【パブリックコメント】

情報システムに係る政府調達における
セキュリティ要件策定マニュアル（案）

2011 年 1 月 31 日

目次

目次（図表）

1章 マニュアルの概要

この章では、「政府機関の情報システムの調達におけるセキュリティ要件策定マニュアル（案）」（以下「本マニュアル」という。）を作成した背景、その目的・位置づけ及び適用範囲について述べる。

1.1 背景

政府機関の情報システムにおいて適切に情報セキュリティ対策を講じるためには、情報システムのライフサイクル（企画・設計・開発・運用・廃棄）における企画段階（調達段階）から情報セキュリティの観点を意識し、その際に必要となる調達仕様にセキュリティ要件を適切に組み込むことが求められる。

また、調達仕様におけるセキュリティ要件の曖昧さや過不足は調達側と供給側の相互理解と合意形成を阻害し、調達側と供給側の双方に不利益を発生させる要因となる。これらに起因して、システムの実態によらず全網羅的な過剰なセキュリティ対策に伴うコスト増加となるおそれ、要件解釈のばらつきによる提案内容の差異からの不公平な競争入札、設計・開発工程での手戻り、運用開始後のセキュリティ事故発生などといった不利益が生じる可能性が考えられる。

このような問題意識を受けて、情報セキュリティ政策会議（議長：内閣官房長官）においても議論がなされた。その後、内閣官房情報セキュリティセンターを事務局とし、経験・知見を有する有識者やベンダーを交えた「情報セキュリティを企画・設計段階から確保するための方策（SBD: Security By Design）に係る検討会」が設置され、情報システムにおける情報セキュリティ対策を考慮したライフサイクル管理強化の実現に向けた具体的な方策の検討について議論が進められた。本マニュアルは、当該検討会において上記の課題に対する解決策として作成されたものである。

1.2 目的

本マニュアルは、政府機関の情報システムの調達仕様書に記載する「セキュリティ要件」の策定方法を解説することによって、情報システムの企画段階からセキュリティ対策を適切に組み込むことを目的としている。

特に、本マニュアルにおける策定方法は、調達を行う者がセキュリティ要件を自ら責任をもって策定するとともに、重要かつ効果的なセキュリティ要件については優先的かつ確実に調達仕様書に記載することを重視している。

1.3 位置づけ

政府では、「情報システムに係る政府調達の基本指針（平成 19 年 3 月 1 日各府省情報化統括責任者（CIO）連絡会議決定）」（以下、「調達指針」という。）によって、情報システムに係る政府調達について統一的なルールを定めている。

本マニュアルは、行政事務従事者が上記の調達指針に基づいて情報システムを調達する際に、セキュリティ要件の策定にあたって活用されることを想定したものである。したがって、本マニュアルの導出対象はセキュリティ要件であって、情報システム全体の要件ではないことに留意する必要がある。

1.4 想定読者

本マニュアルの想定読者は、行政事務従事者のうち、情報システムの調達を担当する調達担当者（以下、「調達担当者」という。）及び情報システムを供給する事業者である。本マニュアルを活用することで、調達担当者にとっては、調達仕様書にセキュリティ要件を適切に組み込むことが可能となる。一方、情報システムを供給する事業者にとっては、調達仕様書に記載されたセキュリティ要件の導出過程における考え方を理解することが可能となる。

1.5 活用範囲

本マニュアルの活用範囲（対象と想定している情報システムの範囲）は、政府機関における「新規構築」及び「更改」を行う情報システム全般である。本マニュアルの活用範囲は、情報システムの規模には依存しないが、費用等との関係から調達段階から情報システムに関する技術の専門家が参画することが難しい中小規模の情報システムの調達に対して特に有効である。

なお、活用のタイミングについては、本マニュアルの目的が政府機関の情報システムの調達仕様書に記載する「セキュリティ要件」の策定であることから、特に情報システム調達時を想定している。

2章 用語等定義

用語	語義
アーカイブ アーカイブデータ	情報システムの運用時に蓄積する情報のうち業務上不要となったものの記録のために保管すべき情報は外部に取り出して情報システムの記憶装置の負担を軽減する必要がある。このような情報をひとまとめにして保存することをアーカイブ、保存されるひとまとめの情報をアーカイブデータと呼ぶ。
アカウント	情報システムを利用するための資格や権限のことであり、情報システムの運用者が対象となる利用者に割り当てる。
アクセス制御 アクセス制御機能	アクセス元（利用者、装置等）に応じて情報システムが管理する情報資産に対するアクセスの内容（例えば、情報の読み出し、書き込み、変更等）を許可又は拒否すること及びそのための機能のこと。
サービス サービス構成	情報システムが利用者に対して提供する機能のこと及び機能構成のこと。
サービス不能化	情報システムが利用者に対して機能を正常に提供することが困難な状態になること。
セキュリティ要件	情報セキュリティを確保するために満たすべき条件のこと。
なりすまし	自身ではない他人のふりをして何らかの行為を行うこと。
マルウェア	コンピュータ上で利用者の意図しないような悪意のある動作を行うことができるプログラムのこと。
証跡	ある事実の存在を証明する情報のこと。
ログ	情報システムの利用状況、動作状況を記録すること及び記録される情報のこと。
暗号、暗号アルゴリズム	情報を第三者に知られることがないように、情報に何らかの変換処理を行うこと及び変換処理の方式のこと。
機密性	情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保すること。
完全性	情報が破壊、改ざん又は消去されていない状態を確保すること。
可用性	情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること。
業務要件	なんらかの目的を達成するために実施する各業務の内容及びその遂行にあたって満たすことが求められる条件のこと。どのようなルールに従って、誰

【パブリックコメント】

用語	語義
	が何をどのようにして処理するのかを条件としてまとめたもの。
実施レベル	5 章参照。
主体	情報システムに対するアクセス等のなんらかの行為を実行する者のこと。主体は利用者、運用者及びシステム管理者等の人間以外に、装置、システム等の場合もある。
統一基準群 政府機関統一管理基準 政府機関統一技術基準	政府機関における統一的な枠組みの中で、それぞれの府省庁が情報セキュリティの確保のために採るべき対策及びその水準を更に高めるための対策の基準を定めたもの。統一基準群には、「政府機関の情報セキュリティ対策のための統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」が含まれ、本マニュアルでは前者を「政府機関統一管理基準」、後者を「政府機関統一技術基準」と表記する。
対策区分 対策方針 対策要件	5 章参照。
調達指針	「情報システムに係る政府調達の基本指針（平成 19 年 3 月 1 日各府省情報化統括責任者（CIO）連絡会議決定）」のこと。
定型設問	4.4 節参照。
電子署名	電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。 ・ 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。 ・ 当該情報について改変が行われていないかどうかを確認することができるものであること。
盗聴	他人のやりとりの内容を気づかれないように聞いたり、通信の内容を傍受したりすること。
判断条件	5 章参照。
利用環境・手段	4 章参照。

3章 本マニュアルの使い方

この章では、調達仕様書に記載すべきセキュリティ要件を導出するための基本的な考え方及び全体の手順について述べる。

3.1 政府調達における利用タイミング

本マニュアルは、情報システムの調達プロセスにおける図 1 に示すように発注側の調達担当者が調達仕様書にセキュリティ要件を記載するための手順を定め、作業を支援するものである。[1]

