DM6-07-071

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

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	各府省庁意見に基づく修正及び表現整備
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のセキュリティ要件作成マニュアル」（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を外部委託により行う場合に、調達者が、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、もって府省庁が調達する情報システム等における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する。

1 章では、セキュリティ要件とセキュリティ機能を検討する際の基本的な考え方と、調達者がセキュリティ要件を提示し、提案仕様を審査する手順の概要を説明する。

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」を作成する際の考え方と手順を説明する。また、付録 A で、セキュリティ要求仕様に記載する項目を説明する。

3 章では、調達に応じて提案者が作成し、応札関係書類に含める「セキュリティ提案仕様」を調達者が審査する際の考え方と手順を説明する。また、付録 B で、セキュリティ提案仕様に記載する項目を説明する。

付録 C では、調達者が機器等の購入に活用する観点から、IT セキュリティ評価及び認証制度について説明する。

参考例Ⅰ～参考例Ⅲでは、様々な情報システムを題材にして、セキュリティ要求仕様の作成方法とセキュリティ提案仕様の審査方法の例を示している。実際の調達に当たっては、それぞれの情報システムで前提条件、求める情報セキュリティ水準等が異なることに留意し、参考例の内容を検証して、加筆・修正を加えた上で利用することが必要である。

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調達者
- 府省庁において情報システムを構成する機器又はソフトウェア製品（以下「機器等」という。）を調達する調達者

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及び機器等の調達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

- 「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」（DM6-08-071）

  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の実施について説明している。

- 「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)」（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で示す場合がある。

- 「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」「外部委託における情報セキュリティ対策実施規程」又は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」と記す。

- 「ISO/IEC 15408: 2005　Information technology – Security techniques- Evaluation criteria for IT security -- Part1, 2, 3」

  以下、「ISO/IEC 15408」と記す。

- 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. セキュリティ要件の検討方法

1.1. セキュリティ要件の検討の基本的な考え方

情報システムにおける情報セキュリティ対策を検討する場合、対象となる情報システムが取り扱う情報やデータに対してどのような「脅威」が存在するかを想定する。脅威が存在するからこそ、何らかの「対策」が必要となる。

例えば、相手に手紙を送る場合、他人に中身を読まれるという脅威が存在するのであれば、封緘をし、価値が高いものを送るのであればさらに書留を利用するといった付加的な対策を行うことが考えられる。これを電子メールに置き換えれば、暗号化技術により、メッセージを暗号化するとともに受信者を限定するといった対策を行うことに相当するといえる。

情報システムが具備すべきセキュリティ機能は、「何を（情報資産）」「何から（脅威）」「どのように守る（対策）」必要があり、したがって「この機能」が必要である、という考え方で決定することが重要である。この流れで検討することにより、過剰なセキュリティ機能を要求したり、逆に不足したりすることを防ぎ、バランスの取れたセキュリティ機能を要求することができる。

1.2. 脅威と対策の基本的な考え方

情報セキュリティにおける「脅威」とは、「保護すべき情報資産」について、確保されるべき「機密性」、「完全性」及び「可用性」を損なわせる可能性のある要因のことである。

政府機関統一基準では、「機密性」、「完全性」及び「可用性」を以下のように定義している（政府機関統一基準「1.1.3 用語定義」）。

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。

一般的に考えられる「脅威」とそれに対する「対策」の例を以下に示す。

- [脅威 1] アカウントのない者がデータにアクセスする。
  → [対策] 主体認証
  → [対策] 主体認証のふるまいに対する証跡管理

- [脅威 2] アカウントのある者が権限を越えたデータアクセスを行う。
  → [対策] アクセス制御及び権限管理
  → [対策] アクセス制御及び権限管理のふるまいに対する証跡管理

- [脅威 3] 利用者のなりすましやデータの改ざんが行われる。
  → [対策] 電子署名によるデータの保護

- [脅威 4] 通信路上のデータが盗聴される。
  → [対策] データの暗号化

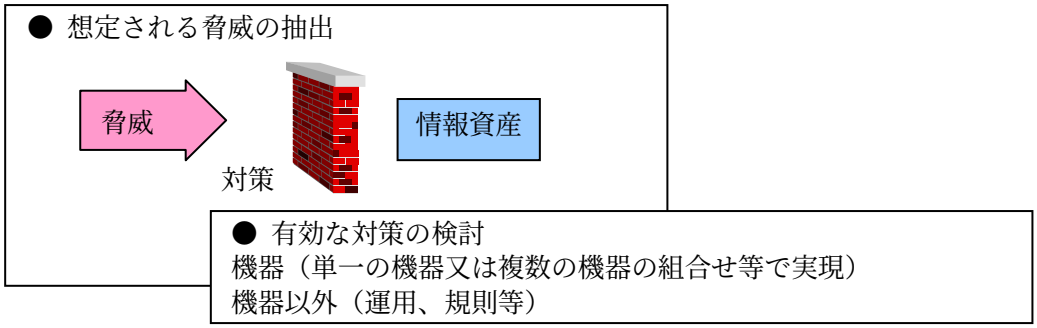


図1-1 脅威と対策の基本的な考え方

1.3. 基本的なセキュリティ機能の概観

政府機関統一基準では、情報セキュリティについての機能として、主体認証、アクセス制御、権限管理、証跡管理、暗号と電子署名が示されている。これらの基本的なセキュリティ機能による対策の概観を図 1-2に示す。

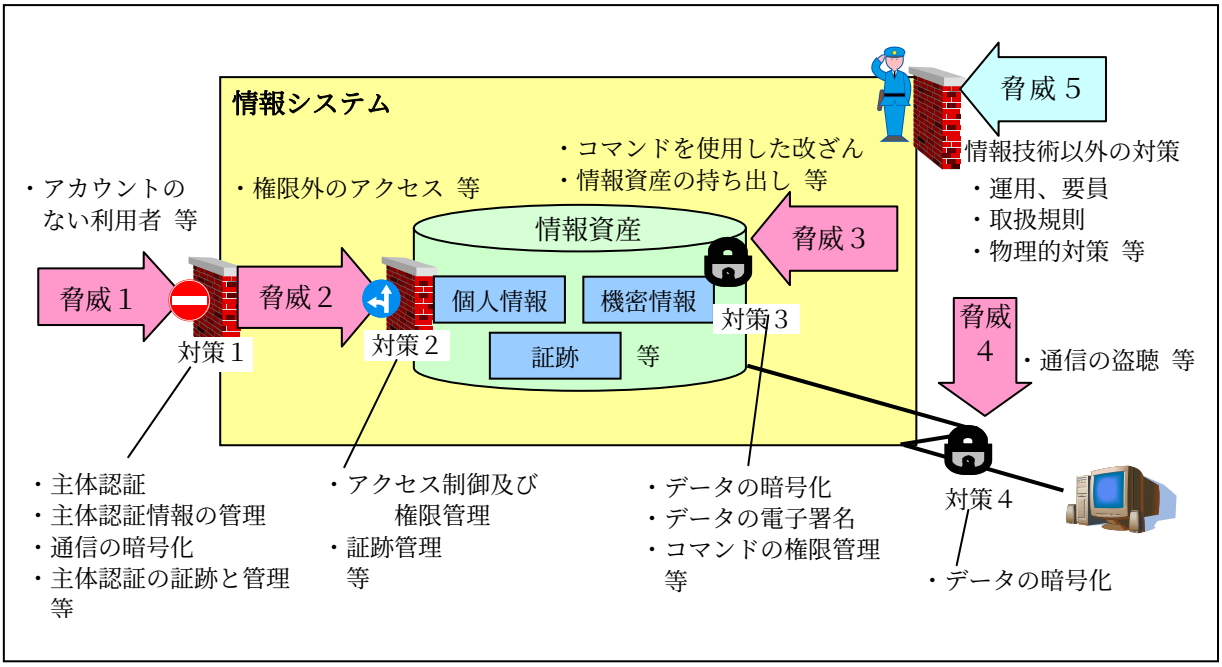


図1-2 基本的なセキュリティ機能による対策の概観

1.4. 脅威と対策の分析

情報システムのセキュリティを確保するためには、想定される脅威に対して必要となる対策を漏れなく組み込んだシステム設計が必要となる。このようなシステム設計では、まず、情報システム全体を俯瞰し、情報資産に対する脅威の洗い出しを行い、それぞれの脅威について、情報システムの構成要素である機器の技術による対策をすべき脅威か、施設等の物理的環境や規則等に基づく運用で対策又は回避をすべき脅威かについて体系的に分類する。例えば、情報システムに許可なく触れさせないために行う入退室管理は、施設による物理的な対策の例である。インターネットを通した不正侵入への対策として導入するファイアウォールは、機器等の技術による対策の例である。また、資格のない者によるデータベースに対するアクセスへの対策として利用するデータベースマネジメントシステム

の主体認証機能も、機器等による技術的な対策の例である。機器等で対策すべき脅威に対しては、それぞれの機器等についてセキュリティ要件をとりまとめ、対策として機器等で装備するセキュリティ機能を決定することになる。なお、情報システムの構成要素である機器等には、

① サーバ装置、端末、通信回線装置等のハードウェア
② 汎用のソフトウェア
③ 開発ソフトウェア

がある。

このような検討の手順は、適切な情報セキュリティ対策を備えた情報システムを設計するために必要なものである。

情報システムにおいてセキュリティ機能が適切に設計されていることを第三者機関が客観的に確認する制度に、「ST 評価・ST 確認」がある。この制度では、情報システムのセキュリティ要件及び設計情報に基づいて開発者がセキュリティ設計仕様書（セキュリティターゲット、ST）を作成して、そのセキュリティ機能について国際標準の ISO/IEC 15408 に基づく評価・確認を受ける。また、情報システムを構成する個別のソフトウェアを開発する場合にも、そのソフトウェアにおいてセキュリティ機能が適切に設計されていることを第三者機関が確認する制度として、ST 評価・ST 確認が利用できる。政府機関統一基準では、情報システムセキュリティ責任者が、構築する情報システム及び開発ソフトウェアについて重要なセキュリティ要件があると認めた場合には、ST 評価・ST 確認を受けることを求めている（政府機関統一基準 4.3.1 (1) (d)及び 6.1.3 (3) (e)）。ST 評価・ST 確認については、「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）を参照されたい。

1.5. 調達におけるセキュリティ要件の提示と提案仕様の審査

前節までに、情報システムにおけるセキュリティ要件と対策の一般的な考え方を説明した。情報システムの構築等を調達する場合には、情報セキュリティ対策を委託先に行わせるため、調達者が求めるセキュリティ要件を提案者に明確に伝え、提案仕様を十分に審査することが、適切な情報セキュリティ対策を実現する上で重要である。

1.5.1. 情報システムの構築等を外部委託する場合の手順

情報システムの構築等を外部委託する場合の、調達から検収までの一般的な業務の流れを図 1-3 に示す。

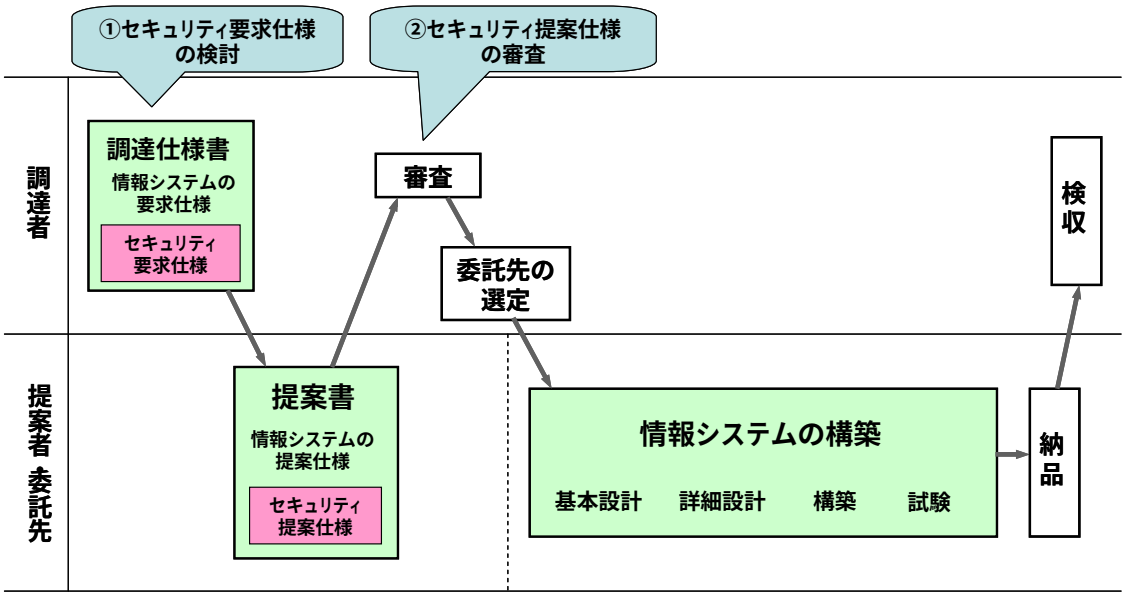


図1-3 調達から検収までの手順

一般に、調達者は調達仕様書に情報システムの要求仕様を記載し、提案者が情報システムの提案仕様を記載した提案書を提出し、調達者が提案書の内容を審査して委託先を決定する。その後、委託先が設計、構築、試験を実施し、各工程の成果が要求仕様を満足していることが確認されると、検収が合格となり納品が完了する。

この手順において、セキュリティ要件及びセキュリティ機能について、調達者と提案者の間で以下のやり取りを行うことが重要である。

- 調達者が、セキュリティ要件を整理した「セキュリティ要求仕様」を調達仕様書に記載し提示すること。
- 提案者が、セキュリティ要求仕様に応えるセキュリティ機能を含む情報セキュリティ対策である「セキュリティ提案仕様」を提案仕様書に記載して提出すること。
- 調達者が、セキュリティ提案仕様を審査すること。

セキュリティ要求仕様及びセキュリティ提案仕様については、次項以降で説明する。

1.5.2. セキュリティ要求仕様とセキュリティ提案仕様

セキュリティ要求仕様及びセキュリティ提案仕様の構成と、本書との関係を図 1-4 に示す。

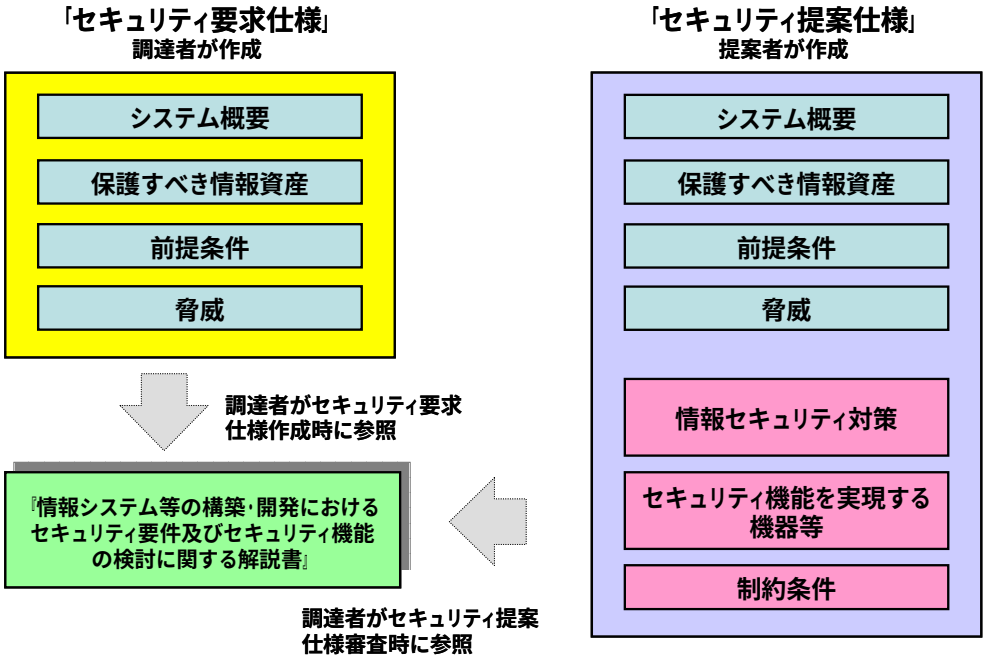


図1-4 セキュリティ要求仕様及びセキュリティ提案仕様の構成と本書の関係

セキュリティ要求仕様には、調達者が「システム概要」「保護すべき情報資産」「前提条件」及び「脅威」を記載する。その作成手順は、本書の第 2 章で説明する。また、セキュリティ要求仕様に記載する項目については、付録 A を参照されたい。

セキュリティ提案仕様には、提案者がセキュリティ要求仕様の内容に加えて、「情報セキュリティ対策」、「セキュリティ機能を実現する機器等」及び「制約条件」を記載する。セキュリティ提案仕様を審査する方法は、本書の第 3 章で説明する。また、セキュリティ提案仕様に記載する項目については、付録 B を参照されたい。

1.5.3. セキュリティ要求仕様に関する留意点

セキュリティ要求仕様及びセキュリティ提案仕様を前項の手順に従いやり取りする場合には、調達者は、以下の点に留意して調達手続きを準備する。

- 調達者は、セキュリティ要求仕様を作成し、セキュリティ提案仕様を正しく評価するための能力を確保すること。
- 提案者が具体性の高いセキュリティ提案仕様を作成するために十分なセキュリティ要求仕様を調達者が提示すること。このためには、調達者は、外部委託を行うに当たり、情報システム等の概要、保護すべき情報資産、前提条件及び脅威を十分に明らかにすること。
- 調達者は、特に、調達する情報システム等の外部の条件である物理的条件（建家、電源、入退室管理等）及び運用条件（省庁対策基準で定め、又は当該情報システム等に関する実施手順で定めることとなる運用に関する事項等）について、セキュリティ要求仕様において提示すること。
- 調達者によるセキュリティ要求仕様の作成、提案者によるセキュリティ提案仕様の作成及び調達者によるセキュリティ提案仕様の審査について、技術的な検討に必要な期間を確保すること。

セキュリティ提案仕様を適切に審査するためには、構築する情報システム等について、セキュリティ要求仕様に含める事項が具体化されていることが必要である。これが十分に具体化されていない場合には、セキュリティ提案仕様を評価する前提が提案ごとに異なることとなり、公平な評価が困難になる。[1]

[1] 提案者が、セキュリティ要求仕様におけるこれらの外部条件が不足しているか不明確であると判断した場合には、提案の前提を明確にするために、セキュリティ提案仕様において外部条件の追加又は変更を提案することも考えられる。調達の透明性を確保するためには、提案者が外部条件を提案する必要が生じないように、セキュリティ要求仕様において十分な情報を提示することが重要である。

2. セキュリティ要求仕様の作成手順

セキュリティ要求仕様を作成する手順を以下に説明する。

2.1. 基本的な方針

セキュリティ要求仕様をまとめる際には、以下の方針に従うものとする。

１）「政府機関統一基準」に基づく省庁対策基準の遵守[2]

- 「情報」を守ることを目的とする（政府機関統一基準 1.1.2「(2) 適用対象範囲」））。
- 機密性、完全性及び可用性の観点から情報の格付けを行う（同 3.1.1「(1) 情報の格付け」）。
- 情報セキュリティについての機能は、①主体認証機能、②アクセス制御機能、③権限管理機能、④証跡管理機能、⑤保証のための機能、⑥暗号と電子署名の６つの機能を基本とする（同「4.1 情報セキュリティについての機能」）。
- 情報セキュリティについての脅威への対策として、①セキュリティホール対策、②不正プログラム対策、③サービス不能攻撃対策を含む対策を実施する（同「4.2 情報セキュリティについての脅威」及び「第 5 部 情報システムの構成要素についての対策」）。

２）「最適化ガイドライン」の適用[3]

- 本書では、情報システムの構築等を「最適化ガイドライン」に定められた工程、文書体系等に沿って行うものとする。

[2] 府省庁においては、省庁対策基準及びこれに基づく各種実施手順に従って情報セキュリティ対策を講ずるため、政府機関統一基準が直接に府省庁に適用されるわけではない。ただし、省庁対策基準及びこれに基づく各種実施手順は府省庁ごとのものであるため、本書では、便宜上、共通に参照できる政府機関統一基準を遵守するものとして説明している箇所がある。

[3] 本書では、情報システムの構築には「業務・システム最適化指針（ガイドライン）」（「最適化ガイドライン」）が適用されるものとして、構築において作成する仕様書の体系、名称や内容も、この指針に合わせて記述している。ただし、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に関する本書の説明は、業務・システム最適化の対象でない情報システム構築等に対しても一般的に有効である。

2.2. セキュリティ要求仕様の作成

「最適化ガイドライン」では、その「第２　業務システム最適化企画指針（ガイドライン）」において「仕様書（要件定義書）」（以下「要件定義書」という。）の策定を求めている。この仕様書からセキュリティ要求仕様を導く手順を以下にまとめる。「最適化ガイドライン」の対象とならない調達においては、「最適化ガイドライン」における要件定義書に相当するドキュメントから必要な情報を抽出することができる。

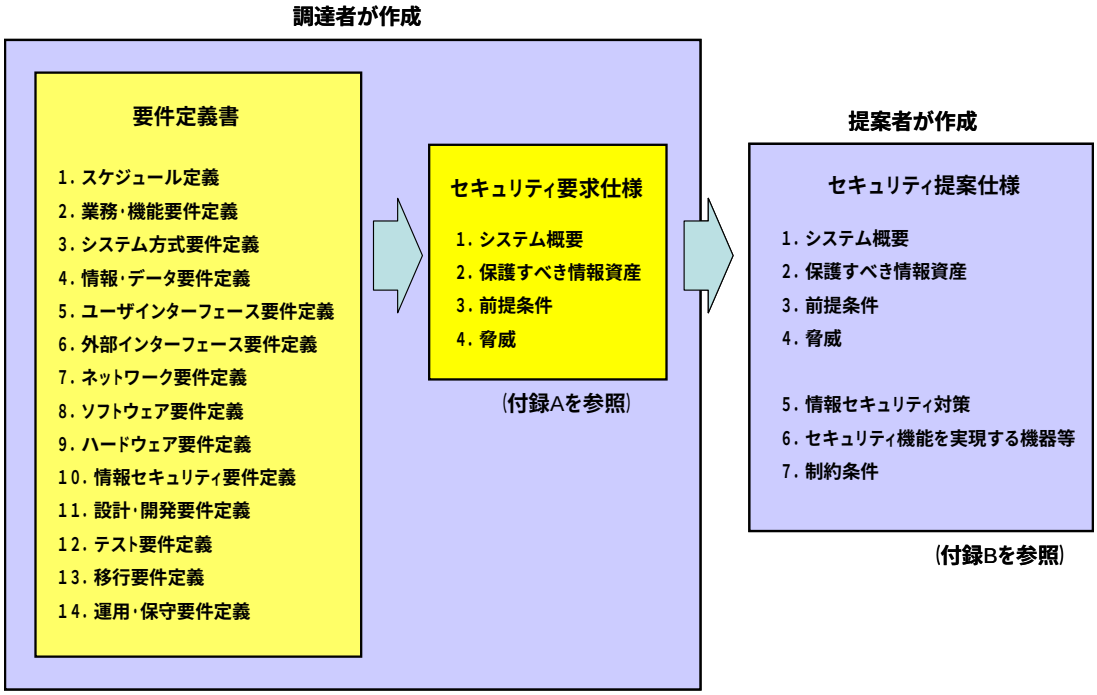


図2-1 セキュリティ要求仕様とセキュリティ提案仕様の関係

要件定義書、セキュリティ要求仕様及びセキュリティ提案仕様の関係を図 2-1に示す。調達者は、要件定義書に記載されている 14 の要件定義と整合するセキュリティ要求仕様を作成する。

セキュリティ要求仕様は、提案者が情報システムの概要を理解しセキュリティ提案仕様を作成するために必要となる情報（システム概要、保護すべき情報資産、前提条件、想定される脅威）を正しくかつ明確に示したものとする必要がある。セキュリティ要求仕様に記載すべき項目については付録 A を参照されたい。以下にセキュリティ要求仕様のまとめ方について説明する。

2.2.1. システム概要のまとめ方

「システム概要」には、対象とするシステムの構成、想定する利用者及びシステムの機能概要について簡潔に記載する。

システム概要のまとめ方を図 2-2 に示す。

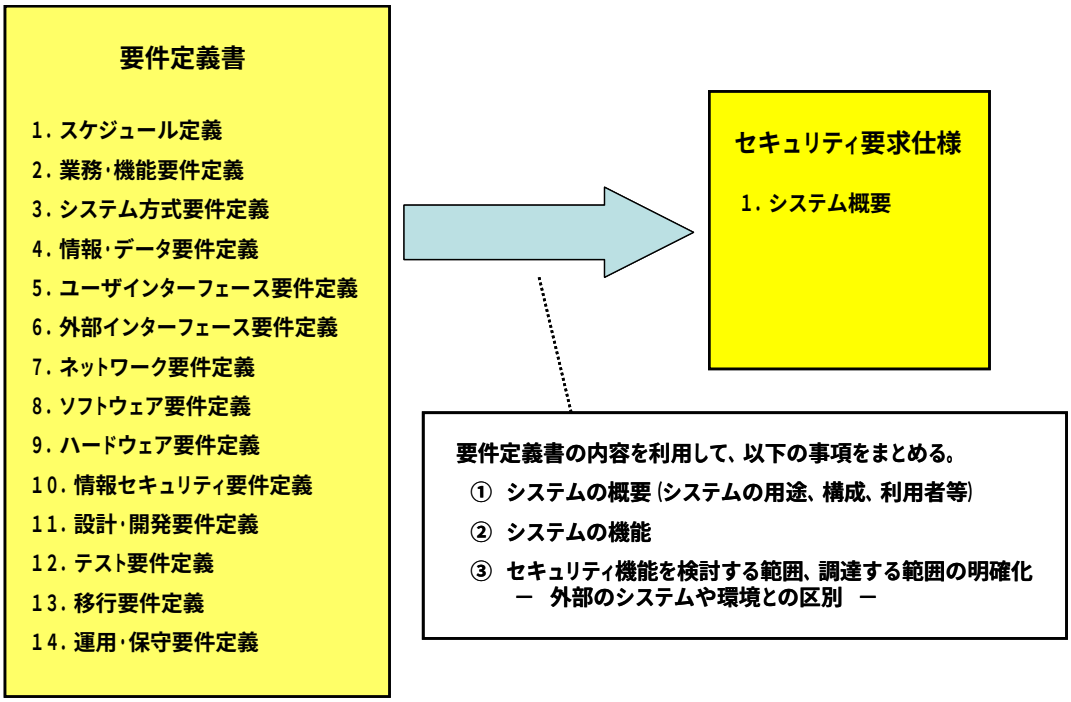


図2-2 システム概要のまとめ方

システム概要をまとめる際には、要件定義書の中で定義している要件の内容を確認し、調達仕様書として一貫した仕様とする。

【注釈】システム概要に記述すべき事項が同時に提示する要件定義書等に具体的に記述されている場合、それらの参照箇所を示すことで、当該事項をセキュリティ要求仕様から省略することもできる。

以下に、システムの構成、想定する利用者及びシステムの機能概要のまとめ方を示す。

2.2.1.1. システムの構成

対象とするシステムの構成を、以下の観点から記述する。

- ネットワーク及び機器構成
- 関連する他システムとの関係

【注釈】連携すべき外部システムが存在する場合、対象とするシステムと外部システムとの間でやり取りされるプロトコルやテータ形式を規定するインタフェースを明確に示す必要がある。

2.2.1.2. 想定する利用者

対象とする情報システム等を運用する際に想定する利用者を書き出し、以下の観点から説明する。この場合の利用者とは、システムを業務のために利用する者だけでなく、システム管理者、システム運用者等、システムに関与するすべての者を含む。

- 役割：システムで行う操作や、責務等について記述する。
- 権限：システムの利用に関して与えられる権限や特権について記述する。

【注釈】本項の記述は、システム運用時に必要なセキュリティ対策を検討するために、当該システムを誰がどのように利用・管理するかをできるだけ明確に示す。

2.2.1.3. システムの機能概要

対象とするシステムが提供するサービス等を記述する。

【注釈】システムの機能概要の記述はセキュリティ機能を理解するために必要なシステムの主なサービス機能の概要記述に留め、サービス機能の詳細は、システム要件及び機能要件等調達仕様書の別の要件定義を参照することとする。

2.2.1.4. システム概要の記述例

以下に「予算執行等管理システム」を例として、セキュリティ要求仕様のシステム概要の記述例を示す。このシステム例は、「物品調達、物品管理、謝金・諸手当、補助金及び旅費の各業務・システム最適化計画」（2004 年（平成 16 年）9 月 15 日各府省情報化統括責任者（CIO）連絡会議決定、
http://www.kantei.go.jp/jp/singi/it2/cio/dai11/11siryou2.pdf）で示された考え方に基づき、経済産業省によってシステム化が進められている「予算執行等管理システム」を参考にしている。以下、本システムを「予算管理システム」という。

