

「令和6年度 ISMAP ポータルサイト及び制度運営支援システム
の機能改修」

(仕 様 書)

1	はじめに	4
1.1	背景	4
1.2	目的	4
1.3	基本方針	4
1.3.1	クラウドサービスの活用	4
1.3.2	将来的な拡張性	5
1.4	用語の定義	5
2	対象業務の概要	7
2.1	全体概要	7
2.2	利用者区分	8
2.3	業務フロー	9
2.3.1	クラウドサービス審査・管理業務	9
2.3.2	情報発信業務	10
2.3.3	その他業務	11
3	機能要件	12
3.1	機能一覧	12
3.1.1	登録審査ステータス	14
3.1.2	クラウドサービスリストに掲載される項目	15
3.2	画面	15
3.2.1	トップページ	15
3.2.2	問い合わせ画面	17
3.3	帳票一覧	18
3.4	データ移行	18
4	システム稼働環境の要件	20
4.1	クラウド環境	20
4.2	クライアント端末環境	20
4.3	ネットワーク環境	20
5	非機能要件	21
5.1	性能・拡張性要件	21
5.1.1	システムパフォーマンス	21
5.1.2	拡張性	21
5.2	可用性・信頼性要件	21
5.3	セキュリティ要件	21
5.3.1	セキュリティ対策方針	21
5.3.2	セキュリティ要件	22
5.3.3	セキュリティ対策の改善	25
5.4	教育・研修要件	25
6	設計要件	25
7	テスト要件	26
7.1	テスト範囲	26
7.2	テスト計画の策定	26
7.3	テスト方法	26
7.4	テストデータ	27
8	移行に関する要件	28
9	保証要件	28
10	プロジェクト管理要件	30
10.1	プロジェクト管理業務	30

10.2	スケジュールの策定	30
10.3	プロジェクト体制	30
10.4	品質及びリスク管理	32
10.5	課題管理	33
10.6	コミュニケーション管理	33
11	開発範囲	33
11.1	作業範囲	33
11.2	環境	33
11.3	成果物	34
11.4	スケジュール	35
11.5	納入要件	35
11.5.1	納入物件及び納入期限	35
11.5.2	納入場所	36
11.6	検収要件	36
11.6.1	システム構築時	36
12	留意事項	36

1 はじめに

「ISMAP ポータルサイト及び制度運営支援システム」（以下「現行システム」という。）は、「政府情報システムのためのセキュリティ評価制度（ISMAP）」¹の運用を円滑に行うために、ISMAP 運用支援機関である独立行政法人情報処理推進機構（以下「IPA」という。）が運用するシステムである。

ISMAP 制度は、運用開始から3年を経過する中で、運用面での課題も明らかになってきており、IPA では、制度所管省庁（内閣サイバーセキュリティセンター、デジタル庁、総務省、経済産業省）と連携しながら、制度運営や審査の効率化等の改善の取組を進めている。

本書は、具体的な課題について運用や対応が決まった方策を、現行システムの改修により実現するためのシステム調達仕様を示すものである。今回の改修では、審査の迅速化及び明確化に資する改修と利用者拡大を見越したコミュニケーションの向上に資する改修を実施する。

なお、ISMAP 制度の概要については、「ISMAP - 政府情報システムのためのセキュリティ評価制度」ポータルサイト²で公開している。

1.1 背景

第200回国会において成立した「情報処理の促進に関する法律の一部を改正する法律」（令和元年法律第67号）³の施行に伴い、IPAに政府調達におけるクラウドサービスの安全性評価制度の実施業務が追加され、また、「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（令和2年1月30日 サイバーセキュリティ戦略本部決定）⁴において、IPAは制度運用に係る実務及び評価に係る技術的な支援を行うことと位置づけされた。さらに、ISMAP 基本規程⁵において、制度の運用に係る事務の一部をISMAP 運用支援機関としてのIPAに委任することが定められ、令和2年5月からIPAで事業が開始された。また、令和4年には、リスクの小さな業務・情報の処理に用いるSaaSを対象にした仕組みである「ISMAP-LIU（イスマップ・エルアイユー：ISMAP for Low-Impact Use。以下、ISMAP-LIUという）」が新たに設けられ、令和4年11月1日から運用が開始された。

この制度の運用を円滑に行うために、IPAはServiceNow、AWS、Boxなどのクラウドサービスを組み合わせることでポータルサイト機能及び電子申請受付機能を実現する現行システムを構築し、令和3年5月から運用を開始した。また、令和5年には、現行システムにISMAP-LIUの電子申請受付機能等を追加するシステム改修を行い、令和5年10月から運用を開始した。

1.2 目的

本書に係る改修（以下、本改修と言う。）は、ISMAP及びISMAP-LIUの運用に関する課題に対応するための具体的な方策を、現行システムに追加することを目的とする。具体的には、審査の迅速化及び明確化に資する改修と利用者拡大を見越したコミュニケーションの向上に資する改修を実施する。

1.3 基本方針

本改修の遂行にあたり、以下の基本方針に従うものとする。

1.3.1 クラウドサービスの活用

- (1) 既に構築済のシステム（ISMAP ポータルサイト）を改修する形で機能追加を実装することから、現行システムで利用しているクラウドサービスを活用することを前提とする。
- (2) 現行システムは、監査機関、クラウドサービス事業者、調達府省庁等、IPA及びIPAから業務を委託された監査機関選定組織から、インターネットを含むネットワークを経由して利用することを想定しており、機能追加によってもこの条件は変わらない。

¹ ISMAP ポータルサイト「政府情報システムのためのセキュリティ評価制度（ISMAP）基本規程」：
https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010007

² 「ISMAP - 政府情報システムのためのセキュリティ評価制度」ポータルサイト：
<https://www.ismap.go.jp>

³ 「情報処理の促進に関する法律の一部を改正する法律」（令和元年法律第67号）：
<https://www.meti.go.jp/press/2020/05/20200515001/20200515001.html>

⁴ 「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（令和2年1月30日 サイバーセキュリティ戦略本部決定）：
<https://www.nisc.go.jp/active/general/pdf/wakugumi2020.pdf>