調達指針は、調達仕様書の作成にあたって留意すべき事項として「提案に不可欠な情報の網羅」及び「曖昧な要求要件の排除」を挙げている。調達担当者は、情報システムのセキュリティ要件に関しても同様の点に留意し、セキュリティ機能の提案に不可欠な情報を曖昧性ができる限りない形で調達仕様書に記載するとともに、各府省庁の情報セキュリティポリシーに準ずる必要がある。本マニュアルはこのような場面での活用を想定している。

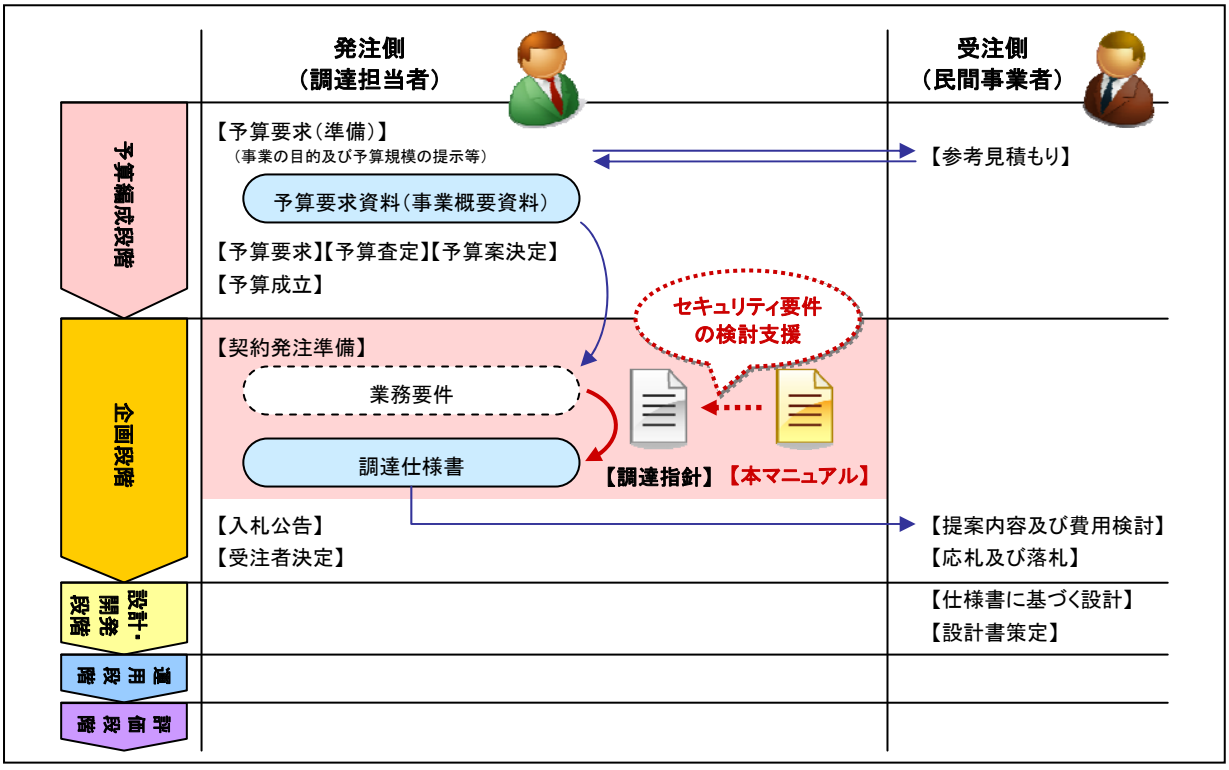


図 1 情報システムの調達プロセスにおける本マニュアルの位置づけ

[1] 必要な情報セキュリティ対策が予算不足によって実施できない事態を避けるためには、本マニュアルを予算編成段階から活用し、情報セキュリティの確保に必要なコストを見極めて予算編成に反映することが望ましい。

表 1 は調達指針において定められている「調達仕様書」に記載すべき事項である。本マニュアルが策定の対象とするセキュリティ要件の記載箇所は、主に「5 信頼性等要件」、「6 情報セキュリティ要件」、「8 テスト要件定義」、「10 運用要件定義」及び「11 保守要件定義」である。また、セキュリティ要件の策定過程で明らかになる業務要件には、セキュリティ要件を満たすセキュリティ機能を提案する際に不可欠な情報となる可能性が高いものが含まれるため、そのような情報は「1 調達件名」、「2 作業の概要」及び「7 情報システム稼働環境」に記載する。

表 1 調達指針が定める調達仕様書に記載する事項

項目		主な記載内容
1	調達件名	情報システムに係る工程名
2	作業の概要	(1) 目的、(2) 用語の定義、(3) 業務の概要、(4) 情報システム化の範囲、(5) 作業内容・納入成果物
3	情報システムの要件	(1) 機能要件、(2) 画面要件、(3) 帳票要件、(4) 情報・データ要件、(5) 外部インタフェース要件
4	規模・性能要件	(1) 規模要件、(2) 性能要件
5	信頼性等要件	(1) 信頼性要件、(2) 拡張性要件、(3) 上位互換性要件、(4) システム中立性要件、(5) 事業継続性要件
6	情報セキュリティ要件	(1) 権限要件、(2) 情報セキュリティ対策
7	情報システム稼働環境	(1) 全体構成、(2) ハードウェア構成、(3) ソフトウェア構成、(4) ネットワーク構成、(5) アクセシビリティ要件
8	テスト要件定義	要求仕様の適合性を検証するためのテストに係る要件
9	移行要件定義	(1) 移行に係る要件、(2) 教育に係る要件
10	運用要件定義	(1) システム操作・監視等要件、(2) データ管理要件、(3) 運用施設・設備要件
11	保守要件定義	(1) ソフトウェア保守要件、(2) ハードウェア保守要件
12	作業の体制及び方法	(1) 作業体制、(2) 開発方法、(3) 導入、(4) 瑕疵担保責任
13	特記事項	その他、特記すべき要件
14	妥当性証明	調達仕様書の妥当性を確認した調達担当課室の長の氏名

※ 下線部分はセキュリティ要件またはその関連情報の記載が想定される箇所

出典:「情報システムに係る政府調達の基本指針(平成19年3月1日各府省情報化統括責任者(CIO)連絡会議決定)」に基づき作成

3.2 手順の全体像

情報システムのセキュリティ要件を策定するためには、情報セキュリティに影響を与える「要因の洗い出し」が必要である。そのためには、対象の情報システムにおける保護すべき情報及びその取り扱い方を明らかにすることが不可欠である。これは業務要件を明らかにすることに他ならない。

そこで、本マニュアルが定める手順は、図 2 のようにセキュリティ要件の策定に必要な「(1) 業務要件の検討」を行った後に、「(2) セキュリティ要件の策定」を行うものとしている。それぞれの手順の概要は下記の通りである。

(1) 業務要件の検討

調達担当者は、情報システムを調達する「目的」及び対象とする「業務」を洗い出した上で、「主体(情報を取り扱う者)」「情報」及び「利用環境・手段」の 3 つの観点を意識して業務の特徴を整理する。その上で、調達担当者は抽出した「業務要件」を「システム概要図」と呼ぶ図に表して俯瞰することによって業務要件に不足や矛盾点がないことを確かめるとともに、「定型設問」に回答することによって業務要件の詳細化を図り作業の質を高める。