セキュリティ要求仕様の例　《1．システム概要》

1.システム概要

1.1.システム全体概要

本予算管理システムは、「物品調達、物品管理、謝金・諸手当、補助金及び旅費に関する各業務・システム最適化計画」に基づきシステム化を行うものである。

予算管理システムのアプリケーションは、各業務を処理する個別業務アプリケーション、決議書等の文書の「起案」から「審査」、「決裁」、「他の関連システムへのデータ連携」という一連の業務プロセスを実現する共通業務アプリケーションから構成され、職員情報を管理する人事・給与関係業務情報システムや会計事務システム等の関連システムと連携することで実現される。このような業務処理の一元化・集中化により、システムや情報の安全性・信頼性を確保するとともに、システム構造上の汎用性・拡張性を確保し、かつ運用におけるコスト低減と省力化を目指す。予算管理システムで扱うアプリケーションの範囲を図 1.1 に示す。

なお、システムの各要件の詳細については、本調達仕様書の分冊「業務要件」、「情報・データ要件」、「機能要件」、「システム要件」、「運用要件」、「移行要件」、「セキュリティ要件」及び各種別添資料に示す。

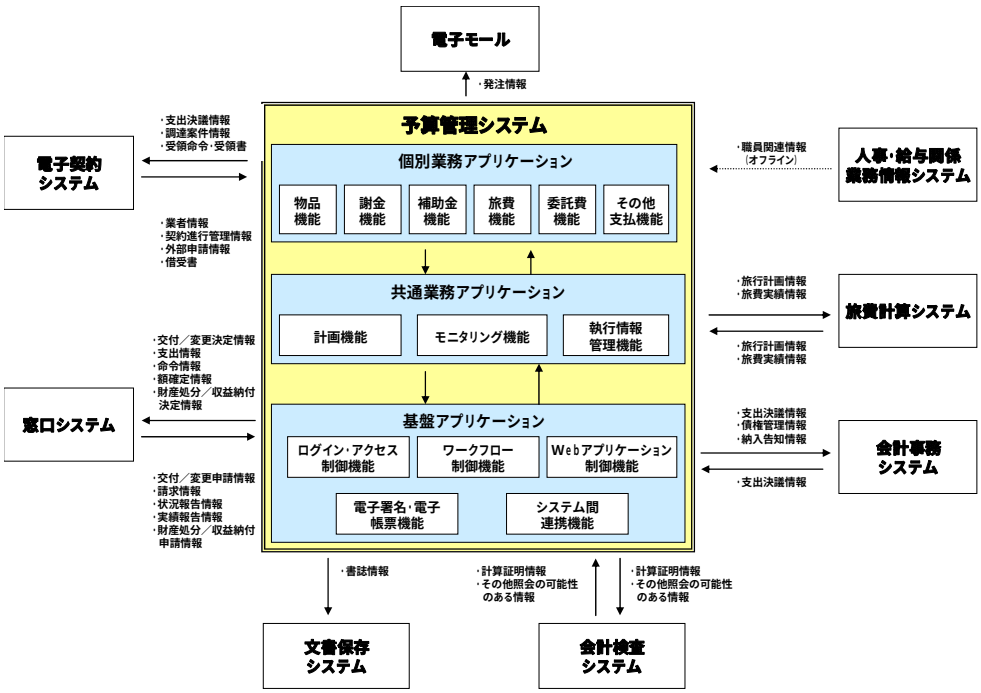


図 1.1 予算管理システムの全体像

1.2. システム構成

1.2.1. システム構成概要

本システムにより業務処理を遂行するには、人事・給与関係業務情報システムから職員情報を入手し、電子モールから物品の調達に関する情報を入手する等、関連システムとの連携が必須となる。また、N 人の全職員の利用（常時利用は 2 割程度と想定）により発生した多数の業務を迅速に処理し、日々増加する大量のデータを適切に管理する必要がある。これらの業務特性から、

効率的に業務が処理できること、一元化された情報の安全な管理等に配慮したシステム構成が必要であり、その要件を以下に示す。また、システムの構成例を図 1.2 に示す。

- システム全体の情報の機密性を確保するため、業務処理を行う機器、インターネットを介して民間の事業者との間でデータ交換をする機器、データを一元管理する機器のそれぞれを論理的又は物理的に分離してネットワークセグメントを分けるとともに、それぞれのセグメント間には適切にファイアウォールを設置する等の情報セキュリティ対策を実施する。
- システム全体の可用性を確保し運用を容易にするため、業務を実行する機器の稼動状況監視やアクセス監視、負荷分散等を可能とする構成とする。
- １つのデータセンター拠点内に配置することを基本とするが、サーバを分散するか統合するかについては費用対効果を考慮した上で最適な構成とする。
- 拡張性を考慮した構成とすること。例えば機能を図 1.2 に示す単位で分割し、それを搭載するハードウェア等も表 1.1 で示すように機能単位に分割する等、業務量の変動に応じてシステム増強、負荷分散が柔軟に行えるようにする。
- システムの性能目標は、スループットとして参照系処理 3 秒以内、更新系処理 8 秒以内、稼働率 99.5%以上とする。（現時点の想定目標値であり、最終目標値は基本設計以降で接続システムとの調整を踏まえて決定する。）

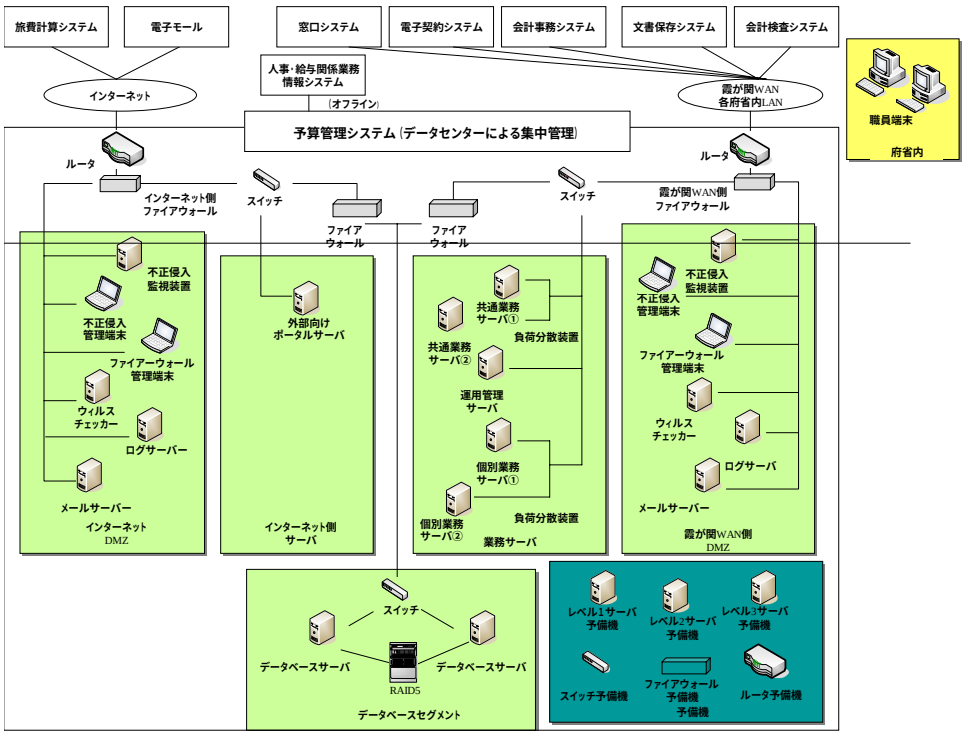


図 1.2 予算管理システムの構成例

1.2.2. ハードウェア機器構成例

システムのハードウェア機器構成例を以下に示す。各機器の具体的な要件は、本調達仕様書の分冊「システム要件」に示す。

【注釈】機器調達の場合は質の高い製品を選択するための基準として、第三者評価済みの認証製品から選定することを求める等、必要に応じて調達者の要求水準を示す。

表 1.1 予算管理システムのハードウェア機器構成例

セグメント	ハードウェア機器（例）	機能概要
霞ヶ関 WAN 側 DMZ	ファイアウォール	IP アドレスやプロトコルでのフィルタリングを行い、不正侵入や攻撃を防ぐ機能を提供するサーバ
	不正侵入監視装置	本システムへの不正侵入をリアルタイムに監視し、セキュリティを向上させるサーバ
	不正侵入監視端末	不正侵入装置からの各種情報を管理する端末
	ファイアウォール管理端末	ファイアウォールによるフィルタリングの設定、監視等の管理を行う端末
	ウィルスチェッカー	ウィルスの検知・除去を行うサーバ
	ログサーバ	霞ヶ関 WAN 側 DMZ 内に設置された各種サーバのログファイルを収集・管理するサーバ
	メールサーバ	メールの配信機能を提供するサーバ
業務サーバ	ファイアウォール	（霞ヶ関 WAN 側 DMZ 同様）
	共通業務サーバ	電子決裁、アクセス管理、執行情報管理、他システムインタフェースの各種処理を行うサーバ
	個別業務サーバ	物品管理・調達、謝金・諸手当、補助金、旅費の各業務の処理を行うサーバ
	運用管理サーバ	本システムで使用する機器の死活管理、負荷監視、資源監視等を行い、異常を知らせる等、本システムの運用を支援するサーバ
インターネット側サーバ	ファイアウォール	（霞ヶ関 WAN 側 DMZ 同様）
	外部向けポータルサーバ	インターネットから接続する際の窓口となり、共通業務サーバ、個別業務サーバへの処理の要求を行うサーバ
インターネット DMZ	（霞ヶ関 WAN 側 DMZ と同等構成）	
データベースセグメント	データベースサーバ	本システムで必要な情報の管理、履歴管理を行うサーバ
その他	予備機	サーバやスイッチ、ファイアウォール、ルータの故障等に備えて保有する予備の機器
	職員端末	予算管理システムでの各処理を行う端末

1.2.3. 外部システム連携方法

本システムが連携する外部システムの概要を下表に示す。各システムとの連携方式については、本調達仕様書の分冊「システム要件」を参照できる。

【注釈】連携すべき外部システムが存在する場合、その外部システムとのインタフェース方式を明確に示す。

表 1. 2 予算管理システムの外部連携システム

外部システム	システム連携概要
人事・給与関係業務情報システム	職員情報及び関連する各種人事給与用コード情報の参照
電子契約システム	物品調達業務、委託費業務において、互いの文書作成、審査、決裁ワークフローを連携させる
会計事務システム	予算・決算業務の業務・システム最適化計画に基づき再構築される官庁会計事務データ通信システム
文書保存システム	文書管理業務・システム最適化計画に基づき整備される文書保存システム
窓口システム	行政情報の電子的提供業務及び電子申請等受付業務の業務･システム最適化計画に基づき共通業務･システムとして整備された電子申請の窓口システム
電子モール	物品調達、物品管理、謝金・諸手当、補助金及び旅費の各業務・システム最適化計画に基づき、小額物品の簡易的な調達を実現するために、インターネット上に構築する仮想店舗街
旅費計算システム	物品調達、物品管理、謝金・諸手当、補助金及び旅費の各業務・システム最適化計画に基づき、最も経済的な経路の選定及び出張計画書作成を行うシステム
会計検査システム	計算証明書類情報等を格納し、会計検査のために加工・編集を行うシステム

1.3. 想定する利用者

本情報システム等で想定する利用者の分類ごとに、その役割と権限を示す。各関係者による運用要件の詳細は、本調達仕様書の分冊「運用要件」に示す。

【注釈】システム運用時に必要なセキュリティ対策を検討するために、対象とするシステムが誰によりどのように利用・管理されるのかをできるだけ明確に示すべきである。この例では、システムの主な関係者の分類を行い、それぞれの役割と権限の概要記述に留め、想定するシステムの運用形態の詳細は、運用要件等別途調達者が提示する場合の例を示している。

表 1.3 予算管理システムの想定利用者

関係者分類	関係者名称	役割・権限の説明	
責任者	統括責任者	役割	本システムの運用に関する責任者
		権限	運用・保守作業の承認、緊急時の指示・管理、各関連部門との連絡窓口に関する権限と責任
責任者	業務責任者	役割	統括責任者の業務管理支援に関する責任者
		権限	以下に関する権限と責任 運用・保守作業の管理、入退室管理、各要員の管理･承認、問合せ・苦情管理、緊急時の指示･管理補佐、外部システムとの連絡窓口
システム管理者	運用責任者	役割	本システムの運用における府省庁側の責任者
		権限	以下のシステム運用に関する権限と責任 システム構成管理・承認、運用・保守作業の指示・管理、緊急時対応の管理、各運用要員の管理、システム以上検出時の関係者への連絡・確認
システム運用者	運用業者	役割	本システムの運用及び監視作業を実施する委託先業者の担当者
		権限	以下のシステム運用の実施に関する権限と責任 システムの定期運用、運用状況報告、障害対応、システムの定常監視、作業管理・報告、ヘルプデスク窓口対応
システム運用者	保守業者	役割	本システムの保守作業を実施する委託先業者の担当者
		権限	以下の保守作業に関する権限と責任 定期保守、障害時の開発関係者への連絡･対応
サービスの利用者	職員	役割	本システムのサービス機能を利用する処理者
		権限	それぞれの処理者の役割に応じたサービス機能の実施
監査者	監査者	役割	本システムの運用に係る監査者
		権限	システム監査、業務監査の実施

1.4. システム機能概要

本システムが提供する業務機能について、図 1.1 に示す各機能の概要を示す。システム機能の詳細については、本調達仕様書の分冊「システム要件」及び「機能要件」に示す。

【注釈】ここでは、システムの主なサービス機能の概要記述に留め、サービス機能の詳細は、システム要件及び機能要件等の他の文書で提示する場合の例としている。

表 1.4 予算管理システムの主なサービス機能

アプリケーション分類	主なサービス機能	サービス機能の内容
個別業務アプリケーション	物品機能	物品調達及び物品管理に係る業務アプリケーション機能
	謝金機能	委員会実施申請、謝金・諸手当支出決定等に係る業務アプリケーション機能
	補助金機能	補助金等の交付、状況報告、財産処分等の各種処理に係る業務アプリケーション機能
	旅費機能	旅行計画、出張精算等に係る業務アプリケーション機能
	委託費機能	委託費調達、委託契約、支払、状況報告、財産処分等の各種処理に係る業務アプリケーション機能
	その他支払機能	支出負担行為、支出決定の業務アプリケーション機能
共通業務アプリケーション	計画機能	予算執行計画を作成する機能
	モニタリング機能	決裁案件のモニタリングや監査を支援する機能
	執行情報管理機能	予算執行情報を管理する機能
基盤アプリケーション	ログイン・アクセス制御機能	アプリケーションへのログイン認証機能（統合認証サーバによるシングルサインオン）、アプリケーション機能単位の権限（登録・参照・更新・削除）に基づくアクセス制御機能
	ワークフロー制御機能	文書の起案から審査、決裁等の一連の業務ワークフローを実現する機能
	Web アプリケーション機能	ワークフロー機能により回覧される文書の起案、審査、決裁処理を Web ブラウザで対話的に実現する機能
	電子署名・電子帳票機能	ワークフロー機能により回覧される文書の決裁時に、決裁者の電子署名を付与し電子帳票に埋め込み保存する機能
	システム間連携機能	連携する外部システムとの間でリアルタイム連携若しくはバッチ連携を実現するための連携基盤機能

セキュリティ要求仕様の例　《1．システム概要》

2.2.2. 保護すべき情報資産のまとめ方

「保護すべき情報資産」を洗い出すためには、機密性、完全性及び可用性の観点から情報の格付けを行う必要がある（政府機関統一基準 3.1.1「(1) 情報の格付け」）。図 2-3 に示すように、保護すべき情報資産の抽出には要件定義書を参照するが、主に「業務・機能要件定義」、「情報・データ要件定義」及び「セキュリティ要件定義」の情報が利用できる。

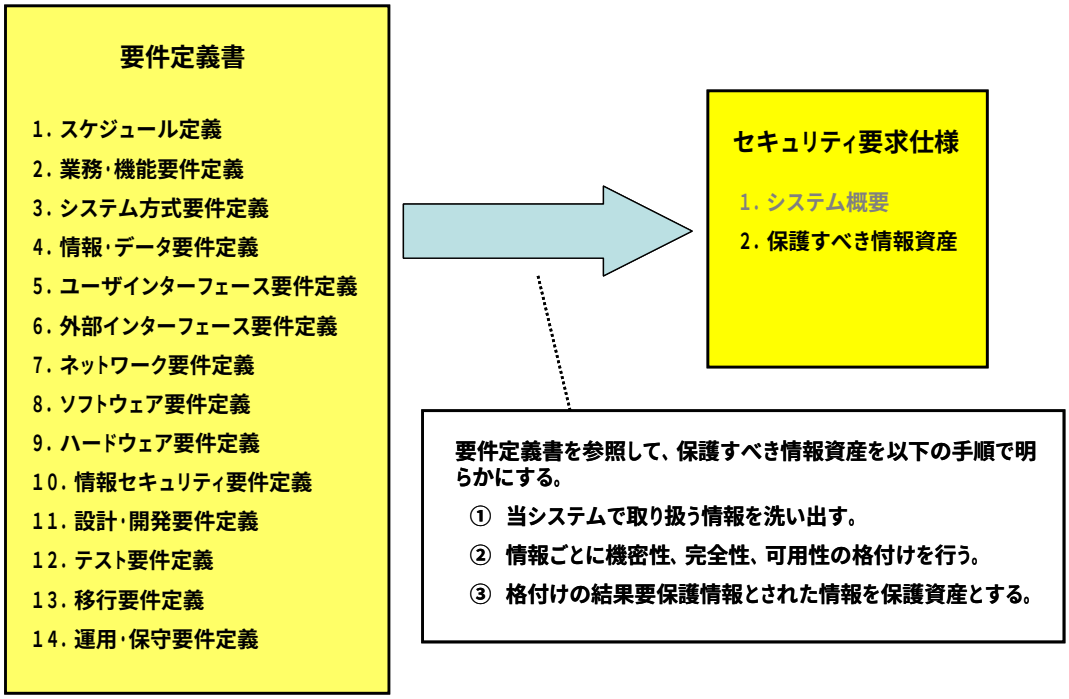


図2-3 保護すべき情報資産のまとめ方

2.2.2.1. 保護すべき情報資産の洗い出し手順

保護すべき情報資産の洗い出し手順を以下に示す。

要件定義書の「情報セキュリティ要件定義」の中に、情報資産の格付けをした図 2-4のような情報資産評価表が存在する場合は、それが参考になる。

「情報資産評価表」

情報システム名	情報名（データ名）	情報の格付け		
		機密性	完全性	可用性

図2-4 情報資産評価表

情報資産評価表が存在しない場合、以下の手順で情報の格付けを検討するための情報資産評価表を作成する。

（１） 情報名（データ名）の抽出

「最適化ガイドライン」に示された以下の標準記述様式等を活用して、情報名（データ名）を洗い出す。

- 情報システム機能構成図のシステム機能名から想定できる情報名
- 情報体系整理図の集合体（クラス名）
- 実体関連図の対象情報名
- データ定義表のファイル名

（２） 保護すべき情報資産の抽出

情報名（データ名）ごとに要機密情報（機密性２情報及び機密性３情報）、要保全情報（完全性２情報）及び要安定情報（可用性２情報）に該当するかどうか情報の格付けを行う。情報の格付けを表すこれらの用語は、政府機関統一基準で定義されている（政府機関統一基準「1.1.3 用語定義」）。また、情報の格付け及び格付けを明示する手順は、政府機関統一基準では「情報セキュリティ委員会」が整備することとしている（政府機関統一基準「3.1.1 情報の格付け」）。図 2-5 に保護すべき情報資産の格付けのまとめ方を示す。

1) 情報（情報名、データ名）を抽出し、「情報資産評価表」に記入する。

「情報資産評価表」

情報システム名	情報名（データ名）	情報の格付け		
		機密性	完全性	可用性

2) 情報の格付けを行う。

・要機密情報：　機密性2情報及び機密性3情報
・要保全情報：　完全性2情報
・要安定情報：　可用性2情報
・要保護情報：　要機密情報、要保全情報及び要安定情報

3) 要保護情報を保護すべき情報資産とする。

図2-5 保護すべき情報資産の決定

ここでは、情報資産を情報名（データ名）で整理し、機密性、完全性、可用性の格付けを行い、要保護情報か否かを判定する。情報資産の保管場所、保管形態の遷移が脅威に影響する場合は、それぞれを区別して格付けを行う。また、情報資産には、業務データ等の一次的な保護資産と、システムの信頼性維持やセキュリティ機能の動作に使用する二次的な保護資産がある。通常、調達者が意識して洗い出すものは一次的な保護資産であり、二次的な保護資産は提案者が提示する。ただし、監査ログ等の二次的な保護資産であっても、省庁対策基準において取得が求められている等によりセキュリティ提案仕様に含めるべきものであると調達者が判断したものについては、調達者が提示することになる。保護すべき情報資産の検討を行う際には、当該システムの運用に係る省庁対策基準等との整合性を考慮する必要がある。

2.2.2.2. 保護すべき情報資産の記述例

以下に「予算管理システム」を例として、セキュリティ要求仕様における保護すべき情報資産の記述例を示す。

2.保護すべき情報資産

本情報システム等において保護すべき情報資産を抽出し、物品、謝金、補助金、旅費、委託費、その他支払に関する情報に分け、政府機関統一基準に従い、機密性、完全性、可用性の格付けとともに整理・評価した結果を以下に示す。ここで機密性が２又は３の情報資産（機密性２情報、機密性３情報）は要機密情報、完全性が２の情報資産（完全性２情報）は要保全情報、可用性が２の情報資産(可用性２情報)は要安定情報とし、要機密情報、要保全情報、要安定情報のいずれかの場合、要保護情報とする。

【注釈】ここでは、「業務・システム最適化指針（ガイドライン）に基づき、保護すべき情報資産を分類し、整理する。情報資産を情報名（データ名）で整理し、機密性、完全性、可用性の格付け、及び要保護情報か否かを示す。情報資産の保管場所、保管形態の遷移が脅威に影響する場合は、それぞれを区別して格付けを行った情報資産評価表を提示している。

（１） 物品に関する情報資産評価

【注釈】本システムの例では、下記の物品に関する情報以外の情報資産評価表として、謝金、補助金、旅費、委託費その他支払いに関する情報資産評価表が存在することを想定しているが、ここでは省略する。

表 2.1 物品に関する情報資産評価

#	情報資産名	情報提供元（もしくは情報先）情報システム	情報提供元（もしくは情報先）情報システム	保管場所	保管形態	保管期間	機密性	完全性	可用性	要保護
1	個別予算執行計画情報	職員	予算管理システム	予算管理DB	電子媒体	5年	2	2	2	○
2	物品管理計画情報	職員	予算管理システム	予算管理DB	電子媒体	5年	2	2	2	○
3	歳出予算情報	会計事務システム	予算管理システム	予算管理DB	電子媒体	5年	2	2	2	○
		予算管理システム	職員	—	—					
4	調達案件情報	職員	予算管理システム	予算管理DB	電子媒体	5年	2	2	2	○
		外部委託業者	予算管理システム							
		予算管理システム	文書保存システム	文書保存システム	—					
5	支出決議情報	職員	予算管理システム	予算管理DB	電子媒体	5年	2	2	2	○
		予算管理システム	会計事務システム	会計事務システム	—					
		予算管理システム	電子契約システム	電子契約システム	—					
		予算管理システム	文書保存システム	文書保存システム	—					
6	支払実績	会計事務システム	予算管理システム	予算管理DB	電子媒体	5年	2	2	2	○
7	発注情報	職員	予算管理システム	予算管理DB	電子媒体	5年	2	2	2	○
		予算管理システム	電子モール	電子モール	—					

2.2.3. 前提条件のまとめ方

対象システムの利用環境におけるセキュリティに関する「前提条件」は、物理的、接続的（ネットワーク環境）及び人的側面から記述する。どの前提条件を設定するかよって想定される脅威が異なってくるため、脅威を想定する上で必要となる前提条件はすべて記述する。

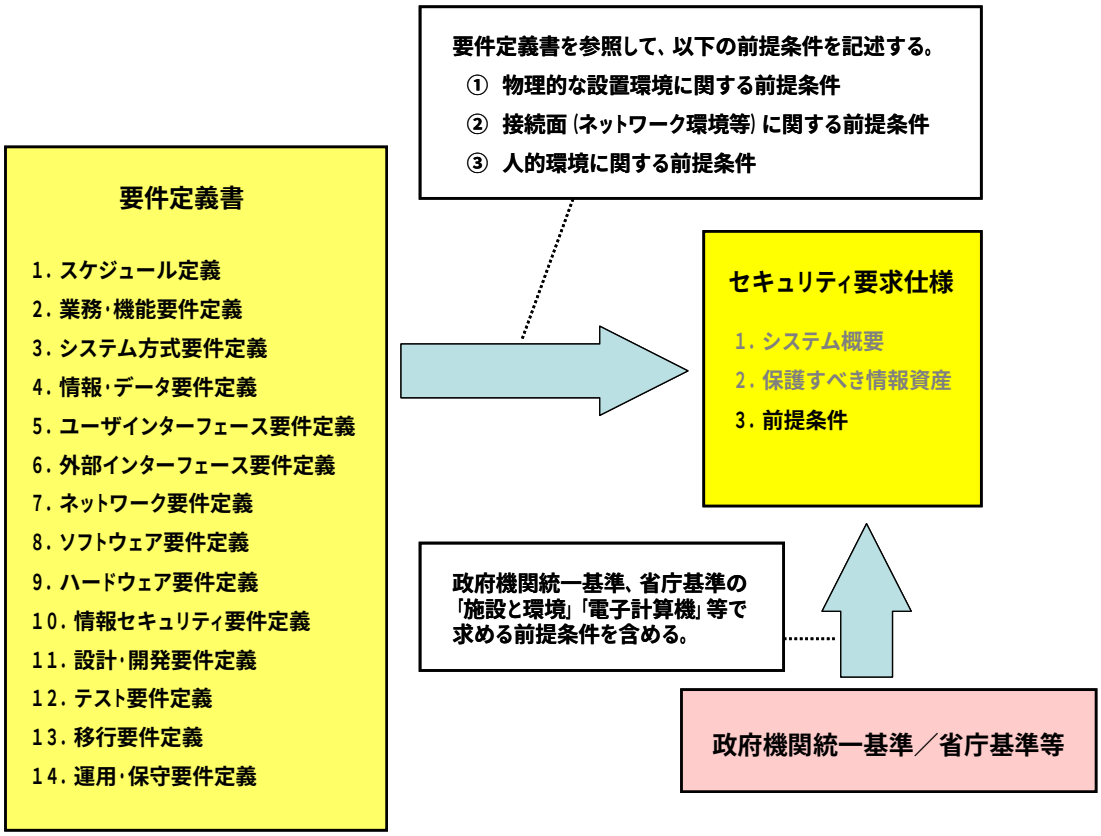


図2-6 前提条件のまとめ方

前提条件は、図 2-6に示す要件定義書の内容を踏まえて定義する。また、政府機関統一基準「第５部 情報システムの構成要素についての対策」の「5.1 施設と環境」、「5.2 電子計算機」、「5.3 アプリケーションソフトウェア」及び「5.4 通信回線」に基づき定めた省庁対策基準の遵守事項等のうちシステム運用環境において前提とする事項を含める（図 2-6 参照）。対象とするシステムにおいてリスク低減のために講ずることとしている対策（この対策の手段が調達の対象外であれば、その旨を明示すること）等、調達者から提示すべき事項は、前提条件として記述する。特に、省庁対策基準は、調達の段階では通常は提案者に

提示しないことから、提案者が考慮すべき省庁対策基準の遵守事項の内容を前提条件として的確に示す必要がある。

【注釈】前提条件は以下のような点を考慮して記述する必要がある。例えば人的な信頼性の前提を幅広く設定すると、想定する脅威は少なくなり、情報システムとして具備すべきセキュリティ機能も限定的となるが、一度リスクが顕在化すると情報システムのセキュリティを維持することが直ちに困難となる。一方、人的な信頼性の前提を置かない場合、増大した脅威への対策として、情報システム側で過度な IT セキュリティ機能が必要となり、効率を度外視した厳格な運用管理が必然的に求められる等、対策のためにより多くのコストと負担を要することになる。
調達者においては、組織の省庁対策基準等における情報資産に対する保護方針に基づき、リスクとコストのバランスを考慮して、前提条件を設定する必要がある。

2.2.3.1. 前提条件の検討手順

以下に前提条件を検討するための例を示す。

（1） 物理的な設置環境に関する前提条件

物理的な設置環境に関する前提条件とは、サーバを設置する場所の建屋・セキュリティ区域の特定、耐震･防火に関する基準、電源供給に関する基準、セキュリティ区域への入退室管理や物品の受渡管理の基準等に関する条件を示すものであり、政府機関統一基準では「5.1 施設と環境」等がこれに相当する。例えば、以下の事項がある。

- 「入退室が厳密に管理された部屋に設置されるものとする。」
- 「だれでも操作できる公共の場に設置されるものとする。」

（2） 接続面（ネットワーク環境等）に関する前提条件

接続面（ネットワーク環境等）に関する前提条件とは、サーバシステムが接続されるネットワーク環境や通信回線の基準、情報セキュリティ上の何らかのリスクを伴う外部サービスをネットワーク経由で利用する場合の条件等を示すものであり、政府機関統一基準では「5.4 通信回線」等がこれに相当する。例えば、以下の事項がある。