⁵

- (3) 可能な限り既に提供されているサービスを設定変更して機能を追加することを基本とし、開発は最小限にとどめる。

1.3.2 将来的な拡張性

- (1) 将来的に制度の追加、変更が発生する可能性があることを念頭に、急なシステム変更にも柔軟に対応できるよう、現行システムの拡張性を阻害しないこと。

1.4 用語の定義

表 1 用語一覧にて、本書で使用される主な用語を解説する。

表 1 用語一覧

No.	用語	定義
1	ISMAP	政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program）の通称（イスマップ）
2	クラウドサービス	「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（平成 30 年 6 月 7 日各府省情報化統括責任者（CIO）連絡会議決定）で定義された、「事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの」をいう。
3	クラウドサービス事業者	クラウドサービスを自ら提供する事業者をいう。
4	監査機関	クラウドサービスに対する監査を実施する主体となる法人をいう。
5	制度所管省庁	ISMAP 及び ISMAP-LIU を運用する省庁で、内閣サイバーセキュリティセンター、デジタル庁、総務省及び経済産業省をいう。
6	ISMAP 運営委員会	サイバーセキュリティ戦略本部決定に基づき制度所管省庁の下に設置される、有識者等で構成された ISMAP 及び ISMAP-LIU の運用に係る最高意思決定機関をいう。また、ISMAP 運営委員会を運営する事務局を内閣官房内閣サイバーセキュリティセンターに置く。
7	監査機関選定組織	IPA から業務が委託され、共に ISMAP 運用支援機関としての業務を行う事業者。主に監査機関の登録審査・管理を行う。
8	ISMAP 運用支援機関	ISMAP 及び ISMAP-LIU の運用に係る事務を ISMAP 運営委員会から委任された機関。 具体的には IPA 及び監査機関選定組織をいう。
9	調達府省庁等	ISMAP 及び ISMAP-LIU においてクラウドサービスを調達する国の行政機関、独立行政法人及び指定法人をいう。
10	登録	ISMAP 運営委員会が、申請のあったクラウドサービスについて、ISMAP 及び ISMAP-LIU で定める要求事項を満たすことを確認した上で当該クラウドサービスを ISMAP 及び ISMAP-LIU クラウドサービスリストに記載する行為、又は申請のあった法人について、監査機関として ISMAP で定める要求事項を満たすことを確認した上で当該法人を ISMAP 監査機関リストに記載する行為をいう。
11	監査	ISMAP 及び ISMAP-LIU において、登録を求めるクラウドサービスにおいてクラウドサービス事業者が行った統制に関する言明に対し、監査機関が ISMAP で定められた基準・手続等に基づき実施する情報セキュリティ監査をいう。
12	ISMAP クラウドサービスリスト	ISMAP 運営委員会が ISMAP で要求する基準に基づいたセキュリティ対策を実施していることを確認したクラウドサービスを記載する公開のリストをいう。
13	ISMAP 監査機関リスト	ISMAP 運営委員会が監査機関として ISMAP で定める要求事項を満たすことを確認した法人を記載する公開のリストをいう。
14	ISMAP-LIU	ISMAP の内、影響度が低いと評価される業務、情報に用いられる SaaS サービスを対象とする評価制度（ISMAP for Low-Impact Use）の通称（イスマップ エルアイユー）

No.	用語	定義
15	ISMAP-LIU クラウドサービスリスト	ISMAP 運営委員会が ISMAP-LIU で要求する基準に基づいたセキュリティ対策を実施していることを確認したクラウドサービスを記載する公開のリストをいう。
16	コンテンツ	ISMAP ポータルサイトに掲載する情報ページをいう。 制度案内、申請書類(様式)、ISMAP 監査機関リスト、ISMAP クラウドサービスリスト、ISMAP-LIU クラウドサービスリスト、FAQ などがある。

2 対象業務の概要

2.1 全体概要

図 1 全体概要図に業務及びシステムの全体概要を示すとともに、今回の改修項目を示す。

個別業務に係る改修点に関する説明は「2.3 業務フロー」に、今回の改修で実現する具体的な機能の要件は「3 機能要件」に記載する。

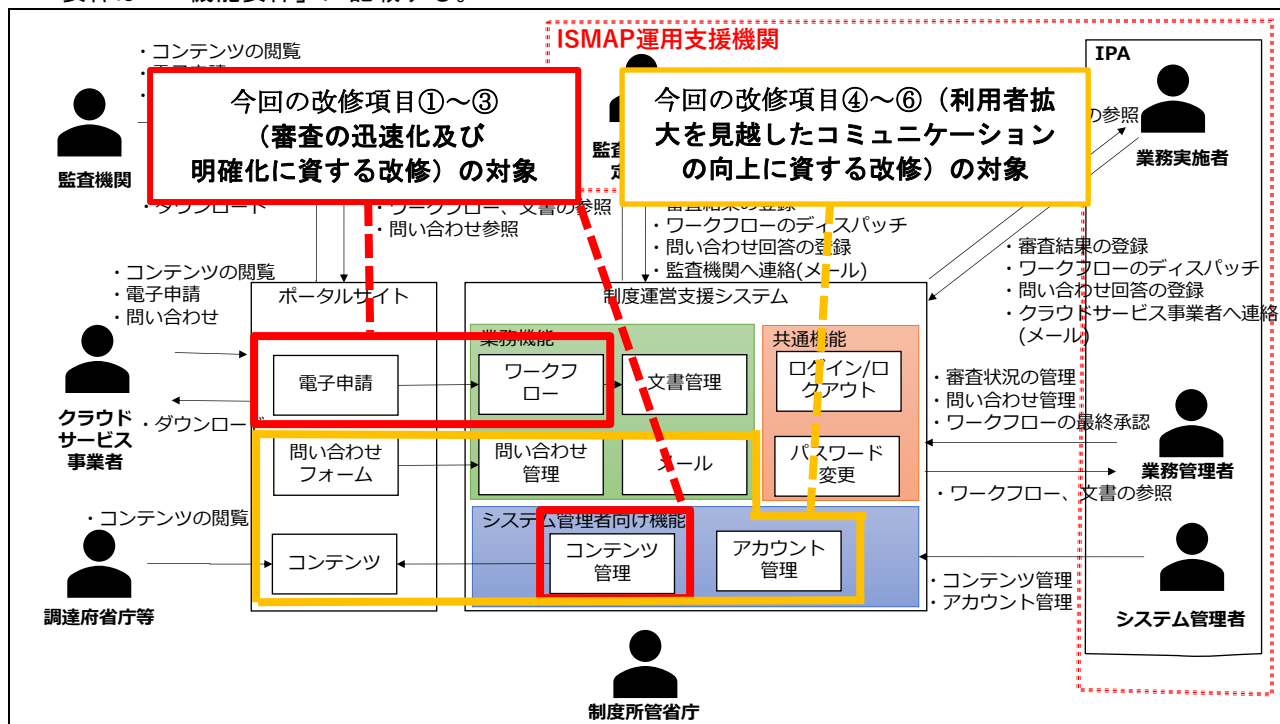


図 1 全体概要図

◇今回の改修の概要

今回の改修では、審査の迅速化及び明確化のため、並びに、利用者拡大を見越したコミュニケーションの向上のために、以下の改修項目を実施する。

(審査の迅速化及び明確化に資する改修項目)

- ①審査ステータスの表示の見直し
- ②クラウドサービスリスト作成支援機能の追加
- ③登録番号採番の適正化・登録通知書の自動発行機能の追加

(利用者拡大を見越したコミュニケーションの向上に資する改修項目)

- ④登録済みのCSP、監査機関のみを対象とした情報発信機能の追加
- ⑤IPA側からの問い合わせ機能の追加
- ⑥問い合わせ回答の複数担当者への通知機能の追加

2.2 利用者区分

現行システムの利用者を表 2 利用者区分に示す。

表 2 利用者区分

No.	利用者	説明説明	ログイン対象	利用者規模等
1	監査機関	「1.4 用語の定義」参照。	○	10 社程度
2	クラウドサービス事業者	「1.4 用語の定義」参照。	○	100 社程度
3	制度所管省庁	「1.4 用語の定義」参照。	×	10 名程度
4	調達府省庁等	「1.4 用語の定義」参照。	△	100 組織程度
5	一般利用者	制度に興味のある民間企業の担当者等	×	コンテンツの参照は 100 万 PV/月以内とする
6	業務実施者	業務を行う IPA 職員。	◎	10 名程度
7	業務管理者	業務管理を行う IPA 職員。	◎	
8	システム管理者	システムの管理を行う IPA の職員。	◎	
9	監査機関選定組織	「1.4 用語の定義」参照。	◎	10 名程度

ログイン対象 ◎:制度運営支援システム ○:電子申請 △:情報閲覧(ログインあり) ×:ログインなし

2.3 業務フロー

今回の改修対象となる具体的な業務と改修点を記載する。なお、下記の①～⑥の番号は 2.1 全体概要の改修項目の番号に対応する。

2.3.1 クラウドサービス審査・管理業務

本業務は、ISMAP におけるクラウドサービスの審査及び管理に係る業務である。クラウドサービス事業者からの申請手続きに係る審査及び管理業務全般を本ポータルサイトにおいて実現している。また、クラウドサービス事業者は、本ポータルサイトを通じて、自身の申請の状況（審査中など）の確認や各種申請を行う。