(2) セキュリティ要件の策定

調達担当者は、(1) にて検討した業務要件を踏まえ、「対策要件集」から調達する情報システムにふさわしいセキュリティ要件を選定して、「調達仕様書」に記載する。対策要件集とは、情報システムの標準的なセキュリティ要件をまとめたものである。本マニュアルでは、このセキュリティ要件の選定作業を可能な限り定型化するため、優先すべきセキュリティ対策の方向性を導出する「判断条件」、セキュリティ対策の実施の程度を表す「実施レベル」といった独自の概念を用いた手順を定めている。

なお、業務要件の検討方法として上記の(1)と同等の検討結果を得る他の方法があれば、それを代替的に用いても構わない。また、既存の情報システムの拡充の場合には、追加部分のみではなく既存部分も含めた情報システム全体を対象に上記の手順を実施する必要がある。[2]

2 情報システムに新たな構成要素が加わり、既存部分と追加部分が相互に影響し合うことによって生じるセキュリティ課題の検討が必要となるため。

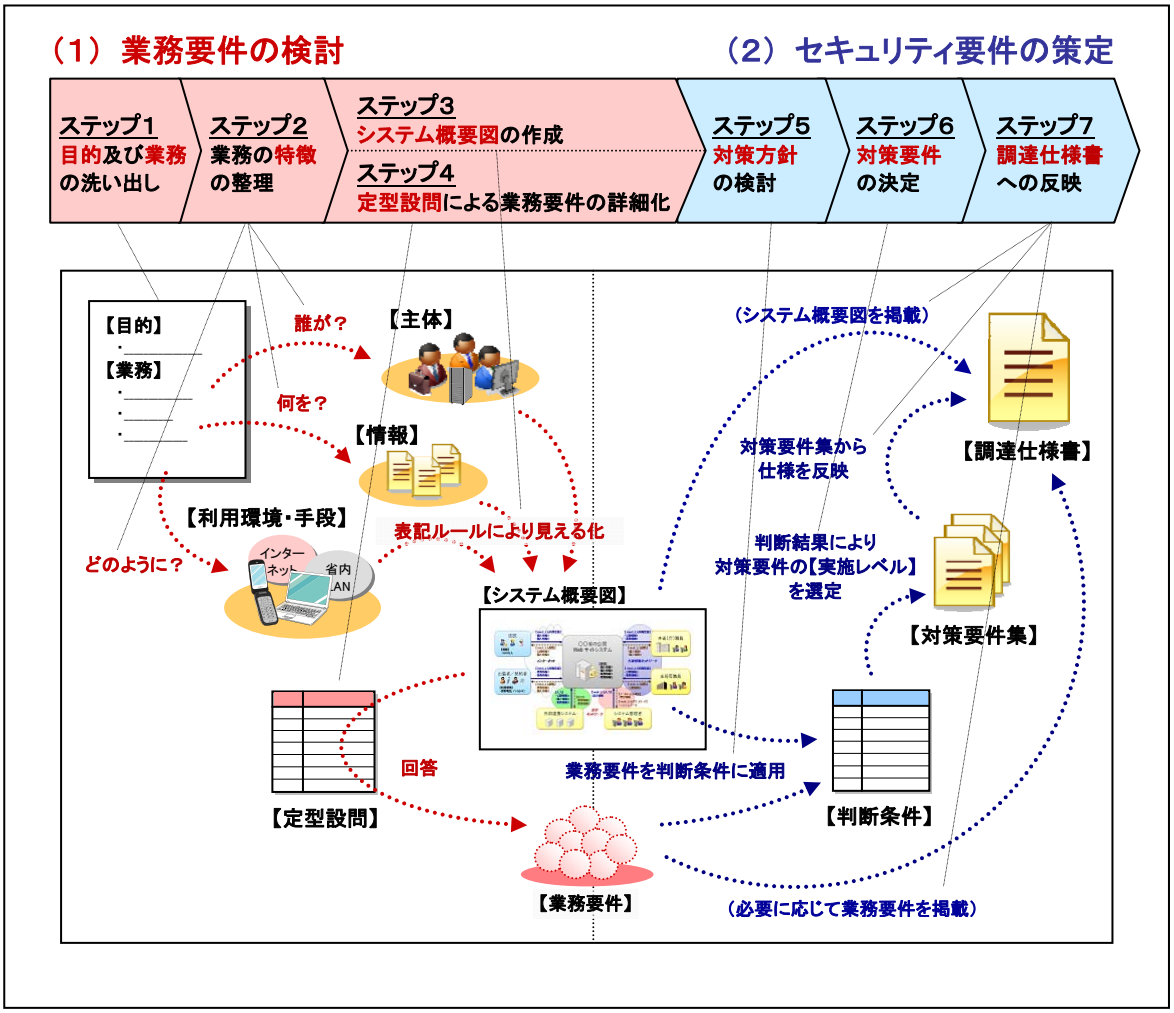


図 2 セキュリティ要件策定手順の全体像

4章 業務要件の検討

この章では業務要件の検討手順を解説する。調達担当者は、以降の手順に従って「システム概要図」と呼ぶ図の作成を通じて基本的な業務要件を洗い出し、その上で「定型設問」に回答することよって業務要件の詳細化を図る。

システム概要図とは、表 2 の 3 つの観点から、「業務」と「業務における情報の取り扱い方」を中心に視覚化して、業務要件を俯瞰するためのものである。調達担当者は、システム概要図の作成によって、「どのような情報が、どこからどこに、どのような手段を介してやりとりされるのか」といった情報システムの構築に必要な「情報の流れ」を把握することができる。情報の流れの把握は、情報セキュリティに関する脅威が発生しやすい箇所、すなわちリスクを検討すべき箇所の特定に有効である。また、システム概要図の内容は具体的である方が良いが、業務要件の見通しが悪くなるほどの過度な詳細化は好ましくない。

以降では、調達担当者が実施するシステム概要図の作成手順及び定型設問による業務要件の詳細化の手順について解説する。

表 2 システム概要図作成のための 3 つの観点

観点	説明	例
主体	行政サービスの利用や提供を行う情報システム、あるいは当該業務を実施する者のこと	国民、行政事務を担当する者、システム運用者・管理者等
情報	主体が行政サービスや業務を通じて取り扱う対象であって、送受信等の処理をされる対象のこと	申請書、許可証、個人情報等
利用環境・手段	主体が、情報を処理（作成、保存、送受信等）するために用いる環境・手段のこと	端末、サーバ、記憶媒体、IC カード、ネットワーク等

4.1 目的及び業務の洗い出し（ステップ 1）

まず、情報システムの「名称」及び情報システム導入の「目的」を定める。目的の方向性は、例えば、「業務効率の向上」「業務コストの低減」「行政サービスの改善」「新たな行政サービスの実現」などが考えられるが、できるだけ具体的かつ明確な表現を用いて目的を明文化すると良い。