- 「信頼できないネットワークとは接続されないものとする。」

（3） 人的環境に関する前提条件

人的環境とは、対象とするシステムの管理者や業務担当職員の信頼性に関する条件、当該システムにかかわる組織・体制として実現すべきことに関する条件、当該システムの使用方法として当然実現されるべきことに関する条件等を示すものであり、政府機関統一基準では第１部、第２部及び第６部の一部等がこれに相当する。例えば、以下の事項がある。

- 「システムの関与者は全員セキュリティ教育を受けているものとする。」

2.2.3.2. 前提条件の記述例

セキュリティ要求仕様の例　《3．前提条件》

3.本システムの運用時の前提条件

本システムの運用環境における前提条件又は省庁対策基準に基づく前提条件について、物理的、接続的（ネットワーク環境等）、人的側面から示す。

3.1. 物理的な設置環境に関する前提条件

【注釈】この例では、サーバを設置するマシンルームとこれを含むデータセンターに対して、所定の基準を満たすことを前提として挙げている。

物理前提-1	**予算管理システムのサーバを設置するデータセンター** 本システムのマシンルームを含むデータセンターは、電力供給部分（分電盤を境界点とする。）まで準備されているものとする。データセンターは以下の基準を満たすものとする。 ・　情報システムの設備環境基準（JEITA3 IT-1002）

3.2. 接続面（ネットワーク環境等）に関する前提条件

【注釈】この例では、当該システムが接続する既存 WAN 及び LAN 環境について、当該システムが脅威を個別に想定する必要のないことを前提として挙げている。

接続前提-1	**霞ヶ関 WAN 及び各府省内 LAN の信頼性** 霞ヶ関 WAN 及び各府省内 LAN は、それぞれ求められるセキュリティ水準を満たすように正しく構成され、適切に設定・管理されているものとする。

3.3. 人的環境に関する前提条件

【注釈】この例では、重要な情報システムとしては位置付けられないことを想定し、システム管理者は定められた規則に反する行為を意図的には行わないが、職員等のシステム運用者（システムの運用にかかわるその他の者）については、規則に反する行為を行うことを想定した前提を挙げている。一方、特に機微な情報を取り扱う等一部の重要な情報システムにおいては、システム管理者が規則に反する行為を行うことも想定する。この場合には、セキュリティ対策として、システム管理者による操作を記録する監査証跡の取得とその保全が求められるものと考えられる。

人的前提-1	**システム管理者の信頼性** システム管理者は、本システムの管理を適切かつ厳格に実施する知識・技量・使命感を有し、的確かつ迅速なシステム管理操作を実施するよう訓練され、定められた規則に反する行為を意図的には行わないものとするが、誤操作は免れない。
人的前提-2	**職員その他のシステム運用者の信頼性** 国家公務員である職員や委託によるシステム運用者は、それぞれ国家公務員法、契約のもとに職務を遂行することが通常認められるが、倫理観や罰則による抑制が効かない状況においては例外的に信頼性が損なわれる。

セキュリティ要求仕様の例　《3．前提条件》

2.2.4. 脅威のまとめ方

対象とする情報システムの運用時に想定される「脅威」を検討する。脅威の検討方法を図 2-7に示す。

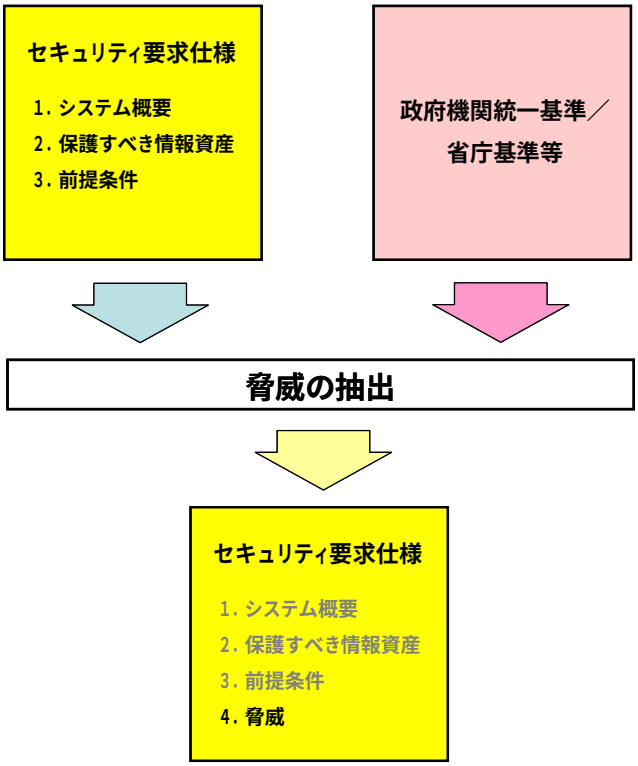


図2-7 脅威のまとめ方

脅威は、セキュリティ要求仕様に含める「システム概要」「保護すべき情報資産」及び「前提条件」を基に検討する。また、政府機関統一基準に基づく省庁対策基準等において想定している脅威も含める。特に、政府機関統一基準の「4.2 情報セキュリティについての脅威」では、セキュリティホール対策、不正プログラム対策及びサービス不能攻撃対策を示しているが、これらに限らず、省庁対策基準等で想定しているその他の脅威も併せて検討する。

2.2.4.1. 脅威の検討手順

以下に具体的に検討する際のポイントを示す。

脅威を検討する際には、「どのような攻撃者が、どの保護資産に対して、どのような脅威となる行為を行う可能性があるか」を洗い出し、結果として「どの事象が脅威となり得るのか」を明確にする。その際、想定する脅威事象が「前提条件」と矛盾しないように留意

する（矛盾する脅威が想定された場合、前提条件が不適切である可能性があり、再度前提条件を含めて見直す必要がある。）。

また、脅威の抽出は漏れがないことが重要であり、保護資産に対して許容範囲を超えるリスクが存在する場合、そのリスクに関連する脅威事象を洗い出し、新たな情報セキュリティ対策を講ずることを求める必要がある。一般的に、脅威を検討する対象システムに類似するシステム（業務機能、システムアーキテクチャ、システム構成等の類似性に基づく）において既に検討されている脅威セットや、関連するモデルシステムとして検討された脅威セット等を参考とし、対象とするシステムの保護の観点と前提条件を踏まえて脅威の洗い出しを行い、脅威事象の設定・記述を行う。また、その際に、政府機関統一基準の「4.2 情報セキュリティについての脅威」において想定している脅威も参考になる。

2.2.4.2. 脅威の記述例

セキュリティ要求仕様の例　《４．脅威》

4. 脅威

本システムの運用環境において想定される脅威の例を示す。

【注釈】この例では、インターネットからの脅威を主として挙げている。

No	脅威分類	脅威タイトル / 脅威内容
脅威-1	情報漏えい 改ざん	**インターネットからの DB データへの不正アクセス** インターネット上の攻撃者が、データベースサーバの予算管理 DB 上のデータを、不正に参照、変更する可能性がある。
脅威-2	情報漏えい 改ざん	**インターネット上を流れる通信データの不正利用** インターネット上の攻撃者が、通信路上を流れる通信データを詐取し、データの内容を参照、破壊する可能性がある。

セキュリティ要求仕様の例　《４．脅威》

3. セキュリティ提案仕様の審査のポイント

調達者は、提案者から提出されたセキュリティ提案仕様を、本章に示す視点で審査する。

セキュリティ提案仕様には、「システム概要」、「保護すべき情報資産」、「前提条件」、「脅威」、「情報セキュリティ対策」、「セキュリティ機能を実現する機器等」及び「制約条件」の７項目が記載される。

これらのうち、「保護すべき情報資産」、「前提条件」及び「脅威」の確認については、「3.1 『保護すべき情報資産』、『前提条件』及び『脅威』の確認」で説明する。また、「情報セキュリティ対策」の審査については「3.2 情報セキュリティ対策の審査」で、「セキュリティ機能を実現する機器等」の審査については「3.3 セキュリティ機能を実現する機器等の審査」で、「制約条件」の審査については「3.4 制約条件の審査」で説明する。

なお、「システム概要」は、セキュリティ要求仕様の「システム概要」を転記するものであり、審査の対象とはしない。ただし、セキュリティ要求仕様の記述から変更されていれば、その妥当性を確認する。

3.1. 「保護すべき情報資産」、「前提条件」及び「脅威」の確認

セキュリティ提案仕様に記述されている「保護すべき情報資産」、「前提条件」及び「脅威」を審査する。これらには、セキュリティ要求仕様において調達者が提示した「保護すべき情報資産」、「前提条件」及び「脅威」を受けて過不足なく盛り込まれることが原則である[4]。この観点から、セキュリティ要求仕様とセキュリティ提案仕様の対応を確認する。

セキュリティ要求仕様の内容に対してセキュリティ提案仕様で追加・変更がなされている場合には、当該事項について、その理由がセキュリティ提案仕様に明確に記載されており、妥当であることを確認する。特に、追加された「保護すべき情報資産」及び「脅威」

[4] セキュリティ要求仕様の「保護すべき情報資産」、「前提条件」及び「脅威」は、その内容を提案者が過不足なく取り込んでセキュリティ提案仕様を作成できるように、十分に具体的かつ詳細なものであることが理想的である。このため、本解説書では、提案者が「保護すべき情報資産」、「前提条件」及び「脅威」の内容に追加・変更を加える場合には、追加・変更の提案を明確にするために、別項の「制約条件」に記述するよう調達において求める方法も想定した。

については過剰ではないか、追加・変更された「前提条件」については前提としてよいかを注意深く確認する。また、二次的な保護資産は、必ずしもセキュリティ要求仕様には含めず、提案者がセキュリティ提案仕様に含めて提案するものであり、必要に応じ、その妥当性を次節の「3.2 情報セキュリティ対策の審査」において確認する。

3.2. 情報セキュリティ対策の審査

提案された情報セキュリティ対策について、セキュリティ要求仕様で示された脅威に対抗するためにシステムが備えるべきセキュリティ機能が検討され、対策として明確に提案されているか否かを審査する。また、提案された情報セキュリティ対策に沿ったセキュリティ機能を実現するシステム構成要素を確認し、構成要素が持つセキュリティ機能の妥当性を評価する。

【注釈】セキュリティ提案仕様に記載されたセキュリティ対策の妥当性を、前提条件を含むセキュリティ要求仕様に基づき評価する。提案された個々のセキュリティ対策を、技術的セキュリティ対策、物理的セキュリティ対策、運用に関するセキュリティ対策及び保証に関するセキュリティ対策等に分類し、それぞれの観点での妥当性評価、及びこれらの相互関係によって実現されるシステム全体としてのセキュリティの妥当性評価を行う。特に、重要なセキュリティ機能が欠落していないかどうか、また、局所的に過剰なセキュリティ機能又は不必要なセキュリティ機能が提案されていないかどうかを確認する。

3.2.1. 技術的セキュリティ対策の審査ポイント

技術的セキュリティ対策の提案例を以下に示す。

技術対策-1	**利用者識別認証** 各利用者に対して、利用者 ID 及びパスワードを使用することにより、利用者の識別と認証を行う。また、セキュリティ上重要な機能の利用を許可する場合の利用者の識別と認証に際しては、IC カードを利用する。
技術対策-2	**通信の暗号化** 個人情報を含む機密性３情報をネットワーク経由で移送する場合には、その通信を SSL 等で適切に暗号化する。
・・・	・・・

この例では、主体認証機能と通信の暗号化機能が提案されており、政府機関統一基準では、「4.1.1 主体認証機能」及び「5.1 施設と環境」に関連する事項がある。このほか、政府機関統一基準の「4.1 情報セキュリティについての機能」、「4.2 情報セキュリティについての脅威」及び「第５部 情報システムの構成要素についての対策」を参照して必要な情報セキュリティ対策が記載されているかどうかを確認する。主たる分類としては、主体認証

機能、アクセス制御機能、権限管理機能、証跡管理機能、暗号化及び電子署名機能（鍵管理機能を含む。）等の機能を組み込むことにより、保護資産への脅威やセキュリティホール・不正プログラム・サービス不能攻撃等から発生する脅威に対抗するための技術的な情報セキュリティ対策の方針等が提案されていることを確認する。

3.2.2. 物理的セキュリティ対策の審査ポイント

物理的セキュリティ対策の提案例を以下に示す。

物理対策-1	**セキュリティ区画における安全区域遵守事項の実現** 重要資産を扱うマシンルーム、マシンルームのある建物、建物のある敷地等の場所ごとに、その重要度に応じた情報セキュリティ対策（入退室管理、施錠管理、監視（監視カメラの設置）等）を施す。
・・・	・・・

調達者がセキュリティ要求仕様で提示した前提条件に合致した物理的セキュリティ対策の方針等が記述されていることを確認する。

3.2.3. 運用に関するセキュリティ対策の審査ポイント

運用に関するセキュリティ対策の提案例を以下に示す。

運用対策-1	**省庁対策基準等の規則への準拠** セキュリティ要求仕様において提示された運用に関する規則に準じる。

調達者がセキュリティ要求仕様で提示した前提条件に合致した運用に関するセキュリティ対策が記述されていることを確認する。

3.2.4. 保証に関するセキュリティ対策の審査ポイント

本書において、保証[5]に関するセキュリティ対策とは、技術的セキュリティ対策、物理的セキュリティ対策又は運用に関するセキュリティ対策が確実に実施され又はその機能を発揮するために採る対策をいう。保証に関するセキュリティ対策の提案例を以下に示す。

保証対策-1	**評価･認証を受けた製品等の利用の検討** システム構成要素の製品を導入する場合、情報セキュリティに関する評価・認証を受けた製品等の利用を検討する。セキュリティを確保する上で重要な製品等については、システム仕様を満たしかつ IT セキュリティ評価及び認証制度又は CCRA[6]加盟国の制度にて認証を受けた製品の有無を調査の上、適合する製品があればその製品を適用する。

この例では、政府機関統一基準に基づき認証製品の利用に関する保証を提案しており、政府機関統一基準では 4.3.1(1)(f)及び 6.1.1(2)(d)が関連する事項である。このほか、保証に関するセキュリティ対策としては、セキュリティ要求仕様に応じて、ソフトウェア開発プロセスの信頼性、システムを構成する機器等の信頼性、システムのセキュリティ設計に関する信頼性、システムのセキュリティ実装及び設定の信頼性、システム運用時の信頼性等を担保するために、これらの信頼性の保証に関するセキュリティ対策が提案されることがある。これらの対策に関係する事項が、政府機関統一基準では「第２部 組織と体制の整備」、「4.1.5 保証のための機能」、「4.3.1 情報システムのセキュリティ要件」及び「6.1.3 ソフトウェア開発」等にある。

3.2.5. 脅威と情報セキュリティ対策の対応の審査ポイント

提案された情報セキュリティ対策のそれぞれがどの脅威に対抗し、どの前提条件を満たすものなのか、またそれぞれが政府機関統一基準又は省庁対策基準のどの項目に該当する対策であるかが示されていることを確認する。調達者は、提案された情報セキュリティ対策が、セキュリティ要件仕様の脅威や前提条件に対して漏れがないことを確認する。また、情報セキュリティ対策の省庁対策基準への準拠を確認する。

【注釈】省庁対策基準等を提案者に開示していない場合、省庁対策基準等と提案された情報セキュリティ対策との整合確認は、調達者側で実施する必要がある。

[5] 情報セキュリティに関連して、「保証」という語は文脈により異なる意味で使われることに留意する必要がある。本書における「保証に関するセキュリティ対策」は、別途定めた一次的な対策である技術的セキュリティ対策、物理的セキュリティ対策及び運用に関するセキュリティ対策が確実に実施され又はその機能を確実に発揮するために採る対策である。他方、政府機関統一基準では「4.1 情報セキュリティについての機能」に「4.1.5 保証のための機能」があるが、これは、本書における「保証に関するセキュリティ対策」のうち、技術的に実現するものを指す。また、本書付録 C の「3 評価保証レベル（EAL）」における保証は、ISO/IEC 15408 に基づき情報セキュリティ対策を評価する際に、評価において参照する資料の範囲や評価の方法により定まる評価の精度を表す指標である。詳しくは当該節を参照されたい。

[6] CCRA については、付録 C を参照されたい。

これらの対応状況は、セキュリティ要求仕様に対して必要な情報セキュリティ対策を提案していることの根拠として示されるべきであり、以下の表のような内容が適切に埋められ、妥当な内容となっていることを確認する。

表 3-1 情報セキュリティ対策と脅威、前提条件、基準との対応表の例１

No	脅威	前提条件	政府機関統一基準又は 省庁対策基準等との対応
技術対策-1	脅威-1，脅威-2	―	統 4.1.1(1)(b)-(c)
技術対策-2	脅威-3	―	統 4.1.1(1)(c)，統 5.4.1(1)(i)
技術対策-3	脅威-1，脅威-4，脅威-5	―	統 4.1.1(1)(d)-(h)
物理対策-1	―	物理前提-1	統 5.1.1(1)(a)
物理対策-2	―	物理前提-2，接続前提-1	統 5.1.1(3)(a)-(f)
運用対策-1	脅威-6	人的前提-1	統 2.2.1(1)(a)-(h)，統 2.2.1(2)(a)-(c)
保証対策-1	脅威-7	人的前提-2	統 6.1.2(4)(a)-(e)，統 6.1.2(5)(a)-(c)

上記の表では、セキュリティ要求仕様で対策の提案を求めた脅威及び前提条件と、提案する個々の情報セキュリティ対策との対応関係を表している。また、提案者が提案する情報セキュリティ対策と政府機関統一基準又は省庁対策基準等との対応関係を表している。このような表から、提案を求めた脅威及び前提条件に対して漏れなく情報セキュリティ対策が提案されていることを確認することができる。また、政府機関統一基準又は省庁対策基準等との対応状況を確認し、提案意図の妥当性を評価することができる。

表 3-2 情報セキュリティ対策と脅威、前提条件、基準との対応表の例２

No	脅威	前提条件	政府機関統一基準又は 省庁対策基準等との対応	機密性	完全性	可用性
技術対策-1	脅威-1，脅威-2	―	統 4.1.1(1)(b)-(c)	○		
技術対策-2	脅威-3	―	統 4.1.1(1)(c), 統 5.4.1(1)(i)	○		
技術対策-3	脅威-1，脅威-4, 脅威-5	―	統 4.1.1(1)(d)-(h)	○	○	
物理対策-1	―	物理前提-1	統 5.1.1(1)(a)	○		
物理対策-2	―	物理前提-2, 接続前提-1	統 5.1.1(3)(a)-(f)	○		
運用対策-1	脅威-6	人的前提-1	統 2.2.1(1)(a)-(h), 統 2.2.1(2)(a)-(c)	○	○	○
保証対策-1	脅威-7	人的前提-2	統 6.1.2(4)(a)-(e), 統 6.1.2(5)(a)-(c)	○	○	○

上記の表では、さらにそれぞれの情報セキュリティ対策について、関連する情報の機密性、完全性、可用性の要求の別も示した例であり、これらの要求の別を示すことで提案の妥当性をより正確に評価することができる。

3.3. セキュリティ機能を実現する機器等の審査

セキュリティ機能が要求される情報システムを構築するためには、開発ソフトウェアでセキュリティ機能を実現するほかに、セキュリティ機能を持つ機器等を適切に選定して使用することが有効である。具体的には、提案された情報セキュリティ対策を実現する機器等について、IT セキュリティ評価及び認証制度を含む ISO/IEC 15408 に基づく制度において認証された認証製品リスト（例えば CCRA ポータルの認証製品リスト、各国の認証機関が公開している認証製品リスト等）を考慮してその機器等が選定されているかを審査する。

なお、政府機関統一基準では、ISO/IEC 15408 に基づく認証に関連して、以下の遵守事項を定めている。

> 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) (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】

> 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】

3.3.1. 提案された認証製品の審査ポイント

情報システムを構成する機器等の提案に関して、IT セキュリティ評価及び認証制度を含む ISO/IEC 15408 に基づく制度における認証の取得有無を提案の評価に活用する場合には、その製品種別と認証製品の適用根拠等を含む提案の妥当性を示す以下の情報を提案者に提示させる。

（1） 提案する認証製品の説明

技術的セキュリティ対策を実現するために認証製品を提案させる場合には、提案者に、以下の表に示すような、当該製品を適用する根拠を示す説明を提示させる。

表 3-3 提案する認証製品の説明例

技術的セキュリティ対策	製品種別	対策の具体化 / 適用根拠	認証製品例
利用者識別認証	IC カード	利用者識別認証に IC カードを利用するため	A 社 a 製品 B 社 b 製品
高信頼データ転送	回線暗号化装置	特定のノード間のルーティング機能及び暗号化通信機能を実現するため	C 社 c 製品

（2） 認証の内容

提案させる認証製品について、提案者に、以下の表に示すような認証の内容に関する情報を提示させる[7]。

表 3-4 提案する認証製品に関する認証の内容

提供する情報名	説　明
認証製品名称	認証製品の名称であり、検証された構成情報等が含まれる場合がある。
製品分類	認証製品リストを提供する各国制度で付加された分類情報
認証取得実績	TOE 名称：評価対象（Target Of Evaluation）の名称 TOE バージョン:評価対象のバージョン。通常バージョンごとに認証が与えられる。 TOE 種別：評価対象の種別 認証番号（認証国）：認証製品に対して一意に付加される識別番号 認証年月日：認証が与えられた日 適用する保証要件：EAL 等、評価対象が適合している保証のレベル等を示すもの 製造者：通常は製品提供者
製品概要	認証製品の提供する機能やサービスの概要
セキュリティ機能	セキュリティ機能の説明
適用方法	提案対象のシステムへの適用に関する概要説明 システムのどの部分に対して、どのように適用するのか等が必要に応じて示される場合がある。

調達者は、認証製品リストを検索し、製品認証情報や ST（セキュリティターゲット）の内容と、提案者から提示された上記情報の整合性を確認する。特に、想定するセキュリティ機能が認証の対象（TOE: Target Of Evaluation）に含まれていること、認証において前

[7] これらの情報は、各国の認証制度や「CC ポータル」で検索して得ることもできる。本書の「付録C　セキュリティ評価及び認証制度を活用した機器等の購入について」の「6. 認証製品リストの利用法」をあわせて参照されたい。

提としている物理的な前提条件、人的環境に関する前提条件等が、構築・調達する情報システムにおける前提条件に合致していることを確認する。

3.4. 制約条件の審査

セキュリティ提案仕様の「制約条件」は、セキュリティ要求仕様において調達者が提示した「保護すべき情報資産」、「前提条件」及び「脅威」に対して提案者が明示的に追加・変更を提案する場合に記述する項目である。

調達者は、提案された制約条件について、追加・変更の理由がセキュリティ提案仕様に明確に記載されており、妥当であることを確認する。例えば、「保護すべき情報資産」及び「脅威」を追加する提案については過剰ではないか、「前提条件」を追加・変更する提案については前提として適切か、等を審査する。

4. 参照

以下に、参考情報の参照箇所を示す。

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)
http://www.nisc.go.jp/active/general/pdf/k303-071.pdf

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
http://www.nisc.go.jp/active/general/pdf/k303-071c.pdf

業務・システム最適化指針（ガイドライン）（2006 年（平成 18 年）3 月 31 日）
http://www.e-gov.go.jp/doc/scheme.html
の「業務・システムの最適化の取組」

ISO/IEC 15408:2005 Information Technology ― Security Techniques ― Evaluation Criteria for IT Security
http://www.ipa.go.jp/security/jisec/evalbs.html

物品調達、物品管理、謝金・諸手当、補助金及び旅費の各業務・システム最適化計画
（2004 年（平成 16 年）9 月 15 日）
http://www.kantei.go.jp/jp/singi/it2/cio/dai11/11siryou2.pdf

予算執行等管理システム
http://www.meti.go.jp/policy/it_policy/shiryoteikyo/setumeikai.htm

情報システムの設備環境基準（JEITA3 IT-1002）
http://www.jeita.or.jp/japanese/standard/list/list.asp?cateid=8&subcateid=44

CCRA ポータル Web サイト
http://www.commoncriteriaportal.org/

IT セキュリティ評価及び認証制度（JISEC） Web サイト
http://www.ipa.go.jp/security/jisec/index.html

行政情報の電子的提供業務及び電子申請等受付業務の業務・システム最適化計画
http://www.soumu.go.jp/s-news/2005/050824_1.html

電子自治体のシステム構築のあり方に関する検討会
http://www.soumu.go.jp/denshijiti/denshi_kentoukai.html#a
「国・地方連携事業について」
http://www.soumu.go.jp/denshijiti/pdf/060322_s10.pdf

行政情報の電子的提供業務及び電子申請等受付業務の業務・システム最適化計画
http://www.e-gov.go.jp/doc/scheme.html
http://www.e-gov.go.jp/doc/20040730doc2.pdf

行政機関の保有する個人情報の適切な管理のための措置に関する指針について（平成 16 年 9 月 14 日、行政管理局長から各府省等官房長等あて通知）

http://www.soumu.go.jp/gyoukan/kanri/040914_1.html

IT セキュリティ評価及び認証制度と ISO/IEC 15408 に関する有用な情報として
http://www.ipa.go.jp/security/jisec/index.html

脅威の検討の参考情報として
- セキュリティ脅威とその対策方針パッケージ
  http://www.ipa.go.jp/security/jisec/spd_Package.html

- ISO/IEC TR15446　　B6.セキュリティ対策方針から脅威へのマッピングの例
  http://www.ipa.go.jp/security/ccj/documents/PP-ST_guideN3374.pdf

電子政府の推進についての参考情報として
http://www.e-gov.go.jp/doc/scheme.html

電子政府におけるセキュリティに配慮した OS を活用した情報システム等に関する調査研究
http://www.nisc.go.jp/inquiry/index.html

付録

付録 A：セキュリティ要求仕様に記載すべき項目

付録 B：セキュリティ提案仕様に記載すべき項目

付録 C：IT セキュリティ評価及び認証制度を活用した機器等の購入について

付録 A　セキュリティ要求仕様に記載すべき項目

調達者が作成するセキュリティ要求仕様に記載すべき項目と内容を以下に示す。

（1） システム概要：情報システム又は開発ソフトウェア全体の概要情報を記述する。（「2.2.1 システム概要のまとめ方」を参照）

1）識別情報：対象となる情報システム又は開発ソフトウェアの管理及び識別に必要なラベル情報及び記述情報を含める。

2）システム記述：情報システム又は開発ソフトウェアのセキュリティ機能を検討する範囲について、物理的な範囲（システム構成上の範囲等）及び論理的な範囲（サービスや機能等）を定める。情報システム又は開発ソフトウェアの動作概要等を記述して「脅威の抽出～セキュリティ機能」が正確に理解できる情報を含める。

（2） 保護すべき情報資産：情報システム又は開発ソフトウェアのセキュリティ機能が保護すべき情報資産を示す。情報資産の価値に応じて脅威が発生した場合のためのセキュリティ機能が必要となる。（「2.2.2 保護すべき情報資産のまとめ方」を参照）

（3） 前提条件：情報システム又は開発ソフトウェアのセキュリティを考慮する際に必要な前提条件を記述する。前提条件には、物理的な設置環境に関する前提条件、接続面に関する前提条件及び人的環境に関する前提条件を含める。また、情報システム又は開発ソフトウェアが使用される組織のセキュリティ方針がある場合にも記述する。府省庁においては、省庁対策基準等が組織のセキュリティ方針に該当する。（「2.2.3 前提条件のまとめ方」を参照）

（4） 脅威：情報システム又は開発ソフトウェアにおいて保護すべき情報資産を脅かす脅威を記述する。（「2.2.4 脅威のまとめ方」を参照）

あわせて、情報システム又は開発ソフトウェアに重要なセキュリティ要件があると認めた場合には、ST 評価・ST 確認について以下を記載するものとする。

1）委託先は、受注した情報システム又は開発ソフトウェアについて ST を作成し、ST 評価・ST 確認を受けること。

2）ST 評価・ST 確認を受ける過程でセキュリティ機能の問題が指摘された場合には、対応を行うこと。

【その他特記事項】

- 暗号化又は電子署名の付与のアルゴリズムを導入する場合は、電子政府推奨暗号リストに記載された暗号リストから選択すること（政府機関統一基準 4.1.6(1)(e)）。
- 機器等の認証取得に関する政府機関統一基準における次の強化遵守事項を採用する場合には、その内容に沿う事項を記述する。

  機器等の調達等を含む情報システムの構築において、その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。（政府機関統一基準 4.3.1(1)(f)）

付録Ｂ　セキュリティ提案仕様に記載すべき項目

提案者が作成するセキュリティ提案仕様に記載すべき項目と内容を以下に示す。

（1） システム概要：提案する情報システム又は開発ソフトウェア全体の概要情報を記述する。通常は、セキュリティ要求仕様のシステム概要と同一又は同等の内容となる。

1）識別情報：提案する情報システム又は開発ソフトウェアの管理及び識別に必要なラベル情報及び記述情報を含める。

2）システム記述：提案する情報システム又は開発ソフトウェアのセキュリティ機能を検討する範囲を物理的又は論理的に定める。情報システム又は開発ソフトウェアの動作概要等を記述して「脅威の抽出～セキュリティ機能の規定」が正確に理解できる情報を含める。