(1) サービス登録審査（ISMAP）

IPA は、クラウドサービス事業者からの ISMAP クラウドサービスリストへの登録申請を受け付け、審査を実施する。IPA による審査後、ISMAP 運営委員会へ諮る。なお、更新時の申請も本業務が準用される。

本業務は、ISMAP クラウドサービス登録規則 3 章～7 章に係る業務に該当する。本業務に係るシステム化の業務フロー(案)については別紙 1 クラウドサービス審査・管理業務フロー「(1)サービス登録審査（ISMAP）」シートを参照のこと。

本業フローにおける今回の改修対象は以下の 3 点である。

①：既存の仕組みでは、登録申請 WF においてクラウドサービス事業者側に表示する区分が細分化されておらず、審査の詳細なステータスの把握が困難であるとの課題があった。**本改修により、審査のステータスとしてクラウドサービス事業者側に表示する区分を追加する。**

③-1：既存の仕組みでは、登録通知書を発行する際に登録番号を作業順に自動採番する仕組みであったが、実務では申請順に登録番号を採番する必要があり、自動採番の仕組みが支障となっていた。**本改修により、自動採番を行わず、IPA 職員が画面上で入力した登録番号を採用する仕組みに変更する。**

③-2：既存の仕組みでは、ISMAP 運営委員会の結果として ISMAP クラウドサービスリストへ登録することが認められた場合に、「登録通知書」を手作業により作成し、登録申請 WF に登録してクラウドサービス事業者に送付する運用であり、作業量の増加が課題となっていた。**本改修では、これらの作業を効率化するため、システムに登録済みの情報（画面上で入力した登録番号を含む）から当該帳票を自動生成する機能を追加する。**

(2) サービス登録審査（ISMAP-LIU）

IPA は、クラウドサービス事業者からの ISMAP-LIU クラウドサービスリストへの登録申請を受け付け、審査を実施する。IPA による審査後、ISMAP 運営委員会へ諮る。なお、更新時の申請も本業務が準用される。

本業務は ISMAP-LIU クラウドサービス登録規則 7 章～11 章に係る業務に該当する。本業務に係るシステム化の業務フロー(案)については別紙 1_クラウドサービス審査・管理業務フロー「(2)サービス登録審査（ISMAP-LIU）」参照のこと。

今回の改修対象は以下の 3 点である。（上記(1)サービス登録審査（ISMAP）と同様の改修内容を、ISMAP-LIU にも実装する）

①（再掲）：既存の仕組みでは、登録申請 WF においてクラウドサービス事業者側に表示する区分が細分化されておらず、審査の詳細なステータスの把握が困難であるとの課題があった。**本改修により、審査のステータスとしてクラウドサービス事業者側に表示する区分を追加する。**

③-1（再掲）：既存の仕組みでは、登録通知書を発行する際に登録番号を作業順に自動採番する仕組みであったが、実務では申請順に登録番号を採番する必要があり、自動採番の仕組みが支障となっていた。**本改修により、自動採番を行わず、IPA 職員が画面上で入力した登録番号を採用する仕組みに変更する。**

③-2（再掲）：既存の仕組みでは、ISMAP 運営委員会の結果として ISMAP クラウドサービスリストへ登録することが認められた場合に、「登録通知書」を手作業により作成し、登録申請 WF に登録してクラウドサービス事業者に送付する運用であり、作業量の増加が課題となっていた。**本改修では、これらの作業を効率化するため、システムに登録済みの情報（画面上で入力した登録番号を含む）から当該帳票を自動生成する機能を追加する。**

2.3.2 情報発信業務

本業務は、ポータルサイトを通じ、監査機関やクラウドサービス事業者、調達府省庁等に対し、情報を提供する業務である。今回の改修に係る業務を具体的に下記(1)～(2)に記載する。

(1) コンテンツ管理

ポータルサイトに掲載するコンテンツの管理を行う業務である。主なコンテンツとしては、制度案内、申請書類(様式)、ISMAP 監査機関リスト、ISMAP クラウドサービスリスト、ISMAP-LIU クラウドサービスリスト、FAQ である。

本業務に係るシステム化の業務フロー(案)については別紙 2 情報発信業務業務フロー「(1) コンテンツ管理」参照のこと。

今回の改修対象は以下の 2 点である。

②: 既存の仕組みでは、ISMAP 及び ISMAP-LIU クラウドサービスリストを公開する際に、以下の作業をポータルサイトの画面から手動で行っており、登録サービス数の増加に伴い、作業量の増加が課題となっていた。

- (1) コンテンツ管理機能を用いてコンテンツを 1 件ずつ作成する。(新規登録又は更新登録されるサービス 1 件につき 6~7 件のコンテンツを作成する)
- (2) 作成した個々のコンテンツに対し、PDF ファイルをアップロードして添付ファイルとして紐づける。(作成したコンテンツの数だけ繰り返し実施する)
- (3) 作成した個々のコンテンツを、登録申請 WF から自動生成されたクラウドサービスリストの所定の項目に紐づける。(作成したコンテンツの数だけ繰り返し実施する)

本改修により、上記(1)及び(3)の作業を、必要な情報を入力した Excel ファイルを読み込ませることにより一括で実施する機能を追加する。

なお、(2)の作業は、従来と同様に手動で実施する。

④: 既存の仕組みでは、誰でも閲覧できる情報とアカウント種別に応じた情報の閲覧が可能になっているが、アカウント種別(「監査機関」、「クラウドサービス事業者」)について、ISMAP 監査機関リスト、ISMAP クラウドサービスまたは ISMAP-LIU クラウドサービスリストに登録済みの監査機関、クラウドサービス事業者と未登録の監査機関、クラウドサービス事業者を分けて、情報を公開する機能を有していない。

本改修により ISMAP 監査機関リストに登録済みの監査機関ユーザ、ISMAP クラウドサービスリストまたは ISMAP-LIU クラウドサービスリストに登録済みクラウドサービス事業者ユーザのみが情報を閲覧できる機能を追加する。

(2) 問い合わせ

監査機関、クラウドサービス事業者等からの問い合わせを受付ける。一旦、IPA にて一次受付を行い、適切な組織、担当者へアサインを行う。担当者が回答を登録後、最終的に IPA 管理者が確認を行った後、問い合わせ元へ回答を発信する。

システム化の業務フロー(案)については別紙 2 情報発信業務業務フロー「(2) 問い合わせ」参照のこと。

今回の改修対象は以下の 2 点である。

⑤: 既存の仕組みでは、IPA 側から問い合わせを新規に起票できるが、連絡先(監査機関、クラウドサービス事業者)を設定できず、実質的に IPA 側から監査機関、クラウドサービス事業者に対して問い合わせを行なえないことが、課題となっている。

本改修により、業務実施者(IPA)が新規で問い合わせを起票する際に、CSP 及び監査機関の連絡先を指定できるようにする。

⑥: 既存の仕組みでは、問い合わせの起票者のみに対して問い合わせの回答が送信される仕組みとなっているが、問い合わせ側の担当者に変更になった場合や、回答の送信先を複数人にしたい場合に対応ができないことが課題となっている。