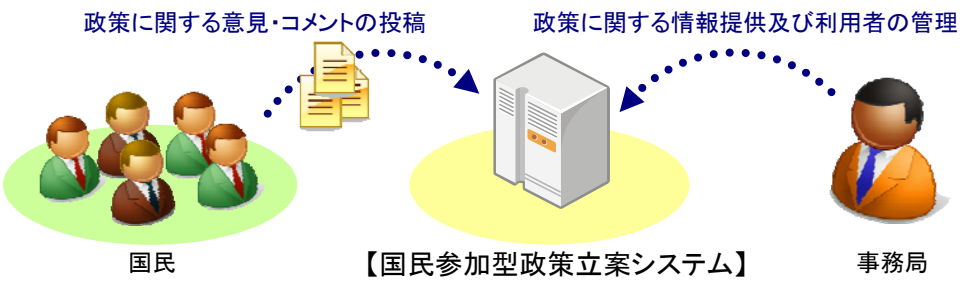
続いて、目的に見合う具体的な「業務」を整理する。業務とは、例えば、行政事務、国民等に対する行政サービスの提供等である。この段階で整理すべき内容は概略を簡潔にまとめたもので良い。同時に業務に関わる人物や付随書類等も整理しておくと後の作業に有効である。

以上の検討結果は、表 3 のように簡単な箇条書きの体裁でまとめる程度で良いが、表 4 のように簡易な図の体裁でまとめておくと客観的により分りやすいものとなる。

表 3 目的と業務の洗い出しの例（箇条書きの場合）

項目	内容
名称	国民参加型政策立案システム
目的	インターネットを活用して政策に関する提案・意見を国民から広く募り、参加者同士による議論及び投票等によって、国民参加による政策立案のしくみを確立すること。
業務	(1) 「国民」による政策に関する意見・コメントの投稿 (2) 「事務局」からの政策に関する情報提供及び利用者の管理

表 4 目的と業務の洗い出しの例（図示の場合）

項目	内容
名称	国民参加型政策立案システム
目的	インターネットを活用して政策に関する提案・意見を国民から広く募り、参加者同士による議論及び投票等によって、国民参加による政策立案のしくみを確立すること。
業務	

4.2 業務の特徴の整理(ステップ 2)

4.2.1 主体の洗い出し

ステップ 1 にて洗い出した業務に関与する主体(人物、組織、情報システム等)を洗い出す。また、表 5 のように業務や行政サービスを細分化しておくと後の作業が進めやすくなる上、主体の洗い出し漏れにも気づきやすい。細分化にあたっては、対象とする業務領域における特有の業務イベント(例えば、サービスや人事制度上、特定の時期に集中的に発生する業務等)を洗い出すと重要な業務の気づきにつながるため有効である。さらに、情報システムの運用業務を意識し、「情報システムの管理者」「連携する既存の情報システム」なども必要に応じて主体に加えること。

表 5 主体の洗い出し及び業務の細分化の例

主体	業務	業務 (細分化後)	業務(細分化後)の概要	情報	利用環境・手段
国民	政策に関する意見・コメントの投稿	利用登録			
		意見・コメントの投稿、投票			
		意見・コメントの閲覧			
事務局	政策に関する情報提供及び利用者の管理	意見に対する回答、修正			
		事務局からの周知			
		利用者の管理			
システム管理者	情報システムの利用状況の把握及び管理	利用状況の把握			
		不正利用及び障害の監視、追跡			
		システムのバックアップと復旧			

※ 下線部は、表 3 または表 4 の内容を踏まえ検討を行い新たに追加した部分。灰色の箇所は次節以降にて記入。

4.2.2 情報の洗い出し

洗い出した主体ごとに「業務」の概要を明文化し、各業務にて取り扱う「情報」を表 6 のように洗い出す。業務や行政サービスの「目的」及び「誰の情報が誰から誰に流れるのか」を意識して検討すると、情報の洗い出しの漏れに気づきやすい。一方、行政サービスの関連制度や行政サービスの利用方法等によって必要書類の書式や処理の流れ等が規定されている場合には、そのような点から情報を洗い出すと検討作業の確実性が増す。

また、ここまでの検討の過程で業務や主体の細分化や追加の必要性に気付く場合があるため、そのような場合は必要に応じてステップ 1 に戻り手順を繰り返し実施する。

表 6 業務の概要及び情報の洗い出しの例

主体	業務	業務（細分化後）	業務(細分化後)の概要	情報	利用環境・手段
国民	政策に関する意見・コメントの投稿	利用登録	個人情報を登録して、サービスの利用資格を得る。	「個人情報」（氏名、ニックネーム、性別、年齢、職種、連絡先等）	
		意見・コメントの投稿、投票	新規の意見や他者の意見に対するコメントの投稿及び投票を行う。	「意見」「コメント」（タイトル、本文、投稿者名、投稿日時等）	
		意見・コメントの閲覧	意見やコメントを検索し、閲覧する。	「意見」「コメント」（タイトル、本文、投稿者名、投稿日時等）	
事務局	政策に関する情報提供及び利用者の管理	意見に対する回答、修正	意見に対する事務局回答の投稿及び不適切な意見の削除を行う。	「回答」（本文、投稿者名、投稿日時等）	
		事務局からの周知	サービス停止や注意事項等の利用者に対する周知を行う。	「お知らせ文面」	
		利用者の管理	利用者の登録情報の確認、修正、等の管理業務を行う。	「個人情報」（氏名、ニックネーム、性別、年齢、職種、連絡先等）	
システム管理者	情報システムの利用状況の把握及び管理	利用状況の把握	利用者の登録状況、アクセス状況、意見やコメントの集計を行う。	「利用統計」（全体及び意見ごとのアクセス数、利用者の登録数等）	
		不正利用及び障害の監視、追跡	アクセス状況の監視及びログ等を元にした原因究明を行う。	「履歴」（アクセス、認証、利用ログ等）	
		システムのバックアップと復旧	システムのデータを定期バックアップ及び障害時の復旧を行う。	「システムデータ」	

※　下線部は、表 5 の内容を踏まえ検討を行い新たに追加した部分。灰色の箇所は次節以降にて記入。

4.2.3 システム化対象の決定

ステップ 1 にて明確化した導入目的を踏まえ、ここまでの作業で明らかにした業務のうちシステム化対象とする業務を決定する。ここで定める範囲がセキュリティ要件の策定対象となる。

4.2.4 業務に用いる環境の決定

システム化対象に定めた「業務」の実施にあたって各主体が用いる「利用環境・手段」を決定し、表 7 のように整理する。利用環境・手段とは、例えば、主体が情報システムにアクセスするために用いる機器、情報の作成、保存等に用いる機器及び情報を送受信するためのネットワーク等のことである。

表 7 利用環境・手段の洗い出しの例

主体	業務	業務（細分化後）	業務(細分化後)の概要	情報	利用環境・手段
国民	政策に関する意見・コメントの投稿	利用登録	個人情報を登録して、サービスの利用資格を得る。	「個人情報」（氏名、ニックネーム、性別、年齢、職種、連絡先等）	PC、携帯電話、スマートフォン、インターネット
		意見・コメントの投稿、投票	新規の意見や他者の意見に対するコメントの投稿及び投票を行う。	「意見」「コメント」（タイトル、本文、投稿者名、投稿日時等）	
		意見・コメントの閲覧	意見やコメントを検索し、閲覧する。	「意見」「コメント」（タイトル、本文、投稿者名、投稿日時等）	
事務局	政策に関する情報提供及び利用者の管理	意見に対する回答、修正	意見に対する事務局回答の投稿及び不適切な意見の削除を行う。	「回答」（本文、投稿者名、投稿日時等）	PC、内部ネットワーク
		事務局からの周知	サービス停止や注意事項等の利用者に対する周知を行う。	「お知らせ文面」	
		利用者の管理	利用者の登録情報の確認、修正、等の管理業務を行う。	「個人情報」（氏名、ニックネーム、性別、年齢、職種、連絡先等）	
システム管理者	情報システムの利用状況の把握及び管理	利用状況の把握	利用者の登録状況、アクセス状況、意見やコメントの集計を行う。	「利用統計」（全体及び意見ごとのアクセス数、利用者の登録数等）	PC、管理用 LAN
		不正利用及び障害の監視、追跡	アクセス状況の監視及びログ等を元にした原因究明を行う。	「履歴」（アクセス、認証、利用ログ等）	
		システムのバックアップと復旧	システムのデータを定期バックアップ及び障害時の復旧を行う。	「システムデータ」	

