【パブリックコメント】

情報システムに係る政府調達における
セキュリティ要件策定マニュアル（案）

【付録C. マニュアル活用例】

2011 年 1 月 31 日

目次

1章　ワークシート 3
1.1 目的及び業務の洗い出し（ステップ1）のためのワークシート 3
1.2 業務の特徴の整理（ステップ2）のためのワークシート 3
1.3 システム概要図の作成（ステップ3）のためのワークシート 4
1.4 定型設問による業務要件の詳細化（ステップ4）のためのワークシート 5
1.5 判断条件による対策方針の検討（ステップ5）のためのワークシート 6
1.6 対策要件の決定（ステップ6）のためのワークシート 7
1.7 調達仕様書への反映（ステップ7）のためのワークシート 8

2章　活用例 10
2.1 行政情報提供システム 10
2.2 国民参加型政策立案システム 21
2.3 電子申請・届出システム 33

1章 ワークシート

以下の各ワークシートは、本マニュアルの各ステップにおいて検討結果を記入及び整理するためのものである。2 章では具体的な情報システムの題材に、各ワークシートの記入例を示す。

1.1 目的及び業務の洗い出し(ステップ 1)のためのワークシート

項目	内容
名称	
目的	
業務	(1) (2) (3)

1.2 業務の特徴の整理(ステップ 2)のためのワークシート

主体	業務	業務 (細分化後)	業務(細分化後)の概要	情報	利用環境・手段

1.3 システム概要図の作成(ステップ 3)のためのワークシート

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

1.4 定型設問による業務要件の詳細化（ステップ 4）のためのワークシート

ID	観点	設問	回答
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】 システム所管部署との関係は？	
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】 外部からの遠隔利用は必要か？	
C-5		【信頼性】 異常停止の許容時間は？	

1.5 判断条件による対策方針の検討(ステップ 5)のためのワークシート

名称	観点分類	判断条件	判断結果
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。	
C. 情報受信後の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保存する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか。	
D. 利用者の限定要否	主体	情報システムにアクセスする主体は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか。	
E. アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか。	
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。	

1.6 対策要件の決定（ステップ 6）のためのワークシート

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

※　各対策要件の「実施レベル」欄について、決定した実施レベルに対応する空白箇所に「○」を記入すること。

1.7 調達仕様書への反映（ステップ 7）のためのワークシート

大項目		小項目	記載内容
1	調達件名	情報システムに係る工程名	*（※ ステップ 1 の検討結果のうち「名称」を反映）*
2	作業の概要	(1) 目的	*（※ ステップ 1 の検討結果のうち「目的」を反映）*
		(2) 用語の定義	
		(3) 業務の概要	*（※ ステップ 2 及びステップ 4 の結果を反映）*
		(4) 情報システム化の範囲	
		(5) 作業内容・納入成果物	
3	情報システムの要件	(1) 機能要件	
		(2) 画面要件	
		(3) 帳票要件	
		(4) 情報・データ要件	
		(5) 外部インタフェース要件	
4	規模・性能要件	(1) 規模要件	
		(2) 性能要件	
5	信頼性等要件	(1) 信頼性要件	*（※ 対策要件 DA-2-1 を求める場合に記入）*
		(2) 拡張性要件	
		(3) 上位互換性要件	
		(4) システム中立性要件	
		(5) 事業継続性要件	
6	情報セキュリティ要件	(1) 権限要件	*（※ 対策要件 AT-1、AT-2、AU-1、AU-2、AC-1、AC-2、PR-1、DA-1-1 を求める場合に記入）*
		(2) 情報セキュリティ対策	
7	情報システム稼働環境	(1) 全体構成	*（※ ステップ 3 にて作成したシステム概要図を記載）*
		(2) ハードウェア構成	
		(3) ソフトウェア構成	
		(4) ネットワーク構成	
		(5) アクセシビリティ要件	
8	テスト要件定義	要求仕様の適合性を検証するためのテストに係る要件	*（※ 対策要件 AT-3-1 を求める場合に記入）*

【パブリックコメント】

大項目		小項目	記載内容
9	移行要件定義	(1) 移行に係る要件	
		(2) 教育に係る要件	
10	運用要件定義	(1) システム操作・監視等要件	
		(2) データ管理要件	
		(3) 運用施設・設備要件	*(※ 対策要件 PH-1 を求める場合に記入)*
11	保守要件定義	(1) ソフトウェア保守要件	*(※ 対策要件 AT-3-2 を求める場合に記入)*
		(2) ハードウェア保守要件	
12	作業の体制及び方法	(1) 作業体制	
		(2) 開発方法	
		(3) 導入	
		(4) 瑕疵担保責任	
13	特記事項	その他、特記すべき要件	
14	妥当性証明	調達仕様書の妥当性を確認した調達担当課室の長の氏名	

2章 活用例

2.1 行政情報提供システム

2.1.1 目的及び業務の洗い出し(ステップ 1)

項目	内容
名称	行政情報提供システム
目的	インターネットを経由して A 省の行政情報を、国民に提供するしくみを確立すること
業務	(1) 「国民」が、「行政情報提供システム」から行政情報を取得 (2) 「事務局」が、「行政情報提供システム」に行政情報を登録 (3) 「事務局」が、「行政情報提供システム」の閲覧傾向の把握と、システムの運用と管理