（2） 保護すべき情報資産：提案する情報システム又は開発ソフトウェアのセキュリティ機能が保護すべき情報資産を示す。通常は、セキュリティ要求仕様に記載された保護すべき情報資産に、二次的な情報資産を加えたものとなる。

（3） 前提条件：情報システム又は開発ソフトウェアのセキュリティを考慮する際に必要な前提条件を記述する。前提条件には、物理的な設置環境に関する前提条件、接続面に関する前提条件及び、人的環境に関する前提情報を含める。また、情報システム又は開発ソフトウェアの運用時に適用される省庁対策基準等がセキュリティ要求仕様で提示されていれば、これも記述する。通常は、セキュリティ要求仕様に記載された前提条件を取り込むこととなる。

（4） 脅威：セキュリティ要求仕様に挙げられた脅威を記述する。

（5） 情報セキュリティ対策：保護すべき情報資産を脅威から保護するための情報セキュリティ対策を記述する。情報セキュリティ対策は、セキュリティ提案仕様、政府機関統一基準及び本書等を参照して、以下の項目について記述すること。

1）情報セキュリティ対策として技術対策、物理対策、運用対策、保証対策を提案すること。

2）提案する各対策と脅威、前提条件、政府機関統一基準との対応、情報資産評価表との関連性を示すこと。

（6） セキュリティ機能を実現する機器等：セキュリティ提案仕様を実現するために必要なセキュリティ機能を実現する機器等の製品名、具備するセキュリティ機能、その製品の IT セキュリティ評価及び認証制度に基づく認証取得の有無を記載する。

（7） 制約条件：セキュリティ要求仕様として提示された保護すべき情報資産、前提条件及び脅威に対してセキュリティ提案仕様において追加・変更等を加える場合に、その内容及び理由を記述する。

あわせて、以下を記載するものとする。

（8） 情報システム又は開発ソフトウェアに関する ST 評価・ST 確認：調達者がセキュリティ要求仕様において ST 評価・ST 確認の実施を委託先に求めた場合、提案者は、当該調達を受託した場合には、ST 評価・ST 確認を受けることを宣言する。

付録Ｃ　IT セキュリティ評価及び認証制度を活用した機器等の購入について

1. IT セキュリティ評価及び認証制度（JISEC）とは

機器等又はシステムにセキュリティ機能が正確に実装され、想定されている脅威に対して有効に動作することを、認定された中立性の高い第三者（評価機関）が評価する我が国の制度である。評価は、国際基準 ISO/IEC 15408 に基づいて実施され、その評価結果を認証機関（独立行政法人 情報処理推進機構）が検証した上で、合格した認証製品情報を公開している。

2. 国際的な相互承認制度の枠組み

Common Criteria Recognition Arrangement（CCRA）と呼ばれる国際的な相互承認アレンジメントでは、参加するメンバー国を２種類のカテゴリー「Certificate Authorizing Participants（認証国）」と「Certificate Consuming Participants（受入国）」に分類している。ISO/IEC 15408 に基づいて、ある認証国で評価・認証された機器等及びシステムは、他の認証国・受入国でも認証の効力を持たせることができる。2006 年 3 月時点で、認証国として 10 ヶ国（アメリカ・イギリス・ドイツ・フランス・カナダ・オーストラリア・ニュージーランド・日本・オランダ・ノルウェー）が、また、受入国として 12 カ国、合計 22 ヶカ国が参加している（例：日本で評価・認証した製品は、他の加盟国でもその「認証」が有効である。）。

3. 評価保証レベル（EAL）とは

EAL（Evaluation Assurance Level）とは、製品に実装されているセキュリティ機能の信頼度（保証）を、設計から出荷までの開発プロセスにおける仕様書、記録、利用者や管理者のためのマニュアル、製品そのもの等の証拠を根拠に、確からしさの程度（レベルに応じて詳細に検証）によって示したものである。セキュリティ機能の多寡や強度を示すものではないことに注意が必要である。EAL1～7 までの 7 段階があるが、CCRA の適用範囲は EAL4 までである。

表 3-1 評価保証レベル

レベル	評価の内容
EAL1	ST、機能仕様書、マニュアル、構成管理、独立したテストの実施
EAL2	EAL1 に追加して、構造設計、セキュリティ機能の動作テスト、脆弱性の分析,出荷プロセス
EAL3	EAL2 に追加して、誤操作対策、開発環境の情報セキュリティ対策、開発の手順・規則類
EAL4	EAL3 に追加して、構成管理自動化ツール、詳細設計、実装(ソースコード)のサンプル、侵入攻撃

ISO/IEC 15408 での保証の考え方は、宣言した範囲のセキュリティ機能が正しく動作し、保護すべき情報資産が脅威にさらされることがないことを、宣言した保証の範囲で検証することである。

【注釈】ISO/IEC 15408 では、EAL1～EAL7 によって保証要件（評価の内容）がパッケージ化されている。すなわち、ISO/IEC 15408 に示されているすべての保証要件のうち、評価に適用する保証要件を選択する標準パターンが、EAL1～EAL7 として定められている。これに対し、既定の EAL には含まれていない保証要件を「追加」として適用することもでき、「EAL2+（追加の保証要件［複数設定可］）」のように表記する。

4. 活用時の留意事項

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を活用する際は、以下の点に留意する。

本制度による認証は、評価･認証の対象としたセキュリティ機能及びそのセキュリティ機能の保証の範囲で、セキュリティターゲット（ST）に記載された内容の限りにおいて有効である。例えば、ST に記載されたものとは異なるバージョンの製品には、当該認証は適用できない。また、ST に記載された前提条件を満たさない環境でその製品を使用する場合には、認証の効果が発揮されない。

本制度では、評価の対象とする機能の範囲は、評価の申請者（又は開発者）が自由に設定できる。そのため、販売されている製品・システムと、評価された範囲とが一致していない場合もある。調達者が必要としている機能が、評価された範囲に含まれていない場合もあり注意が必要である。したがって、調達において認証製品を選定する際には、安易に認証実績のみで選択するのではなく、本書に示すような手順で利用環境やセキュリティ要件を明確にし、認証された製品の ST がその利用環境やセキュリティ要件を満たしているかどうかを確認した上で判断する必要がある。

5. 代表的な製品のセキュリティ機能の解説

ここでは、代表的な製品であるオペレーティングシステム（OS）、ファイアウォール、データベースマネジメントシステム（DBMS）について、これらが具備する代表的なセキュリティ機能を説明する。

5.1. オペレーティングシステム

オペレーティングシステム（Operating System）は、通常その頭文字をとって OS と呼ぶ。ファイルの単位でコンピュータ内の様々なソフトウェアやデータを管理し制御する（ファイル管理機能）。第三者によるコンピュータ内のデータの不正入手、破壊、書換えを防ぐためには、OS の管理の対象であるファイルをいかに保護するかが重要課題となる。

OS は、アクセスする利用者が確かにアクセスを許可された利用者であるかどうかを確認する手段を提供する（利用者認証機能）。また、ファイルの所有者（作成者）が自分のファイルに対する他の利用者のアクセス権限を設定することによりアクセス制御を行う手段を提供する（この機能を、任意アクセス制御又は自由裁量アクセス制御（DAC: Discretionary Access Control）という。）。また、OS 上で実行される操作の記録やそれをレポートする監査機能、装置への入出力を保護し信頼性を高めるための入出力の高信頼化機能等を提供する。

一方、一般の OS による既存の防御技術では対処できない不正アクセス（トロイの木馬、バッファオーバフロー、内部犯行、ファイアウォール・侵入検知・暗号化・パッチ処理等の不完全な設定）に対して OS が備えるべき機能として、利用者認証強化機能、強制アクセス制御機能（MAC：Mandatory Access Control）、オブジェクトの再利用保護、完全仲介機能等が挙げられる。一般にこれらの機能を具備した OS はセキュア OS とも呼ばれている。

セキュア OS は、特に特権機能や重要データを侵害者から守る効果があるが、運用面で負担がかかるため、適用効果、適用に際しての問題点、運用への影響、業務への影響等を十分検討した上で採否を決定することが重要である。

セキュア OS については、「電子政府におけるセキュリティに配慮した OS を活用した情報システム等に関する調査研究」（内閣官房情報セキュリティセンター）が参考になる。

http://www.nisc.go.jp/inquiry/index.html

5.2. ファイアウォール

ファイアウォールは、外部ネットワーク等からの不正侵入を防ぐためのいわゆる防護壁として機能する機器又はソフトウェアである。LAN 等内部ネットワークをインターネット等の外部ネットワークに接続すると、外部の第三者からの不正アクセスや不正侵入等の攻撃を受けることになる。与えられた規則に基づき通信を許可し又は阻止することにより外部からの攻撃や内部からの情報の漏えいを防止する機能を備えたハードウェアやソフトウェアを、総称してファイアウォールと呼ぶ。

ファイアウォールが備えるべき機能として、①情報フロー制御（ネットワーク上を転送する情報の流れを制御する。）、②アクセス制御（利用者及び利用対象サーバを制限する。）、③監査（情報フロー制御やアクセス制御を実施する機器及びサーバの稼働状況や利用状況が適切であるかどうかを検査する。）、④認証（利用者又は利用対象サーバ等がアクセスを認められた利用者又はサーバであるかを確認する。）、⑤管理（①～④の機能を動作させるために必要な設定を、限定された管理者が行う。）等が挙げられる。また、高度なファイアウォール機能としては、⑥監視（ネットワーク上のトラフィック、機器やサーバの使用状況、アクセスログ等を監視する。）、⑦暗号化（転送データ、パスワード等の暗号化を行う。）等の機能が具備される場合もある。これらの①から⑦までの機能は、ファイアウォールが備えるセキュリティ機能である。

ファイアウォールは、その設置場所により 2 種類に分類できる。①外部ファイアウォールは、外部からの攻撃を阻止し、内部からの情報の漏えいを防止するため、外部ネットワークと内部ネットワークの接続点に設置する。②内部ファイアウォールは、内部ネットワークにおいても各グループ間での不用意な情報の流出、流入の防止、また内部でのアクセス制御を目的として内部のサブネットワークの相互接続点に設置する。

ファイアウォールによる情報フロー制御及びアクセス制御の代表的な実現方式は、パケットフィルタリング方式とアプリケーションゲートウェイ方式である。

（1）パケットフィルタリング方式

パケットフィルタリング方式とは、OSI（Open Systems Interconnection）参照モデルの主にネットワーク層又はトランスポート層のデータパケットに付加された送信元・先のアドレス、ポート番号、情報の方向等に基づいて情報フロー制御及びアクセス制御を行う方式である。

パケットフィルタリングの仕組みを簡単に示す。①パケットの方向（外部から内部、内部から外部）を確認する。②外部から内部へのパケットについては、パケットの送信先アドレス、送信元アドレス、プロトコル等が登録されたルールに基づいて許可される場合、内部ネットワークに通過させ、そうでなければ通過を拒否する。③ 内部から外部へのパケットの場合も、②と同様である。

（2）アプリケーションゲートウェイ方式

アプリケーションゲートウェイ方式では、ネットワークを相互接続するゲートウェイ機能をアプリケーション層で実現することで情報フロー制御及びアクセス制御を行う。制御の対象は、送信元・先アドレス、ポート番号のほか、個々のアプリケーションのプロトコルやデータ構造等プロトコル各層にわたり、アプリケーションごとの詳細な制御を行うことできる。その反面、アプリケーションに応じてそのためのゲートウェイを設けることが必要となる。

アプリケーションゲートウェイ方式の仕組みを簡単に示す。①送信側コンピュータはファイアウォールコンピュータに接続許可を求める。②ファイアウォールコンピュータは登録されたルールに従って許可されたコンピュータだけと通信を開始する。この認証にはパスワード認証等のメカニズムが使用される。③送信側コンピュータからパケットが送信されファイアウォールコンピュータはそれを受け取る。④ファイアウォールコンピュータは受け取ったパケットを受信側コンピュータに送信する。

5.3. データベースマネジメントシステム

データベースマネジメントシステム（DBMS: Database Management System）は、データベースの作成・更新及びデータに対するアクセスを管理するためのソフトウェアである。情報システムを構築する際にはミドルウェアとして利用され、トランザクションの受付機能やビジネスロジックを実現するアプリケーション機能からデータベースの管理機能を分離することで、任意に定義されたデータへのアクセス制御方針を厳密に実現するとともに、データの機密性や完全性を高める機能を提供する。管理するデータの表現形式や、

データにアクセスするためのインタフェースが標準化されており、それぞれの DBMS 製品が提供するセキュリティ機能も共通するものが多く存在する。

DBMS が提供する代表的なセキュリティ機能としては、①利用者の識別・認証機能、②データベースオブジェクトへの任意アクセス制御機能、③コミット及びロールバック機能、④特権割当機能、⑤ロール割当機能、⑥監査機能、⑦セキュリティ管理機能等が提供される。また、データの暗号化機能やデータベースアクセスのための通信データを暗号化する機能等を提供する DBMS 製品もある。

6. 認証製品リストの利用法

CCRA に加盟している認証国では、各国の ISO/IEC 15408 に基づく IT セキュリティ認証機関の Web サイトで認証製品に関する情報を公開している。また、CCRA 加盟国で認証された認証製品のリストを集約して公開する Web サイト（The official website of the Common Criteria Project：ここでは CC ポータルという。）が存在する。各国の認証機関の Web サイトや CC ポータルでは、様々な分野の機器等について認証取得情報を収集することができる。この情報は、セキュリティ提案仕様に含まれる認証製品について、認証取得の内容を調査し、提案の妥当性を判断するために利用できる。

以下に認証取得が進んでいる製品分野を示す。

- **アクセスコントロールデバイス/システム**
  データに対するアクセス制御を実現するミドルウェア製品、シングルサインオン認証製品等
- **境界保護デバイス/システム**
  ファイアウォール機能を持つソフトウェアやアプライアンス製品等
- **データベース**
  データベースマネジメントシステム等
- **データ保護**
  暗号化、アクセス制御、確実な消去、改変検知等によってデータを保護するためのミドルウェア製品等
- **検知デバイス/システム**
  ネットワーク型、ホスト型の侵入検知システム等
- **IC・スマートカード・スマートカード関連デバイス/システム**
  IC チップ、スマートカード、IC チップ上で動作する組込みソフトウェア等
- **鍵管理システム**
  認証局構築ソフトウェア、OCSP サーバソフトウェア、ディレクトリサーバソフトウェア、タイムスタンプサーバソフトウェア等

- **ネットワーク関連デバイス/システム**
  ネットワーク管理･診断ソフトウェア、IPSec 等 VPN 製品、スイッチ・ルータ製品等
- **オペレーティングシステム**
  UNIX、Linux、ホスト OS、ミニコン OS、PC 等のオペレーティングシステム
- **その他のデバイス/システム**
  デジタル複合機コントローラ、テレフォニーシステム等

6.1. 認証製品リストから得られる情報

ISO/IEC 15408 に基づく各国認証制度の Web サイトや CC ポータルでは、それぞれの認証製品について、以下に示す情報を掲載している。

評価対象の名称： 認証された製品の評価された部分の名称を示す。製品全体を評価対象とした場合は製品名が記載されるが、製品の部分や特定の条件のもとに認証を取得している場合は、それらの情報を含んだ名称となっている場合がある。

バージョン： 評価の対象となったバージョンが記載される。認証は特定のバージョンに対して有効なものであるため、検討する製品が提案されたバージョンについて認証を取得しているかどうかを確認する必要がある。

開発者情報： 開発者の企業名、問合せ窓口情報（担当者への連絡先等）が記載される。

適合する保証要件： 適合する保証要件が記載される。採用した EAL で表される場合が多い。

PP 適合： 適合する PP（Protection Profile：製品やシステムの種別ごとに、考慮する脅威やその対策、対策を実現するセキュリティ要件等を記述した ISO/IEC 15408 に基づく文書であり、評価・認証済みとして登録されたもの）がある場合に、当該 PP を特定する情報が記載される。

認証取得情報： 各認証制度での認証番号、認証取得日等が記載される。

認証報告書： 各認証制度で認証されたことを示す詳細な報告書の pdf ファイルをダウンロードすることができる。

ST（セキュリティターゲット）：ST の pdf ファイルをダウンロードすることができる。

認証書： 制度によっては認証書の写しの pdf ファイルをダウンロードすることができる。

その他：　　認証製品の製品情報、評価機関名等が記載される。

CC ポータルサイトから上記の情報を検索する手順は、以下のとおりである。

（1） CC ポータル Web サイトのホームページを表示する。
http://www.commoncriteriaportal.org/

（2） CC ポータル Web サイトの認証製品リストを表示する。
前記（1）のホームページで “Consumers”、“Developers” 又は “Experts” のいずれかを選択し、次に “List of Evaluated Products” を選択して認証製品リストを表示する。

（3） 認証製品リストから、目的とする認証製品を検索し、その認証に関する情報を得る。

また、国ごとの Web サイトは、（1）のホームページで “Consumers”、“Developers” 又は “Experts” のいずれかを選択し、次に “List of CCRA Members” を選択して所在を知ることができる。

6.2. 認証製品情報の利用

認証製品の利用が提案されている場合には、前節の手順で得た当該製品の認証に関する情報について以下の手順により確認し、提案の妥当性の判断に資することができる。

（1） 前節の手順で得た認証製品の製品名称、バージョン、認証取得年月日、有効期限等の情報が、提案された製品に合致することを確認する。

（2） ST の以下の内容が、提案における当該製品の使用方法等に合致することを確認する。

- 評価対象範囲（TOE）
- セキュリティ機能（ST の 6 章）
- 前提条件、想定する脅威、使用者に求められる対策等（ST の 3 章、4 章及び 8 章）

（3） ST に記述されている保証要件又は評価保証レベル（EAL）が、府省庁の期待するものであることを確認する。

参考例

参考例Ⅰ　Web システム

参考例Ⅱ　インターネットサービスシステム

参考例Ⅲ　複合機システム

参考例Ⅰ

Web システム

ここでは、府省庁における Web システムを例に、基本設計調達時に調達者が作成するセキュリティ要求仕様の例と、セキュリティ提案仕様を調達者が審査する際のポイントを示す。

ただし、ここで扱う Web システムはあくまでも一般的なモデルであり、実際の府省庁における Web システムではないことに留意すること。

実際の調達に当たっては、それぞれの情報システムにより保護すべき情報資産、前提条件、脅威及び求める情報セキュリティ水準等が異なることに留意し、本付録に示すセキュリティ要求仕様及びセキュリティ提案仕様の審査ポイントに対して適切に追加、変更等を加えること。

1. セキュリティ要求仕様

1.1. システム概要

1.1.1. システム全体概要

本 Web システムは、国民等の一般利用者がインターネットを介して府省庁から提供される情報を、「いつでも」、「どこでも」自由に閲覧できる情報提供システムである。

一般利用者は、自身の所有する PC 等の一般利用者端末を利用して Web システムにアクセスすることにより、府省庁が提供する情報の閲覧や、各種フォーマット等のダウンロードを行うことができる。さらに、一般利用者はあらかじめ Web システムに利用者登録を行うことにより、利用者登録を行った一般利用者にだけ提供される情報を閲覧することも可能である。

なお、システム要件の詳細については、本調達仕様の「業務要件」、「情報・データ要件」、「機能要件」、「システム要件」、「運用要件」、「移行要件」、「セキュリティ要件」及び各種添付資料をあわせて参照されたい。

Web システムにかかわるサービスの全体像を図 1.1 に示す。

【注釈】システムの詳細については、調達において提示する他の仕様書に具体的な記述があれば、それらの参照箇所を示すことで本セキュリティ要求仕様書に詳細を記述する必要はない。

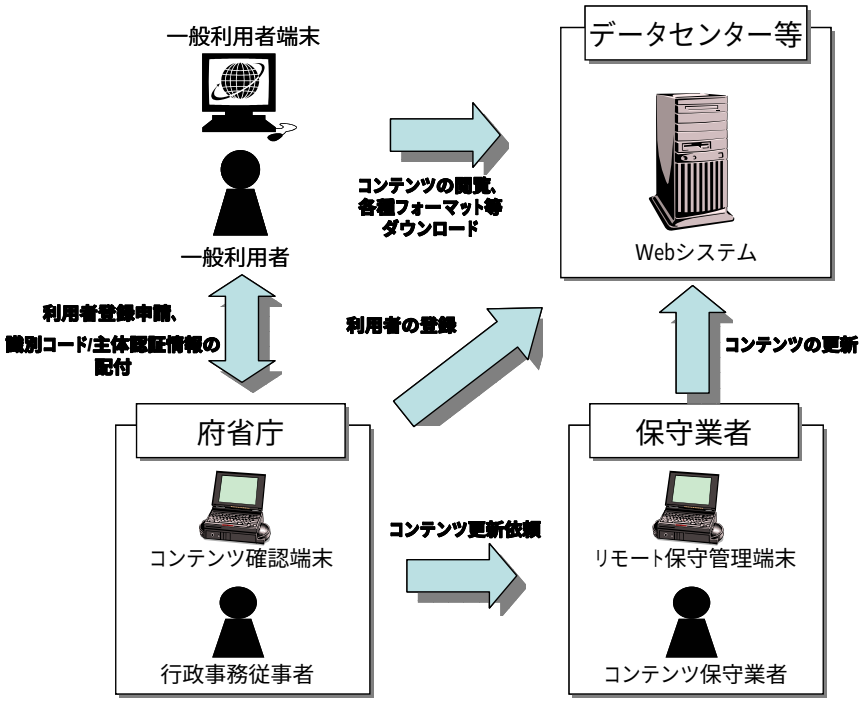


図 1.1 業務サービスの全体像

1.1.2. システム構成

1.1.2.1. システム構成概要

Web システムの構成を図 1.2 に示す。なお、図中の点線で囲った部分が本調達の範囲である。

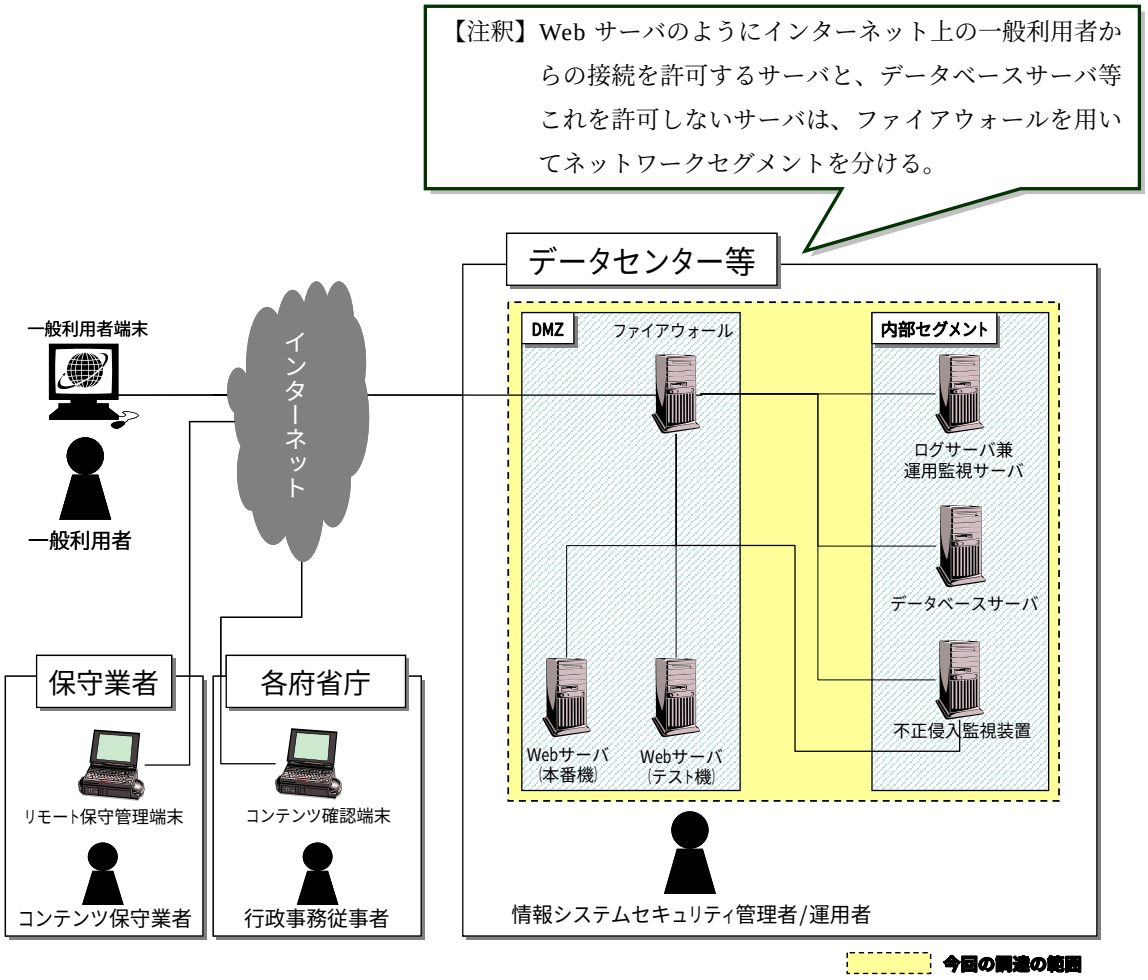


図 1.2 Web システムの構成例

1.1.2.2. ハードウェア機器構成例

システムのハードウェア機器構成例を以下に示す。各機器の具体的要件は、本調達仕様書の分冊である「システム要件」に示す。

【注釈】機器調達の際には、セキュリティ機能の装備に関して第三者による評価済みの認証製品から選択することを求める等、必要に応じて調達者の要求水準を示す必要がある。

表 1-1 Web システムのハードウェア機器構成例

セグメント	ハードウェア機器（例）	機能概要
DMZ	ファイアウォール	ファイアウォールは、あらかじめ設定されたアクセス制御ルールに従って、IP アドレスやプロトコルによる通信パケットのフィルタリングを行い、不正アクセスを防止する機能を提供する。
	Web サーバ	Web サーバは、インターネットを介して、一般利用者にコンテンツを提供する。このコンテンツは府省庁より提供される。 Web サーバは、本番機と、コンテンツの更新の際の事前確認に使用するテスト機の 2 台により構成される。
内部セグメント	データベースサーバ	データベースサーバには、利用者登録を行った一般利用者の個人情報や、新着情報等の動的にコンテンツを生成するための情報等が保存される。 データベースサーバは、Web サーバからの問合せを受けて、データベースサーバ内の情報を提供する。
	ログサーバ兼運用監視サーバ	ログサーバ兼運用監視サーバは、Web サーバ（本番機）において取得したコンテンツへの利用履歴を定期的に解析し、その結果を自身に保存するとともに Web サーバ（テスト機）へ転送する。 また、各サーバにて記録した証跡を収集し、不正侵入及び不正アクセスがなされた痕跡がないか解析を行う。
	不正侵入監視装置	不正侵入監視装置は、あらかじめ設定された検知ルールに基づいて通信メッセージの監視を行い、Web システムに対する不正侵入及び不正アクセスをリアルタイムに検知する。

1.1.2.3. 外部システム連携方法

Web システムと連携する外部システムは、表 1-2 に示す端末以外には特に存在しない。各端末との連携方式については、本調達仕様書の分冊「システム要件」を参照されたい。

【注釈】連携すべき外部システムが他に存在する場合、その外部システムとのインタフェースを明確にし、表 1-2 に追記する必要がある。

表 1-2 Web システムを利用する外部端末

外部端末	概要
コンテンツ確認端末	コンテンツ確認端末は府省庁の施設内に設置され、府省庁 LAN 及びインターネットを介して Web システムに接続する。 コンテンツ確認端末は、行政事務従事者によるコンテンツの確認や、一般利用者の利用者登録等に利用される。
リモート保守管理端末	リモート保守管理端末は、コンテンツ保守業者の施設内に設置され、コンテンツ保守業者の施設内 LAN 及びインターネットを介して Web システムに接続する。 リモート保守管理端末は、コンテンツ保守業者によるコンテンツの更新等に利用される。
一般利用者端末	一般利用者端末は、一般利用者により所有され、インターネットを介して Web システムにアクセスする。 一般利用者端末は、一般利用者によるコンテンツの閲覧等に利用される。

1.1.3. システム機能概要

1.1.3.1. Web システムの機能

Web システムが利用者に提供する機能の概要を、表 1-3 に示す。機能の詳細については、本調達仕様書の分冊「システム要件」及び「機能要件」を参照されたい。

【注釈】ここでは、セキュリティ要求仕様では Web システムの機能の記述は概要に留め、詳細は「システム要件」及び「機能要件等」、別途調達者から提示する仕様書に記述することを想定している。