※ 下線部は、表 6 の内容を踏まえ検討を行い新たに追加した部分。

4.3 システム概要図の作成（ステップ 3）

前節までの作業結果を元にして、表 8 のように表記ルールに従ってシステム概要図を作成する。システム概要図は、利用者と情報システム等の主体同士の関係、利用環境・手段、情報の流れが具体的に分かり、かつ簡潔で見やすいものとなるように工夫する。表 9 のチェックリストを利用して点検を行うと、図の品質が向上する。

表 8 システム概要図の表記ルール及び作成例

表記ルール	
1	主体（人やシステム）を表す図形を決定する。
2	調達対象となる情報システムを図の中央付近に記載する。
3	業務（情報のやりとり）が発生する主体の間を矢印で結ぶ。
4	矢印の向きと情報の流れができるだけ一致するように業務及び情報の名称（または略称）を記載する。
5	利用環境・手段のうち、機器は機器を用いる主体の付近に記載し、ネットワークは情報のやりとりを表す矢印の付近（背景部分）に記載する。
6	サーバや端末等の機器が情報を蓄積する場合、その付近にその情報の名称を記載する。
7	すべての情報を書き込み切れない場合は各ステップの検討結果を別表に整理して採番し、図には番号等を記載する。
8	異なる主体であっても情報や利用環境・手段等に共通点がある場合には、一括して記載するなどして、図が難解にならないように工夫する。
システム概要図	

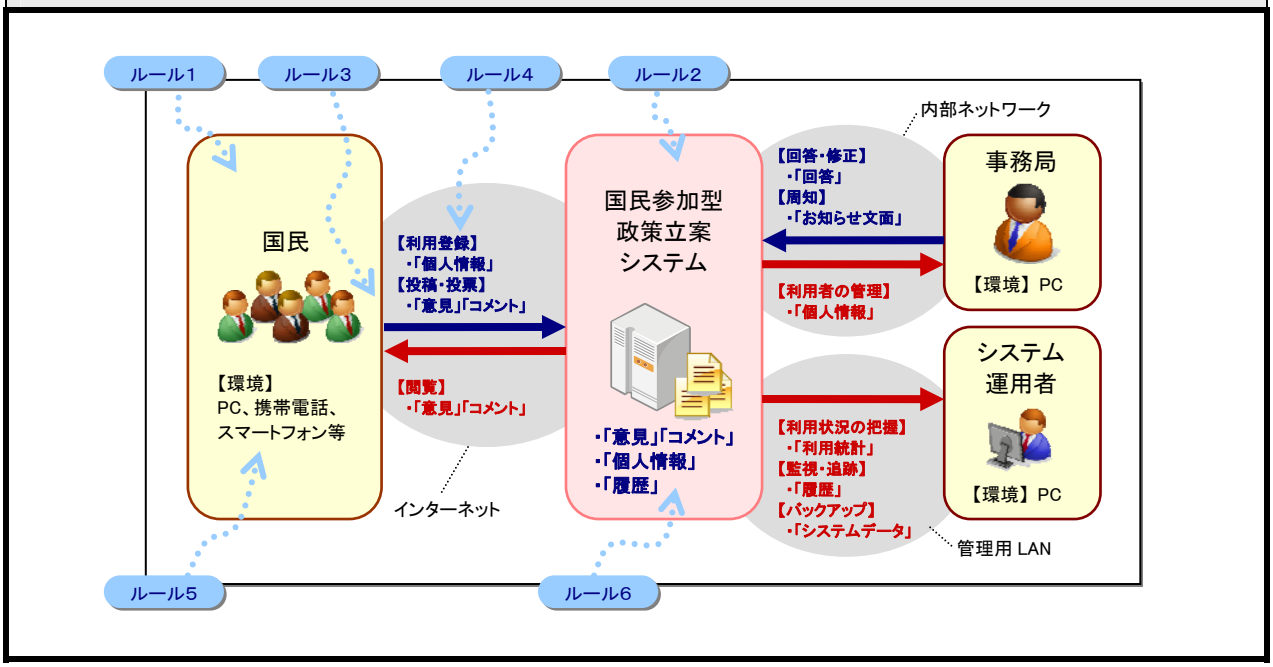


表 9 システム概要図作成のための「チェックリスト」

項番	チェック内容
1	情報システム化の対象とする業務が記載されているか
2	各業務の主体(国民、行政事務を担当する者、システム管理者等)が記載されているか
3	各業務にて取り扱う情報が記載されているか
4	各業務において情報の取扱い及び交換に用いる環境が記載されているか
5	主体、情報システム、関連する他の情報システムの関係を把握できるか

4.4 定型設問による業務要件の詳細化（ステップ 4）

調達担当者は業務要件をセキュリティ要件の導出に必要となる更なる詳細化を図るため、完成したシステム概要図を踏まえつつ表 10 の設問の回答を検討する。設問は「主体」「情報」「利用環境・手段」の 3 つの観点ごとに設けられている。各設問の回答例を参考にして、ここまでの作業によって洗い出した「主体」の業務ごとに回答を検討する。

なお、主体や業務のバリエーションが多い場合、すべての設問の回答を検討することが難しい可能性がある。そのような場合にはすべての設問に回答することなく 5 章の作業に進み、5 章にて業務要件に不足があると思われた場合に 4 章に再度戻って業務要件を検討する方法でも良い。また、本マニュアルの設問や回答例にとらわれることなく、本マニュアルの利用組織にて自由に追加、変更などして構わない。

表 10 業務要件詳細化のための「定型設問」

ID	観点	設問	回答例
A-1	主体	【数量】 おおよその人数規模は？	「1 万人未満」
A-2		【主体分類】 主体の分類は？	「国民」「事務局」「システム管理者」
A-3		【集合特性】 特定か不特定か？	「特定（匿名性なし）」「特定（匿名性あり）」「不特定（匿名性なし）」「不特定（匿名性あり）」
A-4		【所属】 システム所管との関係は？	「府省庁外」「システム所管の部局に所属している」「システム所管の部局に所属しない府省庁内」
A-5		【頻度】 1人あたりのアクセス頻度は？	「1日に1回程度」「週に1回程度」「月に1回程度」
A-6		【利用時間】 1日の主な利用時間帯は？	「日中」「日中及び夜間（0時以降除く）」「24時間」
A-7		【信頼性】 役割どおりに振る舞えるか？	「誤操作が発生しやすい（マニュアル等を読まない）」「誤操作はあまり発生しない（役割どおりに振る舞えることが多い）」「運用規定に従って確実な操作を行える（ほぼ確実に役割どおりに振る舞える）」
B-1	情報	【数量】 おおよそのデータ量は？	「1000文字以内」
B-2		【所有者】 情報の所有者は誰か？	「利用者」「サービス提供者」
B-3		【範囲】 公開・提供可能な範囲は？	「制限なし」「制限あり」