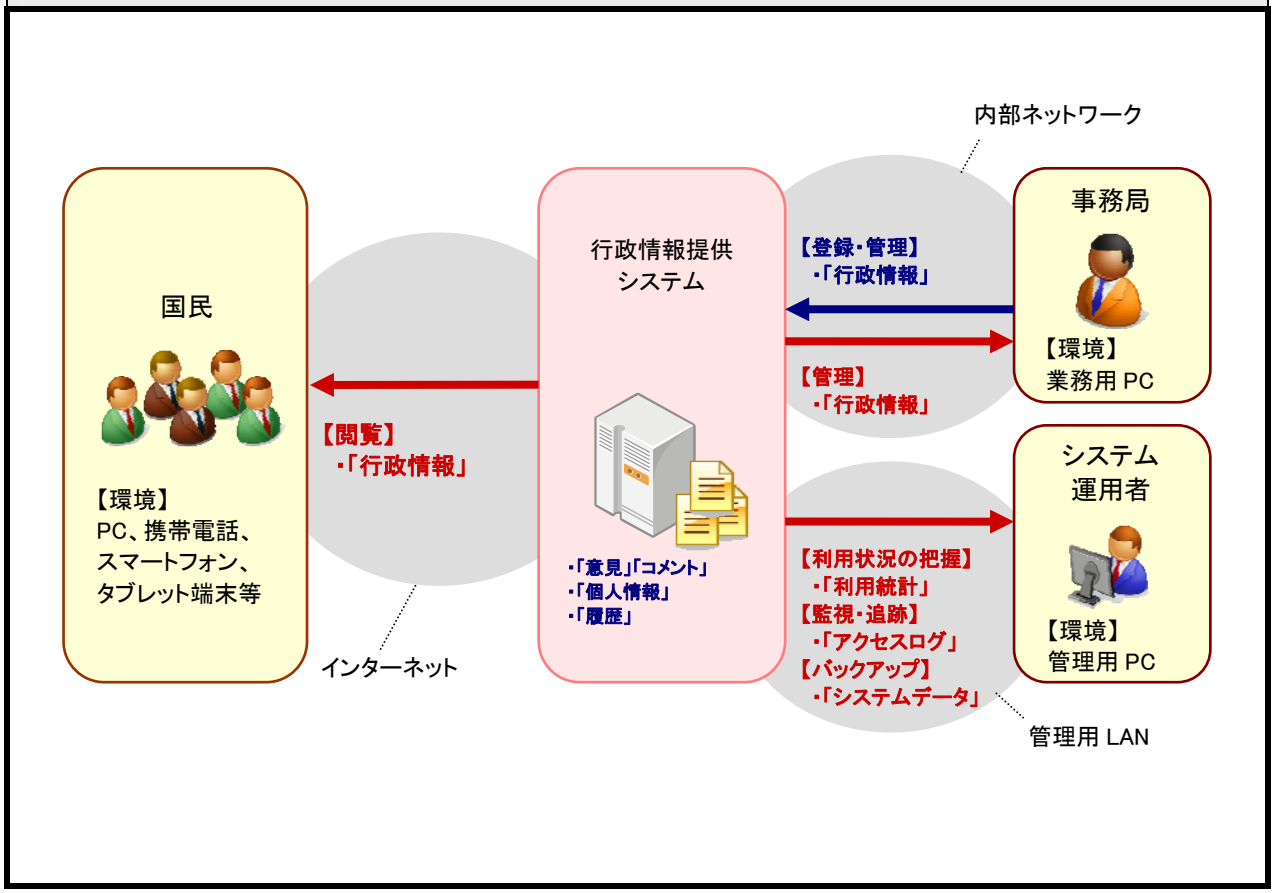
2.1.2 業務の特徴の整理(ステップ 2)

主体	業務	業務 (細分化後)	業務(細分化後)の概要	情報	利用環境・手段
国民	行政情報の閲覧	閲覧	行政情報を表示し、内容を確認する。	「行政情報」	インターネット、PC、携帯電話、スマートフォン、タブレット端末
事務局	行政情報の登録	登録	サーバにコンテンツ(行政情報)を登録する。	「行政情報」	内部ネットワーク、業務用 PC
		管理	サーバに登録済みのコンテンツ(行政情報)を更新及び削除する。	「行政情報」	
システム管理者	閲覧傾向の把握と、システムの運用と管理	利用状況の把握	利用者のアクセスした日時及び対象に関するログ等の集計を行う。	「利用統計」(Web サイトのページ毎のアクセス頻度の統計情報)	管理用 LAN、管理用 PC
		不正利用及び障害の監視、追跡	アクセス状況の監視及びログ等を元にした原因究明を行う。	「アクセスログ」	
		システムのバックアップと復旧	システムのデータを定期的にバックアップ及び障害時の復旧を行う。	「システムデータ」	

2.1.3 システム概要図の作成（ステップ 3）

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

システム概要図



2.1.4 定型設問による業務要件の詳細化（ステップ 4）

（国民）

ID	観点	設問	回答
A-1	主体	【数量】 おおよその人数規模は？	100 万人程度
A-2		【主体分類】 主体の分類は？	国民
A-3		【集合特性】 特定か不特定か？	不特定（匿名性あり）
A-4		【所属】 システム所管部署との関係は？	府省庁外
A-5		【頻度】 1人あたりのアクセス頻度は？	年に数回程度
A-6		【利用時間】 1日の主な利用時間帯は？	特定できない（24 時間）
A-7		【信頼性】 役割どおりに振る舞えるか？	誤操作が発生しやすい（マニュアル等を読まない）
B-1	情報	【数量】 おおよそのデータ量は？	「行政情報」: 数百 KB～数十 MB 程度
B-2		【所有者】 情報の所有者は誰か？	「行政情報」: システム所管部署
B-3		【範囲】 公開・提供可能な範囲は？	「行政情報」: 公開
B-4		【漏えい】 漏えい時の影響度は？	「行政情報」: なし
B-5		【改変】 不正改変時の影響度は？	「行政情報」: 行政の信頼が損なわれる
B-6		【取扱】 閲覧のみか？変更が発生するか？	変更あり
B-7		【保存】 システム内に保存するか？	サーバ内に保存（保存期限あり）
B-8		【検証】 完全性の事後検証は必要か？	不要
C-1	利用環境・手段	【伝達手段】 情報を送受信する方法は？	Web ブラウザ
C-2		【処理環境】 サーバ又は端末の種類は？	PC、携帯電話、スマートフォン等
C-3		【通信環境】 利用するネットワークは？	インターネット
C-4		【通信環境】 外部からの遠隔利用は必要か？	必要
C-5		【信頼性】 異常停止の許容時間は？	半日程度

【パブリックコメント】

（事務局）

ID	観点	設問	回答
A-1	主体	【数量】 おおよその人数規模は？	数名程度
A-2		【主体分類】 主体の分類は？	事務局
A-3		【集合特性】 特定か不特定か？	特定（匿名性なし）
A-4		【所属】 システム所管部署との関係は？	システム所管部署に所属している
A-5		【頻度】 1人あたりのアクセス頻度は？	1日1回程度
A-6		【利用時間】 1日の主な利用時間帯は？	24 時間
A-7		【信頼性】 役割どおりに振る舞えるか？	運用規定に従って確実な操作を行える（ほぼ確実に役割どおりに振る舞える）
B-1	情報	【数量】 おおよそのデータ量は？	「行政情報」: 数百 KB～数 MB 程度
B-2		【所有者】 情報の所有者は誰か？	「行政情報」: システム所管部署
B-3		【範囲】 公開・提供可能な範囲は？	「行政情報」: 公開
B-4		【漏えい】 漏えい時の影響度は？	「行政情報」: なし
B-5		【改変】 不正改変時の影響度は？	「行政情報」: 行政の信頼が損なわれる
B-6		【取扱】 閲覧のみか？変更が発生するか？	変更あり
B-7		【保存】 システム内に保存するか？	サーバ内に保存（保存期限あり）
B-8		【検証】 完全性の事後検証は必要か？	不要
C-1	利用環境・手段	【伝達手段】 情報を送受信する方法は？	条件なし
C-2		【処理環境】 サーバ又は端末の種類は？	条件なし
C-3		【通信環境】 利用するネットワークは？	内部ネットワーク
C-4		【通信環境】 外部からの遠隔利用は必要か？	不要
C-5		【信頼性】 異常停止の許容時間は？	半日程度

