

（2） 前提条件・使用環境の確認

認証されたセキュリティ機能は、使用する前提条件、使用環境により、不十分であったり、不適切であったりする場合がある。このため、認証の前提条件、環境条件を認証報告書又はセキュリティ設計仕様書で調べ、使用する環境に合致しているか否かを確認する必要がある。

（3） セキュリティ保証要件及び評価保証レベル（EAL）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においては、ISO/IEC 15408 に基づき、セキュリティ保証要件が明示される。セキュリティ保証要件とは、セキュリティ機能が当該製品において実現されていることを評価する際にその根拠とした証拠等の範囲・程度を示すものである。また、評価保証レベル（EAL: Evaluation Assurance Level）とは、標準的なものとして定めたセキュリティ保証要件であり、レベル 1 からレベル 7 までの 7 段階の EAL が定められている。一般に、認証におけるセキュリティ保証要件は EAL で示すことが多い。

セキュリティ保証要件及び EAL は、認証製品のセキュリティ機能に関して実施した評価の程度を示すものであり、セキュリティ機能やセキュリティ機能強度を表すものではない。

調達において機器等における認証取得を提案の評価の要素に加える場合には、その評価において求める EAL を指定することもできるが、機器等を利用する情報システムや業務の重要性等に見合った EAL を指定することが重要である。特に、高い EAL を指定する場合は、 製品の調達コストや調達の透明性・公平性に対して影響を与えることもあるので、 しかるべき EAL の指定が望まれる。

EAL の選定の目安として以下のものが挙げられている（独立行政法人 情報処理開発機構）。

EAL1：クローズな環境での運用を前提に安全な利用や運用が保証された場合に用いられる製品の保証レベル。

EAL2：利用者や開発者が限定されており、安全な運用を脅かす重大な脅威が存在しない場合に用いられる製品の保証レベル。

EAL3：不特定な利用者が利用できる環境。不正対策が要求される場合に用いられる製品の保証レベル。

EAL4：商用製品やシステムにおいて高度なセキュリティ確保を実現するために、セキュリティを考慮した開発と生産ラインを導入して生産される製品の保証レベル。

4.2. 認証製品情報の利用法

前節で述べた認証製品に関する情報の調査法は、「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」の５章で詳細に説明している。

付録　セキュリティ設計仕様書（ST）

ST は、ISO/IEC 15408 Part 1 附属書 C に定義されている。ここでは、ST の内容に関する解説的な説明を示す。

本書の手順においては、ST は、情報システムの構築等の基本設計がほぼ完了した時点で、設計したセキュリティ機能を評価するために作成する。委託先は、ST の第三者評価を評価機関に依頼し、その後、認証機関に ST 評価の結果を持って ST 確認を申請する。なお、評価中に ST に関して設計上の不備や不足のあることが判明した場合にも、情報システム等の設計の手直し等を行うことで、セキュリティ機能に問題のない情報システムの構築等が可能となる。

図 A に、ST の構成を示す。

図 A.　ST の構造　（ISO/IEC 15408 に基づき IPA にて作成）

以下に、ST に含める項目を ISO/IEC 15408 に従い説明する。

（1） ST 概説

ST 全体の序説。ST や TOE（評価対象、Target Of Evaluation）の概要、が簡潔に記述されている。

1）ST 参照
- ST を一意に識別するための情報

2）TOE 参照
- TOE を一意に識別するための情報

3）TOE 概要
- TOE の使用法、動作環境の記述と、主要なセキュリティ機能の特徴の要約
- TOE 種別

4）TOE 記述
- TOE の範囲を明確にする情報

（2） 適合性主張

ST の適合状況が記述されている。

1）CC[6]適合主張
- 適合された CC のバージョン、言語
- CC Part 2 と Part 3 への適合/拡張

2）パッケージ主張
- EAL の適合、または追加

3）PP 主張
- PP の適合（正確適合、論証適合）

4）適合主張根拠
- PP に適合している際、その適合の根拠

（3） セキュリティ課題定義

TOE が対処する必要がある、セキュリティ上の課題を定義する。 脅威、前提条件、組織のセキュリティ方針（OSP: Organisational Security Policies）が記述されている。