【パブリックコメント】

ID	観点	設問	回答例
B-4		【漏えい】漏えい時の影響度は？	「利用者に金銭被害が発生」「利用者に回復不可能な被害が発生」「サービス提供者に回復不可能な被害が発生」「特になし」
B-5		【改変】不正改変時の影響度は？	「利用者に金銭被害が発生」「利用者に回復不可能な被害が発生」「サービス提供者に回復不可能な被害が発生」「特になし」
B-6		【取扱】閲覧のみか？変更が発生するか？	「閲覧のみ」「変更あり」
B-7		【保存】システム内に保存するか？	「サーバ内に保存（保存期限なし）」「サーバ内に保存（保存期限あり）」「保存しない」
B-8		【検証】完全性の事後検証は必要か？	「必要」「不要」
C-1	利用環境・手段	【伝達手段】情報を送受信する方法は？	「Web ブラウザ」「専用ソフトウェア」「媒体」
C-2		【処理環境】サーバ又は端末の種類は？	「サーバ」「クライアント PC」「携帯電話」
C-3		【通信環境】利用するネットワークは？	「内部ネットワーク」「専用回線」「インターネット」
C-4		【通信環境】 外部からの遠隔利用は必要か？	「必要」「不要」
C-5		【信頼性】異常停止の許容時間は？	「数時間」「半日程度」「1日程度」「数日程度」「1週間程度」「特になし」

5章 セキュリティ要件の策定

この章では、4 章にて検討した業務要件を材料として、調達担当者が情報システムに必要なセキュリティ対策を検討し、調達仕様書に記載するべきセキュリティ要件を策定する。

本マニュアルでは、情報システムにおいて考えられる基本的なセキュリティ対策のための要件を表 11 に示す構成の「対策要件集」にまとめている。

この対策要件集は、セキュリティ対策をその目的に応じて図 3 のように6種類の大区分(以下「対策区分」という。)に整理し、対策区分の中には対策の方向性を表す中区分(以下「対策方針」という。)を設けている。さらに、各対策方針には合致するいくつかの具体的な対策方法の要件の小区分(以下「対策要件」という。)を定め、対策要件ごとにその実施レベル(3 段階)に対応する調達仕様書の記載例を掲載している。

調達担当者は、この対策要件集から調達仕様書に記載する対策要件を選定する。本マニュアルでは、この作業をできる限り定型的に行えるようにするため、優先的に実施することが望ましい対策要件を判断するための条件(これを「判断条件」と呼ぶ)を定めている。

次節以降では、このような対策要件集及び判断条件を利用して、調達仕様書にセキュリティ要件を記載する方法を解説する。

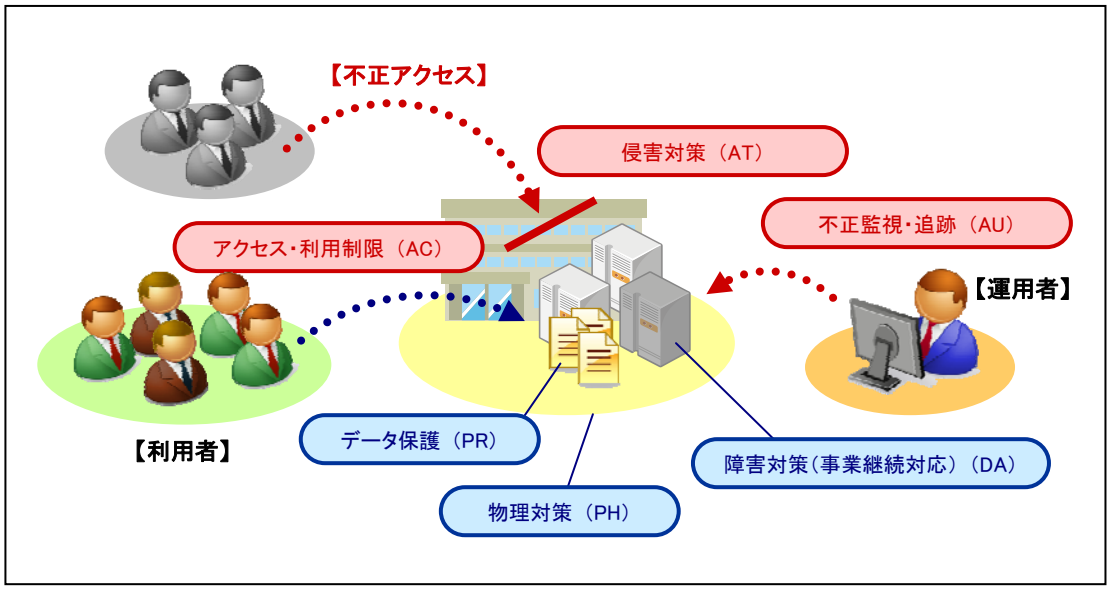


図 3 対策要件集における対策区分

表 11 対策要件集の構成

対策区分	対策方針	対策要件	判断条件対応関係（※）	実施レベル有無		
				低位	中位	高位
侵害対策 (AT: Attack)	通信回線対策(AT-1)	通信経路の分離 (AT-1-1)	A or F		有	有
		不正通信の遮断 (AT-1-2)	A		有	
		通信のなりすまし防止 (AT-1-3)			有	有
		サービス不能化の防止 (AT-1-4)			有	有
	不正プログラム対策 (AT-2)	マルウェアの感染防止 (AT-2-1)	-	有		
		マルウェア対策の管理 (AT-2-2)	A or B			有
	セキュリティホール対策 (AT-3)	構築時の脆弱性対策 (AT-3-1)	-	有		
		運用時の脆弱性対策 (AT-3-2)	A	有	有	
不正監視・追跡 (AU: Audit)	証跡管理(AU-1)	証跡の蓄積・管理 (AU-1-1)	B or C	有	有	
		証跡の保護 (AU-1-2)		有	有	有
		時刻の正確性確保 (AU-1-3)	-	有		
	不正監視(AU-2)	侵入検知 (AU-2-1)	A		有	有
		サービス不能化の検知 (AU-2-2)				有
アクセス・利用制限 (AC: Access)	主体認証(AC-1)	主体認証 (AC-1-1)	D		有	有
	アカウント管理(AC-2)	ライフサイクル管理 (AC-2-1)	D		有	
		アクセス権管理 (AC-2-2)	D and E			有
		管理者権限の保護(AC-2-3)	-	有		
データ保護 (PR: Protect)	機密性・完全性の確保 (PR-1)	通信経路上の盗聴防止 (PR-1-1)	B or C		有	
		保存情報の機密性確保 (PR-1-2)			有	有
		保存情報の完全性確保 (PR-1-3)				有
物理対策 (PH: Physical)	情報搾取・侵入対策 (PH-1)	情報の物理的保護 (PH-1-1)	-	有		
		侵入の物理的対策 (PH-1-2)		有		
障害対策（事業継続対応） (DA: Damage)	構成管理(DA-1)	システムの構成管理 (DA-1-1)	B	有	有	
	可用性確保(DA-2)	システムの可用性確保 (DA-2-1)	-	有		