（システム管理者）

ID	観点	設問	回答
A-1	主体	【数量】 おおよその人数規模は？	数名程度
A-2		【主体分類】 主体の分類は？	システム管理者
A-3		【集合特性】 特定か不特定か？	特定（匿名性なし）
A-4		【所属】 システム所管部署との関係は？	システム所管部署に所属している
A-5		【頻度】 1人あたりのアクセス頻度は？	月1回程度（月例の保守業務を想定）
A-6		【利用時間】 1日の主な利用時間帯は？	24 時間
A-7		【信頼性】 役割どおりに振る舞えるか？	運用規定に従って確実な操作を行える（ほぼ確実に役割どおりに振る舞える）
B-1	情報	【数量】 おおよそのデータ量は？	「利用統計」「アクセスログ」「システムデータ」： 不明
B-2		【所有者】 情報の所有者は誰か？	「利用統計」「アクセスログ」「システムデータ」： システム所管部署
B-3		【範囲】 公開・提供可能な範囲は？	「利用統計」「アクセスログ」「システムデータ」： 非公開
B-4		【漏えい】 漏えい時の影響度は？	「利用統計」「アクセスログ」「システムデータ」： 国民からの信頼が損なわれる
B-5		【改変】 不正改変時の影響度は？	「利用統計」「アクセスログ」「システムデータ」：国民からの信頼が損なわれる
B-6		【取扱】 閲覧のみか？変更が発生するか？	「利用統計」「アクセスログ」： 閲覧のみ 「システムデータ」： 変更あり
B-7		【保存】 システム内に保存するか？	サーバ内に保存
B-8		【検証】 完全性の事後検証は必要か？	不要
C-1	利用環境・手段	【伝達手段】 情報を送受信する方法は？	条件なし
C-2		【処理環境】 サーバ又は端末の種類は？	条件なし
C-3		【通信環境】 利用するネットワークは？	内部ネットワーク
C-4		【通信環境】 外部からの遠隔利用は必要か？	不要
C-5		【信頼性】 異常停止の許容時間は？	半日程度

2.1.5 判断条件による対策方針の検討（ステップ 5）

名称	観点分類	判断条件	判断結果
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。	×
C. 情報受信後の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保存する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか。	×
D. 利用者の限定要否	主体	情報システムにアクセスする主体は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか。	×
E. アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか。	×
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。	×

2.1.6 対策要件の決定(ステップ 6)

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

※ 各対策要件の「実施レベル」欄について、決定した実施レベルに対応する空白箇所に「○」を記入すること。

2.1.7 調達仕様書への反映（ステップ 7）

大項目		小項目	記載内容
1	調達件名	情報システムに係る工程名	行政情報提供システム
2	作業の概要	(1) 目的	インターネットを経由して A 省の行政情報を、国民に提供するしくみを確立すること
		(2) 用語の定義	
		(3) 業務の概要	【業務内容】 国民 ・ 行政情報を表示し、内容を確認する。 事務局 ・ サーバにコンテンツ（行政情報）を登録する。 ・ サーバに登録済みのコンテンツ（行政情報）を更新及び削除する。 システム管理者 ・ 利用者のアクセスした日時及び対象に関するログ等の集計を行う。 ・ アクセス状況の監視及びログ等を元にした原因究明を行う。 ・ システムのデータを定期的にバックアップ及び障害時の復旧を行う。 【業務特性】 ・ 主たる利用者は、最大 100 万人程度の不特定多数の国民であり、1人あたり年に数回程度のアクセスが想定され、1日の主な利用時間帯は特定できない。 ・ 行政情報はWebにより原則公開可能な情報のみを提供し、1度の閲覧（1ページあたり）のデータ量は数百 KB から数十 MB 程度を想定する。 ・ 国民はインターネットを介して、標準的な PC、携帯電話、スマートフォン等によってアクセスし、各機器が備える標準的な Web ブラウザを利用する。
		(4) 情報システム化の範囲	
		(5) 作業内容・納入成果物	
3	情報システムの要件	(1) 機能要件	
		(2) 画面要件	
		(3) 帳票要件	
		(4) 情報・データ要件	
		(5) 外部インタフェース要件	
4	規模・性能要件	(1) 規模要件	
		(2) 性能要件	
5	信頼性等要件	(1) 信頼性要件	・ サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として半日程度

【パブリックコメント】

大項目		小項目	記載内容
			を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。
		(2) 拡張性要件	
		(3) 上位互換性要件	
		(4) システム中立性要件	
		(5) 事業継続性要件	
6	情報セキュリティ要件	(1) 権限要件	(通信回線対策) ・ 不正の防止及び発生時の影響範囲を限定するため、所属する府省庁とは情報の管理ポリシが異なる外部と通信を行う電子計算機及び内部のみと通信を行う電子計算機を通信回線上で分離すること。 ・ 通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。 ・ 情報システムのなりすましを防止するために、サーバの認証機能を備えること。 ・ サービスの継続性を確保するため、構成機器が備えるサービス停止の脅威の軽減に有効な機能を活用して情報システムを構築すること。 (不正プログラム対策) ・ マルウェア(ウィルス、ワーム、ボット等)による脅威に備えるため、マルウェアの感染を防止する機能を備えるとともに、新たに発見されるマルウェアに対応するために機能の更新が可能であること。 (証跡管理) ・ 情報システムに対する不正の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関する証跡を蓄積し、2 年間の期間保管すること。 ・ 証跡の不当な消去や改ざんを防止するため、証跡に関するアクセス制御機能を備えること。 ・ 不正行為の追跡や情報セキュリティ侵害時において証跡の解析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。 (不正監視) ・ 不正行為を迅速に対処するため、通信回線を介して所属する府省庁外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。 (アカウント管理) ・ アカウント管理者による不正を防止するため、アカウントの管理権限を制御する機能を備えること。 (構成管理) ・ 障害・事故等の発生要因を減らすとともに、障害・事故等の発生時には迅速に対処するため、構築時の情報システムの構成(ハードウェア、ソフトウェア及びサービス構成に関する詳細情報)が記載された文書を提出するとともに、文書どおりの構成とすること。
		(2) 情報セキュリティ対策	

【パブリックコメント】

大項目		小項目	記載内容
7	情報システム稼働環境	(1) 全体構成	*～ 略 ～（作成したシステム概要図を記載）*
		(2) ハードウェア構成	
		(3) ソフトウェア構成	
		(4) ネットワーク構成	
		(5) アクセシビリティ要件	
8	テスト要件定義	要求仕様の適合性を検証するためのテストに係る要件	・ 情報システムを構成するソフトウェア及びハードウェアの脆弱性に悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。
9	移行要件定義	(1) 移行に係る要件	
		(2) 教育に係る要件	
10	運用要件定義	(1) システム操作・監視等要件	
		(2) データ管理要件	
		(3) 運用施設・設備要件	・ 情報の漏えいを防止するため、記憶装置の設置時のロック及び暗号化等によって、情報搾取行為を防止・検知するための機能を備えること。 ・ 物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、安全区域に設置可能な設計とすること。
11	保守要件定義	(1) ソフトウェア保守要件	・ 運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。
		(2) ハードウェア保守要件	
12	作業の体制及び方法	(1) 作業体制	
		(2) 開発方法	
		(3) 導入	
		(4) 瑕疵担保責任	
13	特記事項	その他、特記すべき要件	
14	妥当性証明	調達仕様書の妥当性を確認した調達担当課室の長の氏名	