表 1-3 Web システムの機能

機能	機能の概要
コンテンツの閲覧	一般利用者は、自身の一般利用者端末を利用して Web システムにアクセスし、コンテンツの閲覧や各種フォーマット等のダウンロードができる。なお登録済み利用者限定のコンテンツを閲覧する際には、一般利用者は利用者登録実施時に払い出された識別コードと主体認証情報を用いた認証を受ける必要がある。
コンテンツの登録	府省庁の行政事務従事者は、Web システムにおいて一般利用者に提供するコンテンツの作成及び登録をコンテンツ保守業者に依頼する。コンテンツ保守業者は、行政事務従事者の依頼を受けて、コンテンツの作成及び登録作業を行う。 なお、コンテンツ保守業者がコンテンツを作成するための機能は、Web システムの機能ではない。当機能については、表 1-4 を参照されたい。 また、コンテンツには、一般利用者の誰でもが閲覧可能な一般公開用のコンテンツと、あらかじめ利用者登録をした一般利用者のみが閲覧可能な登録済み利用者限定のコンテンツがある。
利用者登録	登録済み利用者限定のコンテンツの閲覧を希望する際には、一般利用者は、あらかじめ行政事務従事者に申請し、利用者登録を行う必要がある。利用者登録は、所定の申込書に記入の上、郵送又は FAX を用いて行政事務従事者に送付する。利用者登録の結果、登録した一般利用者一人一人に対して、登録済み利用者限定のコンテンツを閲覧する際に必要となる識別コードと主体認証情報が払い出される。払い出された識別コードと主体認証情報は、安全な方法により一般利用者本人に配付される。 なお、利用者登録時に登録した一般利用者の情報は、一般利用者本人又は行政事務従事者のみが更新できる。
コンテンツの更新	コンテンツ保守業者はリモート保守管理端末を利用して、コンテンツの更新を行う。
コンテンツの確認	府省庁の行政事務従事者はコンテンツ確認端末を利用して、コンテンツ保守業者が登録又は更新した Web サーバ上のコンテンツが依頼通りかどうかを確認する。

Web システムが提供する機能ではないが、Web システムの全体像を理解する上で必要な

機能の概要を表 1-4 に示す。

表 1-4 Web システム外の機能

機能	機能の概要
コンテンツの作成	委託を受けたコンテンツ保守業者は、Web システムにおいて提供するコンテンツの作成を行う。ただし、コンテンツの作成機能はコンテンツ保守業者が用意する機器等を使用することとし、Web システムにおいては提供されない。

1.1.3.2. Web コンテンツの更新手順

Web コンテンツの更新は、以下の手順により実行される。（図 1.3 参照）

なお、図 1.3 に示す手順の中で、点線で囲っている項目は、Web システムの機能を利用しない処理である。

① 行政事務従事者は、コンテンツ保守業者にコンテンツ更新依頼とコンテンツ更新内容の通知を行う。
② コンテンツ保守業者は、行政事務従事者から通知されたコンテンツ更新内容に従って、コンテンツを作成する。
③ コンテンツ保守業者は、リモート管理端末を利用して Web サーバ（テスト機）へコンテンツを反映する。
④ コンテンツ保守業者は、行政事務従事者に Web サーバ（テスト機）上のコンテンツの確認依頼を行う。
⑤ 行政事務従事者は、Web サーバ（テスト機）上のコンテンツの確認を行う。
⑥ ⑤において問題がない場合、行政事務従事者はコンテンツ保守業者に Web サーバ（テスト機）上コンテンツの Web サーバ（本番機）への反映を依頼する。
⑦ ⑤において問題がある場合、行政事務従事者はコンテンツ保守業者へコンテンツの修正を依頼する。
⑧ コンテンツの修正依頼を受けたコンテンツ保守業者は、コンテンツの修正を行い、③以降を繰り返す。
⑨ Web サーバ（本番機）への反映依頼を受けたコンテンツ保守業者は、Web サーバ（本番機）への反映を行い、再度行政事務従事者にコンテンツ確認依頼を行う。
⑩ 行政事務従事者は、Web サーバ（本番機）上のコンテンツを確認する。
⑪ ⑩において問題がない場合、行政事務従事者はコンテンツ保守業者へ承認を通知する。
⑫ ⑩において問題がある場合、行政事務従事者は⑤以降を繰り返す。
⑬ 承認通知を受けたコンテンツ保守業者は、作業報告書を作成し、行政事務従事者へ提出する。
⑭ 行政事務従事者は作業報告書を確認し、コンテンツ更新作業を終了する。

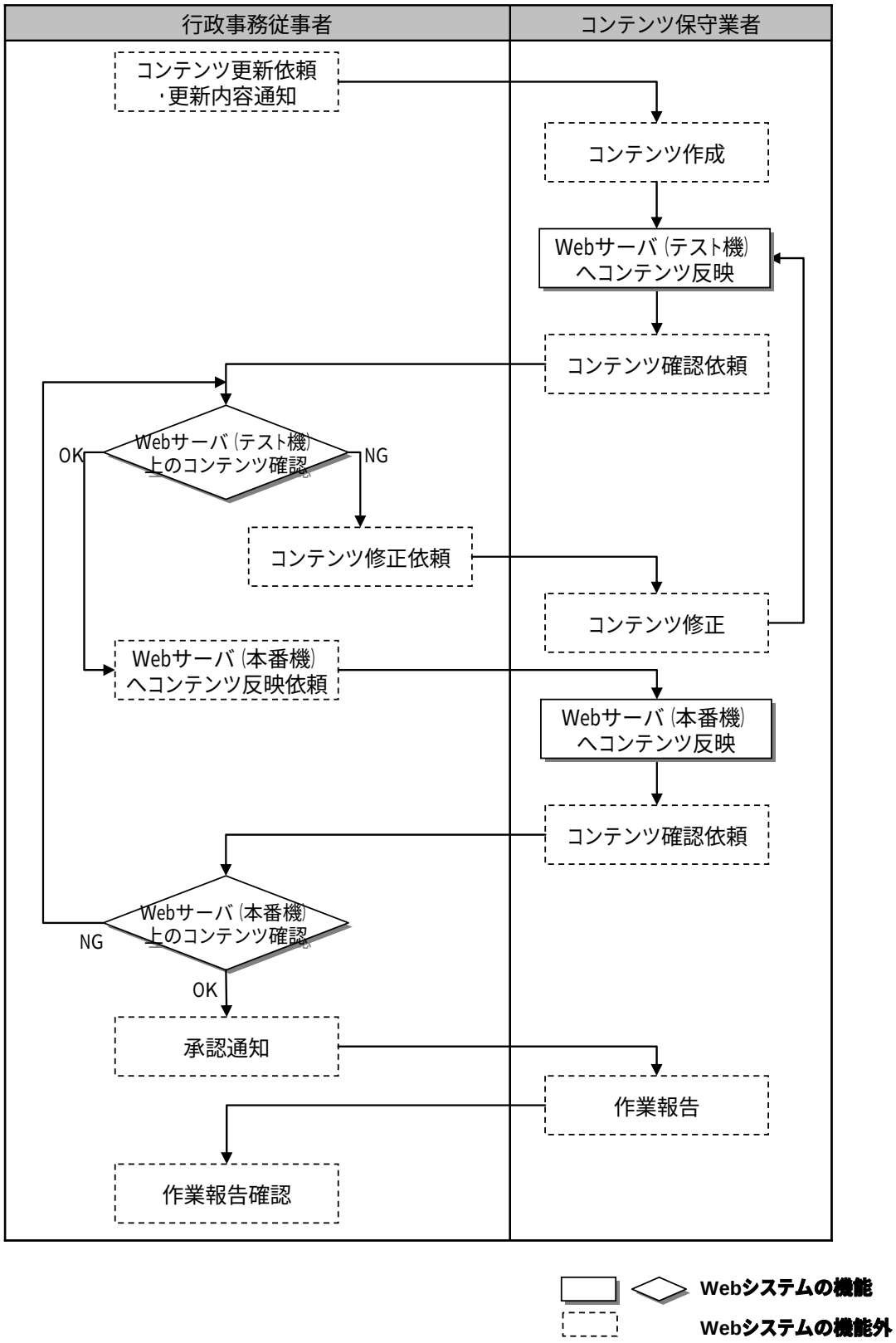


図 1.3 Web コンテンツの更新手順

1.1.4. システムにおける想定ユーザ

Web システムが想定するユーザの分類ごとに、その役割と権限を示す。各関係者による運用要件の詳細は、本調達仕様書の分冊「運用要件」を参照されたい。

【注釈】システム運用時に必要なセキュリティ対策を検討するために、当該システムが誰によりどのように利用・管理されるのかをできるだけ明確に示すことが望ましい。この例では、システムの主な関係者の分類を行い、それぞれの役割と権限の概要記述に留め、想定するシステムの運用形態の詳細は、運用要件等、別途調達者から提示することを想定している。

表 1-5 Web システムの想定ユーザ

関係者名称	役割・権限の説明	
行政事務従事者	役割	行政事務従事者は、各府省庁に所属し、コンテンツ確認端末を利用してコンテンツの確認、Web コンテンツの利用履歴解析結果の確認を行う。また、一般利用者の利用者登録を受け付け、識別コードと主体認証情報の払い出しを行い、一般利用者の登録情報の管理を行う。
	権限	行政事務従事者は、Web システムに対して以下の権限を有する。 • Web サーバ（本番機、テスト機）上のコンテンツの参照に関する権限 • Web サーバ（テスト機）上の Web コンテンツの利用履歴解析結果の閲覧に関する権限 • 一般利用者の利用者登録に関する権限 • 一般利用者が利用者登録時に登録した情報（主体認証情報含む）の更新に関する権限
情報システム セキュリティ管理者	役割	情報システムセキュリティ管理者は、Web システムのサーバ機器が設置されるデータセンター等の施設内に存在し、サーバ機器及び通信回線装置に直接接続されたコンソールを利用して、各機器の監視等を行う。又は運用担当者に作業を任せ、その作業内容の確認を行う。また、運用担当者及びコンテンツ保守業者の任命及びユーザ登録を行う。なお、運用担当者及びコンテンツ保守業者のユーザ登録は Web システムの機能外である。
	権限	情報システムセキュリティ管理者は、Web システムに対して以下の権限を有する。 • サーバ機器及び通信回線装置の監視に関する権限 • 不正侵入監視装置及びログサーバ兼運用監視サーバ上の証跡及び証跡解析結果の参照に関する権限 • サーバ機器のバックアップに関する権限 • セキュリティパッチ、ウイルス定義ファイル、不正侵入監視装置パターンファイルの更新に関する権限
運用担当者	役割	運用担当者は、Web システムのサーバ機器が設置されるデータセンター

関係者名称	役割・権限の説明	
		等の施設内に存在し、サーバ機器及び通信回線装置に直接接続されたコンソールを利用して、各機器の監視等を行う。
	権限	運用担当者は、Web システムに対して以下の権限を有する。 • サーバ機器及び通信回線装置の監視に関する権限 • 不正侵入監視装置及びログサーバ兼運用監視サーバ上の証跡及び証跡解析結果の参照に関する権限 • サーバ機器のバックアップに関する権限 • セキュリティパッチ、ウイルス定義ファイル、不正侵入監視装置パターンファイルの更新に関する権限
コンテンツ保守業者	役割	コンテンツ保守業者は、保守業者施設内からリモート管理端末を利用して、コンテンツの登録・更新を行う。また、行政事務従事者からの障害連絡を受け付け、障害原因の一次切り分けを行う。
	権限	コンテンツ保守業者は、Web システムに対して以下の権限を有する。 • Web サーバ（テスト機）上のコンテンツの登録・更新に関する権限 • Web サーバ（本番機）へ Web サーバ（テスト機）上のコンテンツを反映させる権限
一般利用者	役割	一般利用者は、一般利用者端末を利用して、府省庁が提供するコンテンツを閲覧する。
	権限	一般利用者は、コンテンツ（登録済み利用者である場合は登録済み利用者限定コンテンツを含む。）を参照する権限、及び自身の登録済み利用者情報を参照、変更する権限を有する。
情報システム セキュリティ責任者	役割	情報システムセキュリティ責任者は、Web システムに対する情報セキュリティ対策の管理に関する事務を統括する。行政事務従事者、及び情報システムセキュリティ管理者の任命及びユーザ登録を行い、管理や教育を実施する。なお、行政事務従事者及び情報システムセキュリティ管理者のユーザ登録は Web システムの機能外である。
	権限	情報システムセキュリティ責任者が Web システムに対して有する権限はない。

1.2. 保護すべき情報資産

政府機関統一基準においては、府省庁において取り扱う情報について、表 1-6 の定義に従い格付けを行うことを求めている。なお、機密性が２又は３の情報資産を「要機密情報」、完全性が２の情報資産を「要保全情報」、可用性が２の情報資産を「要安定情報」という。さらに、要機密情報、要保全情報、要安定情報のいずれかに当てはまる情報を「要保護情報」という。

【注釈】情報の格付けの定義について、各府省庁において詳細化等を行っている場合には、その規定に合わせて見直す必要がある。

表 1-6 情報の格付けの定義

項番	分類	内容
1	機密性１情報	機密性２情報又は機密性３情報以外の情報
2	機密性２情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、その漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報
3	機密性３情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報
4	完全性１情報	完全性２情報以外の情報（書面を除く）
5	完全性２情報	行政事務で取り扱う情報（書面を除く）のうち、その改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適確な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報
6	可用性１情報	可用性２情報以外の情報（書面を除く）
7	可用性２情報	行政事務で取り扱う情報（書面を除く）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報

Web システムにおける保護すべき情報資産を抽出し、政府機関統一基準に従って、機密性、完全性、可用性の格付けと共に整理・評価した結果を表 1-7 に示す。

【注釈】情報資産を情報名（データ名）で整理し、機密性、完全性、可用性の格付け、及び要保護資産か否かの提示を行う。

【注釈】情報資産は、業務データ等の一次的な保護資産、システムの信頼性維持やセキュリティ機能の動作を保証するために必要となる二次的な保護資産がある。通常ここでは、前者の一次保護資産を主たる対象として情報を整理する。情報システムのしくみとして当然組み込まれるようなセキュリティ機能（証跡管理機能等）に関連する二次的な保護資産（証跡等）であれば、保護すべき情報資産として整理してもよい。どの情報を保護すべき情報資産とするかについては、省庁対策基準等との整合を考慮する必要がある。

表 1-7 保護すべき情報資産の一覧

資産	機密性	完全性	可用性	要保護	概要
一般公開コンテンツ	1	2	2	○	Web システムで公開される、すべての一般利用者が閲覧可能なコンテンツ情報。Web サーバ又はデータベースサーバに保存される。

【注釈】一般公開コンテンツは、一次的な保護資産に分類される。一般公開コンテンツは、インターネットを利用できる者であれば誰でも Web システムに接続し、閲覧できる情報である。よって、一般公開コンテンツの機密性は特に重要ではないが、もし誤った情報を提供してしまった場合、コンテンツを提供している府省庁の信用に関わるため、コンテンツの完全性を保護することは重要である。また、一般公開コンテンツは一般利用者がいつでも情報を閲覧できる状態である必要があるため、可用性を保護することも重要である。

資産	機密性	完全性	可用性	要保護	概要
登録済み利用者限定コンテンツ	3	2	2	○	Web システムで公開される、登録済みの一般利用者のみが閲覧可能なコンテンツ情報。Web サーバ又はデータベースサーバに保存される。

【注釈】登録済み利用者限定コンテンツは、一次的な保護資産に分類される。登録済み利用者限定コンテンツの完全性を保護することは、一般公開コンテンツと同様、重要である。また、登録済み利用者限定コンテンツは一般公開コンテンツとは異なり、誰でも閲覧できるわけではなく、限られた者のみが閲覧できる情報であることを想定している（例えば、府省庁にて保有している、個人にかかわる情報等）。よって、登録済み利用者限定情報は、その機密性を保護することも重要である。なお、登録済み利用者限定コンテンツ以外の要機密情報は、Web サーバに保存しないことが望ましい（政府機関統一基準 5.3.3(1)(d)）。また、一般公開コンテンツと同様に、登録済み利用者限定コンテンツの可用性を保護することも重要である。

資産	機密性	完全性	可用性	要保護	概要
コンテンツ利用履歴	2	2	1	○	一般公開コンテンツ、及び登録済み利用者限定コンテンツの利用履歴、及びその解析結果。ログサーバ兼運用監視サーバ、及び Web サーバ（テスト機）に保存される。

【注釈】コンテンツ利用履歴は、一次的な保護資産に分類される。一般利用者がコンテンツを利用した履歴情報は、統計的に解析等を実施することにより、将来のコンテンツの拡充・改善の際に重要な役割を果たすことが想定される。よって、コンテンツ利用履歴の完全性を保護することは重要である。また、Web システムではコンテンツ利用履歴を一般に公表することを前提としていないため、機密性を保護することも重要である。

資産	機密性	完全性	可用性	要保護	概要
証跡	2	2	1	○	Web システムのセキュリティ監査機能によって取得された証跡及びその解析結果。ログサーバ兼運用監視サーバに保存される。

【注釈】証跡は、二次的な保護資産に分類される。Web システムに実装されるセキュリティ機能が正しく動作しているかどうかを確認するためには、当然、証跡を取得する機能が必要である。取得した証跡が改ざんされた場合、脅威の発生が検知できない危険性がある。よって、証跡の完全性を保護することは重要である。さらに、Web システムではコンテンツ利用履歴と同様、証跡を一般に公表することは前提としていないため、機密性を保護することも重要である。

なお、政府機関統一基準解説書「4.1.4 証跡管理機能」においては、証跡管理の必要性について次のとおりに記述している。

「情報システムの利用においては、当該情報システムの制御及び管理の実効性を高め、また情報セキュリティに関する問題が発生した場合にこれに適切に対処するために、当該情報システムの動作及びその他必要な事象を記録し、事後にこれを調査する証跡管理を行う必要がある。また、証跡管理により、外部又は内部の者による不正利用又は過失行為を事前に抑止し、また事後に追跡することが可能となる。」

資産	機密性	完全性	可用性	要保護	概要
登録済み 利用者情報	3	2	1	○	利用者登録をした一般利用者に関する個人情報。また、登録済み利用者限定コンテンツを閲覧するための識別コード及び主体認証情報も含まれる。データベースサーバに保存される。

【注釈】登録済み利用者情報は一次的な保護資産に分類されるが、登録済み利用者の識別コード及び主体認証情報のみは、二次的な保護資産に分類される。Web サーバに接続する一般利用者が登録済み利用者であるかどうかを確認するために、あらかじめ登録された識別コード及び主体認証情報を用いることが想定される。

なお、政府機関統一基準解説書「4.1.1 主体認証機能」においては、主体認証の必要性について次のとおりに記述している。

「情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権限のない者が、悪意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。」

1.3. Web システムの運用時の前提条件

Web システムの運用時の前提条件について、物理的、接続的（ネットワーク環境等）、人的側面から示す。

【注釈】当該システムにおいて、リスク低減のためにあらかじめ講じている規則や施設等（調達の範囲外であれば、その旨を明示する必要がある。）については、調達者から情報を与えるものであり、システムの運用環境における前提条件として本節に記述する。

1.3.1. 物理的な設置環境に関する前提条件

【注釈】物理的な設置環境とは、例えばサーバを設置する場所の建屋やセキュリティ区域の特定、耐震・防火に関する基準、電源供給に関する基準、セキュリティ区域への入退室管理や物品受渡し管理の基準、等に関する条件を示すものであり、政府機関統一基準では、「5.1 施設と環境」等がこれに相当する。

【注釈】この例では、サーバを設置するマシンルームとこれを含むデータセンターに対して、所定の基準を満たすことを前提として挙げている。
基準の例としては、下記のものが挙げられる。
・情報システムの設備環境基準（JEITA3 IT-1002）
・行政機関の保有する個人情報の適切な管理のための措置に関する指針について（平成 16 年 9 月 14 日、行政管理局長から各府省等官房長等あて通知）

表 1-8 物理的な設置環境に関する前提条件

識別子	前提条件のタイトル / 内容
物理前提-1	**物理的保護** Web システムにかかわるハードウェア（図 1.2 の点線で囲った範囲内のハードウェア機器）は、許可された者のみが入室できる区画に設置される。

1.3.2. 接続面（ネットワーク環境等）に関する前提条件

【注釈】接続面（ネットワーク環境等）とは、例えばシステムが接続されるネットワーク環境や通信回線の基準、何らかの外部サービスをネットワーク経由で利用する場合の条件等を示すものであり、政府機関統一基準では、「5.4 通信回線」等がこれに相当する。

表 1-9 接続面に関する前提条件

識別子	前提条件のタイトル / 内容
接続前提-1	**インターネットへの接続環境** Web システムの内部ネットワークとインターネット等の外部ネットワークは、特定個所のみで接続されている。
接続前提-2	**情報システムセキュリティ管理者及び運用担当者が使用するコンソール** コンソールは、Web システムにかかわるサーバ及び通信回線装置に直接接続される。また、サーバ・通信回線装置の運用管理に必要な機能はこのコンソールからのみ利用可能であり、それは情報システムセキュリティ管理者又は運用担当者のみが使用できる。

1.3.3. 人的環境に関する前提条件

【注釈】人的環境とは、例えば当該システムの情報システムセキュリティ管理者や行政事務従事者に対する信頼性に関する条件、当該システムに関わる組織・体制として実現すべきことに関する条件、当該システムの使用方法として当然実現されるべきことに関する条件等を示すものであり、政府機関統一基準では、第１部、第２部及び第６部の一部等がこれに相当する。

表 1-10 人的環境に関する前提条件

識別子	前提条件のタイトル / 内容
人的前提-1	**行政事務従事者及び情報システムセキュリティ管理者の信頼性** 国家公務員である行政事務従事者及び情報システムセキュリティ管理者は、国家公務員法の下に業務を実施し、さらに Web システムの管理を適切かつ厳格に実施するための知識とスキルを持つよう教育・訓練されるため、悪意のある行為は実施しない。
人的前提-2	**一般利用者の主体認証情報保護** 行政事務従事者が払い出した一般利用者の主体認証情報は、信頼された安全な方法により一般利用者に配付される。 また一般利用者は、自身に配付された主体認証情報を、他者に漏らさないように適切に管理する。

1.4. 脅威

Web システムの運用環境において想定される脅威を表 1-11 に示す。

【注釈】保護すべき情報資産に対してリスクが発生し、セキュリティ対策を講じることが求められる脅威を漏れなく抽出する必要がある。セキュリティ要求仕様を提示するタイミング（システムの基本設計前、システム詳細設計前、システム運用前、システム更新前等）により、脅威識別の抽象度や、ここで示すべき脅威の範囲が異なる場合もある。一般的に、類似システム（業務機能、システムアーキテクチャ、システム構成等の類似性に基づく。）にて既に検討された脅威セットや、モデルシステムとして検討された脅威セット等を参考とし、当該システムの保護の観点と前提条件を踏まえて脅威の洗い出しを行い、脅威事象の設定・記述を行う。また政府機関統一基準の「4.2 情報セキュリティについての脅威」等、政府機関統一基準の指標が適用される場合は、当基準が想定している脅威事象を明示するよう脅威識別を検討する。

表 1-11 想定する脅威の一覧

識別子	脅威分類	脅威タイトル / 内容
脅威-1	情報漏えい、改ざん	**インターネット上における機密情報の盗聴、改ざん** インターネット上の攻撃者が､ネットワーク上を流れる通信データを盗聴又は改ざんすることにより、保護すべき情報資産が漏えい又は改ざんされる。

【注釈】インターネット等の不特定多数の利用者が存在するネットワークにおいては、ネットワーク上を送受信される情報の機密性、完全性、可用性が損なわれる可能性がある。
この例では、登録済み利用者情報等の要保護情報をインターネットを介して送受信する際に、要保護情報の盗聴、改ざんが発生することを想定している。

識別子	脅威分類	脅威タイトル / 内容
脅威-2	情報漏えい、改ざん	**不正プログラムの感染** コンピュータウイルス等の不正プログラムが Web システムに感染し、保護すべき情報資産を漏えいさせ、又は改ざん、破壊する。

【注釈】 政府機関統一基準解説書「4.2.2 不正プログラム対策」においては、脅威について「不正プログラムは、これに感染した情報システム及びデータを破壊することから完全性、可用性に対する脅威となるだけでなく､主体認証情報等の秘密情報や業務上の機密情報を漏えいさせることから機密性に対する脅威ともなる。」と記述している。
この例では、Web システムに関わるサーバが不正プログラムに感染し、サーバ内に保存されている保護すべき情報資産の漏えい、改ざん、破壊が発生することを想定している。

識別子	脅威分類	脅威タイトル / 内容
脅威-3	不正侵入	**リモートアクセスによる不正侵入** インターネット上の攻撃者が、Web システムのセキュリティホールを利用して不正侵入し、保護すべき情報資産を侵害する。

【注釈】政府機関統一基準解説書「4.2.1 セキュリティホール対策」においては、脅威について「セキュリティホールは、情報システムを構成する電子計算機及び通信回線装置上で利用しているソフトウェアに存在する可能性があり、そのセキュリティホールを攻撃者に悪用されることにより、サーバ装置への不正侵入、サービス不能攻撃、ウイルス感染等の脅威の発生原因になる等、情報システム全体のセキュリティの大きな脅威となる。」と記述している。
この例では、攻撃者が Web システムに関わるサーバ及び通信回線装置のソフトウェアに存在するセキュリティホールを利用してサーバ・通信回線装置に侵入し、サーバ・通信回線装置内に保存されている保護すべき情報資産の漏えい、改ざん、破壊が発生することを想定している。

識別子	脅威分類	脅威タイトル / 内容
脅威-4	不正利用	**一般利用者による不正利用** 一般利用者が、利用が許可されているサービスを利用し、Web システム上の保護すべき情報資産に対して、自身に権限のない操作を行う。

【注釈】Web システムにおいては、一般利用者に与えられている権限は、表 1.4 に示すとおり、府省庁が提供するコンテンツ（登録済み利用者である場合は登録済み利用者限定コンテンツも含む。）を参照する権限、及び自身の登録済み利用者情報を参照、変更する権限である。
この例では、一般利用者が、上記に示した自身に与えられた権限を逸脱した行為（例えば、コンテンツの変更や、自身以外の登録済み利用者情報の参照、変更等。）を実施することを想定している。

識別子	脅威分類	脅威タイトル / 内容
脅威-5	なりすまし	**正規利用者へのなりすまし** インターネット上の攻撃者が、登録済み利用者やコンテンツ保守業者、行政事務従事者に成りすまして Web システムにアクセスし、保護すべき情報資産を侵害する。

【注釈】政府機関統一基準解説書「6.1.3 ソフトウェア開発」の（3）においては、脅威について「開発するソフトウェアの機能、ネットワークの接続状況等から、不正侵入、DoS 攻撃、なりすまし等の脅威を分析する必要がある。」と記述している。

この例では、Web システムはインターネットを利用できる誰もが Web システムに接続できることから、攻撃者が登録済み利用者やコンテンツ保守業者、行政事務従事者になりすまして Web システムに接続することを想定している。なお、情報システムセキュリティ管理者及び運用担当者については、「接続前提-2」に示すとおり、情報システムセキュリティ管理者及び運用担当者はサーバ・通信回線装置のコンソールのみを利用して Web システムに接続するため、インターネットから攻撃者が情報システムセキュリティ管理者または運用担当者になりすまして Web システムに接続することはない。

攻撃者が登録済み利用者になりすました場合、登録済み利用者限定コンテンツの漏えいや、登録済み利用者情報の漏えい、改ざん、消去等の被害が発生することが想定される。

攻撃者がコンテンツ保守業者になりすました場合、コンテンツの改ざんや削除が発生することが想定される。

攻撃者が行政事務従事者になりすました場合、登録済み利用者限定コンテンツの漏えいが発生することが想定される。

識別子	脅威分類	脅威タイトル / 内容
脅威-6	なりすまし	**正規サーバへのなりすまし** インターネット上の攻撃者が、Web システムの正規のサーバになりすました偽のサーバを設置し、一般利用者から個人情報等の機密情報を取得する。

【注釈】政府機関統一基準解説書「6.1.3 ソフトウェア開発」の（3）においては、脅威について「開発するソフトウェアの機能、ネットワークの接続状況等から、不正侵入、DoS 攻撃、なりすまし等の脅威を分析する必要がある。」とある。

Web のインタフェースは標準的な HTML を用いて記述されるため、攻撃者が酷似した画面を作成することは比較的容易である。また Web サーバへの接続は主にドメイン名を用いて行われるため、攻撃者が紛らわしい名前を使用することも想定される。よってこの例では、攻撃者が正規の Web サーバに酷似した画面や名前を利用した偽のサーバを設置した場合、一般利用者は正規サーバと間違えて偽のサーバに接続し、自身の個人情報等を偽サーバに送信してしまうことを想定している。

識別子	脅威分類	脅威タイトル / 内容
脅威-7	DoS	**サービス不能攻撃** インターネット上の攻撃者が、サービス不能攻撃を行うことにより、Web システムの可用性が損なわれる。

【注釈】政府機関統一基準解説書「4.2.3 サービス不能攻撃」においては、脅威について「インターネットを経由して外部に提供しているサービスを実現する電子計算機、並びにそのアクセスに利用される通信回線及び通信回線装置は、利用者が自由にアクセス可能である利便性を確保するために、サービス不能攻撃により、通常の利用者がサービスを利用できなくなるといった可用性に対するリスクがある。」と記述している。