※ 各対策要件の判断条件対応関係に記載の判断条件が満たされる場合、当該対策要件については「中位」又は「高位」の実施レベルに対応する仕様書記載例の採用を検討し、判断条件対応関係が「－」の対策要件については判断条件の結果によらず「低位」の実施レベルに対応する仕様書記載例の採用を検討することを表す。(5.1 節参照)

5.1 判断条件による対策方針の検討（ステップ 5）

調達担当者は、表 11 の各対策要件について、それぞれ優先的に実施すべき対策であるか否かを検討する。具体的には、4 章にて検討した業務要件を踏まえ、表 11 の各対策要件の「判断条件対応関係」の欄に記載のアルファベットに該当する判断条件（表 12）が満たされるか否かを検討する。

確認の結果、該当する判断条件が満たされていない場合または「判断条件対応関係」の欄が空欄である場合は、その対策要件については「低位の実施レベルに該当する仕様書記載例の採用を次節以降で検討する。一方、該当する判断条件が満たされる場合は、その対策方針について「中位または高位」の実施レベルの仕様書記載例の採用」を次節以降で検討する。

以下は、上記の考え方に基づく検討の例であり、同様の例を図 4 に示す。

■ AT-1-1 の場合

表 11 において、AT-1-1 の「判断条件対応関係」の欄には「A or F」と記載されている。例えば、「A」または「F」の判断条件が満たされる場合、「中位」または「高位」の実施レベルに該当する仕様書記載例の採用を検討すること。一方、指定の判断条件が満たされない場合には「低位」の仕様書記載例を採用することになるが、AT-1-1 は低位の仕様書記載例が定められていないため省略となる。

■ AT-2-1 の場合

「判断条件対応関係」の欄は空欄（「-」）である。このような対策要件については、判断条件の結果によらず、「低位」の仕様書記載例を採用すること。

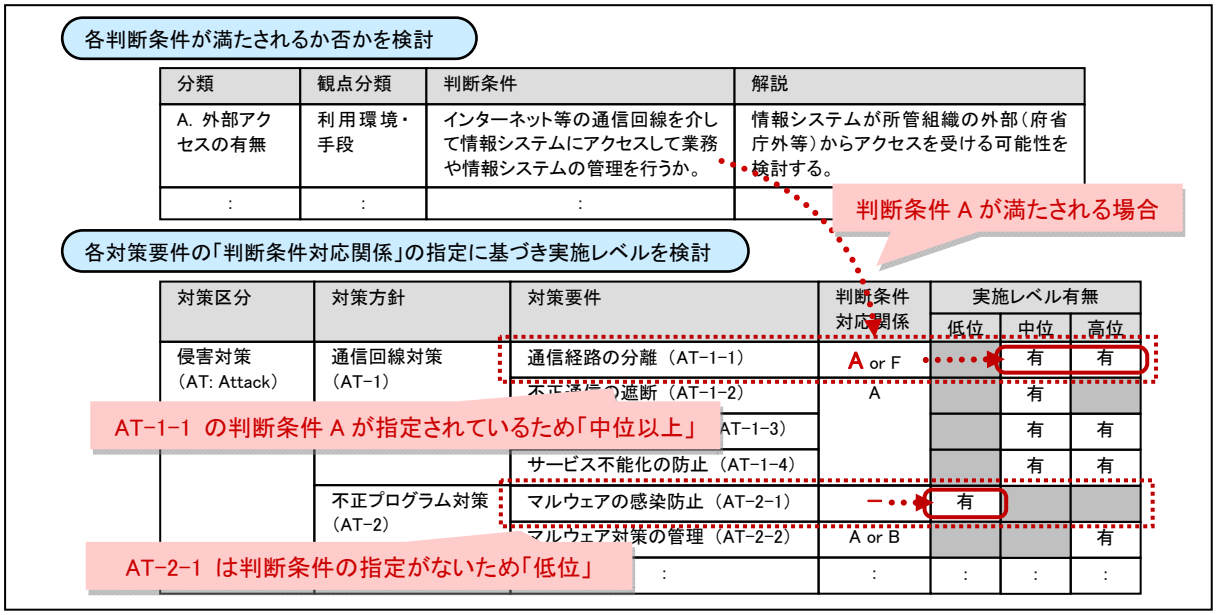


図 4 判断条件による検討の例

表 12 対策方針決定のための「判断条件」

名称	観点分類	判断条件	解説
A. 外部アクセスの有無	利用環境・手段	インターネット等の通信回線を介して（情報の管理ポリシーが異なる）外部から情報システムにアクセスしてサービスの利用、業務の遂行、情報システムの管理等を行うか。	情報システムを所管する組織の外部（情報管理ポリシーが異なる外部）からアクセスを受ける可能性を検討する。判断にあたっては、ステップ 2 の利用環境・手段の検討結果、定型設問 C-3、C-4 等を参考にすると良い。
B. 情報の重要度	情報	漏えいした場合や正常にアクセスできない場合に、深刻な損害を被る可能性がある重要性の高い情報を取り扱うか。	漏えい、改ざん、消失等によって発生するプライバシー侵害や金銭的被害等の損害の度合いを見極め、情報の重要性を検討する。判断にあたっては、例えば、定型設問 B-3 の情報の取り扱い範囲、B-4、B-5 の損害度合の回答を参考にすると良い。
C. 情報受信後の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保存する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか。	情報の重要性が非常に高く物理対策が突破されることも想定する必要がある場合、あるいはモバイル PC による情報処理が必要な場合などは追加的対策が重要になる。判断にあたっては、定型設問 B-7 にてシステム内に保存することを確認している場合かつ定型設問 B-4、B-5 の想定被害の程度を考慮すると良い。
D. 利用者の限定要否	主体	情報システムにアクセスする主体は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか。	情報システムのサービスや業務機能を、特定の利用者や運用者のみに提供するか否かを検討する。判断にあたっては、定型設問 A-3 にて確認された主体の集合特性を参考にすると良い。
E. アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか。	利用者や運用者に応じてアクセス権を管理し、アクセス権に応じてサービスや業務機能の提供内容を制御する必要があるか否かを検討する。例えば、ステップ 2 にて情報システムの利用者として多様な主体が洗い出され、主体の種類ごとに提供する機能やサービスを切り替える等の制御が必要である場合には本判断条件に合致する可能性がある。
F. 複数部局による利用	主体	情報の取り扱い方や利用目的等が異なる複数の部局等の間で共用されるか。	情報システムを広く共用するが、情報システム内の情報管理体制の異なる部局ごとに分け、互いにアクセスできない状態を保つ必要性があるか否かを検討する。例えば、ステップ 2 にて情報システムを利用する主体として多様な主体が洗い出され、各主体の所属が情報管理ポリシーの異なる部局である場合に本判断条件に合致する可能性がある。

5.2 対策要件の決定（ステップ 6）

調達担当者は、調達仕様書に記載する対策要件を決定する。前節の検討結果に応じて、対策要件ごとに以下のように検討する。

- **「低位」の実施レベルの仕様書記載例の採用を検討する場合**

  低位の実施レベルに該当する仕様書記載例の内容や一般的な実現例を参考にして、調達コスト等を勘案して調達仕様書の記載内容を検討する。低位の仕様書記載例が示されていない対策要件の場合は、調達仕様書に記載すべき仕様書記載例はないとみなす。