2.2 国民参加型政策立案システム

2.2.1 目的及び業務の洗い出し(ステップ 1)

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

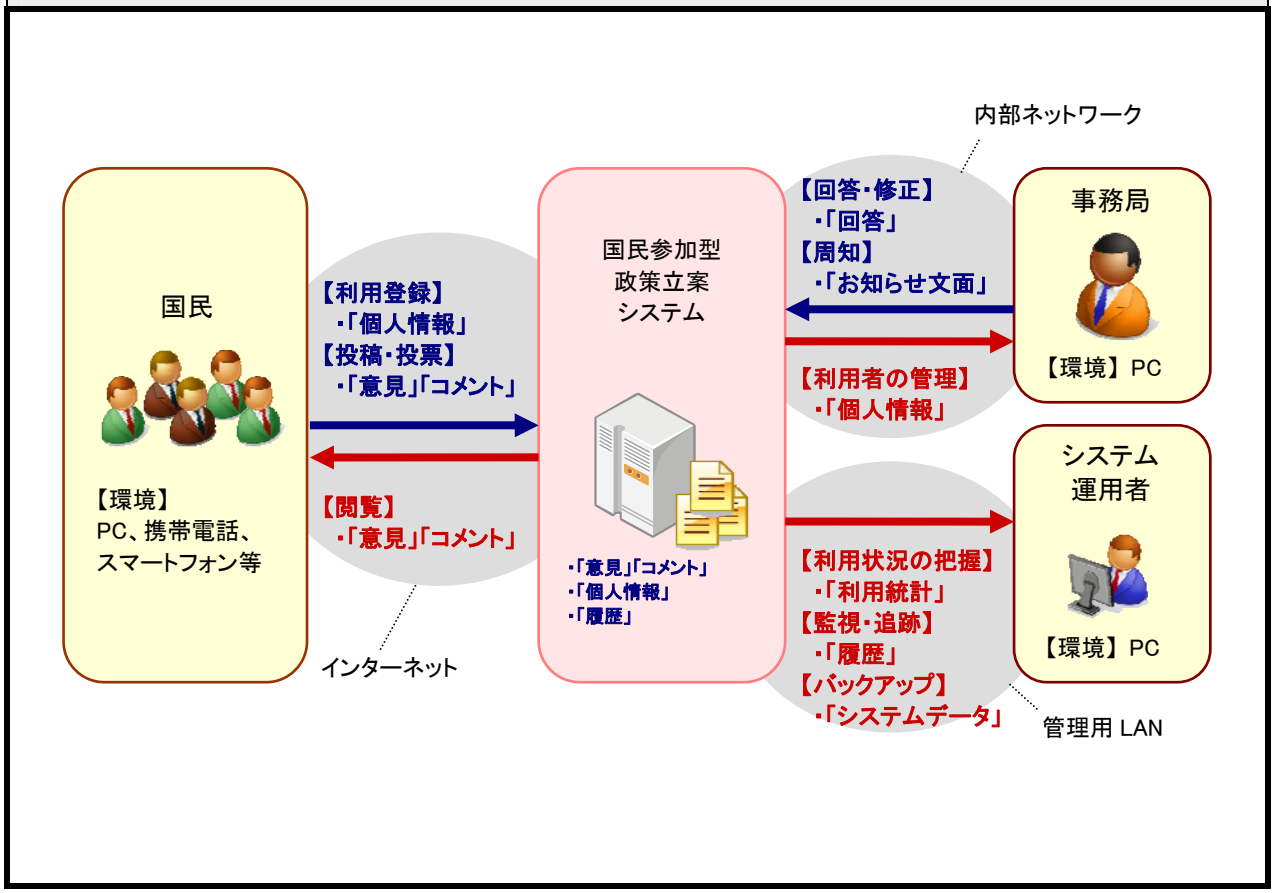
2.2.2 業務の特徴の整理(ステップ 2)

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

2.2.3 システム概要図の作成（ステップ 3）

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

システム概要図



2.2.4 定型設問による業務要件の詳細化（ステップ 4）

（国民）

ID	観点	設問	回答
A-1	主体	【数量】 おおよその人数規模は？	1 万人程度
A-2		【主体分類】 主体の分類は？	国民
A-3		【集合特性】 特定か不特定か？	特定（匿名性あり）
A-4		【所属】 システム所管部署との関係は？	府省庁外
A-5		【頻度】 1人あたりのアクセス頻度は？	週に1回程度
A-6		【利用時間】 1日の主な利用時間帯は？	特定できない（24 時間）
A-7		【信頼性】 役割どおりに振る舞えるか？	誤操作が発生しやすい（マニュアル等を読まない）
B-1	情報	【数量】 おおよそのデータ量は？	「個人情報」: 200 文字程度 「意見・コメント」: 1000 文字程度
B-2		【所有者】 情報の所有者は誰か？	「個人情報」: 国民（本人） 「意見・コメント」: 投稿者
B-3		【範囲】 公開・提供可能な範囲は？	「個人情報」: 非公開 「意見・コメント」: 公開
B-4		【漏えい】 漏えい時の影響度は？	「個人情報」: 利用者に精神的苦痛を与える可能性 「意見・コメント」: なし
B-5		【改変】 不正改変時の影響度は？	「個人情報」: サービス利用に支障 「意見・コメント」: なし
B-6		【取扱】 閲覧のみか？変更が発生するか？	変更あり
B-7		【保存】 システム内に保存するか？	サーバ内に保存（保存期限あり）
B-8		【検証】 完全性の事後検証は必要か？	不要
C-1	利用環境・手段	【伝達手段】 情報を送受信する方法は？	Web ブラウザ
C-2		【処理環境】 サーバ又は端末の種類は？	PC、携帯電話、スマートフォン
C-3		【通信環境】 利用するネットワークは？	インターネット
C-4		【通信環境】 外部からの遠隔利用は必要か？	必要
C-5		【信頼性】 異常停止の許容時間は？	半日程度