本改修により、問い合わせフォーム上で、複数の宛先(10 件程度を想定)を設定できる機能を追加する。

2.3.3 その他業務

(1) アカウント登録管理業務

監査機関やクラウドサービス事業者が申請する際のアカウントを登録する業務である。システム化の業務フロー(案)については、別紙3_アカウント管理フロー参照のこと。

④:既存の仕組みでは、アカウント種別は「監査機関」、「クラウドサービス事業者」、「政府機関等」の3つが存在するが、そのうち「監査機関」、「クラウドサービス事業者」について、そのユーザが ISMAP 監査機関リスト、ISMAP クラウドサービスリストまたは ISMAP-LIU クラウドサービスリストに登録済の監査機関、クラウドサービス事業者に属するユーザか否かが判別できないことが課題となっている。

本改修によって、従来のアカウント種別（「クラウドサービス事業者」、「監査機関」）を、ISMAP 監査機関リストに登録済みであるか、及び ISMAP クラウドサービスリストまたは ISMAP-LIU クラウドサービスリストに登録済みであるかどうかによって、「クラウドサービス事業者」、「監査機関」のアカウントを更に細分化して管理できるようにする。

3 機能要件

3.1 機能一覧

審査の迅速化、明確化の観点で本改修で実現する機能は、以下のとおり。

表 3 では、監査機関及びクラウドサービス事業者が利用するポータルサイトの機能要件を示す。

表 4 では、ISMAP 運用支援機関が利用する制度運営支援システムの機能要件を示す。

表 3 ポータルサイト機能一覧

No.	機能名称	利用者	改修番号	概要
1	電子申請 (ISMAP/ISMAP-LIU)	クラウドサービス事業者	①	<p>利用者はポータルサイトへログイン後、ISMAP 運用支援機関へ登録申請書類を提出し自身の申請状況の確認などを行う。本改修によって追加する機能の要件は以下の通り。</p> <ul style="list-style-type: none"> クラウドサービス登録申請 (ISMAP/ISMAP-LIU) 時に、「申請履歴詳細画面」の「ステータス」の項目にて、申請者の申請状況をより詳細に確認できるようにするため、「ステータス」として表示可能な項目を追加すること ※ステータスの詳細については、3.1.1 登録審査ステータスを参照のこと。
2	情報閲覧・ダウンロード	監査機関 クラウドサービス事業者	④	<p>利用者は、制度の案内や申請書類などサイトに掲載された各種情報の閲覧またはダウンロードを行う。本改修により追加する機能の要件は下記の通り。</p> <ul style="list-style-type: none"> 「登録済みクラウドサービス事業者」のアカウント及び「登録済み監査機関」のアカウントに応じて、閲覧またはダウンロードできる情報を制御できるようにすること。 トップページに登録済み監査機関用、登録済みクラウドサービス事業者用のページを追加すること。 ※改修後の画面イメージの詳細については、3.2.1 トップページを参照のこと。
	問い合わせ	監査機関 クラウドサービス事業者	⑥	<p>利用者は ISMAP 運用支援機関へ問い合わせを行う。本改修によって追加する機能の要件は以下の通り。</p> <ul style="list-style-type: none"> 未ログイン及びログイン後の問い合わせフォームに「追加連絡先」の項目を追加すること ログイン後の問い合わせの場合、問い合わせ起票後も、「追加連絡先」を登録できるようにすること ※改修後の画面イメージの詳細については 3.2.2 問い合わせ画面を参照のこと。

表 4 制度運営支援システム機能一覧

No.	機能名称	利用者	改修番号	概要
1	電子申請 (ISMAP/ISMAP-LIU)	業務実施者 (IPA) 業務管理者 (IPA)	①	ISMAP 運用支援機関は、審査プロセスの有効性の担保、効率化のため、電子申請と連携させ、ワークフローによる申請の管理を行う。本改修によって追加する機能の要件は以下の通り。 <ul style="list-style-type: none"> ワークフローの「ステータス (バック)」と連動し、申請者に表示可能なステータスを変更すること ※ステータスの詳細については、3.1.1 登録審査ステータスを参照のこと。
			③-1	本改修によって追加する機能の要件は以下の通り。 <ul style="list-style-type: none"> ワークフロー中に採番される、「登録番号」の自動採番を無効にすること 新規申請の場合、ISMAP 運営委員会結果登録画面にて、「登録番号」を入力可能にすること
			③-2	本改修によって追加する機能の要件は以下の通り。 <ul style="list-style-type: none"> 申請情報及び画面上から入力された情報に基づき 3.3 帳票一覧に示す帳票が出力されること 出力された当該帳票を確認できること ワークフローと連携し、出力された当該帳票が申請者に共有されること クラウドサービス登録申請ワークフロー画面の、ISMAP 運営委員会結果承認にて差戻を行なった際、出力された当該帳票が削除されること また、ISMAP 運営委員会結果登録を再度行った際に、当該帳票が再出力されること
2	問い合わせ管理	業務実施者 (IPA) 業務管理者 (IPA) 監査機関選定 組織	⑤	ISMAP 運用支援機関は、監査機関、クラウドサービス事業者等からの問い合わせを一元管理する。本改修によって追加する機能の要件は以下の通り。 <ul style="list-style-type: none"> 業務実施者 (IPA) が問い合わせを起票した際、「連絡先」の項目が設定できること ISMAP 運用支援機関が問い合わせを起票した旨のメールを新たに定義し、上記で設定した「連絡先」に対して通知されること
			⑥	本改修によって追加する機能の要件は以下の通り。 <ul style="list-style-type: none"> ISMAP 運用支援機関による回答送信時のメールが「追加連絡先」の項目に入力された連絡先にも送信されること。

No.	機能名称	利用者	改修番号	概要
3	コンテンツ管理	業務実施者 (IPA) 業務管理者 (IPA) システム管理者 (IPA)	②	<p>ISMAP 運用支援機関は、ポータルサイトに掲載するコンテンツを登録する。本改修により追加する機能の要件は以下の通り。</p> <ul style="list-style-type: none"> 2.3.2(1)コンテンツ管理の②(1)の作業においてクラウドサービスリストの各項目に登録されるコンテンツを Excel ファイルを用いて一括で作成可能にすること ※項目については3.1.2クラウドサービスリストに掲載される項目を参照のこと 2.3.2(1)コンテンツ管理の②(3)の作業においてクラウドサービスリストの各項目に紐づけられるコンテンツを Excel ファイルを用いて一括で紐づけ可能にすること ※項目については3.1.2クラウドサービスリストに掲載される項目を参照のこと
			④	<p>ISMAP 運用支援機関は、ポータルサイトに掲載するコンテンツを登録する。本改修により追加する機能の要件は以下の通り。</p> <ul style="list-style-type: none"> アカウント種別（「登録済み監査機関」、「登録済みクラウドサービス事業者」）に応じて、指定したアカウント種別の利用者アカウントだけが参照できるコンテンツを作成・管理できること
4	アカウント管理	システム管理者 (IPA)	④	<p>ISMAP 運用支援機関は、ポータルサイトの申請者アカウントの管理及び、制度運営支援システムの利用者のアカウントの管理を行う。本改修により追加する機能の要件は以下の通り。</p> <ul style="list-style-type: none"> 新たに「登録済み監査機関」、「登録済みクラウドサービス事業者」のユーザグループを作成し、既存のユーザグループ「監査機関」、「クラウドサービス事業者」による管理に加え、ISMAP 監査機関リスト、ISMAP クラウドサービスリストまたは ISMAP-LIU クラウドサービスリストに登録済みの事業者のみを分けて管理できるようにすること ISMAP 監査機関リスト、ISMAP クラウドサービスリストまたは ISMAP-LIU クラウドサービスリストへの登録もしくは削除を契機に、登録または削除の対象となった事業者のユーザが所属するユーザグループを自動的に切り替えること 切り替えの具体的な方法（イメージ、設計、開発方針）については提案書に記載すること