- **「中位」または「高位」の実施レベルの仕様書記載例の採用を検討する場合**

  「付録A. 対策要件集」に記載されている「実施レベルの選定の考え方」を参考にして、「中位」と「高位」のどちらの仕様書記載例を採用するべきかを検討する。また、費用対効果の観点から可能な限り「中位」の実施レベルの仕様書記載例を採用することが望ましい。なお、検討の結果、「高位」の仕様書記載例を採用する必要はないと判断された対策要件のうち「中位」の仕様書記載例が示されていない対策要件については記載を省略する。

5.3 調達仕様書への反映（ステップ 7）

調達担当者は、仕様記載例を決定した後は、対策要件集の「仕様書記載時の注意事項」の解説及び以下の点に留意して調達仕様書の該当部分に記載する。

(1) 記載内容のさらなる具体化

本マニュアルの判断条件等によって導出された対策要件の一部については、対策要件集の仕様書記載例のままではなく、調達するシステムのより詳細な特性に応じて記載内容を慎重に検討し、具体化する必要がある。

(2) 対策要件の記載箇所

本マニュアルによる検討結果を調達仕様書に記載する際の記載箇所を表 13 に例示したが、記載箇所に迷う場合は少なくとも表 1 の「6. 情報セキュリティ要件」の項目に記載すると良い。

(3) 既存設備の利用を想定した仕様の調整

既存の情報システムとネットワーク設備を共用する等のように既存の設備を用いる場合で、当該設備によって既に満たされている対策要件が存在する場合には、当該対策要件を調達仕様にそのまま記載するのではなく、当該設備を共用することを調達にあたっての前提条件として調達仕様書に記載する。

(4) 記載内容の妥当性の点検

仕様書記載時の注意事項が指定されていない対策要件については、仕様書記載例の例文を修正することなく記載することが可能である。ただし、調達する情報システムの特性を考慮して記載内容の妥当性を点検することが望ましい。この点検作業にあたっては、各対策要件の解説に記載されている「想定脅威」「効果」「一般的な実現方法」等の情報を参考にすると良い。また、最高情報セキュリティアドバイザー及び各府省情報化統括責任者（CIO）補佐官に記載内容の妥当性の確認を求め、必要な助言を受けた上で記載内容を改善するなどにより、その妥当性の担保を行うこと。

表 13 本マニュアルの検討結果の記載箇所の例（調達指針の記載例の場合）

記載内容		記載箇所の例
名称		「1. 調達件名」
業務、主体、情報、利用環境・手段の洗い出し結果		「2. 作業の概要」の「(1) 目的」及び「(2) 業務の概要」
システム概要図		「7. 情報システム稼働環境」の「(1) 全体構成」
定型設問の回答		「2. 作業の概要」
対策要件	通信経路の分離（AT-1-1）	「6. 情報セキュリティ要件」
	不正通信の遮断（AT-1-2）	「6. 情報セキュリティ要件」
	通信のなりすまし防止（AT-1-3）	「6. 情報セキュリティ要件」
	サービス不能化の防止（AT-1-4）	「6. 情報セキュリティ要件」
	マルウェアの感染防止（AT-2-1）	「6. 情報セキュリティ要件」
	マルウェア対策の管理（AT-2-2）	「6. 情報セキュリティ要件」
	構築時の脆弱性対策（AT-3-1）	「8. テスト要件定義」
	運用時の脆弱性対策（AT-3-2）	「11. 保守要件定義」
	証跡の蓄積・管理（AU-1-1）	「6. 情報セキュリティ要件」
	証跡の保護（AU-1-2）	「6. 情報セキュリティ要件」
	時刻の正確性確保（AU-1-3）	「6. 情報セキュリティ要件」
	侵入検知（AU-2-1）	「6. 情報セキュリティ要件」
	サービス不能化の検知（AU-2-2）	「6. 情報セキュリティ要件」
	主体認証（AC-1-1）	「6. 情報セキュリティ要件」
	ライフサイクル管理（AC-2-1）	「6. 情報セキュリティ要件」
	アクセス権管理（AC-2-2）	「6. 情報セキュリティ要件」
	管理者権限の保護(AC-2-3)	「6. 情報セキュリティ要件」
	通信経路上の盗聴防止（PR-1-1）	「6. 情報セキュリティ要件」
	保存情報の機密性確保（PR-1-2）	「6. 情報セキュリティ要件」
	保存情報の完全性確保（PR-1-3）	「6. 情報セキュリティ要件」
	情報の物理的保護（PH-1-1）	「10. 運用要件定義」の「(3) 運用施設・設備要件」
	侵入の物理的対策（PH-1-2）	「10. 運用要件定義」の「(3) 運用施設・設備要件」
	システムの構成管理（DA-1-1）	「6. 情報セキュリティ要件」
	システムの可用性確保（DA-2-1）	「5. 信頼性等要件」の「(1) 信頼性要件」

※「記載箇所の例」の欄に記載の各項目は、表 1 の項目に対応している。

6章 その他の考慮事項

(1) 対策要件集及び政府機関統一基準群の関係について

調達担当者は、対策要件集を参考にして調達仕様書を作成することによって、「付録B. 政府機関統一基準群対応表」に示すとおりに政府機関統一管理基準及び統一技術基準の各遵守事項と対応関係を持つ調達仕様書を作成することができる。付録Bを参考にして調達仕様書を確認した結果、調達担当者が内容に過不足があると判断した場合には、政府機関統一管理基準及び統一技術基準の遵守事項を踏まえ調達仕様書の記載内容を見直すこと。

(2) 開発の環境及び作業実施上のセキュリティ確保について

政府機関統一管理基準の遵守事項 1.5.2.3(1)(a)には、ソフトウェア開発に関して「統括情報セキュリティ責任者は、ソフトウェア開発について、セキュリティに係る以下の対策事項を情報システムセキュリティ責任者に求めるための規定を整備すること。」と規定されている。当該遵守事項を踏まえ、表 1に示した調達仕様書の項目のうち「12 作業の体制及び方法」等に必要事項を記載すること。

(3) 政府ドメインの利用について

政府機関統一管理基準の遵守事項 1.5.2.7(1)(a)では、政府機関の情報システムが使用するドメイン名に関して規定している。当該遵守事項の内容を考慮し、ドメイン名の取得や利用が調達範囲に含まれる場合には、調達仕様書に必要事項を記載すること。

(4) 性能に関する将来の見通しの必要性について

政府機関統一技術基準の遵守事項 2.3.2.1(1)(a)では、「情報システムセキュリティ責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を将来の見通しを含め検討し、確保すること。」と規定されている。また、遵守事項 2.3.4.1(1)(b)では、情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、通信回線及び通信回線装置に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。」と規定されている。当該遵守事項を踏まえ、表 1 に示した調達仕様書の項目のうち「4 規模・性能要件」等に、情報システムの運用予定期間を考慮した仕様を記載すること。

(5) 暗号アルゴリズムについて

政府機関統一管理基準の遵守事項 1.5.2.5(1)(a)(ア)では、暗号化及び電子署名に用いる暗号アルゴリズムについて、「電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること。」と規定されている。調達仕様書において暗号化及び電子署名を用いる対策を求める場合には、この遵守事項及び情報システムの運用期間中の危殆化の可能性が高い暗号アルゴリズムを利用しないことを求める内容も合わせて記載すること。