（事務局）

ID	観点	設問	回答
A-1	主体	【数量】 おおよその人数規模は？	数名程度
A-2		【主体分類】 主体の分類は？	事務局
A-3		【集合特性】 特定か不特定か？	特定（匿名性なし）
A-4		【所属】 システム所管部署との関係は？	システム所管部署に所属している
A-5		【頻度】 1人あたりのアクセス頻度は？	1日1回程度
A-6		【利用時間】 1日の主な利用時間帯は？	24 時間
A-7		【信頼性】 役割どおりに振る舞えるか？	誤操作はあまり発生しない（役割どおりに振る舞えることが多い）
B-1	情報	【数量】 おおよそのデータ量は？	「回答」「お知らせ文面」: 1000 文字程度 「個人情報」: 200 文字程度
B-2		【所有者】 情報の所有者は誰か？	「回答」「お知らせ文面」: 事務局 「個人情報」: 国民（本人）
B-3		【範囲】 公開・提供可能な範囲は？	「回答」「お知らせ文面」: 公開 「個人情報」: 非公開
B-4		【漏えい】 漏えい時の影響度は？	「回答」「お知らせ文面」: なし 「個人情報」: 利用者に精神的苦痛を与える可能性
B-5		【改変】 不正改変時の影響度は？	「個人情報」: サービス利用に支障 「回答」「お知らせ文面」: なし
B-6		【取扱】 閲覧のみか？変更が発生するか？	変更あり
B-7		【保存】 システム内に保存するか？	サーバ内に保存（保存期限あり）
B-8		【検証】 完全性の事後検証は必要か？	不要
C-1	利用環境・手段	【伝達手段】 情報を送受信する方法は？	Web ブラウザ
C-2		【処理環境】 サーバ又は端末の種類は？	PC
C-3		【通信環境】 利用するネットワークは？	内部ネットワーク
C-4		【通信環境】 外部からの遠隔利用は必要か？	不要
C-5		【信頼性】 異常停止の許容時間は？	半日程度

（システム管理者）

ID	観点	設問	回答
A-1	主体	【数量】 おおよその人数規模は？	数名程度
A-2		【主体分類】 主体の分類は？	システム管理者
A-3		【集合特性】 特定か不特定か？	特定（匿名性なし）
A-4		【所属】 システム所管部署との関係は？	システム所管部署に所属している
A-5		【頻度】 1人あたりのアクセス頻度は？	1日1回程度
A-6		【利用時間】 1日の主な利用時間帯は？	24 時間
A-7		【信頼性】 役割どおりに振る舞えるか？	運用規定に従って確実な操作を行える（ほぼ確実に役割どおりに振る舞える）
B-1	情報	【数量】 おおよそのデータ量は？	「利用統計」「履歴」「システムデータ」： 不明
B-2		【所有者】 情報の所有者は誰か？	「利用統計」「履歴」「システムデータ」： システム所管部署
B-3		【範囲】 公開・提供可能な範囲は？	「利用統計」「履歴」「システムデータ」： 非公開
B-4		【漏えい】 漏えい時の影響度は？	「利用統計」「履歴」「システムデータ」：国民からの信頼が損なわれる
B-5		【改変】 不正改変時の影響度は？	「利用統計」「履歴」「システムデータ」：国民からの信頼が損なわれる
B-6		【取扱】 閲覧のみか？変更が発生するか？	「利用統計」「履歴」： 閲覧のみ 「システムデータ」： 変更あり
B-7		【保存】 システム内に保存するか？	サーバ内に保存
B-8		【検証】 完全性の事後検証は必要か？	不要
C-1	利用環境・手段	【伝達手段】 情報を送受信する方法は？	条件なし
C-2		【処理環境】 サーバ又は端末の種類は？	条件なし
C-3		【通信環境】 利用するネットワークは？	内部ネットワーク
C-4		【通信環境】 外部からの遠隔利用は必要か？	不要
C-5		【信頼性】 異常停止の許容時間は？	半日程度

2.2.5 判断条件による対策方針の検討（ステップ 5）

名称	観点分類	判断条件	判断結果
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。	○
C. 情報受信後の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保存する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか。	×
D. 利用者の限定要否	主体	情報システムにアクセスする主体は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか。	○
E. アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか。	×
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。	×

2.2.6 対策要件の決定(ステップ 6)

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

※ 各対策要件の「実施レベル」欄について、決定した実施レベルに対応する空白箇所に「○」を記入すること。

2.2.7 調達仕様書への反映(ステップ 7)

大項目		小項目	記載内容
1	調達件名	情報システムに係る工程名	国民参加型政策立案システム
2	作業の概要	(1) 目的	インターネットを活用して政策に関する提案・意見を国民から広く募り、参加者同士による議論及び投票等によって、国民参加による政策立案のしくみを確立すること。
		(2) 用語の定義	
		(3) 業務の概要	【業務内容】 国民 ・ 個人情報を登録して、サービスの利用資格を得る。 ・ 新規の意見や他者の意見に対するコメントの投稿及び投票を行う。 ・ 意見やコメントを検索し、閲覧する。 事務局 ・ 意見に対する事務局回答の投稿及び不適切な意見の削除を行う。 ・ サービス停止や注意事項等の利用者に対する周知を行う。 ・ 利用者の登録情報の確認、修正、等の管理業務を行う。 システム管理者 ・ 利用者の登録状況、アクセス状況、意見やコメントの集計を行う。 ・ アクセス状況の監視及びログ等を元にした原因究明を行う。 ・ システムのデータを定期バックアップ及び障害時の復旧を行う。 【業務特性】 ・ 主たる利用者は、最大 1 万人程度の特定の国民であり、利用者登録を行った上で、1人あたり週に 1 回程度のアクセスが想定され、1日の主な利用時間帯は特定できない。 ・ 意見・コメントは Web により投稿するものとし原則公開とする。意見・コメントの 1 件のデータ量は 1000 文字程度を想定する。 ・ 国民はインターネットを介して、標準的な PC、携帯電話、スマートフォン等によってアクセスし、各機器が備える標準的な Web ブラウザを利用する。
		(4) 情報システム化の範囲	
		(5) 作業内容・納入成果物	
3	情報システムの要件	(1) 機能要件	
		(2) 画面要件	
		(3) 帳票要件	
		(4) 情報・データ要件	