識別子	脅威分類	脅威タイトル / 内容
脅威-8	不正操作、 誤操作	**運用担当者及びコンテンツ保守業者の不正操作／誤操作** 運用担当者又はコンテンツ保守業者が、不正な操作又は誤った操作を実施することにより、Web システム内の保護すべき情報資産が侵害される。

【注釈】この例では、運用担当者がデータセンター等で各機器の監視等をする際に、故意にあるいは誤ってサーバ内に保存されている保護すべき資産を変更・削除したり、不正に持ち出したりする脅威や、コンテンツ保守業者が行政事務従事者の依頼を受けてコンテンツを更新する際に、故意にあるいは誤って別のコンテンツを変更・削除したり、本来公開すべきでないコンテンツを公開してしまったりする脅威を想定している。

一般利用者が不正操作及び誤操作により保護すべき情報資産を侵害する可能性は、自身の登録済み利用者情報を故意にあるいは誤って変更または削除することが想定される。しかし、故意に自身の情報を変更または削除する利点は Web システムでは想定されない。また、誤って修正した自身の情報は、再度、正しい内容に修正することが可能であり、また完全に削除してしまった場合であっても再度登録を申請すればよい。よって、この例では、一般利用者の不正操作及び誤操作による保護すべき情報資産の侵害は脅威として含めていない。

2. セキュリティ提案仕様の審査ポイント

本章では、Web システムに関するセキュリティ要求仕様を受けて策定したセキュリティ提案仕様を審査する際の要点を示す。なお、その前提として、調達者は、提案者に対して、セキュリティ提案仕様に①「システム概要」、②「保護すべき情報資産」、③「前提条件」、④「脅威」、⑤「情報セキュリティ対策」及び⑥「セキュリティ機能を実現する IT 機器」の各項目を記載することを求める必要がある。

このうち⑤の「情報セキュリティ対策」の審査ポイントについては、本章の「2.1 情報セキュリティ対策」で解説する。また、⑥の「セキュリティ機能を実現する IT 機器」の審査ポイントについては、本章の「2.2 認証製品の適用」及び本文の「3.3 セキュリティ機能を実現する機器等の審査」を参照されたい。

一方、セキュリティ提案仕様の①の「システム概要」は、セキュリティ要求仕様にある記述を転記するものであることから、審査の対象とする必要はない。また、②の「保護すべき情報資産」、③の「前提条件」及び④の「脅威」は、セキュリティ要求仕様の記述を転記していれば審査の対象とする必要はないが、当該記述を基本としつつ、提案者が変更等を提案する場合もある。その場合における審査ポイントについては、本文の「3.1 『保護すべき情報資産』、『前提条件』及び『脅威』の審査」を参照されたい。

このほか、セキュリティ提案仕様に「制約条件」が記述されている場合もあり、その場合の審査の観点については、本文の「3.4 制約条件の審査」を参照されたい。

2.1. 情報セキュリティ対策

本節では、Web システムの運用環境において想定される脅威に対抗するために、提案者が提案すると想定される情報セキュリティ対策の例を示すとともに、調達者が情報セキュリティ対策を審査する際のポイントをそれぞれの注釈に示す。

【注釈】調達者は、以下に示す情報セキュリティ対策が、1.4 節で列挙した脅威への対策として有効であるか、あるいは 1.3 節で列挙した前提条件を満たすことが可能であるか、という視点で審査する。なお、各セキュリティ対策と、脅威及び前提条件との対応については、2.1.5 節に示されている。

2.1.1. 技術的セキュリティ対策

Web システムにおける技術的セキュリティ対策の提案例を以下に示す。

技術対策-1	**主体認証** Web システムでは、各ユーザに対して以下の場合に識別コード（ID）と主体認証情報（パスワード）を用いた主体認証を行う。 • 行政事務従事者、情報システムセキュリティ管理者、運用担当者及びコンテンツ保守業者に対して、Web システムにアクセスする場合に、主体認証を行う。 • 一般利用者に対して、登録済み利用者限定コンテンツを閲覧する場合に、主体認証を行う。 また Web システムでは、主体認証情報（パスワード）を通信又は保存する際に、その内容を暗号化又はハッシュ化する。

【注釈】本対策は、政府機関統一基準の「4.1.1 主体認証機能」に相当し、各ユーザの識別と認証を実施することで、Web システムのユーザを許可されたユーザのみに限定し、不正なユーザによるシステムの利用を防止することを目的とする。Web システムでは、脅威-3,4,5 に対抗することを想定している。さらに、主体認証情報が露呈すると第三者によるなりすましが容易に可能となるため、主体認証情報は第三者に露呈しないよう暗号化またはハッシュ化により保護することが必要である。
また本対策が選択された場合には、2.1.3 節の運用対策-4 もあわせて検討する必要がある。
なお、この例では、主体認証の実現手段として ID とパスワードを選択しているが、これ以外にも生体情報、電子証明書、IC カード等が実現手段として選択されていても良い。

技術対策-2	**サーバの識別と認証** Web システムでは、一般利用者が登録済み利用者限定コンテンツを閲覧する際に、SSL/TLS によりサーバの識別と認証を行う手段を提供する。

【注釈】本対策は、政府機関統一基準の「5.3.3 ウェブ」に相当し、サーバの識別と認証を実施することで、一般利用者にサーバの正当性を確認する手段を提供し、第三者による Web システムへのなりすましを防止することを目的とする。Web システムでは、脅威-6 に対抗することを想定している。
なお、この例では、サーバの識別と認証の実現手段として SSL/TLS を選択しているが、これと同等レベル以上の識別と認証を実現する手段であれば SSL/TLS 以外でも良い。
また、本対策で使用するサーバ証明書として府省認証局が発行した証明書を適用する場合は、その府省認証局のルート証明書を一般利用者端末に安全にインストールするための手段を検討する必要がある。

技術対策-3	**アクセス制御** Web システムでは、各ユーザに対して、各ユーザの権限に基づいた以下のようなアクセス制御を行う。 • ファイアウォールによるアクセス制御 • OS のファイルシステムによるアクセス制御 • データベースによるアクセス制御 • Web サーバによるアクセス制御 • アプリケーションによるアクセス制御

【注釈】本対策は、政府機関統一基準の「4.1.2 アクセス制御機能」に相当し、各ユーザの権限に基づいたアクセス制御を行うことで、保護すべき情報資産に対して、許可されたユーザによる許可された操作のみが実施可能とされることを目的とする。Web システムでは、脅威-3,4,5 に対抗すること及び接続前提-1,2 を達成することを想定している。
なお、この例では、ファイアウォール、OS のファイルシステム、データベース、Web サーバ、アプリケーションの 5 箇所でのアクセス制御を選択しているが、最低限ファイアウォールとデータベースは選択されている必要がある。

技術対策-4	**証跡管理（証跡の取得）** Web システムでは、主体認証の失敗、暗号化の失敗等のセキュリティ機能の動作結果に関する証跡やユーザの操作に関する証跡を取得する。 また、取得した証跡に対しては、適切にアクセス制御を実施する。

【注釈】本対策は、政府機関統一基準の「4.1.4 証跡管理機能」に相当し、セキュリティ機能に関する証跡やユーザの操作に関する証跡を取得することで、保護すべき情報資産に対する侵害や、ユーザの不正操作及び誤操作の痕跡を発見することを目的とする。Web システムでは、脅威-3,4,5,7,8 に対抗することを想定している。さらに、取得した証跡が改ざんまたは削除されると上記の痕跡を発見することが困難となるため、証跡はアクセス制御等により保護することが必要である。
また本対策が選択された場合には、2.1.3 節の運用対策-5 もあわせて検討する必要がある。

技術対策-5	**通信の暗号化** Web システムでは、下記の場合に SSL/TLS による通信の暗号化を行う。 • 一般利用者による登録済み利用者限定コンテンツ閲覧時 • 行政事務従事者による Web システムへのアクセス時 • コンテンツ保守業者による Web システムへのアクセス時

【注釈】本対策は、政府機関統一基準の「4.1.6 暗号と電子署名（鍵管理を含む）」、「5.3.3 ウェブ」及び「5.4.1 通信回線共通対策」）に関係し、通信を暗号化することで、第三者による一般利用者の個人情報や主体認証情報等の要機密情報の盗聴及び改ざんを防止することを目的とする。Web システムでは、脅威-1 に対抗することを想定している。また、通信の暗復号に用いる暗号鍵が漏えいすると第三者による盗聴が容易に可能となるため、暗号鍵は第三者に漏えいしないよう適切に保護する必要がある。

なお、この例では、脅威-1 に対する対策として通信の暗号化を選択しているが、特に行政事務従事者やコンテンツ保守業者と Web システム間の通信路には、専用線や IP-VPN 等の信頼できる通信路を利用する、という対策が選択されていても良い。

また、通信の暗号化の実現手段としては SSL/TLS を選択しているが、これ以外にもサーバ及びクライアント端末上における情報の暗号化/復号等が実現手段として選択されていても良い。

技術対策-6	**不正プログラム対策（アンチウイルスソフトウェアの導入）** Web システムでは、Web サーバ及びデータベースサーバに対し、アンチウイルスソフトウェアを導入する。

【注釈】本対策は、政府機関統一基準の「4.2.2 不正プログラム対策」に相当し、アンチウイルスソフトウェアをサーバ機器に導入することで、Web システムの不正プログラムへの感染を防止することを目的とする。Web システムでは、脅威-2 に対抗することを想定している。

また、本対策が選択された場合には、本参考例 2.1.3 項の運用対策-6 もあわせて検討する必要がある。

技術対策-7	**不正アクセスの監視** Web システムでは、不正侵入監視装置を用いて通信データの監視を行う。 また、不正アクセスの兆候を検知した際には情報システムセキュリティ管理者及び運用担当者に対して通知する。

【注釈】本対策は、不正侵入監視装置を用いて Web システムで発生する通信データの監視及び不正アクセス検知の通知を行うことで、ファイアウォールでは防ぎ切れない第三者及びユーザによる不正アクセスの検知を目的とする。Web システムでは、脅威-3,7 に対抗することを想定している。
また、本対策が選択された場合には、本参考例 2.1.3 項の運用対策-7 もあわせて検討する必要がある。
なお、この例では、不正アクセスの監視の実現手段として不正侵入監視装置を選択しているが、証跡管理のみが実現手段として選択されていても良い。業務要件や費用等を考慮した実現方法が選択されることが望ましい。

技術対策-8	**改ざん検知** Web システムでは、改ざん検知製品を用いて特にその完全性が求められる情報資産（一般公開コンテンツ等）に対する改ざんを監視する。

【注釈】本対策は、改ざん検知製品を用いて特に完全性が求められる情報資産に対して、その情報資産の改ざんの有無を監視することで、第三者及びユーザによる不正な改ざんを検知することを目的とする。Web システムでは、脅威-2,3,4,5,8 に対抗することを想定している。
なお、この例では、改ざん検知の実現手段として改ざん検知製品の導入を選択しているが、証跡管理のみが実現手段として選択されていても良い。業務要件や費用等を考慮した実現方法が選択されることが望ましい。

2.1.2. 物理的セキュリティ対策

Web システムにおける物理的セキュリティ対策の提案例を以下に示す。

物理対策-1	**セキュリティ区画における安全区域遵守事項の実現** Web システムが設置されるデータセンター等及びバックアップメディアを保管する施設において、その場所ごとに、重要度に応じた情報セキュリティ対策（入退室管理、施錠管理、監視（監視カメラ）等）を施す。

【注釈】本対策は、政府機関統一基準の「5.1.1 電子計算機及び通信回線装置を設置する安全区域」に相当し、Web システムを構成する機器が設置される区域への入退室を許可されたユーザのみに制限することで、第三者による機器への物理的なアクセスを防止することを目的とする。Web システムでは、前提条件-1 を達成することを想定している。

2.1.3. 運用に関するセキュリティ対策

Web システムにおける運用に関するセキュリティ対策の提案例を以下に示す。

運用対策-1	**行政事務従事者及び情報システムセキュリティ管理者の信頼性** 行政事務従事者及び情報システムセキュリティ管理者が自身に課せられた役割に対する許可された一連の行為に関し、悪意を持った行為は行わないことを保証するために、情報システムセキュリティ責任者は適切な人選を行い、管理及び教育を実施する。

【注釈】本対策は、政府機関統一基準の「2.2.1 情報セキュリティ対策の教育」に相当し、行政事務従事者及び情報システムセキュリティ管理者の管理、教育を行うことで、ユーザの不正行為を抑止することを目的とする。Web システムでは、人的前提-1 を達成することを想定している。

運用対策-2	**一般利用者の主体認証情報保護** 行政事務従事者は、一般利用者に主体認証情報を配付する際には信頼できる配達業者に主体認証情報を安全に郵送するよう依頼する。また、一般利用者に対して、自身の主体認証情報を他者に漏らさずに管理すべき旨を通知する。

【注釈】本対策は、Web システム外における一般利用者の主体認証情報の漏えいを防止することで、本参考例 2.1.1 項の技術対策-1 の信頼性を補完することを目的とする。Web システムでは、人的前提-2 を達成することを想定している。
なお、この例では主体認証情報の安全な配付に、信頼できる配達業者による郵送を選択しているが、一般利用者に安全に配付できる方法であればこの方法以外でもよい。

運用対策-3	**バックアップ／リストア** 情報システムセキュリティ管理者又は運用担当者は、保護すべき情報資産のバックアップを定期的に行う。また、保護すべき情報資産が侵害された際には、侵害される前の状態に復元させる。 さらに、バックアップを取得した媒体は安全に管理する。

【注釈】本対策は、政府機関統一基準の「4.1.5 保証のための機能」及び「5.2.3 サーバ装置」に関係し、不正アクセスまたはユーザの不正操作・誤操作等により保護すべき情報資産が改ざん・削除された場合にも、当該資産を前回のバックアップ時点に復元させることを目的とする。Web システムでは、脅威-2,3,4,5,8 に対抗することを想定している。また、適切に情報資産を復元させるために、バックアップ媒体は安全に管理する必要がある。さらに、バックアップ取得対象の情報資産が要機密情報である場合は、当該資産を暗号化してバックアップ媒体に保存することも検討する必要がある。

運用対策-4	**権限管理** 情報システムセキュリティ管理者は、主体認証及びアクセス制御に関する情報（主体認証情報、アクセス制御リスト等）を適切に管理する。

【注釈】本対策は、政府機関統一基準の「4.1.3 権限管理機能」に相当し、主体認証及びアクセス制御に関する情報の管理を行うことで、本参考例 2.1.1 項の技術対策-1,3 の信頼性を補完することを目的とする。Web システムでは、脅威-3,4,5 に対抗することを想定している。

運用対策-5	**証跡管理（証跡の監査）** 情報システムセキュリティ管理者又は運用担当者は、本参考例 2.1.1 項の技術対策-4 で取得した証跡の監査を行う。

【注釈】本対策は、政府機関統一基準の「4.1.4 証跡管理機能」に相当し、セキュリティ機能に関する証跡やユーザの操作に関する証跡を監査することで、本参考例 2.1.1 項の技術対策-4 の信頼性を補完することを目的とする。Web システムでは、脅威-3,4,5,7,8 に対抗することを想定している。

運用対策-6	**アンチウイルスソフトウェアの管理** 情報システムセキュリティ管理者又は運用担当者は、各サーバ機器に導入したアンチウイルスソフトウェアの不正プログラム定義ファイルを常に最新の状態に保ち、常時または定期的に不正プログラムの検査を行う。

【注釈】本対策は、政府機関統一基準の「4.2.2 不正プログラム対策）に相当し、アンチウイルスソフトウェアの不正プログラム定義ファイルの最新化、及び不正プログラムの検査を実施することで、本参考例 2.1.1 項の技術対策-6 の信頼性を補完することを目的とする。Web システムでは、脅威-2 に対抗することを想定している。

運用対策-7	**不正侵入監視装置の管理** 情報システムセキュリティ管理者または運用担当者は、本参考例 2.1.1 項の技術対策-7 で導入した不正侵入監視装置の定義ファイルを常に最新の状態に保つ。

【注釈】本対策は、不正侵入監視装置の定義ファイルを常に最新の状態に保つことで、本参考例 2.1.1 項の技術対策-7 の信頼性を補完することを目的とする。Web システムでは、脅威-3,7 に対抗することを想定している。

運用対策-8	**セキュリティホール対策** 情報システムセキュリティ管理者又は運用担当者は、Web システムを構成するすべての機器のセキュリティホールに関する最新の情報を収集する。また、Web システムを構成する機器にセキュリティホールが発見された場合には、セキュリティパッチの適用等の適切な対策を行う。 さらに、Web システムが稼動する前には不要なサービスやアカウントの無効化等を行う。

【注釈】本対策は、政府機関統一基準の「4.2.1 セキュリティホール対策」、「5.2.3 サーバ装置」及び「5.3.3 ウェブ」に相当し、例えば、以下のような対策を行うことで、第三者による不正侵入の防止を目的とする。

- セキュリティパッチを適用する
- 不要なサービスを無効化する
- 不要なアカウントを無効化する
- 入力文字列内の特殊文字を無害化する
- 必要以上の情報を一般利用者に送信しない

Web システムでは、脅威-3 に対抗することを想定している。

運用対策-9	**システムの動作監視** 情報システムセキュリティ管理者又は運用担当者は、要安定情報を保存しているサーバ機器に対して、システムの動作監視を行う。

【注釈】本対策は、政府機関統一基準の「4.2.3 サービス不能攻撃対策」及び「5.2.3 サーバ装置」に関係し、要安定情報を保存しているサーバ機器に対してシステムの動作監視を行うことで、要安定情報を侵害する可能性のあるサービス不能攻撃を発見することを目的とする。Web システムでは、脅威-7 に対抗することを想定している。

運用対策-10	**運用担当者の教育・訓練** 運用担当者が自身に課せられた役割に対する許可された一連の行為に関し、悪意を持った行為または誤った行為を行った際にはすぐ対応できるように、情報システムセキュリティ管理者は運用担当者に対して Web システムの管理を適切かつ厳格に実施するための知識とスキルを持つよう教育・訓練する。また、運用担当者の作業内容を適宜確認する。

【注釈】本対策は、運用担当者に対して教育・訓練を行うことによる運用担当者の不正操作・誤操作の抑止及び作業内容の確認による不正操作・誤操作の検知を目的とする。Web システムでは、脅威-8 に対抗することを想定している。

運用対策-11	**コンテンツ保守業者の作業確認** コンテンツ保守業者が自身に課せられた役割に対する許可された一連の行為に関し、悪意を持った行為または誤った行為を行った際にはすぐ対応できるように、行政事務従事者はコンテンツ保守業者に対して作業報告を行うことを義務付け、適宜その作業確認を行う。

【注釈】本対策は、コンテンツ保守業者の作業確認を行うことで、コンテンツ保守業者の不正操作の抑止、及び不正操作・誤操作の検知を目的とする。Web システムでは、脅威-8 に対抗することを想定している。

2.1.4. 保証に関するセキュリティ対策

Web システムにおける保証に関するセキュリティ対策の提案例を以下に示す。

保証対策-1	**評価・認証を受けた製品等の利用の検討** 製品を導入する場合には、政府機関統一基準に基づき、情報セキュリティに関する評価・認証を受けた製品等の利用を検討する。なお、ハードウェア構成、ソフトウェア構成にてセキュリティを確保する上で重要とした製品等については、システム仕様を満たし、かつ評価・認証を受けた製品の有無を調査する。本参考例 2.2 節に関連する事項がある。

【注釈】本対策は、政府機関統一基準の「4.3.1 情報システムのセキュリティ要件」及び「6.1.1 機器等の導入」に関係し、評価・認証を受けた製品等を利用することで、セキュリティレベルを向上させることを目的とする。

2.1.5. 脅威、前提条件とセキュリティ対策の対応

脅威、前提条件とセキュリティ対策の対応関係を以下に示す。

識別子	脅威	前提条件	政府機関統一基準との対応
技術対策-1	脅威-3,4,5	―	統 4.1.1(1)(b)-(h)
技術対策-2	脅威-6	―	統 5.3.3(1)(e)
技術対策-3	脅威-3,4,5	接続前提-1,2	統 4.1.2(1)(b)
技術対策-4	脅威-3,4,5,7,8	―	統 4.1.4(1)(b)-(e)
技術対策-5	脅威-1	―	統 4.1.6(2)、 5.3.3(1)(c)、5.4.1(1)(f)
技術対策-6	脅威-2	―	統 4.2.2(1)(b)
技術対策-7	脅威-3,7	―	―
技術対策-8	脅威-2,3,4,5,8	―	―
物理対策-1	―	物理前提-1	統 5.1.1(1)(a)
運用対策-1	脅威-8	人的前提-1	統 2.2.1(1)(a)-(i),(2)(a)-(d)
運用対策-2	―	人的前提-2	―
運用対策-3	脅威-2,3,4,5,8	―	統 4.1.5(1)(b)、5.2.3(2)(b)
運用対策-4	脅威-3,4,5	接続前提-1,2	統 4.1.3(1)(b)
運用対策-5	脅威-3,4,5,7,8	―	統 4.1.4(3)(a)
運用対策-6	脅威-2	―	統 4.2.2(2)(a)-(h)
運用対策-7	脅威-3,7	―	―
運用対策-8	脅威-3	―	統 4.2.1(1)(a)-(b),(2)(a)-(h)、 5.2.3(1)(b)-(d)、 5.3.3(1)(a)-(b)
運用対策-9	脅威-7	―	統 4.2.3(1)(a)-(g),(2)(a), 5.2.3(2)(f)
運用対策-10	脅威-8	―	―
運用対策-11	脅威-8	―	―

【注釈】ここでは、すべての技術対策、物理対策、運用対策が、一つ以上の脅威及び前提条件に対応していることを確認する。
また、それぞれの対応が妥当であるか否かについて検討する。

2.2. 認証製品の適用

調達者は、セキュリティ要求仕様において、情報システム等を構成する特定の機器等について、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否かを提案の評価の要素に加えるものとする場合がある。この場合には、セキュリティ提案仕様の「セキュリティ機能を実現する機器等」において提案されている認証製品とその認証の内容を、セキュリティ要求仕様に照らして審査する。審査における留意点については、本文の「3.3 セキュリティ機能を実現する機器等の審査」及び「付録 C　IT セキュリティ評価及び認証制度を活用した機器等の購入について」を参照されたい。

Web システムにおいては、本参考例 2.1.1 項の技術的セキュリティ対策のうち、アクセス制御、アンチウイルス対策、不正アクセスの監視、改ざん検知を実現するために必要なセキュリティ機能について認証取得製品の適用を評価の要素に加えることとすることも考えられる。

参考例II

インターネットサービスシステム

ここでは、一般的なインターネットサービスシステムを例に、調達者が作成するセキュリティ要求仕様の例と、セキュリティ提案仕様を調達者が審査する際のポイントを示す。

読者は、本参考例を参照するに当たり、一般的なインターネットサービスシステムのモデルを示していることに留意すること。

実際の調達に当たっては、それぞれの情報システムにより保護すべき情報資産、前提条件、脅威及び求める情報セキュリティ水準等が異なることに留意し、本付録に示すセキュリティ要求仕様及びセキュリティ提案仕様の審査ポイントに対して適切に追加、変更等を加えて利用すること。

1. セキュリティ要求仕様

本章では、一般的なインターネットに接続して利用するシステムを汎用例として取上げ、実装と運用の両面からインターネットサービスシステムとして考慮すべき情報セキュリティ上の要件を整理し、セキュリティ要求仕様の記述例を示す。

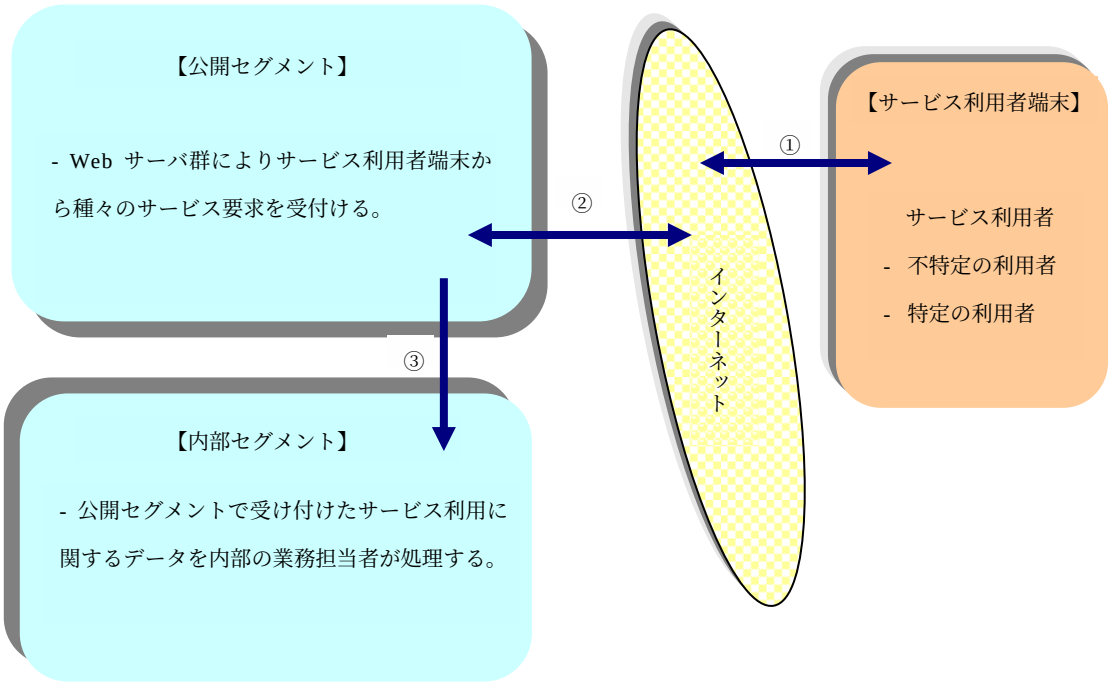
1.1. システム概要

【注釈】 システム概要では、インターネットに接続した利用者に対して、コンテンツの閲覧、電子申請・届出、メールマガジン登録等のサービスを提供する業務システムの概要を記述する。

1.1.1. システム全体概要

インターネットに接続する代表的なシステムは、その情報システムが提供するサービスに対してインターネット上の利用者から直接的にアクセスを受ける公開セグメント及び間接的にアクセスを受ける内部セグメントから構成される。また、公開セグメントは、インターネット上に存在する不特定多数の利用者へサービスを提供する場合及びインターネット上に存在する特定の利用者へサービスを提供する場合に分類される。

ここでは、インターネット上に存在する不特定多数の利用者に向けたサービスの窓口となる公開セグメント及び間接的にサービスの利用者から送られる多様なデータを内部セグメントにおいてサービス業務を担うシステム関係者が処理するという一般的なモデルを取上げる。



① インターネットに接続している利用者がサービス（コンテンツの閲覧、電子申請・届出、メールマガジン登録等）を要求する。
② インターネット上に存在する利用者からサービスの要求を受付ける。
③ 内部のサービス業務を担う担当者が利用者からの要求を受付け、DB サーバへの情報登録等サービスに関する業務を行う。