3.1.1 登録審査ステータス

現行システムでクラウドサービス事業者が自身の申請状況を確認できるステータスを表 5 に、改修後のステータスのイメージを表 6 に示す。

表 5 現行のステータス

ステータス (バック)	ステータス (フロント)
受理確認中	受理確認中

技術審査中	審査中
CS 審査委員会開催待ち	審査中
ISMAP 運営委員会開催待ち	審査中
ISMAP 運営委員会結果承認待ち	審査中
登録通知書発送待ち	審査中
完了（登録/非登録）	完了（登録/非登録）

表 6 改修後のステータス（イメージ）

ステータス（バック）	ステータス（フロント）
受理確認中	受理確認中
技術審査中	技術審査中
CS 審査委員会開催待ち	IPA 内委員会開催待ち
ISMAP 運営委員会開催待ち	ISMAP 運営委員会開催待ち
ISMAP 運営委員会結果承認待ち	ISMAP 運営委員会開催待ち
登録通知書発送待ち	ISMAP 運営委員会開催待ち
完了（登録/非登録）	完了（登録/非登録）

3.1.2 クラウドサービスリストに掲載される項目

ISMAP クラウドサービスリスト及び ISMAP-LIU クラウドサービスリストに掲載されるコンテンツの一覧を以下に示す。

項目
言明の対象範囲
基本言明要件のうち実施している統制目標の管理策
後発事象
申請時点における申請者の資本関係及び役員等の情報
リスク評価を行うために必要な情報
契約に定める準拠法・裁判管轄に関する情報
ペネトレーションテストや脆弱性診断等の第三者による検査の実施状況と受入に関する情報

3.2 画面

本書で示す業務及び機能要件を実現する上で必要となる画面を設ける。また図の表示として赤枠の箇所が、本改修で追加する箇所である。

原則として、クラウドサービスにおいて提供している画面がある場合は、それらに対して最小限のカスタマイズのみで使用することを想定する。画面の構成や入力方法、最終的な項目は IPA と相談し決定すること。

3.2.1 トップページ

従来のアカウント種別（「監査機関」、「クラウドサービス事業者」、「政府機関等」）に応じたトップページに加え、今回の改修で新たに追加される「登録済み監査機関アカウント」、「登録済みクラウドサービス事業者アカウント」に対応した、新たなトップページを追加する。ISMAP 監査機関リスト、ISMAP クラウドサービスリストまたは ISMAP-LIU クラウドサービスリストに登録済みの事業者か否かは、新設するユーザグループを用いて判別する。

登録済み監査機関アカウントでログインした際のトップページの見え方のイメージを図 2 に、登録済みクラウドサービス事業者アカウントでログインした際のトップページの見え方のイメージを図 3 に示す。なお、最終的な画面項目や表現、レイアウト等

については、IPA と協議の上決定すること。

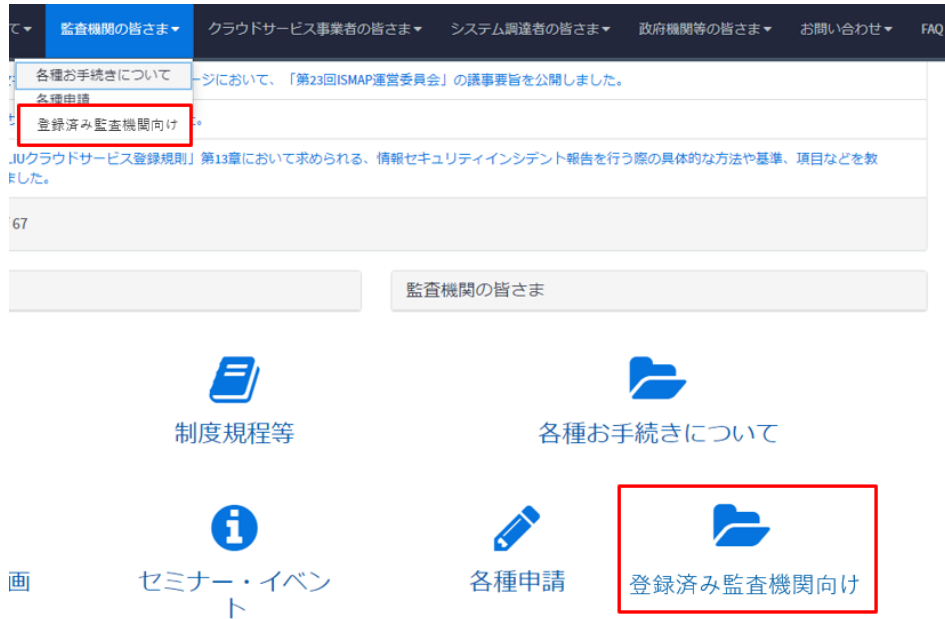


図 2 登録済み監査機関アカウントでログインした際のトップページ (イメージ)



図 3 登録済みクラウドサービス事業者アカウントでログインした際のトップページ (イメージ)

3.2.2 問い合わせ画面

問い合わせ画面イメージを以下に示す。

なお、最終的な画面項目や表現、レイアウト等については、IPA と協議の上決定することとする。

お問い合わせ

本ページでは、政府情報システムのためのセキュリティ評価制度（ISMAP）に関するお問い合わせを受け付けます。
以下フォームへ内容を記入の上、[登録]ボタンを押してください。

※アカウントをお持ちの方はログインユーザー向けのお問い合わせ登録画面からお問い合わせください。

個人情報の取り扱いについて
お問い合わせ時にご記入いただいた個人情報は、お問い合わせ内容に関するISMAP運用支援機関からのご連絡以外の目的では使用いたしません。
詳しくは、[プライバシーポリシー](#)をご覧ください。

*姓
[]

*名
[]

*姓（全角カナ）
[]

*名（全角カナ）
[]

省略

*お問い合わせタイトル
[]

*お問い合わせ内容（全角4000文字以内）
[]

前回お問い合わせ番号

追加連絡先（本申請に関する通知の受け取りを希望する方がいる場合、ご入力ください）

追加連絡先 E-mail(1) []	追加連絡先 E-mail(4) []
追加連絡先 E-mail(2) []	追加連絡先 E-mail(5) []
追加連絡先 E-mail(3) []	

図 4 未ログインユーザー向け問い合わせフォーム（イメージ）

お問い合わせ

本ページでは、政府情報システムのためのセキュリティ評価制度（ISMAP）に関するお問い合わせを受け付けます。
以下フォームへ内容を記入の上、[登録]ボタンを押してください。

個人情報の取り扱いについて
お問い合わせ時にご記入いただいた個人情報は、お問い合わせ内容に関するISMAP運用支援機関からのご連絡以外の目的では使用いたしません。
詳しくは、[プライバシーポリシー](#)をご覧ください。

*お問い合わせ種類
ISMAP関連

*お問い合わせタイトル
[]

*お問い合わせ内容（全角4000文字以内）
[]

前回お問い合わせ番号

追加連絡先（本問い合わせに関する通知の受け取りを希望する方がいる場合、ご入力ください）

追加連絡先 E-mail(1) []	追加連絡先 E-mail(4) []
追加連絡先 E-mail(2) []	追加連絡先 E-mail(5) []
追加連絡先 E-mail(3) []	