【パブリックコメント】

大項目		小項目	記載内容
		(5) 外部インタフェース要件	
4	規模・性能要件	(1) 規模要件	
		(2) 性能要件	
5	信頼性等要件	(1) 信頼性要件	・ サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として半日程度を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。
		(2) 拡張性要件	
		(3) 上位互換性要件	
		(4) システム中立性要件	
		(5) 事業継続性要件	
6	情報セキュリティ要件	(1) 権限要件	（通信回線対策） ・ 不正の防止及び発生時の影響範囲を限定するため、所属する府省庁とは情報の管理ポリシが異なる外部と通信を行う電子計算機及び内部のみと通信を行う電子計算機を通信回線上で分離すること。 ・ 通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。 ・ 情報システムのなりすましを防止するために、サーバの認証機能を備えること。 ・ サービスの継続性を確保するため、構成機器が備えるサービス停止の脅威の軽減に有効な機能を活用して情報システムを構築すること。 （不正プログラム対策） ・ マルウェア（ウィルス、ワーム、ボット等）による脅威に備えるため、マルウェアの感染を防止する機能を備えるとともに、新たに発見されるマルウェアに対応するために機能の更新が可能であること。 （証跡管理） ・ 情報システムに対する不正の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関する証跡を蓄積し、2 年間の期間保管すること。 ・ 証跡の不当な消去や改ざんを防止するため、証跡に関するアクセス制御機能を備えること。 ・ 不正行為の追跡や情報セキュリティ侵害時において証跡の解析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。 （不正監視） ・ 不正行為を迅速に対処するため、通信回線を介して所属する府省庁外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。 （主体認証） ・ 情報システムによるサービスを許可された者のみに提
		(2) 情報セキュリティ対策	

【パブリックコメント】

大項目		小項目	記載内容
			供するため、情報システムにアクセスする主体のうち国民の認証を行う機能として、ID パスワード認証を採用すること。 （アカウント管理） ・ アカウント管理者による不正を防止するため、アカウントの管理権限を制御する機能を備えること。 （データ保護） ・ 通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。 ・ 情報システムに蓄積された情報の搾取や漏えいを防止するため、保護すべき情報を利用者が直接アクセス可能な機器に保存しないこと。 （構成管理） ・ 障害・事故等の発生要因を減らすとともに、障害・事故等の発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。
7	情報システム稼働環境	(1) 全体構成	*（ステップ 3 にて作成したシステム概要図を記載）*
		(2) ハードウェア構成	
		(3) ソフトウェア構成	
		(4) ネットワーク構成	
		(5) アクセシビリティ要件	
8	テスト要件定義	要求仕様の適合性を検証するためのテストに係る要件	・ 情報システムを構成するソフトウェア及びハードウェアの脆弱性に悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。
9	移行要件定義	(1) 移行に係る要件	
		(2) 教育に係る要件	
10	運用要件定義	(1) システム操作・監視等要件	
		(2) データ管理要件	
		(3) 運用施設・設備要件	・ 情報の漏えいを防止するため、記憶装置の設置時のロック及び暗号化等によって、情報搾取行為を防止・検知するための機能を備えること。 ・ 物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、安全区域に設置可能な設計とすること。
11	保守要件定義	(1) ソフトウェア保守要件	・ 運用開始後、新たに発見される脆弱性を悪用した不正

【パブリックコメント】

大項目		小項目	記載内容
		(2) ハードウェア保守要件	を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。
12	作業の体制及び方法	(1) 作業体制	
		(2) 開発方法	
		(3) 導入	
		(4) 瑕疵担保責任	
13	特記事項	その他、特記すべき要件	
14	妥当性証明	調達仕様書の妥当性を確認した調達担当課室の長の氏名	

2.3 電子申請・届出システム

2.3.1 目的及び業務の洗い出し（ステップ 1）

項目	内容
名称	電子申請・届出システム
目的	インターネットを活用し、 自宅等の身近な場所から各種申請・届出の手続き等を可能にすることで、利用者の利便性の向上を図るとともに、B 省における事務処理の簡素化と効率化を図ること。
業務	(1) 「国民」が、「電子申請・届出システム」に申請等の手続きをする (2) 「事務局」が、「電子申請・届出システム」で承認等の手続きをする

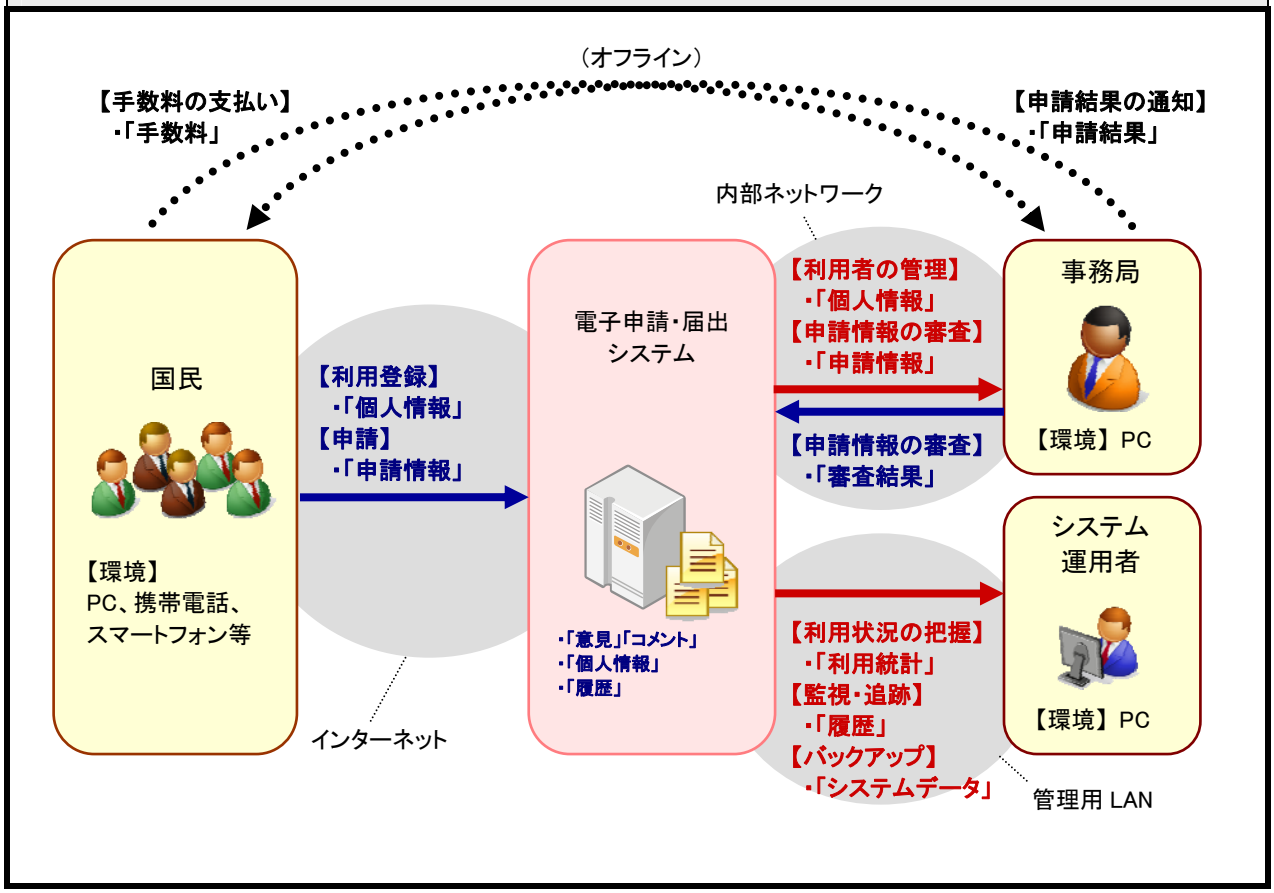
2.3.2 業務の特徴の整理(ステップ 2)

