NISC National Information Security Center

# 情報システムに係る政府調達における セキュリティ要件策定マニュアル（案）の概要

2011年1月31日

# マニュアルの構成

## 1章　マニュアル概要
背景、目的、位置づけ、想定読者、適用範囲

## 2章　用語等定義
用語等定義

## 3章　本マニュアルの使い方
政府調達における利用タイミング、手順の全体像

## 4章　業務要件の検討
システム概要図の作成、定型設問による業務要件の詳細化

## 5章　セキュリティ要件の策定
対策要件集及び判断条件、対策方針の検討・決定、調達仕様書への反映

## 6章　その他の考慮事項

セキュリティ要件を策定し、
調達仕様書に反映する
具体的解説部分。

## 付録A　対策要件に関する解説
本マニュアルの対策要件に関する具体的解説

## 付録B　政府機関統一基準群対応表
本マニュアルの対策要件と政府機関統一基準群の遵守事項との対応関係

## 付録C　マニュアル活用例
本マニュアルを活用したセキュリティ要件の検討例

## 1章　マニュアル概要

● **目的**

政府機関の情報システムの企画段階から情報セキュリティ対策を適切に組み込むため、セキュリティ要件の策定方法を解説する。もって、調達担当者が自ら調達するシステムの特性に応じて重要かつ効果的な要件を優先的に確実にセキュリティ要件を調達仕様書に記載することを目的。

● **位置づけ**

政府機関の情報システムが「情報システムに係る政府調達の基本指針（H19.3.1 CIO 連絡会議決定）」に基づいて調達される際の、セキュリティ要件の策定にあったて活用されることを想定。