図 1.1.1 インターネットサービスシステムの全体イメージ

1.1.2. システム構成

Web アプリケーションを軸としたインターネットサービスシステムにおいて、２つのセグメントを定義する。

- **公開セグメント**
- **内部セグメント**

1.1.2.1. システム構成概要

本情報システムは、サービス利用者の個人情報の取扱い及び情報システムの可用性に配慮したシステム構成が必要不可欠である。以下に、一般的なシステム構成例を示す。

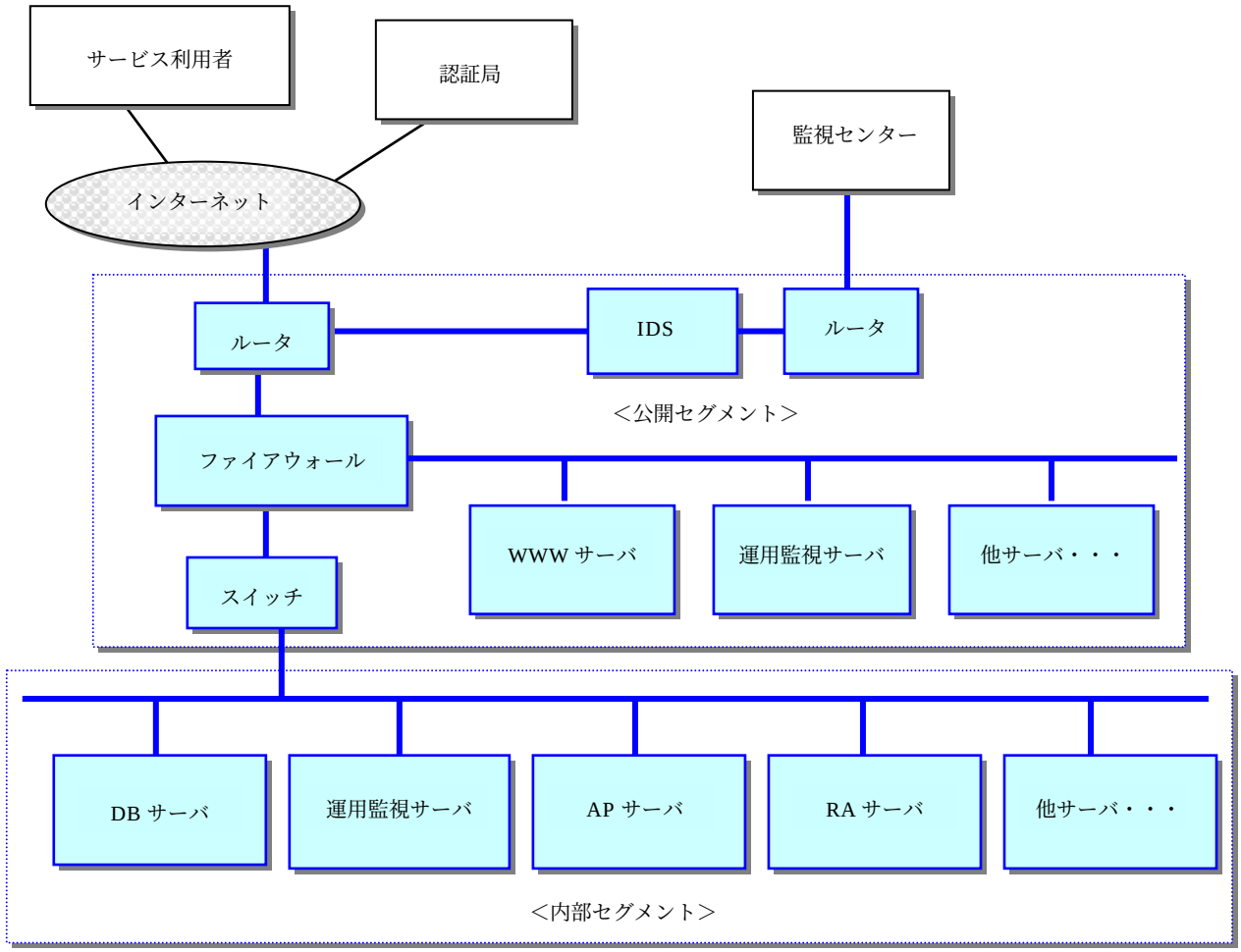


図 1.1.2 システム構成例

1.1.2.2. ハードウェア機器構成例

システムのハードウェア機器構成例を以下に示す。

表 1.1.1 ハードウェア機器構成例

セグメント	ハードウェア機器	機能概要
公開セグメント	ファイアウォール	ネットワーク通信データに対して、IP アドレスやサービスポート等の属性情報によりフィルタリングを行い、不正侵入や攻撃を防止する機能を提供する。また、アドレス変換やアプリケーションゲートウェイの機能を提供する。
	ルータ、スイッチ	インテリジェント型のハブ機能を提供し、ネットワーク通信データのルーティングやフィルタリングを行う。
	IDS	攻撃内容を自動解析する侵入検知システムであり、ネットワークやサーバへの不正なアクセスを検出する。
	WWW サーバ	インターネットを介してサービス利用者に対してコンテンツ情報の閲覧や各種サービス機能を提供する。
	外部運用監視サーバ	公開セグメントに設置された機器の稼働状況に関する監視を行う。
	他サーバ	他サーバ設置時、他サーバの機能概要。
内部セグメント	DB サーバ	サービス利用者の情報、本情報システムの運用に必要な情報等を管理する。
	AP サーバ	本情報システムが提供する利用者向けと業務向けの各種サービス機能を提供するアプリケーションプログラムを稼働させる。
	RA サーバ	認証局（CA）と連携して、証明書の発行や失効申請を審査する等、サービス利用者と CA の間で証明書の管理を行う機能を提供する。
	内部運用監視サーバ	内部セグメントに設置された機器の稼働状況に関する監視を行う。
	他サーバ	他サーバ設置時、他サーバの機能概要。

1.1.2.3. 外部システム連携方法

本システムが連携する外部システムの概要を下表に示す。

表 1.1.2 外部連携システム

外部システム	システム連携概要
監視センター	本情報システムと安全な通信回線で接続される端末装置が設置されるセンターであり、インターネットと本情報システム間で送受信されるパケットの監視を実施する。
認証局	サービス利用者に対し、公開鍵証明書、 CRL、相互認証証明書、自身の公開鍵証明書（CA 証明書）等の発行管理を行う。

1.1.3. システム機能概要

本情報システムが提供するサービス利用者向け機能及びサービス提供者向け機能について概要を示す。また、本情報システムとして実装が必要であると考えられる最低限のセキュリティ機能に関する概要を併せて示す。

1.1.3.1. サービス利用者と運用関係者向け機能

表 1.1.3 主なサービス機能

アプリケーション分類	主なサービス機能	サービス機能の内容
サービス利用者向け機能（不特定の利用者向け）	サービス紹介サービス	種々のインターネットサービスシステムに応じたサービス利用者向け機能
	行政情報提供サービス	
	法令情報提供サービス	
	各種ドキュメントのダウンロードサービス	
	メールマガジン登録サービス	
	他サービス機能	
サービス利用者向け機能（特定の利用者向け）	特定の利用者向けコンテンツ閲覧サービス	種々のインターネットサービスシステムに応じたサービス利用者向け機能
	電子申請・届出サービス	
	他サービス機能	
運用関係者向け機能	利用者管理機能	種々のインターネットサービスシステムに応じた運用管理系機能
	セション管理機能	
	各種業務機能	
	運用管理機能	
	監視機能	
	他サービス機能	

1.1.4. システムにおける想定ユーザ

本情報システムが想定するユーザ（本情報システムの関連者）の分類ごとに、その役割と権限を示す。

【注釈】 システムの運用時に必要な情報セキュリティ対策を検討する際には、セキュリティ要求仕様においてそのシステムが誰によりどのように利用・管理されるのかを具体的に示す必要がある。ここでは、システムの主な関係者の分類を行い、それぞれの役割と権限の概要を例示している。システムの内部における運用仕様、及び、外部に対するサービス仕様に応じて、関係者の役割と権限を具体化する必要がある。

表 1.1.4 本情報システムの想定ユーザ

関係者分類	関係者名称	役割・権限の説明	
運営責任者	運営責任者	役割	本システムの運営にかかわる責任者
		権限	運営に関する権限と責任
システム管理者	システム管理者	役割	本システムの管理を実施する者
		権限	管理と保守に関する権限と責任
保守管理者	保守担当者	役割	本システムの保守を実施する者
		権限	保守に関する権限と責任
運用者	運用担当者	役割	本システムの運用を実施する者
		権限	運用に関する権限と責任
業務担当者	業務担当者	役割	本システムが提供する業務サービスを利用して業務を実施する者
		権限	業務に関する権限と責任
利用者	サービス利用者	役割	インターネットを介して本システムが提供するサービスを利用する者
		権限	利用者向けのサービスを利用する権限
監視者	監視担当者	役割	本システムの監視にかかわる責任者
		権限	監視に関する権限と責任

1.2. 保護すべき情報資産

本情報システムが保護すべき情報資産を示す。機密性、完全性及び可用性の各観点から、一連のサービス業務で処理されるデータの中で、漏えい、改ざん及び破壊が発生すると行政事務の遂行等に悪影響が生ずると想定されるものを保護対象の情報資産としている。

【注釈】 以下に示す『一般的な保護すべき情報資産の考え方と分類』を理解の上、実際に調達の対象とする情報システムの保護すべき情報資産を記述する。

保護すべき情報資産の抽出は、セキュリティ上の脅威を分析し、対策を検討するための最も基礎となる重要な分析行為であり、慎重に抽出する必要がある。

～ **『一般的な保護すべき情報資産の考え方と分類』** ～

一般的に、保護すべき情報資産は、一次的な情報資産と二次的な情報資産に分類される。

一次的な情報資産とは、サービス利用者の個人情報や機密情報等の情報処理業務で直接に取り扱う、保護する必要がある情報資産であって、その情報資産が漏えい、改ざん、破壊等の被害を受けた場合に直接的な悪影響が発生するものをいう。一方、二次的な情報資産は、一次的な情報資産を保護するためのセキュリティ機能を実装する場合に、そのセキュリティ機能を実現するために必然的に設定が必要となる認証情報や、監査証跡情報等を指し、その情報資産が漏えい、改ざん、破壊等の被害を受けた場合には、間接的に一次的な情報資産への悪影響が発生する可能性がある。

したがって、一次的な情報資産のみを明示することで、セキュリティ機能を策定するプロセスにおいて必然的に二次的な情報資産を設定することになり、その二次的な情報資産に対する保護機構も実装することになることから、セキュリティ要求仕様において明示する保護すべき情報資産は一次的な情報資産に留めておくことが肝要である。二次的な情報資産までをセキュリティ要求仕様で明示する場合、提案者がセキュリティ対策、セキュリティ機能を策定する際に混乱をもたらす等の弊害を及ぼす可能性があることからも、セキュリティ提案仕様においては、二次的な情報資産は保護すべき情報資産として明示しないことが肝要である。

ただし、組織のセキュリティポリシーとして保護の対象として予め明示されている場合は、保護すべき情報資産としてセキュリティ要求仕様に明示することが必要である。例えば、監査証跡の記録や識別認証機能を前提とした認証情報等は組織のセキュリティポリシーとして明示されているケースが多く、調達者からの明確な要件事項として提案者に対して通知すべきである。一般的な保護すべき情報資産としては以下のような資産が挙げられる。

- 個人情報
- 情報システムの構成機器、情報システムのネットワーク
- 業務アプリケーション、データベース等のミドルウェア
- 証明書データ
- 情報システムの構成情報
- 監査情報　等

➢ 保護すべき情報資産の例

表 1.2.1 保護すべき情報資産の例

	保護すべき資産	保護の必要性	機密性	完全性	可用性	要保護
①	サービス利用に関するドキュメントデータ（個人情報）	インターネット上においてサービス利用者と本情報システム間で送受信されるサービス利用に関するドキュメントデータ及び本情報システム内に存在するサービス利用に関するドキュメントデータの漏えい、改ざんを防止しなければ、サービス利用者の個人情報を保護できない。	3	2	2	○
①	Web コンテンツデータ	本情報システム内に存在するＷｅｂコンテンツデータに対する改ざん、削除を防止しなければ、正常なサービスを提供できなくなり、社会的な信用を失墜する。	1	2	2	○
①	様式データ	本情報システム内に存在する様式データ及びインターネット上においてサービス利用者と本情報システム間で送受信される様式データに対する改ざんを防止しなければ、正常なサービスを提供できない。	1	2	2	○
②	秘密鍵データ	本情報システム内に存在する秘密鍵データに対する改ざん及び漏えいを防止しなければ、正常なサービスを提供できない。	3	2	2	○
②	システムの構成情報データ	本情報システム内に存在するシステムの構成情報データに対する改ざん、漏えいを防止しなければ、正常なサービスを提供できない。	3	2	2	○
②	証明書データ	本情報システム内に存在する証明書データに対する改ざん、漏えいを防止しなければ、正常なサービスを提供できない。	3	2	2	○
②	監査証跡	本情報システム内に存在する監査証跡記録に対する改ざん、削除、漏えいを防止しなければ、トラブルが発生した場合等の原因を追求できなくなる。	3	2	1	○

【注釈】 「表 1.2.1 保護すべき情報資産の例」では、一般的な観点から、一次的な情報資産を①として、二次的な情報資産を②として例示している。

1.3. 本システムの運用時の前提条件

本情報システムの運用時の前提条件について、物理的な設置環境、接続面（ネットワーク環境等）、人的環境の各側面から示す。

【注釈】 表 1.3.1 から表 1.3.3 において例示している前提条件には、省庁対策基準等に掲げていて当該システムにおける前提条件とすべき事項も含めることになる。ここでは、調達者として考慮している運用の条件や情報を正確に示すことで、提案者は技術的、物理的、運用的の各セキュリティ対策を分類して策定することができるようになる。特に、人的環境面に関しては、運用管理系の業務に携わる人物の信頼性をどのように定義するかで脅威や対策の考え方に大きな違いが生じることになるため注意が必要である。

1.3.1. 物理的な設置環境に関する前提条件

表 1.3.1 物理的な前提条件

No	前提条件のタイトル／前提条件の内容
物理前提-1	**本情報システムを構成する機器群を設置するデータセンター** 本情報システムを構成する情報処理機器、データ、プログラムは、許可された人物のみが入退室ができる場所に設置・保管し、他の情報システムが設置される区域と物理的に隔離されている。 また、本情報システムを構成する機器が設置される場所は、想定される災害に対して十分な耐震性と防火性を備え、更に、電力供給停止に備えた自家発電施設を備えている。

1.3.2. 接続面（ネットワーク環境等）に関する前提条件

表 1.3.2 接続面の前提条件

No	前提条件のタイトル／前提条件の内容
接続前提-1	**ネットワークセグメント間の通信の安全性** インターネットと本情報システムの間、及び、本情報システムと監視センターの間で送受信されるデータは、漏えい、改ざんを防御する対策を施した経路のみを通過する。
接続前提-2	**ネットワークセグメント間の接続** インターネットと本情報システムの間、及び、本情報システムと監視センターの間は、識別された特定箇所のみでネットワーク接続されている。
接続前提-3	**証明書の信頼性** 本情報システムにおいて使用する証明書は、信用できる機関から取得し、証明書自体も信用できる。また、本情報システムにおいて使用する証明書は、信用できる専用装置の管理下に置かれている。

1.3.3. 人的環境に関する前提条件

表 1.3.3 人的な前提条件

No	前提条件のタイトル／前提条件の内容
人的前提-1	**システム管理者の信頼性** 本情報システムに対してインターネットを介さずに操作ができるシステム管理者は、組織において信用できる人物であり、定められた規則を遵守し、不正を行わない人物である。
人的前提-2	**監視担当者の信頼性** 本情報システムを監視する監視担当者は、組織的において信用できる人物であり、定められた規則を遵守し、不正を行わない人物である。
人的前提-3	**監視センターの信頼性** 監視センターから本情報システムに対して行われる監視管理、及び、操作は信用できる。

1.4. 脅威

本情報システムの運用環境において想定される脅威及び情報システムでこれらの脅威への対抗策として想定される対策の例を示す。

1.4.1. 公開セグメントにおいて想定される脅威

【注釈】 ここでは、インターネット上の不特定多数の利用者から直接的なアクセスを受ける公開セグメントにおいて想定される脅威を運用面の脅威を含めて例示している。実際に調達の対象とする情報システムの仕様や特性を考慮した上で脅威を記載すること。

表 1.4.1 公開セグメントにおいて想定される脅威

No	脅威分類	脅威タイトル／脅威内容
脅威(公開)-T1	情報資産の漏えい、改ざん、削除	**不許可サービスの悪用による脅威** インターネット上の攻撃者が明示的に利用を許可されていないサービスを使用することにより、情報資産の漏えい、改ざん、削除が発生する。
脅威(公開)-T2	情報資産の漏えい、破壊	**インターネットを流通するデータに対する脅威** インターネット上の攻撃者がサービス利用者と本情報システムとの間で送受信されるサービスの利用に関する Web 入出力データを含むパケットに対して盗聴、改ざんを行うことにより、サービス利用者の個人情報が漏えい、破壊される。
脅威(公開)-T3	サービスの可用性低下 情報資産の漏えい、改ざん、削除、	**不正なプログラムによる脅威** インターネット上の攻撃者により本情報システムに対して意図的に不正なプログラムを侵入させる、又は偶発的に不正なプログラムが混入することにより、サービスの提供が滞る可能性がある。更に、情報資産の漏えい、改ざん、削除が発生する可能性もある。
脅威(公開)-T4	情報資産の漏えい	**サービス利用者へのなりすましによる脅威** インターネット上の攻撃者が正規のサービス利用者になりすまして不正な操作を行うことにより、情報資産の漏えいが発生する。
脅威(公開)-T5	情報資産の漏えい、改ざん、削除	**運用関係者へのなりすましによる脅威** 本情報システムの運用に携わる者が運用担当者､業務担当者､監査担当者、又は保守担当者になりすまし不正な操作を行うことにより、情報資産の漏えい、改ざん、削除が発生する。
脅威(公開)-T6	情報資産の漏えい、改ざん、削除	**サービス利用者の権限を逸脱した不正行為による脅威** インターネット上のサービス利用者が与えられた操作範囲を逸脱して不正な操作を行うことにより、他のサービス利用者の情報資産を漏えいさせる。

		また、本情報システムの運営にかかわる情報資産に対する不正な操作を行うことにより、Web コンテンツの改ざん、削除が発生する。
脅威(公開)-T7	情報資産の漏えい、改ざん、削除	**運用関係者の権限を逸脱した不正行為による脅威** 本情報システムの運用に携わる者が各々に付与された役割と権限の範囲を逸脱して不正な操作を行うことにより、情報資産の漏えい、改ざん、削除が発生する。
脅威(公開)-T8	サービスの可用性低下	**サービス要求過多による脅威** インターネット上の攻撃者が本情報システムに対して大量のサービス要求を送信し、又は正規のサービス利用者によるサービス要求が一時的に大量発生することにより、ネットワークトラフィックの過多やサーバ機器の過負荷が発生し、サービスが遅延したり停止する可能性がある。
脅威(公開)-T9	真正性の失墜	**事実の否認による脅威** サービス利用者がサービスを利用した事実や利用に関する情報の内容を否認する。
脅威(公開)-T10	サービスの可用性低下	**運用関係者の操作誤りによる脅威** 本情報システムの運用に携わる者が誤操作を行うことにより、本システムが安全な状態を維持できなくなる。
脅威(公開)-T11	サービスの停止 情報資産の破壊	**自然災害による脅威** 地震、火災、落雷等の自然災害により、本情報システムの運用が停止したり、情報資産の破壊が発生する。
脅威(公開)-T12	サービスの停止 情報資産の破壊	**動力源の停止による脅威** 電圧の低下や電源の瞬断、停電等の電力供給停止により、本情報システムの運用が停止したり、情報資産の破壊が発生する。
脅威(公開)-T13	サービスの停止、サービスの可用性低下 情報資産の損失	**機器の故障による脅威** ハードウェアの老朽化や故障により、本情報システムの情報資産に損失が発生する。
脅威(公開)-T14	情報資産の漏えい	**物理的な盗難と破壊による脅威** 攻撃者が本情報システムの設置場所や機器設置の管理不備を悪用することにより、本情報システムが管理する情報資産の漏えいが発生する。

【注釈】　脅威(公開)-T11,T12,T13,T14 が抑制される前提条件が定義されている場合は、脅威(公開)-T11,T12,T13,T14 を識別する必要はない。

1.4.2. 内部セグメントにおいて想定される脅威

【注釈】 ここでは、主として、本情報システムの運用に携わる関係者から直接的なアクセスを受ける内部セグメントにおいて想定される脅威例を示している。実際に調達の対象とする情報システムの仕様や特性を考慮した上で脅威を記載すること。

表 1.4.2 内部セグメントにおいて想定される脅威

No	脅威分類	脅威タイトル／脅威内容
脅威(内部)-T1	サービスの可用性低下 情報資産の漏えい、改ざん、削除、	**不正なプログラムによる脅威** 偶発的に不正なプログラムが混入することにより、サービスの提供が滞る可能性がある。更に、情報資産の漏えい、改ざん、削除が発生する可能性もある。
脅威(内部)-T2	情報資産の漏えい、改ざん、削除	**運用関係者へのなりすましによる脅威** 本情報システムの運用に携わる者が運用担当者､業務担当者､監査担当者又は保守担当者になりすまし不正な操作を行うことにより、情報資産の漏えい、改ざん、削除が発生する。
脅威(内部)-T3	情報資産の漏えい、改ざん、削除	**運用関係者の権限を逸脱した不正行為による脅威** 本情報システムの運用に携わる者が各々に付与された役割と権限の範囲を逸脱して不正な操作を行うことにより、情報資産の漏えい、改ざん、削除が発生する。
脅威(内部)-T4	サービスの可用性低下	**運用関係者の操作誤りによる脅威** 本情報システムの運用に携わる者が誤操作を行うことにより、本システムが安全な状態を維持できなくなる。
脅威(内部)-T5	サービスの停止 情報資産の破壊	**自然災害による脅威** 地震、火災、落雷等の自然災害により、本情報システムの運用が停止したり、情報資産の破壊が発生する。
脅威(内部)-T6	サービスの停止 情報資産の破壊	**動力源の停止による脅威** 電圧の低下や電源の瞬断、停電等の電力供給停止により、本情報システムの運用が停止したり、情報資産の破壊が発生する。
脅威(内部)-T7	サービスの停止、サービスの可用性低下 情報資産の損失	**機器の故障による脅威** ハードウェアの老朽化や故障により、本情報システムの情報資産に損失が発生する。
脅威(内部)-T8	情報資産の漏えい	**物理的な盗難と破壊による脅威** 攻撃者が本情報システムの設置場所や機器設置の管理不備を悪用することにより、本情報システムが管理する情報資産の漏えいが発生する。

【注釈】 脅威(内部)-T5,T6,T7,T8 が抑制される前提条件が定義されている場合は、脅威(公開)-T5,T6,T7,T8 を識別する必要はない。

2. セキュリティ提案仕様の審査ポイント

本章では、インターネットサービスシステムに関するセキュリティ要求仕様を受けて策定したセキュリティ提案仕様を審査する際の要点を示す。なお、その前提として、調達者は、提案者に対して、セキュリティ提案仕様に①「システム概要」、②「保護すべき情報資産」、③「前提条件」、④「脅威」、⑤「情報セキュリティ対策」及び⑥「セキュリティ機能を実現する IT 機器」の各項目を記載することを求める必要がある。

このうち、⑤の「情報セキュリティ対策」の審査ポイントについては、本章の「2.1 情報セキュリティ対策」で解説する。また、⑥の「セキュリティ機能を実現する IT 機器」の審査ポイントについては、本章の「2.2 認証製品の適用」及び本文の「3.3 セキュリティ機能を実現する機器等の審査」を参照されたい。

一方、セキュリティ提案仕様の①「システム概要」は、セキュリティ要求仕様にある記述を転記するものであることから、審査の対象とする必要はない。また、②の「保護すべき情報資産」、③の「前提条件」及び④の「脅威」は、セキュリティ要求仕様の記述を転記していれば審査の対象とする必要はないが、当該記述を基本としつつ、提案者が変更等を提案する場合もある。その場合における審査ポイントについては、本文の「3.1 『保護すべき情報資産』、『前提条件』及び『脅威』の審査」を参照されたい。

このほか、セキュリティ提案仕様に「制約条件」が記述されている場合もあり、その場合の審査の観点については、本文の「3.4 制約条件の審査」を参照されたい。

2.1. 情報セキュリティ対策

インターネットサービスシステムの運用環境において想定される脅威に対抗するために必要となるセキュリティ対策について例を示す。

【注釈】 提案者から提示された情報セキュリティ対策の妥当性を審査する際には、脅威に対する対抗性及び前提条件と組織のセキュリティポリシーの実現性を適切に備えていることを確認する必要がある。調達者は、提案者から提示されたセキュリティ提案仕様を審査する際には、提案者が策定した情報セキュリティの対策と比較検証することにより、その妥当性を判断する目安とすることができる。さらに、「2.2.1. 技術的セキュリティ対策に適合する製品の検討例」をあわせて確認することにより、具体的なセキュリティ機能の観点からセキュリティ対策としての妥当性を審査することができる。

2.1.1. 技術的セキュリティ対策

表 2.1.1 技術的セキュリティ対策

No	技術的セキュリティ対策のタイトル／内容
技術対策-1	**ネットワーク通信データ制御** インターネットと公開セグメントの間、公開セグメントと内部セグメントの間では、本情報システムが提供するサービスに必要となるサービスポートのみのネットワーク通信データを流通させる。また、特定の送信パターンに該当するネットワーク通信データを制御することにより、不正なネットワーク通信データを遮断し、必要最小限のネットワーク通信データのみを流通させる。加えて、正当なサービス利用者によるサービス要求過多時においても、同時接続数の制限や通信量の制限により、過負荷を抑止制御する。 また、本情報システムの動作に不要なサービスプログラムは非活性化する。 更に、インターネットと公開セグメントの間は、識別された特定箇所のみでネットワーク接続する。
技術対策-2	**識別と認証** 本情報システムにかかわる人物を識別し、認証する。 インターネットを経由して本情報システムへアクセスするサービス利用者に対しては、ユーザ ID とパスワードを用いる主体認証及びクライアント認証を併用させることで複合認証を行う。 公開セグメント及び内部セグメントから本情報システムにアクセスするシステム管理者、運用担当者、業務担当者、監査担当者及び保守担当者に対しては、ユーザ ID とパスワードを用いる主体認証を行う。
技術対策-3	**アクセス制御** 本情報システムが提供するサービスを使用するサービス利用者、サービスの運用管理を行う運用担当者、業務担当者、監査担当者、本情報システムを構成する機器群を管理維持するシステム管理者、保守担当者に対して、本情報システムを利用又は管理行為を行う際の操作可能範囲及び本情報システムに存在する情報資産へのアクセス可能範囲を制御する。 アクセス制御は、ユーザ識別属性情報及び本情報システムが持つアクセス制御規則に基づいて制御する。
技術対策-4	**監査証跡の採取と侵害通知** 本情報システムの利用状況、運用状況及び運用維持に関する管理状況を監査証跡として記録する。また、記録した監査証跡を特定の監査証跡属性情報に従って分析を行う。
技術対策-5	**高信頼データ転送** インターネット上のサービス利用者と公開セグメントとの間で送受信されるネットワーク通信データを SSL により暗号化を施す。 また、IDC と監視センター間で送受信されるネットワーク通信データは、VPN により暗号化を施す。
技術対策-6	**不正プログラムの排除** ウィルスやワーム等の不正プログラムの侵入を検知し、その削除、非活性化と、運用者にアラートを通知する。また、不正プログラムを検出するための検出パターンを常に最新状態に維持する。

2.1.2. 物理的セキュリティ対策

表 2.1.2 物理的セキュリティ対策

No	物理的セキュリティ対策のタイトル／内容
物理対策-1	**動力源に関する対策** - 自動的にシャットダウンを制御するソフトウェアを導入する。 - UPS（無停電電源装置）を設置する。 - 予備の電源を確保する。 - 遠隔地にバックアップ用のサイトを設置する。
物理対策-2	**機器の故障に関する対策** - 定期的な保守を実施する。 - 機器構成を二重化する。 - バックアップとリカバリの運用を実施する。 - 機器の廃棄における対策を徹底する。
物理対策-3	**物理的な盗難と破壊に関する対策** - 機器やドキュメント類の施錠管理を実施する。 - 情報システムが設置された区画の入退室管理を徹底する。 - BIOS パスワード等のハードウェア的認証機構を使用する。 - スクリーンセイバーのパスワード機構を使用し、離席時の情報機器のロックを徹底する。

2.1.3. 運用に関するセキュリティ対策

表 2.1.3 運用的セキュリティ対策

No	運用的セキュリティ対策のタイトル／内容
運用対策-1	**システム管理者、監査担当者の信頼性** 運営責任者は、本情報システムにかかわる特権利用者として適切な管理を実施するための技術とモラルを備えた人物をシステム管理者、監査担当者として任命する。また、任命した人物に対して情報セキュリティ教育と啓発を実施し、本情報システムの管理監査行為に関する規則を遵守することに同意させる。
運用対策-2	**運用担当者の不正行為抑止** 個々の運用担当者に対して適切な管理権限を付与し、個々の運用担当者ごとに付与された管理権限の悪用を抑止するために、複数の運用担当者で相互確認を行う等の運用方針を定める。また、運営責任者は、運用担当者の管理行為が適切に遂行されるように運用担当者に対する教育と啓発を実施する。 更に、運用管理行為に関する監査証跡を定期的に監査し、監査管理運用を運用担当者に認識させる。
運用対策-3	**バックアップとリカバリ** 運用担当者が定期的に情報資産のバックアップを行い、操作誤りや異常が発生する前状態に情報資産をリカバリできるように、運営責任者は運用担当者に対してバックアップとリカバリに関する運用規定の教育を指示する。

運用対策-4	**潜在的な脆弱性に対する迅速な対応** 運営責任者は、システム管理者、運用担当者に対して、情報セキュリティに関する問題の最新情報を収集し、本情報システムに潜在する脆弱性が公知となった場合は、迅速な修正情報の適用やバージョンアップ等を実施できるように教育に関する指示を行う。
運用対策-5	**認証システムの信憑性** 信頼できる認証局を採用する。