主体	業務	業務（細分化後）	業務(細分化後)の概要	情報	利用環境・手段
国民	申請を行う	利用登録	個人情報を登録して、サービス利用資格を得る	「個人情報」	PC、携帯電話、スマートフォン、インターネット
		申請	申請情報を入力して提出する	「申請情報」	
		手数料の支払い	申請等に必要な手数料を支払う	「手数料」	オフラインでの実施
事務局	申請	利用者の管理	システムの利用者を追加、修正、削除する	「個人情報」	PC、内部ネットワーク
		申請情報の審査	申請情報の正当性を確認して審査を行う	「申請情報」 「審査結果」	
		申請結果の通知	申請に応じた事務処理を行い、結果を通知する	「申請結果」	オフラインでの実施
システム管理者	情報システムの利用状況の把握及び管理	利用状況の把握	利用者の登録状況、アクセス状況を集計する	「利用統計」	PC、管理用 LAN
		不正利用及び障害の監視、追跡	利用者のアクセス状況の監視及びログ等を元にした原因究明を行う。	「アクセスログ」	
		システムのバックアップと復旧	システムのデータを定期的にバックアップ及び障害時の復旧を行う。	「システムデータ」	

2.3.3 システム概要図の作成（ステップ 3）

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

システム概要図



2.3.4 定型設問による業務要件の詳細化（ステップ 4）

（国民）

ID	観点	設問	回答
A-1	主体	【数量】 おおよその人数規模は？	100万人程度
A-2		【主体分類】主体の分類は？	国民
A-3		【集合特性】特定か不特定か？	特定（匿名性なし）
A-4		【所属】システム所管部署との関係は？	府省庁外
A-5		【頻度】1人あたりのアクセス頻度は？	年に 1 回程度
A-6		【利用時間】1日の主な利用時間帯は？	特定できない（24 時間）
A-7		【信頼性】 役割どおりに振る舞えるか？	誤操作が発生しやすい（マニュアル等を読まない）
B-1	情報	【数量】 おおよそのデータ量は？	「個人情報」: 200 文字程度 「申請情報」: 1000 文字程度
B-2		【所有者】情報の所有者は誰か？	「個人情報」「申請情報」: 国民（本人）
B-3		【範囲】公開・提供可能な範囲は？	「個人情報」「申請情報」: 非公開
B-4		【漏えい】漏えい時の影響度は？	「個人情報」「申請情報」: 利用者に精神的苦痛を与える可能性あり
B-5		【改変】不正改変時の影響度は？	「個人情報」「申請情報」: 利用者に金銭的被害を与える可能性あり
B-6		【取扱】閲覧のみか？変更が発生するか？	変更あり
B-7		【保存】システム内に保存するか？	サーバ内に保存（保存期限あり）
B-8		【検証】完全性の事後検証は必要か？	不要
C-1	利用環境・手段	【伝達手段】情報を送受信する方法は？	Web ブラウザ
C-2		【処理環境】サーバ又は端末の種類は？	PC、携帯電話、スマートフォン
C-3		【通信環境】利用するネットワークは？	インターネット
C-4		【通信環境】 外部からの遠隔利用は必要か？	必要
C-5		【信頼性】異常停止の許容時間は？	半日程度

（事務局）

ID	観点	設問	回答
A-1	主体	【数量】 おおよその人数規模は？	数十名程度
A-2		【主体分類】 主体の分類は？	事務局
A-3		【集合特性】 特定か不特定か？	特定（匿名性なし）
A-4		【所属】 システム所管部署との関係は？	システム所管部署に所属している
A-5		【頻度】 1人あたりのアクセス頻度は？	1日あたり 100 回程度
A-6		【利用時間】 1日の主な利用時間帯は？	日中（9:00～17:30）
A-7		【信頼性】 役割どおりに振る舞えるか？	誤操作はあまり発生しない（役割どおりに振る舞えることが多い）
B-1	情報	【数量】 おおよそのデータ量は？	「個人情報」: 200 文字程度 「申請情報」: 1000 文字程度 「審査結果」: 200 文字程度
B-2		【所有者】 情報の所有者は誰か？	「個人情報」「申請情報」: 国民（本人）「審査結果」: 事務局
B-3		【範囲】 公開・提供可能な範囲は？	「個人情報」「申請情報」「審査結果」: 非公開
B-4		【漏えい】 漏えい時の影響度は？	「個人情報」「申請情報」「審査結果」: 利用者に精神的苦痛を与える可能性あり、国民からの信用が損なわれる
B-5		【改変】 不正改変時の影響度は？	「個人情報」「申請情報」「審査結果」: 利用者に金銭的被害を与える可能性あり、国民からの信用が損なわれる
B-6		【取扱】 閲覧のみか？変更が発生するか？	変更あり
B-7		【保存】 システム内に保存するか？	サーバ内に保存（保存期限あり）
B-8		【検証】 完全性の事後検証は必要か？	不要
C-1	利用環境・手段	【伝達手段】 情報を送受信する方法は？	Web ブラウザ
C-2		【処理環境】 サーバ又は端末の種類は？	PC
C-3		【通信環境】 利用するネットワークは？	内部ネットワーク
C-4		【通信環境】 外部からの遠隔利用は必要か？	不要
C-5		【信頼性】 異常停止の許容時間は？	半日程度

（システム管理者）

ID	観点	設問	回答
A-1	主体	【数量】 おおよその人数規模は？	数名程度
A-2		【主体分類】 主体の分類は？	システム管理者
A-3		【集合特性】 特定か不特定か？	特定（匿名性なし）
A-4		【所属】 システム所管部署との関係は？	システム所管部署に所属している
A-5		【頻度】 1人あたりのアクセス頻度は？	1日1回程度
A-6		【利用時間】 1日の主な利用時間帯は？	24 時間
A-7		【信頼性】 役割どおりに振る舞えるか？	運用規定に従って確実な操作を行える（ほぼ確実に役割どおりに振る舞える）
B-1	情報	【数量】 おおよそのデータ量は？	「利用統計」「アクセスログ」「システムデータ」： 不明
B-2		【所有者】 情報の所有者は誰か？	「利用統計」「アクセスログ」「システムデータ」： システム所管部署
B-3		【範囲】 公開・提供可能な範囲は？	「利用統計」「アクセスログ」「システムデータ」： 非公開
B-4		【漏えい】 漏えい時の影響度は？	「利用統計」「アクセスログ」「システムデータ」：国民からの信用が損なわれる
B-5		【改変】 不正改変時の影響度は？	「利用統計」「アクセスログ」「システムデータ」：国民からの信用が損なわれる
B-6		【取扱】 閲覧のみか？変更が発生するか？	「利用統計」「アクセスログ」： 閲覧のみ 「システムデータ」： 変更あり
B-7		【保存】 システム内に保存するか？	サーバ内に保存
B-8		【検証】 完全性の事後検証は必要か？	不要
C-1	利用環境・手段	【伝達手段】 情報を送受信する方法は？	条件なし
C-2		【処理環境】 サーバ又は端末の種類は？	条件なし
C-3		【通信環境】 利用するネットワークは？	内部ネットワーク
C-4		【通信環境】 外部からの遠隔利用は必要か？	不要
C-5		【信頼性】 異常停止の許容時間は？	半日程度