1）脅威
- TOE やその運用環境によって対抗しなければならない脅威

[6] Common Criteria for Information Technology Security Evaluation の略称。

２）組織のセキュリティ方針(OSP)

・ TOE の運用環境により課せられる、規則、手続き、ガイドラインなど

３）前提条件

・ TOE が機能するために、TOE 利用者が満たす必要がある運用環境の条件

【ポイント】

ST 読者が想定している情報システム等に対して､TOE が脅威や組織のセキュリティ方針に適合しているか否かを判断できるように説明されている。前提条件には、認証製品を利用する際に整備すべき前提条件が記述されている。

（４） セキュリティ対策方針

セキュリティ課題定義によって定義される課題に対し、対抗する解決策を記述する。

１）TOE のセキュリティ対策方針

・ TOE が持つ機能で対抗、または実現する解決策

２）運用環境のセキュリティ対策方針

・ 運用環境において達成する必要があり、TOE を支援するために実装する技術・手続きに関する手段

３）セキュリティ対策方針根拠

・ 脅威への対抗、OSP の実施、前提条件の充足について、すべてのセキュリティ対策方針の効果を分析

【ポイント】

- セキュリティ対策方針の実現方法に関する詳細な説明ではない。
- 脅威あるいは OSP を踏まえてセキュリティ対策方針が「何を」解決するのか記述されている。

脅威、OSP、前提条件に対して、抽出された対応方針で十分であるかどうか検討されて記述されている。

【ポイント】

- 各脅威への対応の十分性（脅威の除去、脅威の軽減、脅威の緩和）が検討されて記述されている。
- 各 OSP の実現に貢献していることが記述されている。

（5） 拡張コンポーネント定義

CC に規定されていない、セキュリティ機能コンポーネントまたはセキュリティ保証コンポーネントを定義する。

1）拡張コンポーネント定義

- CC part2 に規定されていない、ST/PP 作成者が定義したセキュリティ機能コンポーネントの定義
- CC Part3 に規定されていない、ST/PP 作成者が定義したセキュリティ保証コンポーネント定義
- 拡張コンポーネントが存在する場合、「第２章　CC 適合主張」において、「拡張」と記述する
  - CC Part2 拡張
  - CC Part3 拡張

（6） IT セキュリティ要件

TOE セキュリティ対策方針から CC Part2/Part3 を用いた書換えと、セキュリティ機能要件を満たす保証の範囲を記述する

1）セキュリティ機能要件(SFR)

- 自然言語で作成された TOE セキュリティ対策方針からの、TOE の機能性についてのより正確な記述
- CC Part2 の要件記述を利用
  - TOE 及び IT 環境で実現する機能要件が具体的に記述されている。CC Part2 の記述をそのまま使用されている場合と、修整して使用されている場合がある。
    - **Assignment(割付)**：指定された項目を具体化
    - **Selection(選択)**：指定された項目の中から選択
    - **Refinement(詳細化)**：必要に応じて具体化
    - **Iteration(繰り返し)**：同じ条件の繰り返し(複数の組合せ)

2）セキュリティ保証要件(SAR)

- TOE の保障範囲についての正確な記述
- CC Part3 の要件記述を利用

TOE セキュリティ保証要件：TOE への保証要件が記述されている。CC Part3 の保証パッケージ（EAL1～7）の中から選ばれていることもある。商用製品の多くは、EAL4 までが選択されている。

【ポイント】保証要件の妥当性も検討されている。

3）セキュリティ要件根拠

- すべての TOE セキュリティ対策方針が、SFR によって効果的に対処されていることの根拠
- 選択された SAR が適切であることの説明

（7） TOE 要約仕様

TOE がどのようにしてすべての SFR を満たすのかを記述する。

TOE セキュリティ機能と保証手段（セキュリティ保証要件をすべて満たすことを示す資料）が記述されている。

1）TOE 要約仕様

- TOE が提供するセキュリティ機能の技術的メカニズム
  - TOE の一般的な形態、及び実装を理解できる程度の詳細レベル
    （認証： パスワード、トークン、虹彩スキャン、等々）
- TOE 概要、TOE 記述と一環した記述、及び詳細度の増加
  （例えば、TOE 概要<TOE 記述<TOE 要約仕様）

【ポイント】

- ここで定義した機能が TOE に関する各設計書に記述されることになる。