2.1.4. 脅威、前提条件と情報セキュリティ対策の対応

脅威、前提条件と情報セキュリティ対策の対応関係を以下に示す。

2.1.4.1. 公開セグメントにおけるセキュリティ対策の対応

【注釈】 政府機関への適用を想定し、政府機関統一基準との対応を示している。

表 2.1.4 公開セグメントにおける
脅威及び前提条件と情報セキュリティ対策の対応関係

No	脅威	前提条件／ 組織のセキュリティポリシー	政府機関統一基準との対応
技術対策-1	脅威(公開)-T1 脅威(公開)-T3 脅威(公開)-T8	接続前提-2	統 4.2.3 (1)(a) 統 5.2.3 (1)(c) 統 5.4.1 (1)(d)-(i) 統 5.4.2 (1)(a) 統 5.4.3 (1)(a)-(b)
技術対策-2	脅威(公開)-T4 脅威(公開)-T5	－	統 4.1.1 (1)(b)-(d)
技術対策-3	脅威(公開)-T6 脅威(公開)-T7 脅威(公開)-T10	－	統 4.1.2 (1)(b)-(c),(2)(a) 統 4.1.3 (1)(b)-(c)
技術対策-4	脅威(公開)-T6 脅威(公開)-T7 脅威(公開)-T10	－	統 4.1.4 (1)(b)-(e)
技術対策-5	脅威(公開)-T2 脅威(公開)-T9	接続前提-1	統 5.4.1 (1)(i)
技術対策-6	脅威(公開)-T3	－	統 4.2.2 (1)(a)-(b)
物理対策-1	－	物理前提-1	－
物理対策-2	－	物理前提-1	統 5.2.3 (2)(a)-(c)
物理対策-3	－	物理前提-1	統 5.1.1 (1)(a)-(c)
運用対策-1	－	人的前提-1 人的前提-2 人的前提-3	統 2.2.1 (1)(a)-(i),(2)(a)-(d) 統 4.1.1 (2)(a)-(d),(3)(a)-(d) 統 4.1.4 (2)(a)-(c),(3)(a) 統 4.2.2 (2)(a)-(h) 統 4.2.3 (2)(a) 統 5.4.1 (2)(b)-(c),(f)
運用対策-2	脅威(公開)-T5 脅威(公開)-T7 脅威(公開)-T10	－	統 2.2.1 (1)(a)-(d),(2)(a)-(b) 統 4.1.1 (2)(a)-(d),(3)(a)-(d)
運用対策-3	脅威(公開)-T10	－	統 5.2.3 (2)(b)-(c)

【注釈】
本例では、便宜上、技術対策で対応するものとしているが、セキュリティターゲットを策定する場合には、運用面の対策を設けて対応させることが必要となる。

【注釈】
接続前提-1 の内容が調達仕様で要求事項として明示されている場合には、接続前提-1 を設ける必要はない。

【注釈】
物理前提-1 が前提条件として明示されていない場合には、物理対策-1～3 が対抗する脅威（公開）-T11～T14 を明示して脅威の列に記入する。

運用対策-4	脅威(公開)-T1 脅威(公開)-T3	－	統 4.2.1 (2)(a)-(h)
運用対策-5	－	接続前提-3	－

2.1.4.2. 内部セグメントにおけるセキュリティ対策の対応

表 2.1.5 内部セグメントにおける
脅威及び前提条件と情報セキュリティ対策の対応関係

No	脅威	前提条件／ 組織のセキュリティポリシー	政府機関統一基準との対応
技術対策-1	脅威(内部)-T1	接続前提-2	統 4.2.3 (1)(a) 統 5.2.3 (1)(c) 統 5.4.1 (1)(g)-(i) 統 5.4.2 (1)(a) 統 5.4.3 (1)(a)-(b)
技術対策-2	脅威(内部)-T2	－	統 4.1.1 (1)(b)-(d)
技術対策-3	脅威(内部)-T3 脅威(内部)-T4	－	統 4.1.2 (1)(b)-(c),(2)(a) 統 4.1.3 (1)(b)-(c)
技術対策-4	脅威(内部)-T3 脅威(内部)-T4	－	統 4.1.4 (1)(b)-(e)
技術対策-5	－	接続前提-1	統 5.4.1 (1)(i)
技術対策-6	脅威(内部)-T1	－	統 4.2.2 (1)(a)-(b)
物理対策-1	－	物理前提-1	－
物理対策-2	－	物理前提-1	統 5.2.3 (2)(a)-(c)
物理対策-3	－	物理前提-1	統 5.1.1 (1)(a)-(c)
運用対策-1	－	人的前提-1 人的前提-2 人的前提-3	統 2.2.1 (1)(a)-(i),(2)(a)-(d) 統 4.1.1 (2)(a)-(d),(3)(a)-(d) 統 4.1.4 (2)(a)-(c),(3)(a) 統 4.2.2 (2)(a)-(h) 統 4.2.3 (2)(a) 統 5.4.1 (2)(b)-(c),(f)
運用対策-2	脅威(内部)-T2 脅威(内部)-T3 脅威(内部)-T4	－	統 2.2.1 (1)(a)-(d),(2)(a)-(b) 統 4.1.1 (2)(a)-(d),(3)(a)-(d)
運用対策-3	脅威(内部)-T4	－	統 5.2.3 (2)(b)-(c)
運用対策-4	脅威(内部)-T1	－	統 4.2.1 (2)(a)-(h)
運用対策-5	－	接続前提-3	－

2.1.5. 保証に関するセキュリティ対策

本情報システムに求められる開発その他の保証に関するセキュリティ対策を以下に示す。

表 2.1.6 保証に関するセキュリティ対策

No	保証に関するセキュリティ対策のタイトル／内容
保証対策-1	**評価・認証を受けた製品等の利用の検討** 本情報システムの構築に必要な製品を導入する場合には、本情報システムのシステム仕様として必要とする機能において、情報セキュリティに関する評価・認証を受けた製品の導入を検討する。

2.2. 認証製品の適用

調達者は、セキュリティ要求仕様において、情報システム等を構成する特定の機器等について、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否かを提案の評価の要素に加えることとする場合がある。この場合には、セキュリティ提案仕様の「セキュリティ機能を実現する機器等」において提案されている認証製品とその認証の内容を、セキュリティ要求仕様に照らして審査する。審査における留意点については、本文の「3.3 セキュリティ機能を実現する機器等の審査」及び「付録 C　IT セキュリティ評価及び認証制度を活用した機器等の購入について」を参照されたい。

【注釈】 「2.1.1. 技術的セキュリティ対策」をシステムで実現するための手段としては、技術的セキュリティ対策に対応するセキュリティ機能を備えた製品を用いることになる。技術的セキュリティ対策との適合性に関しては、適用する製品がどのような機能範囲で認証を取得しているか、認証を取得している機能範囲内に技術的セキュリティ対策が必要とする機能が含まれているか、技術的セキュリティ対策が求めるセキュリティ機能像に最適化するためのカスタマイズ可能性を備えているかという点に着目して、判断する必要がある。
ここでは、技術対策-1 を取上げ、提案者が認証製品を評価し、提案するプロセスの例を示す。調達者は、提案者から示された認証製品及びプロセスを確認することにより、求める技術対策への当該認証製品の適合性が判断できる。

2.2.1. 技術的セキュリティ対策に適合する製品の検討例

- **技術対策-1［ネットワーク通信データ制御］**

【適用する製品種別と適用の根拠】

ファイアウォール系製品、ルータ系製品、スイッチ系製品等、ネットワーク通信データに対する制御機能を備えた製品を用いる。

これらの製品は、TCP/IP レベルのパケットを構成する属性情報（IP アドレス、ポート番号、通信方向等）を参照し、設定されたフィルタリング条件に従い、パケットの通過や破棄等の制御を施す機能を有することから、技術対策-1 を実現するために有効である。

【適用製品として備えるべきセキュリティ上の要件】

内部ネットワークに対する外部ネットワークからのアクセスの制限や、外部ネットワークとの通信における内部ネットワークのアドレス体系の隠匿等を目的として、これらの製品を導入することができる。

これらの製品は、複数のネットワークの境界点に設置された機器上で動作し、製品を経由するパケットを、事前に設定されたフィルタリング条件 (IP アドレス、ポート番号、プロトコル、通信方向、ネットワークインタフェース及びその組合せ) に従い、転送または破棄する。同様に、製品を経由するパケットの IP アドレス及びポート番号を、事前に設定されたアドレス変換条件に従い変換する。また、あらかじめ設定したイベントに関連する監査証跡の収集や、SNMP 通信あるいはメールを用いたアラートの通知等を行うことができる。

【適用製品として備えるべきセキュリティ機能】

a) パケットフィルタリング機能

フィルタリング条件に従い、パケットに対して、通過又は遮断の制御を行う機能。

b) アドレス変換機能

アドレス変換条件に従って、パケット中の IP アドレス又はポート番号を変換する機能。本機能により、内部ネットワークアドレス又はそのネットワークアドレス体系を保護しながらインターネット等の外部ネットワークと通信することが可能となる。

c) 運用支援機能

インターネットと本情報システムの間の通信を監視、解析して不正なアクセスを検出し、その情報を運用者に提供する機能。

- 証跡取得機能

  パケットフィルタリング等の動作状況を監査証跡として記録する。また、アラートの監視を行い、これを検出した場合、指定された通知方法及び通知先に従い、アラートの発生を通知する。

- 証跡出力機能

  格納されている監査証跡を出力する。

- モニタ出力機能

  現在の動作状況を出力する。

- 監査証跡検索機能

  監査証跡に記録された特定の事象等を検索する。

【本情報システムに対する適用方法】

本適用製品は、インターネット及び本情報システムとの間に設置し、インターネットと本情報システムとの間で送受信するパケットに対して、不正なパケットの検出と破棄、適切な通信量の制御を実施できるようにカスタマイズの上、適用する。

また、インターネットとの間で送受信するパケットの送受信状態を監査証跡として記録し、監査管理に活用できるようにカスタマイズの上、適用する。

更に、インターネットからの不正なアクセスを検知し、リアルタイムに管理者へアラートを通知するようにカスタマイズの上、適用する。

参考例III

複合機システム

ここでは、電子文書を印刷する機能及び紙文書を電子化する機能を持つ複合機を用いた複合機システムを例に、基本設計調達時に調達者が作成するセキュリティ要求仕様の例と、セキュリティ提案仕様を調達者が審査する際のポイントを示す。

実際の調達に当たっては、それぞれの情報システムにより保護すべき情報資産、前提条件、脅威及び求める情報セキュリティ水準等が異なることに留意し、本付録に示すセキュリティ要求仕様及びセキュリティ提案仕様の審査ポイントに対して適切に追加、変更等を加えて利用すること。

1. セキュリティ要求仕様

調達者が作成する複合機システムのセキュリティ要求仕様の例を以下に示す。

1.1. システム概要

1.1.1. システム全体概要

本システムは、利用者に印字サービス及び画像デジタル化サービスを提供する。

印字サービスは、利用者が PC 等の利用者端末に保持する電子文書を、利用者の指示に従い、複合機へ印字するサービスである。本サービスは、出力される印字物が印字を指示した利用者以外の者の目にふれることを防止するため、複合機においてパスワードによる利用者の認証を行った後に印字物の取り出しを可能とする機能も持つ。

また、画像デジタル化サービスは、複合機の画像読取機能により紙文書をデジタル化して画像サーバに格納すると共に、当該データを利用者の利用に供するサービスである。本サービスは、デジタル化した画像データがその利用を許可されていない者の目にふれることを防止する機能も持つ。

複合機システムのサービスを図 1.1 に示す。

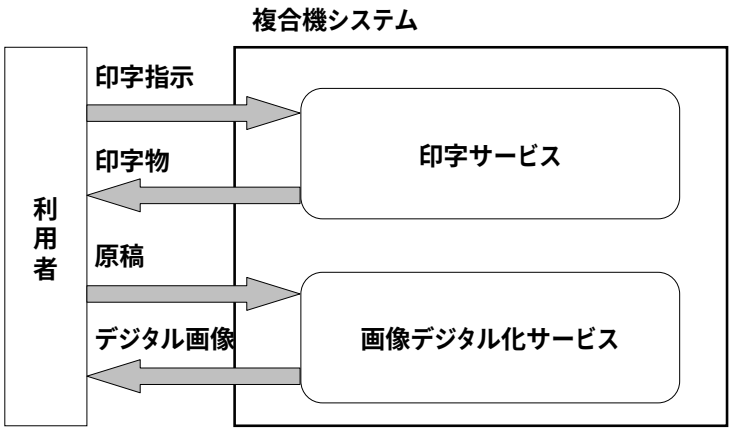


図 1.1 複合機システムの全体像

1.1.2. システム構成

1.1.2.1. システム構成概要

複合機システムは、複合機を単独で稼動させるだけでなく、印字サービス及び画像デジタル化サービスを必要とする他のシステムの一部として稼動させることにも配慮したシステム構成が必要であり、その要件を以下に示す。

- 本システムの利用者端末から印字サービスが利用可能であること。
- 他のシステムからも印字サービスが利用可能とすること。
- 本システムの利用者端末から画像デジタル化サービスが利用可能であること。
- 他のシステムからも画像デジタル化サービスが利用可能とすること。

複合機システムのシステム構成例を以下に示す。図中の太枠内が複合機システムである。

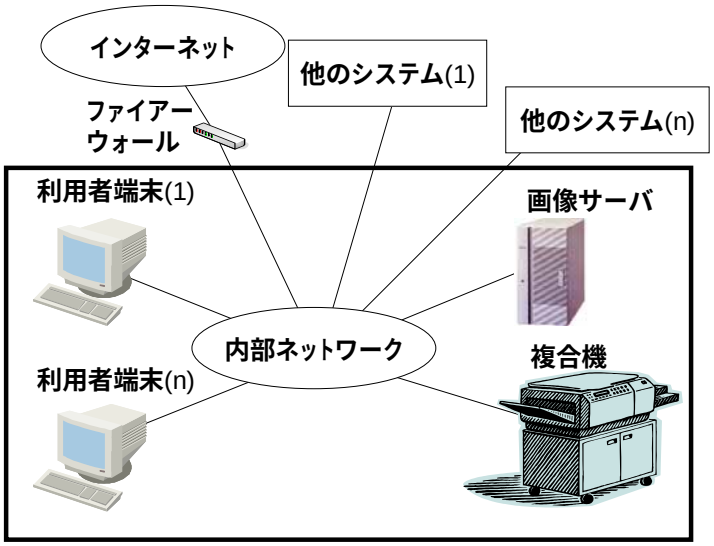


図 1.2 複合機システム

1.1.2.2. ハードウェア機器構成例

本システムのハードウェア機器構成例を以下に示す。

表 1-1 複合機システムの機器構成例

セグメント	ハードウェア機器(例)	機能概要
インターネット接続 LAN	ファイアウォール	IP アドレスやプロトコルに基づく通信データのフィルタリングを行い、不正侵入や攻撃を防ぐ機能を提供する。
内部 LAN	複合機	利用者からの印字指示を受け、電子文書を印字する機能を提供する。また、紙文書をデジタル化し、画像サーバへ送信する画像デジタル化機能を提供する。

	利用者端末	印字サービスを利用するため、複合機に対する印字指示機能を提供する。また、画像デジタル化サービスを利用するため、画像サーバへアクセスし、デジタル化された画像を入手する機能を提供する。
	画像サーバ	画像デジタル化サービスのため、複合機から送信されてきたデジタル画像を保存する機能を提供する。

1.1.2.3. 外部システム連携方法

本システムは、外部システムと連携しないが、他のシステムの一部として稼動することができる。他のシステムとの関係を以下に示す。図中で、複合機システムを太枠内に示し、角を丸くした長方形で複合機システムのサービスを、長方形で複合機システムを構成するコンポーネントを示す。

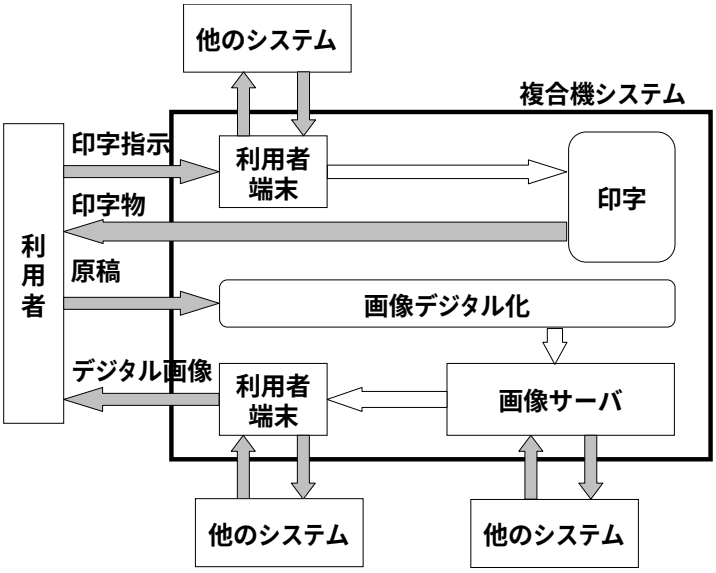


図 1.3 複合機システムと他のシステムとの関係

1.1.3. システム機能概要

本システムが利用者に提供するサービスを示す。

表 1-2 複合機システムのサービス

アプリケーション分類	サービス	サービスの内容
印字アプリケーション	印字サービス	印字サービスは、利用者による印字指示に従い利用者端末に保持する電子文書を複合機に印字するサービスで、印字指示において当該文書に主体認証情報を付し、複合機の操作部から主体認証操作及び印字出力操作を行うことにより印字物を出力するサービスである。
画像デジタル化アプリケーション	画像デジタル化サービス	画像デジタル化サービスは、紙文書をデジタル化して画像サーバに格納するサービスで、画像サーバに登録されている主体認証情報を利用者が入力することにより主体認証を行っ

		た後に、利用者の操作により紙文書のデジタル化処理を開始し、デジタル化した画像データを画像サーバに保存する。また、画像デジタル化サービスは、紙文書のデジタル化を指示した利用者及びその他の利用者に、画像サーバへのアクセスのための主体認証を行った後に、画像サーバに保存された画像データを取得させるサービスである。

1.1.4. システムにおける想定ユーザ

本システムが想定するユーザの分類ごとに、その役割と権限を示す。

表 1-3 複合機システムの想定ユーザの役割と権限

関係者分類	関係者名称	役割・権限の説明	
管理者	運用責任者	役割	・ 本システムの利用者の登録及び管理 ・ 本システムを構成する機器、内部ネットワーク及びソフトウェアの設置・接続・インストール ・ 本システムの各種設定及び設定の変更 ・ 本システムの起動・停止、システムトラブル対応及び日々のシステム運用管理
		権限	本システムの運用において利用者の登録、変更、削除等の操作を行う権限を持つ。また、利用者が複合機から印字物として取り出す前の印字データを削除する権限及び利用者が画像サーバに保存している画像データを削除する権限を持つ。
利用者	職員	役割	利用者は、本システムの印字サービスと、画像デジタル化サービスを利用する。
		権限	利用者は、複合機を使って印字データを印字する権限、印字される前の印字データを削除する権限、複合機を使って紙文書をデジタル化して画像サーバに保存する権限、及び画像サーバに自らが保存した画像データを削除する権限を持つ。

1.2. 保護すべき情報資産

本システムで、保護対象とする情報資産を以下に示す。

1.2.1. 印字データ

複合機から印字される前の印字データを、保護すべき情報資産とする。印字を指示した利用者以外の第三者が印字物を盗み見し又は持ち去ることによる情報漏えいを防ぎ、また、複合機で印字される前の印字データの漏えい及び改ざんを防ぐ必要がある。

1.2.2. 画像データ

画像サーバに保持されている画像データを、保護すべき情報資産とする。取得等を認められた利用者以外の第三者が画像データを盗み見することによる情報漏えいを防ぎ、また、画像データの改ざんを防ぐ必要がある。

1.3. 本システムの運用時の前提条件

本システムの運用時の前提条件について、物理的、接続的（ネットワーク環境等)、人的側面から示す。

1.3.1. 物理的な設置環境に関する前提条件

物理的な設置環境に関する前提条件を以下に示す。

識別子	前提条件のタイトル/内容
物理前提-1	本システムは、入退室管理により区画管理が行われている場所に設置するものとする。

【注釈】
この例では、政府機関統一基準に準拠する安全区域内での利用を想定している。

1.3.2. 接続面（ネットワーク環境等）に関する前提条件

接続面に関する前提条件を以下に示す。

識別子	前提条件のタイトル/内容
接続前提-1	内部ネットワークは、インターネット等の外部ネットワークからの攻撃から保護されているものとする。

【注釈】
この例では、本システムを設置するネットワーク環境として霞ヶ関 WAN や府省庁内 LAN の機器等は既に存在しており、それらの安全性が確保されているものと想定している。

1.3.3. 人的環境に関する前提条件

人的環境に関する前提条件を以下に示す。

識別子	前提条件のタイトル/内容
人的前提-1	運用管理者は、課せられた役割に対して許可された一連の業務を誠意をもって遂行し、悪意ある行為は行わないものとする。
人的前提-2	運用管理者及び利用者は、識別コード及び主体認証情報を適切に管理、利用することができる。

【注釈】
この例では、運用管理者は、規則に反する行為を意図的に行わず信頼できるものと想定するが、情報セキュリティ対策として、運用管理者による操作を記録する監査証跡の取得が求められる場合もある。

1.4. 脅威

本システムの運用環境において想定される脅威を以下に示す。

識別子	脅威分類	脅威タイトル / 脅威内容
脅威-1	情報漏えい 改ざん	本システムにおいて印字を指示した利用者以外の第三者が、複合機から印字された印字物を盗み見ること、又は印字物を持ち去ることにより情報が漏えいする可能性がある。また、印字される前の印字データが漏洩し、又は改ざんされる可能性がある。
脅威-2	情報漏えい 改ざん	画像サーバに保持されている画像データがその取得等を認められた利用者以外の第三者に漏えいし、又は画像データを改ざんされる可能性がある。

2. セキュリティ提案仕様の審査ポイント

本章では、複合機システムに関するセキュリティ要求仕様を受けて策定したセキュリティ提案仕様を審査する際の要点を示す。なお、その前提として、調達者は、提案者に対して、セキュリティ提案仕様に①「システム概要」、②「保護すべき情報資産」、③「前提条件」、④「脅威」、⑤「情報セキュリティ対策」及び⑥「セキュリティ機能を実現する IT 機器」の各項目を記載することを求める。

このうち⑤の「情報セキュリティ対策」の審査ポイントについては、本章の「2.1 情報セキュリティ対策」で解説する。また、⑥の「セキュリティ機能を実現する IT 機器」の審査ポイントについては、本章の「2.2 認証製品の適用」及び本文の「3.3 セキュリティ機能を実現する機器等の審査」を参照されたい。

一方、セキュリティ提案仕様の①の「システム概要」は、セキュリティ要求仕様にある記述を転記するものであることから、審査の対象とする必要はない。また、②の「保護すべき情報資産」、③の「前提条件」及び④の「脅威」は、セキュリティ要求仕様の記述を転機していれば審査の対象とする必要はないが、当該記述を基本としつつ、提案者が変更等を提案する場合もある。その場合における審査ポイントについては、本文の「3.1 『保護すべき情報資産』、『前提条件』及び『脅威』の審査」を参照されたい。

このほか、セキュリティ提案仕様に「制約条件」が記述されている場合もあり、その場合の審査の観点については、本文の「3.4 制約条件の審査」を参照されたい。

2.1. 情報セキュリティ対策

本システムの運用環境において想定される脅威に対抗するために提案者が提案した情報セキュリティ対策の例を以下に示すとともに、調達者が審査する際のポイントをそれぞれの注釈に示す。

2.1.1. 技術的セキュリティ対策

本システムの運用時に必要となる技術的セキュリティ対策の提案例を以下に示す。

技術対策-1	**複合機の利用者の主体認証機能及びアクセス制御機能** 複合機から印字物の取り出しを行おうとする者が正当な主体であることを確認するために、複合機から印字物を取り出す際に利用者を識別・認証し、正当な主体にのみ印字物の取り出しを可能とする手段を持つ。
技術対策-2	**画像サーバの利用者の主体認証機能及びアクセス制御機能** 画像サーバへアクセスする者が正当な主体であることを確認するために、利用者が画像サーバへ画像データを保存する際、及びデジタル化された画像データを取り出す際に、利用者を識別・認証し、正当な主体にのみ認められた操作を可能とする手段を持つ。
・・・	・・・

【注釈】
この例では、複合機の主体認証機能及びアクセス制御機能並びに画像サーバの主体認証機能及びアクセス制御機能が提案されたことを想定している。府省庁が予め主体認証機能及びアクセス制御機能の実施手段を提案者に提示していない場合には、利便性・安全性等のバランスを考え、提案された方式の妥当性について検討する必要がある。

2.1.2. 物理的セキュリティ対策

本システムの運用時に必要となる物理的セキュリティ対策の提案例を以下に示す。

物理対策-1	**安全区域の設置** 本システムを入退室管理により区画管理がなされた場所に設置する。
・・・	・・・

【注釈】
本対策は物理前提-1 を実現するものであるが、これを確実に実施できるかどうか、という観点で検討することが重要である。

2.1.3. 運用に関するセキュリティ対策

本システムに求められる運用に関するセキュリティ対策の提案例を以下に示す。

運用対策-1	**内部ネットワークの信頼性** 外部ネットワークからの不正侵入や攻撃､内部ネットワーク内における盗聴から内部ネットワークを適切に保護する。
運用対策-2	**運用管理者の信頼性** 運用管理者は、課せられた役割に対して許可された一連の業務を誠意をもって遂行し、悪意ある行為は行わないように教育・訓練を受ける。
運用対策-3	**主体認証情報の管理、利用の信頼性** 運用管理者及び利用者は、識別コード及び主体認証情報を適切に管理、利用する。
・・・	・・・

【注釈】
これらの対策は接続前提-1、人的前提-1 及び人的前提-2 を実現するものであるが、これらを確実に実施できるかどうか、という観点で検討することが重要である。

2.1.4. 保証に関するセキュリティ対策

本システムに求められる保証に関するセキュリティ対策の提案例を以下に示す。

保証対策-1	**評価・認証を受けた製品等の利用の検討** ハードウェア構成、ソフトウェア構成にて情報セキュリティを確保する上で重要とした製品等については、システム仕様を満たし、かつ評価・認証を受けた製品の有無を調査し、政府機関統一基準に基づき、IT セキュリティ評価及び認証制度に基づく認証を受けた製品の利用を検討する。

【注釈】
保証に関する対策は、個々の前提条件や脅威に対応するものではなく、システム全体が安全に構築・運用されることを保証するためのものである。システムの性質や扱う情報の重要性を考慮して検討することが重要である。

2.1.5. 前提条件、脅威と情報セキュリティ対策の対応

調達者が提示した前提条件及び脅威と、提案者が提案した本システムのセキュリティ対策の対応を以下に示す。

前提条件	脅威	セキュリティ対策	政府機関統一基準との対応
物理前提-1	―	物理対策-1	統 5.1.1(1)(a)
接続前提-1	―	運用対策-1	統 5.4.3(2)(a)-(b)
人的前提-1	―	運用対策-2	―
人的前提-2	―	運用対策-3	統 4.1.1(2)(a)-(d), (3)(c)(d)
―	脅威-1	技術対策-1	統 4.1.1 (1), 4.1.1 (2)
―	脅威-2	技術対策-2	統 4.1.1 (1), 4.1.1 (2)
・・・	・・・	・・・	・・・

【注釈】
提案された対応表において、セキュリティの対策が必要十分であることを確認しなければならない。セキュリティ要求仕様に記載したすべての前提条件及び脅威が何らかの対策によって対応されていること、提案された対策が脅威への対抗あるいは前提条件の達成に寄与していることを確認する必要がある。

2.2. 認証製品の適用

調達者は、セキュリティ要求仕様において、情報システム等を構成する特定の機器等について、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否かを提案の評価の要素に加えることとする場合がある。この場合には、セキュリティ提案仕様の「セキュリティ機能を実現する機器等」において提案されている認証製品とその認証の内容を、セキュリティ要求仕様に照らして審査する。審査における留意点については、本文の「3.3 セ

キュリティ機能を実現する機器等の審査」及び「付録 C　IT セキュリティ評価及び認証制度を活用した機器等の購入について」を参照されたい。

本参考例においては、複合機及び画像サーバに関して、認証取得を評価の要素に加えることができる。ここでは、提案者が複合機及び画像サーバにおける技術的対策の設計及び実装について認証取得を主張した場合に、府省庁で行うべき審査について解説する。

2.2.6. 技術対策-1 に適合する製品の検討

技術対策-1 は、複合機が備える主体認証機能及びアクセス制御機能で実現される情報セキュリティ機能である。そこで、提案された複合機が 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おり、当該認証の内容がこれらの機能を含み、かつ、当該認証における前提条件等が本システムの前提条件等に合致していれば、複合機におけるこれらの機能の設計及び実装について第三者による評価に基づき信頼することができる。

政府機関統一基準にも示されているとおり、主体認証には知識、所有、生体情報、及びそれ以外の方法がある。複合機の主体認証機能で採用している主体認証の方法は、利用者端末での主体認証情報付加方法と合わせて選択するものであり、この観点で利用者端末での主体認証情報付加方法との整合性についても確認する必要がある。

2.2.7. 技術対策-2 に適合する製品の検討

技術対策-2 は、画像サーバが備える主体認証機能及びアクセス制御機能で実現される情報セキュリティ機能である。そこで、提案された画像サーバが 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おり、当該認証の内容がこれらの機能を含み、かつ、当該認証における前提条件等が本システムの前提条件等に合致していれば、画像サーバにおけるこれらの機能の設計及び実装について第三者による評価に基づき信頼することができる。

主体認証の方法は前項で述べたとおりであり、画像サーバの主体認証機能と、複合機での主体認証情報入力方法の整合性が求められる。このため、認証製品で実現されている主体認証実施方法だけでなく、複合機での主体認証情報入力方法との整合性についても確認する必要がある。