2.3.5 判断条件による対策方針の検討（ステップ 5）

名称	観点分類	判断条件	判断結果
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。	○
C. 情報受信後の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保存する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか。	○
D. 利用者の限定要否	主体	情報システムにアクセスする主体は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか。	○
E. アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか。	×
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。	×

2.3.6 対策要件の決定(ステップ 6)

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

※ 各対策要件の「実施レベル」欄について、決定した実施レベルに対応する空白箇所に「○」を記入すること。

2.3.7 調達仕様書への反映(ステップ 7)

大項目		小項目	記載内容
1	調達件名	情報システムに係る工程名	電子申請・届出システム
2	作業の概要	(1) 目的	インターネットを活用し、 自宅等の身近な場所から各種申請・届出の手続き等を可能にすることで、利用者の利便性の向上を図るとともに、B 省における事務処理の簡素化と効率化を図ること。
		(2) 用語の定義	
		(3) 業務の概要	【業務内容】 国民 ・ 個人情報を登録して、サービス利用資格を得る。 ・ 申請情報を入力して提出する。 ・ 申請等に必要な手数料を支払う。 事務局 ・ システムの利用者を追加、修正、削除する。 ・ 申請情報の正当性を確認して審査を行う。 ・ 申請に応じた事務処理を行い、結果を通知する。 システム管理者 ・ 利用者の登録状況、アクセス状況を集計する。 ・ 利用者のアクセス状況の監視及びログ等を元にした原因究明を行う。 ・ システムのデータを定期的にバックアップ及び障害時の復旧を行う。 【業務特性】 ・ 主たる利用者は、最大 100 万人程度の特定の国民であり、利用者登録を行った上で、1人あたり年に 1 回程度のアクセスが想定され、1日の主な利用時間帯は特定できない。 ・ 申請情報の送信、申請情報の審査ともに Web により行い申請情報 1 件あたりのデータ量は 1000 文字程度、審査結果は 200 文字程度を想定する。 ・ 国民はインターネットを介して、標準的な PC、携帯電話、スマートフォン等によってアクセスし、各機器が備える標準的な Web ブラウザを利用する。 ・ 手数料の支払いは銀行等による振込み、申請処理完了後の結果の通知は郵送により行う。
		(4) 情報システム化の範囲	
		(5) 作業内容・納入成果物	
3	情報システムの要件	(1) 機能要件	
		(2) 画面要件	
		(3) 帳票要件	
		(4) 情報・データ要件	
		(5) 外部インタフェース要件	

【パブリックコメント】

大項目		小項目	記載内容
4	規模・性能要件	(1) 規模要件	
		(2) 性能要件	
5	信頼性等要件	(1) 信頼性要件	・ サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として半日程度を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。
		(2) 拡張性要件	
		(3) 上位互換性要件	
		(4) システム中立性要件	
		(5) 事業継続性要件	
6	情報セキュリティ要件	(1) 権限要件	（通信回線対策） ・ 不正の防止及び発生時の影響範囲を限定するため、所属する府省庁とは情報の管理ポリシが異なる外部と通信を行う電子計算機及び内部のみと通信を行う電子計算機を通信回線上で分離すること。 ・ 通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。 ・ 情報システムのなりすましを防止するために、サーバの認証機能を備えること。 ・ サービスの継続性を確保するため、構成機器が備えるサービス停止の脅威の軽減に有効な機能を活用して情報システムを構築すること。 （不正プログラム対策） ・ マルウェア（ウィルス、ワーム、ボット等）による脅威に備えるため、マルウェアの感染を防止する機能を備えるとともに、新たに発見されるマルウェアに対応するために機能の更新が可能であること。 （証跡管理） ・ 情報システムに対する不正の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関する証跡を蓄積し、2 年間の期間保管すること。 ・ 証跡の不当な消去や改ざんを防止するため、証跡に関するアクセス制御機能を備えること。 ・ 不正行為の追跡や情報セキュリティ侵害時において証跡の解析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。 （不正監視） ・ 不正行為を迅速に対処するため、通信回線を介して所属する府省庁外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。 （主体認証） ・ 情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち国民の認証を行う機能として、ID パスワード認証を採用
		(2) 情報セキュリティ対策	

【パブリックコメント】

大項目		小項目	記載内容
			すること。 (アカウント管理) ・ アカウント管理者による不正を防止するため、アカウントの管理権限を制御する機能を備えること。 (データ保護) ・ 通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。 ・ 情報システムに蓄積された情報の搾取や漏えいを防止するため、保護すべき情報を利用者が直接アクセス可能な機器に保存しないこと。 (構成管理) ・ 障害・事故等の発生要因を減らすとともに、障害・事故等の発生時には迅速に対処するため、構築時の情報システムの構成(ハードウェア、ソフトウェア及びサービス構成に関する詳細情報)が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。
7	情報システム稼働環境	(1) 全体構成	*(ステップ3にて作成したシステム概要図を記載)*
		(2) ハードウェア構成	
		(3) ソフトウェア構成	
		(4) ネットワーク構成	
		(5) アクセシビリティ要件	
8	テスト要件定義	要求仕様の適合性を検証するためのテストに係る要件	・ 情報システムを構成するソフトウェア及びハードウェアの脆弱性に悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。
9	移行要件定義	(1) 移行に係る要件	
		(2) 教育に係る要件	
10	運用要件定義	(1) システム操作・監視等要件	
		(2) データ管理要件	
		(3) 運用施設・設備要件	・ 情報の漏えいを防止するため、記憶装置の設置時のロック及び暗号化等によって、情報搾取行為を防止・検知するための機能を備えること。 ・ 物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置(重要情報を扱う装置)については、安全区域に設置可能な設計とすること。
11	保守要件定義	(1) ソフトウェア保守要件	・ 運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備
		(2) ハードウェア保守要件	

【パブリックコメント】

大項目		小項目	記載内容
			えるとともに、情報システム全体の更新漏れを防止する機能を備えること。
12	作業の体制及び方法	(1) 作業体制	
		(2) 開発方法	
		(3) 導入	
		(4) 瑕疵担保責任	
13	特記事項	その他、特記すべき要件	
14	妥当性証明	調達仕様書の妥当性を確認した調達担当課室の長の氏名	