添付ファイルを追加

図 5 ログイン済みユーザー向け問い合わせフォーム（イメージ）

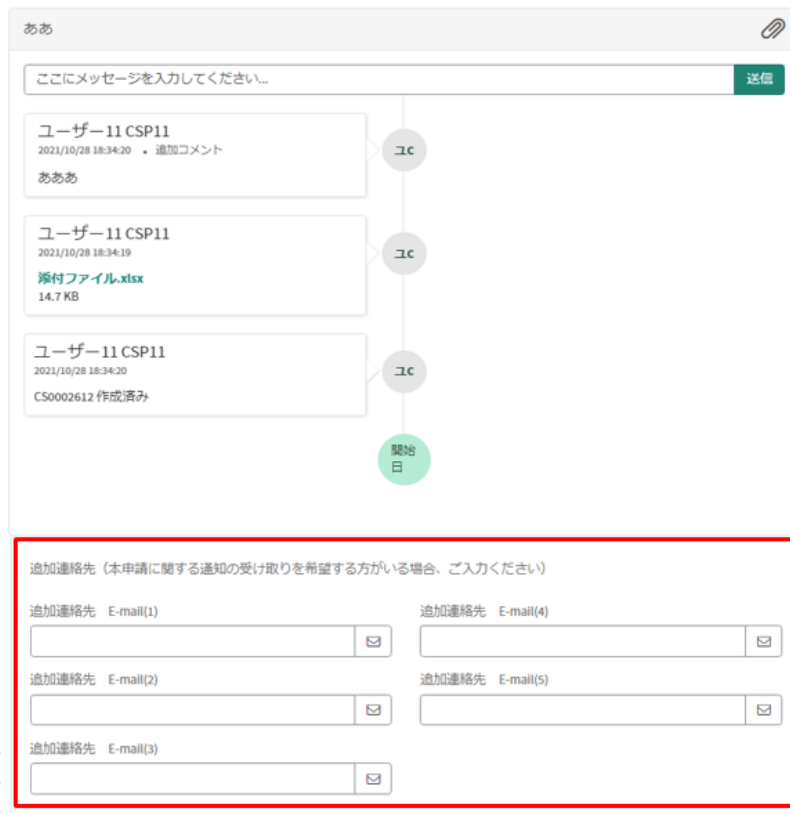


図 6 問い合わせ履歴（詳細）画面（イメージ）

3.3 帳票一覧

今回の改修によって、システムで出力する帳票を表 7 に、帳票の項目と対応するシステム上の情報を表 8 に示す。出力するファイル形式は PDF を想定しているが、最終的な出力項目、出力様式については IPA と協議して決定すること。

また、その他必要と考えられる帳票がある場合は、IPA と協議し決定すること。

なお様式 6/様式 2-7 結果通知書については、従来通り手動での作成を想定する。

表 7 帳票一覧

No	帳票名	帳票の元となる様式等
1	様式 5 登録通知書	ISMAR クラウドサービス登録規則 様式 5 登録通知書
3	様式 2-6 登録通知書	ISMAR-LIU クラウドサービス登録規則 様式 2-6 登録通知書

表 8 帳票の項目と対応するシステム上の情報

項目名	対応するシステム上の情報
年月日	結果通知日付
申請者住所	申請者住所
申請者名	申請者名
代表者役職名	代表者役職名
代表者名	代表者名
登録番号	登録番号
クラウドサービス名称	クラウドサービスの名称
事業者名	社名
事業者住所	住所
登録日（年月日）	登録日
登録の更新期限（年月日）	登録の更新期限

3.4 データ移行

本改修までに、ISMAR 監査機関リスト、ISMAR クラウドサービスリストに登録されている監査機関、

クラウドサービス事業者が既にあること、また ISMAP-LIU クラウドサービスリストに登録されているクラウドサービス事業者がいる想定がされることを踏まえ、表 9 に記載するアカウントを登録する仕組みや手順を用意すること。また、作業分担は表 10 を想定する。

その上で、移行の具体的な方法や作業分担については、提案書に記載すること。その際、なるべく短時間で移行できるようにするための方策につき、併せて提案すること。なお、他の要件等との関係において移行対象データに下記以外のデータが想定される場合は、その内容についても具体的に記載すること。

表 9 移行対象データ

No	データ名	概要
1	登録済み監査機関アカウント	ISMAP 監査機関リストに登録されている監査機関に属する監査機関ユーザー
2	登録済みクラウドサービス事業者アカウント	ISMAP クラウドサービスリストまたは ISMAP-LIU クラウドサービスリストに登録されているクラウドサービス事業者に所属するクラウドサービス事業者ユーザー

表 10 データ移行の作業分担（想定）

No	作業内容	作業者	
		請負者	IPA
1	移行方法の提示	○	-
2	データの作成	-	○
3	データ投入（本番作業）	-	○

※○：主担当を想定

4 システム稼働環境の要件

4.1 クラウド環境

- (1) 既に構築済のシステムを改修する形で実装することから、現行システムで利用しているクラウドサービスを活用することを前提とする
- (2) ソフトウェアについては、原則保有しない。ただし、カスタマイズや外部連携に対する開発部分に関してはこの限りでない。
- (3) 設定変更等を確認するための検証環境を準備すること。

4.2 クライアント端末環境

- (1) 現行システムにおいて、クライアント端末は、IPA の使用する仮想デスクトップ環境及び、一般的な PC 上で動作する主要ブラウザ（Microsoft Edge、Google Chrome 等）において動作し、ブラウザ以外のクライアント用ソフトウェアの導入は不要であるが、改修後もこの条件を維持すること。

4.3 ネットワーク環境

- (1) 現行システムにおいて、ISMAP 運用支援機関とサービスを提供する環境は一般的なインターネット回線を利用して接続することを前提としてるが、改修後もこの条件を維持すること。
- (2) 現行システムと ISMAP 運用支援機関間の通信は、VPN や TLS(SSL) の利用等により 5.3 セキュリティ要件に示すセキュアな通信環境が整備されているが、改修後もこの条件を維持されるものとする。

5 非機能要件

5.1 性能・拡張性要件

5.1.1 システムパフォーマンス

- ① 「2.2 利用者区分」で示した利用者数等を前提にシステム性能に係る設計、構築を行うこと。
- ② 検索結果の表示及び帳票出力等のオンライン処理に係るレスポンスタイムは概ね3秒以内とすること。
- ③ 上記以外の画面遷移に係るレスポンスタイムは概ね0.1秒以内とすること。ただし、ファイルのアップロードに要する時間について含めない。
- ④ 要求するパフォーマンスが満たされない事象が発生した場合、また、事前に要求するパフォーマンスが満たされないことが想定できる場合には、速やかにIPA担当者へ報告した上で速やかに問題の解決を行うこと。

5.1.2 拡張性

- ① 利用者の増加に備え、柔軟にリソースを拡張できるよう配慮されていること。

5.2 可用性・信頼性要件

- (1) 計画的なメンテナンスを除いて、原則24時間365日の稼働を前提とする。
平日休日に関わらず、サービス停止は12時間程度にとどめることを目標とする。月間稼働率は、99.6%以上とする。下記は最低限の目安であり、バックアップシステム構成やシステムダウン時のスイッチングの自動化など可用性を高めるための工夫があれば提案書に記載すること。

【サービス継続要件】

	システム障害時	災害／大規模障害時
目標復旧レベル (RLO)	全業務の再開 (性能は通常より低い水準を許容する)	
目標復旧時間 (RTO)	12時間程度	個別調整
目標復旧時点 (RPO)	4時間程度	日次バックアップからの復旧