● **想定読者**

行政事務従事者のうち、情報システムの調達を担当する調達担当者及び情報システムを供給する事業者。

● **活用範囲**

政府機関における「新規構築」及び「更改」を行う情報システム全般。特に調達段階から技術の専門家が参画することが難しい中小規模の情報システムの調達において有効。

## 2章　用語等定義

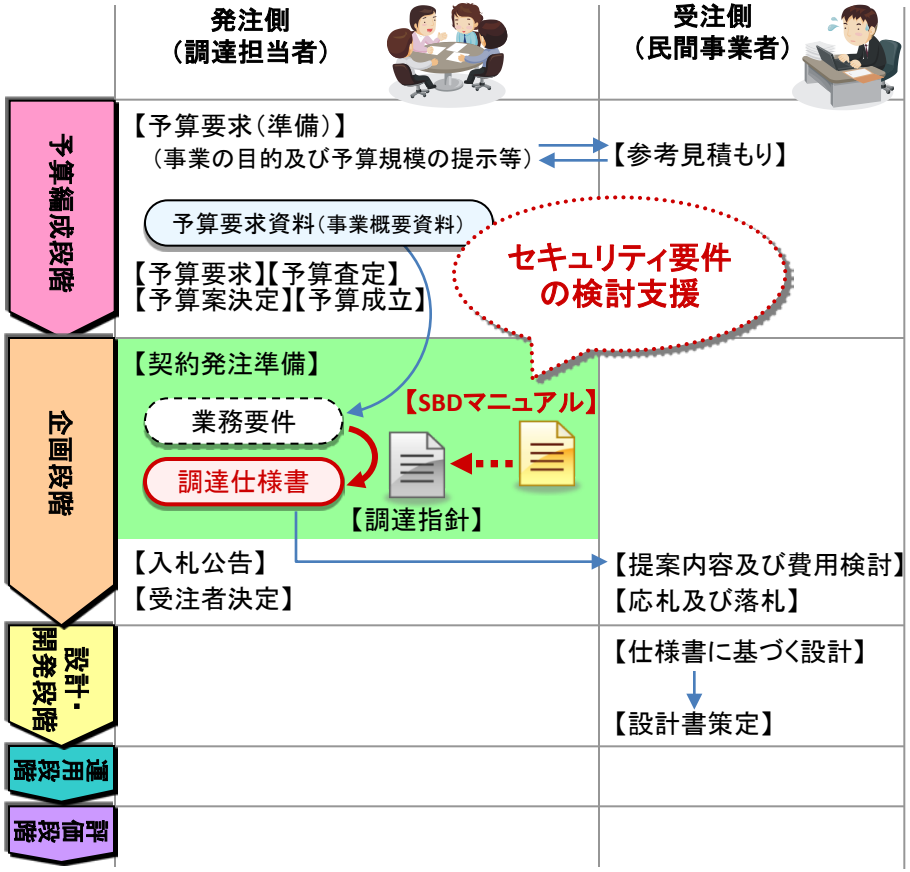
本マニュアルで用いる用語等を定義する。

# 3章　本マニュアルの使い方

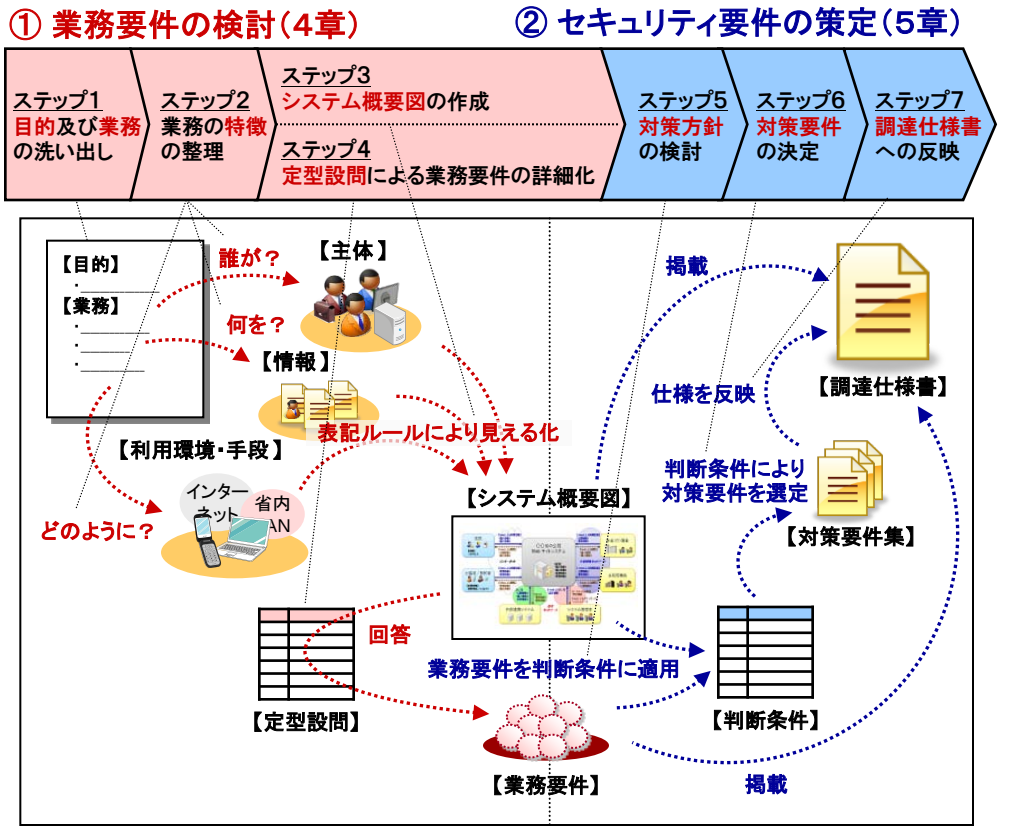
【目的】
情報システムの調達プロセスにおいて、調達担当者が調達仕様書にセキュリティ要件を記載する作業を支援すること。

【作業の流れ】
① 業務要件の検討
対象業務をシステム概要図にまとめ、定型設問に回答する。
② セキュリティ要件の策定
業務要件を判断条件にあてはめ対策要件を決定する。

## 政府調達における利用のタイミング




## 手順の全体像



# 4章 業務要件の検討

【システム概要図の作成】
1. 調達の目的及び業務を洗い出す。
2. 主体、情報、利用環境・手段の観点で業務内容を整理する。
3. 表記ルールに従って業務要件をシステム概要図にまとめる。

【定型設問による業務要件の詳細化】
4. 主体、取り扱う情報、利用環境・手段の3つの観点の定型設問に回答して、業務要件の詳細化を図る。

## ステップ1. 目的及び業務の洗い出し

【目的】 インターネットを活用して国民参加による政策立案のしくみを確立すること

【業務】 (1)「国民」による政策に関する意見・コメントの投稿
(2)「事務局」からの政策に関する情報提供

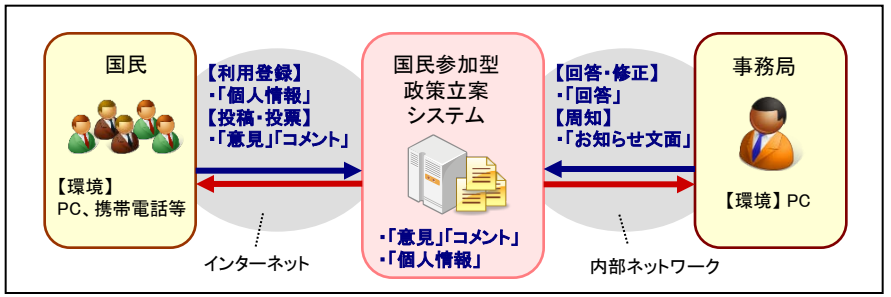
## ステップ2. 業務の特徴の整理

誰が？ （業務の細分化） 何を？ どのようにして？

| 主体 | 業務 | 情報 | 利用環境・手段 |
|---|---|---|---|
| 国民 | 利用登録 | 個人情報 | PC、携帯電話、インターネット |
| | 意見・コメントの投稿・投票 | 意見、コメント | |
| 事務局 | 意見に対する回答、修正 | 回答 | PC、行政情報ネットワーク |
| | 周知 | お知らせ文面 | |