5.3 セキュリティ要件

セキュリティについて十分に考慮し対策を講じたシステムであること。

システムのセキュアな環境の監視、維持、及び利用者が安心してシステムを利用できる環境を実現すること。

5.3.1 セキュリティ対策方針

- (1) IPAが提示するセキュリティポリシーを遵守すること。情報に対する不正アクセス、情報漏えい及び改ざんを防止するため、機密性、完全性及び可用性の観点で対策を行うこと。
- (2) 「政府機関の情報セキュリティ対策のための統一基準（令和5年度版）」を参考にすること。
https://www.nisc.go.jp/pdf/policy/general/ki_jyunr5.pdf
- (3) 開発作業及びシステムに影響を及ぼす可能性がある作業、物品、及びシステムに対し、事前に予測できる範囲内で適切なセキュリティ対策を行うこと。
- (4) 現行システムを構成するソフトウェア等では十分なセキュリティ対策を講じることが困難な場合は、多層防御によりシステム全体のセキュリティを担保すること。
- (5) 現在の技術で実現可能な対策を具体的な方法で行うこと。
- (6) ウェブアプリケーションの実装においては、IPAが公表している「安全なウェブサイトの作り方」の最新版に従うこと。
<https://www.ipa.go.jp/security/vuln/websecurity.html>
- (7) TLS(SSL)通信を行うシステムの構築、運用、保守においては、「TLS 暗号設定ガイドライン」

に従うこと。

https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

- (8) 暗号化機能、電子署名機能を使用するシステムの構築、運用、保守に際しては、「電子政府推奨暗号リスト」に基づくアルゴリズム及びプロトコルを採用すること。
<https://www.cryptrec.go.jp/list.html>
- (9) IPA が公表している「Web Application Firewall 読本」の最新版を参考にすること。
<https://www.ipa.go.jp/security/vuln/waf.html>
- (10) IPA が公表している「『高度標的型攻撃』対策に向けたシステム設計ガイド」の最新版を参考にすること。
<https://www.ipa.go.jp/security/vuln/newattack.html>
- (11) ウェブサイト及びメールアドレスに使用するドメインには、ISMAP のドメイン名「ismap.go.jp」を使用すること。なお、ドメインは取得済みであるため、ドメインの取得は、本調達の対象外とする。

5.3.2 セキュリティ要件

開発及び運用、保守におけるセキュリティ要件を以下に示す。サーバー攻撃等による様々なリスクに対抗できるセキュリティ対策を施すこと。また、検証環境においても同等の対策を講じること。なお、クラウドサービス事業者が実施する運用、保守におけるセキュリティ要件もあることから、請負者はこれを満たすことをシステムを構成するクラウドサービス事業者へ確認すること。

(1) アクセス制御及び証跡

- ① 「2.2 利用者区分」及び請負者に応じた権限の付与及び制御ができる機能を有すること。
- ② 管理者用 ID 等の特権ユーザがアクセス可能な IP アドレスを限定する等、特権ユーザの悪用に対する対策を行うこと。
- ③ 請負者の作業用 ID に関しても前項と同様に悪用に対する対策を行うとともに、所有する ID のリストとログイン履歴を定期的に IPA に報告すること。
- ④ 請負者が運用、保守のために利用する作業用 PC は限定し、通常業務に使用する PC とは区別すること。
- ⑤ 現行システムが正しく利用されていることの検証及び不正操作等がなされていないことの検証を行うために必要なログを取得できること。
- ⑥ ログは 30 日以上、当該システム上で保存され、必要に応じて参照可能であること。
- ⑦ ログは取得、ダウンロード可能であること。
- ⑧ ログが複数ある場合、日時が統一されていること。

(2) 脆弱性対策

- ① 請負者は、クラウドサービス部分の脆弱性対策について、クラウドサービス事業者との責任分担を明確にし、システム全体を通して対策が漏れなく行われることを確実にすること。
- ② 請負者は、クラウドサービス事業者やその他機関がもたらす脆弱性に関する情報を把握し、その脆弱性がもたらすリスクを分析の上、IPA に報告すること。
- ③ 請負者は、脆弱性がもたらすリスクを分析した結果、対策が必要と判断されるときは、対策方法や暫定的な回避策及び対策方法等を IPA に報告し、暫定回避策がシステムに与える影響や対策の実施計画及び対策テストの必要性、対策テストの方法及び実施予定について協議の上、脆弱性対策プランを策定し迅速に対応可能な体制を構築すること。
- ④ 利用しないプロセスやサービスは停止すること。

(3) ウイルス対策

- ① 最新のウイルス対策が行われること。

(4) 修正プログラムの適用

- ① 請負者は、クラウドサービス部分の修正プログラムの適用について、クラウドサービス事業者との責任分担を明確にすること。
- ② 請負者は、現行システムで導入するソフトウェアについて、原則として開発時にサポート対象となる最新バージョンとし、各種不具合修正用プログラムやパッチを適用すること。

- ③ 請負者は、発売元または提供元より入手した修正プログラム等のリリース情報に基づき、適用すべき修正プログラム等を選別し、IPA と協議の上でこれを適用すること。
- (5) ファイアウォール
 - ① 原則として、外部からのアクセスはHTTPS のみ通過させ、外部へのアクセスは必要最小限のプロトコルを通過させるようにすること。なお、配信メールのエラー通知受信や請負者の運用・保守担当者によるリモートアクセスの許可等、必要な設定については設計工程にて定義する。
- (6) データ改竄対策
 - ① 納入前にネットワークスキャンを実施し、不要ポートの閉塞確認を行うこと。ただし、クラウドサービスで適切に対策が行われている場合、この限りではない。
 - ② データのアクセス権設定を適切に行うこと。
 - ③ アプリケーションプログラムへの書き込み権限を適切に管理すること。
- (7) Web コンテンツ等の脆弱性予防対策
 - ① 潜在的な脆弱性に対し、Web アプリケーションファイアウォール等を用いた予防対策を行うこと。
- (8) なりすまし等の対策
 - ① ログイン後の画面に前回ログイン日時を表示する等、ユーザのなりすましによる被害を軽減する対策を施すこと。
 - ② クリックジャッキングの対策として、HTTP レスポンスヘッダに X-FRAME-OPTIONS を設定すること。
- (9) システムの監視
 - ① 不正アクセス、DDos 攻撃、マルウェアなどによる不正通信等サイバー攻撃に対する監視を行い対応すること。
 - ② データセンタ等へ入館が可能な要員を必要最低限とする、監視カメラで出入りを記録する等、物理的な防御を行うこと。
- (10) データの保護
 - ① 申請情報やログ等の保護すべき業務データは一般利用者（監査機関、クラウドサービス事業者、その他インターネット経由の第三者）が直接アクセスできないよう対策を行うこと。
 - ② 現行システムで扱うデータについては、全て暗号化すること。また、IPA にて、鍵の変更、廃棄が可能であること。なお、本システムで扱うデータとは、ユーザアカウント、申請フォーム、添付ファイル、文書管理システム上のファイル、バックアップを指すが、これらの内容を含むログ等がある場合は対象とする。
- (11) 通信の暗号化
 - ① クライアントとサーバ間の通信は暗号化すること。
- (12) アプリケーション・コンテンツの開発
 - ① アプリケーション・コンテンツに不正プログラムや以下に示すような脆弱性が含まれないよう開発時に十分配慮し、受け入れ時に実施するペネトレーションテストにて脆弱性が検出した場合は速やかに対処すること。
 - SQL インジェクション脆弱性
 - OS コマンドインジェクション脆弱性
 - ディレクトリトラバーサル脆弱性
 - セッション管理の脆弱性
 - アクセス制御欠如と認可処理欠如の脆弱性
 - クロスサイトスクリプティング脆弱性
 - クロスサイトリクエストフォージェリ脆弱性
 - クリックジャッキング脆弱性
 - メールヘッダインジェクション脆弱性
 - HTTP ヘッダインジェクション脆弱性
 - eval インジェクション脆弱性
 - レースコンディション脆弱性
 - バッファオーバーフロー及び整数オーバーフロー脆弱性
 - ② 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。
 - ③ 提供するアプリケーション・コンテンツが真正なものであるよう、ウェブサイト改竄の脅威への対策を施すこと。