## ステップ3. システム概要図の作成

表記ルール




## ステップ4. 定型設問による業務要件の詳細化

| ID | 観点 | 設問 |
|---|---|---|
| A-1 | 主体 | 【数量】 おおよその人数規模は？ |
| A-2 | | 【主体分類】主体の分類は？ |
| A-3 | | 【集合特性】特定か不特定か？ |
| A-4 | | 【所属】システム所管組織との関係は？ |
| A-5 | | 【頻度】1人あたりのアクセス頻度は？ |
| A-6 | | 【利用時間】1日の主な利用時間帯は？ |
| A-7 | | 【信頼性】 役割どおりに振る舞えるか？ |
| B-1 | 情報 | 【数量】 おおよそのデータ量は？ |
| B-2 | | 【所有者】情報の所有者は誰か？ |
| B-3 | | 【範囲】公開・提供可能な範囲は？ |
| B-4 | | 【漏えい】漏えい時の影響度は？ |
| B-5 | | 【改変】不正改変時の影響度は？ |
| B-6 | | 【取扱】閲覧のみか？変更が発生するか？ |
| B-7 | | 【保存】システム内に保存するか？ |
| B-8 | | 【検証】完全性の事後検証は必要か？ |
| C-1 | 利用環境・手段 | 【伝達手段】情報を送受信する方法は？ |
| C-2 | | 【処理環境】サーバ又は端末の種類は？ |
| C-3 | | 【通信環境】利用するネットワークは？ |
| C-4 | | 【通信環境】 遠隔操作は必要か？ |
| C-5 | | 【信頼性】異常停止の許容時間は？ |

# 5章 セキュリティ要件の策定 ／ 6章 その他の考慮事項

【判断条件による対策方針の検討】
1. 検討した業務要件に判断条件を適用する。
2. 判断条件が合致した対策要件は中位以上の実施を検討する。
（合致しない対策要件は低位又は省略を検討する）

【対策要件の決定及び調達仕様書への反映】
1. 対策要件集の「実施レベル選定の考え方」を参考にして、実施レベルの最終決定を行う。
2. 対策要件集の「仕様書記載時の注意事項」を参考にして、調達仕様書に記載する。

## ステップ5．対策方針の検討（判断条件をあてはめる）

6種類の判断条件

| 名称 | 観点分類 | 判断条件 |
|---|---|---|
| A. 外部アクセスの有無 | 利用環境・手段 | インターネット等の通信回線を介して（情報の管理ポリシが異なる）外部から情報システムにアクセスしてサービスの利用、業務の遂行、情報システムの管理等を行うか。 |
| B. 情報の重要度 | 情報 | 漏えいした場合や正常にアクセスできない場合に、深刻な損害を被る可能性がある重要性の高い情報を取り扱うか。 |
| ： | ： | ： |
| F. 複数部局による利用 | 主体 | 情報の取り扱い方や利用目的等が異なる複数の部局等の間で共用されるか。 |

## ステップ6．対策要件の決定（実施レベルを検討する）

24種類の対策要件

| 対策区分 | 対策方針 | 対策要件 | 判断条件 | 実施レベル | | |
|---|---|---|---|---|---|---|
| | | | | 低位 | 中位 | 高位 |
| 侵害対策（AT：Attack） | 通信回線対策（AT-1） | AT-1-1 | A or F | | 有 | 有 |
| | | AT-1-2 | A | | 有 | |
| | | AT-1-3 | | | 有 | 有 |
| | | AT-1-4 | | | 有 | 有 |
| | 不正プログラム対策（AT-2） | AT-2-1 | － | 有 | | |
| | | AT-2-2 | A or B | | | 有 |
| | セキュリティホール対策（AT-3） | AT-3-1 | － | 有 | | |
| | | AT-3-2 | A | 有 | 有 | |
| ： | | ： | ： | ： | ： | ： |

AまたはFの判断条件が合致すれば中位以上

判断条件AもBも合致しなければ低位または省略

判断条件の指定がない場合は低位または省略

### 対策要件集（対策要件の解説の構成）