- ④ 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制する等のセキュリティ水準を低下させる設定変更を OS やソフトウェアの利用者に要求することがないように、アプリケーション・コンテンツの提供方法を定めて開発すること。
- ⑤ サービス利用にあたって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供される等の機能がアプリケーション・コンテンツに組み込まれることのないよう開発すること。

(13) 電子メールの対策

- ① システムから発信する電子メールには、SPF、DKIM、DMARC 等の送信ドメイン認証技術や S/MIME 等の電子署名技術の採用によるなりすましの防止策を講ずること。
- ② 電子メールサーバが電子メールの不正な中継を行わないように設定すること。
- ③ インターネットを介して通信する電子メールの盗聴及び改竄の防止のため、SMTP による電子メールのサーバ間通信を TLS (SSL) により保護する、S/MIME 等の電子メールにおける暗号化及び電子署名の技術を採用する等の対策を講ずること。
- ④ 他の利用者と共用する電子メールサービスを利用する場合は、なりすました電子メールが当該電子メールサービスを利用する他の利用者から送信されない仕組みを備えること。他の利用者と共用しない専用の IP アドレスを割り振ることが望ましい。

(14) パスワードに関する対策

IPA もしくは監査機関選定組織 が制度運営支援システムへのログインにパスワードを利用する場合、以下の対策を施すこと。

- ① 初期パスワードをシステムで生成する場合は、推測が困難な文字列で発行する。
- ② 初回ログイン時には、初期パスワードの変更を求める。
- ③ パスワードの変更には、現行のパスワードの入力を求める。
- ④ 入力後の応答メッセージが認証情報の推測のヒントとならない工夫をする。
- ⑤ 入力フィールドでは、パスワードは伏字で表示させるようにする。
- ⑥ パスワードをサーバ内で保管する際は、平文ではなくソルト付きハッシュの形で保管する。
- ⑦ 一定時間内のログイン失敗回数が基準値を超えた場合には、アカウントをロックする。
- ⑧ 原則として、以下のパスワードフィルタの規則を設定する。
 - ・ 10 文字以上で英字と数字と記号がそれぞれ 1 文字以上含まれるものを許可する。
 - ・ ユーザ ID が含まれるものは許可しない。
 - ・ 以前 4 回と同じパスワードは許可しない。
 - ・ 初期パスワード等を含むよくあるパスワードが登録されたパスワード辞書にあるものは許可しない。
- ⑨ 2 要素認証を行うこと。
- ⑩ パスワード忘却等に対する救済措置について、十分にセキュリティに配慮した仕組みを設けること。

(15) その他情報セキュリティに関する事項

- ① 請負者は、その従業員、再請負先、若しくはその他の者による意図せざる変更が加えられないための管理を徹底し、プロジェクト計画書に管理体制を記載すること。
- ② 請負者は、本事業に従事する者を限定すること。本事業の実施期間中に従事者を変更等する場合は、事前に IPA に報告すること。また、請負者は IPA から要請があった場合に、資本関係・役員の情報、本事業の実施場所、本事業の全ての従事者の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍に関する情報を提供すること。
- ③ 請負者は、本事業に係るセキュリティインシデントが発生した場合、速やかに IPA に報告を行い、対処方法を協議のうえ実施すること。
- ④ 請負者は、IPA との秘密情報の受渡に関して、安全管理措置が講じられた方法を採用すること。なお、受渡、廃棄・抹消、及び確認方法等の秘密情報取扱に関する具体的な手順については、IPA と協議の上決定する。
- ⑤ 請負者は、IPA が実施する情報セキュリティ監査またはシステム監査を受け入れるとともに、指摘事項への対応を行うこと。
- ⑥ 請負者は、情報セキュリティ対策が不十分であることが判明した場合、またはそうした状態になることが予見された場合は、必要となる改善策を提案し IPA と協議の上実施するこ

- と。
- ⑦ 請負者は、本事業を再請負する場合は、再請負することにより生ずる脅威に対してセキュリティが十分に確保されるよう、セキュリティ対策の実施を契約等により再請負先に担保させること。なお、再請負先におけるセキュリティの確保については、請負者の責任とする。
 - ⑧ 請負者は、本事業におけるセキュリティ対策に関して、本書に記載された要件以外で必要と考えられる措置がある場合はそれを実施すること。

5.3.3 セキュリティ対策の改善

セキュリティ要件を満たすことができなくなった場合、またはそうした状態になることが予見された場合は、必要な改善策を提案し、IPA と協議の上で実施すること。

5.4 教育・研修要件

- (1) 本改修で追加される機能について、利用者向け研修計画を立てるものとし、研修計画に従って実施すること。（対象職員：12名程度だが、本改修においてはシステム担当者1名で実施予定）
- (2) 研修計画書及び結果報告書を提出すること。
- (3) 職員向け操作マニュアル等を既存のマニュアルに追記する形で提供すること。
- (4) 申請者向け（クラウドサービス事業者）の操作マニュアルを既存のマニュアルに追記する形で提供すること。

6 設計要件

今回の改修で追加された機能に対して、本書に記載されている要件を満たす機能設計、非機能設計を行い、基本設計書及び詳細設計書を作成すること。

設計作業では、業務面及び技術面について実現性や実効性、リスク耐性等を十分に検討すること。なお、設計作業の完了をマイルストーンとして設定し、基本設計書及び詳細設計書について IPA の承認を得てから開発を進めること。

特に以下について配慮し、IPA の承認を得た上で設計書を完成させること。

- 本書で示す要件との間に不整合が生じる可能性がある場合、IPA と協議の上で不整合を解消すること。
- 技術的な実現性が担保できること。
- 同時オペレーションによるデータのコンフリクトや誤ったデータの登録による不整合等、業務運用において起こり得る異常処理を考慮した設計であること。
- 業務における効率性、効果について配慮すること。
- 利用者区分によるアクセス（システムの操作、情報登録、参照、削除等）の制御を考慮した設計を行うこと。
- 設計の観点でセキュリティ面の脆弱性を生まないように配慮すること。

7 テスト要件

7.1 テスト範囲

- (1) 機能要件及び非機能要件を担保するためのテストを行うこと。また、IPA の承認を受け円滑にテストを実施すること。
- (2) 下記のテストが実施されることを想定する。
 - ・ 詳細設計に基づく単体テスト
(SaaS、パッケージ製品等を利用した場合は変更を加えた範囲)
 - ・ 基本設計に基づく結合テスト
 - ・ 本書及び提案書に基づくシステムテスト
 - ・ 本書及び提案書に基づく受入れテスト支援
- (3) IPA が受入れテスト期間中に実施するセキュリティテスト(ウェブアプリケーションのセキュリティテストを含む)において、発見された問題を解消すること。また、セキュリティテストの実施に際し、実施日、実施内容等についてクラウドサービス事業者と調整を行うこと。
- (4) IPA が受入れテストに併せて実施するペネトレーションテストについて発見された問題に対して解消すること。ペネトレーションテストと同等のテストを総合テストで実施することが望ましい。ペネトレーションテストで実施される想定内容を以下に記載する。
 - ・ クロスサイトスクリプティング
 - ・ SQL インジェクション
 - ・ セッション管理
 - ・ 認証機能の安全性
 - ・ ファイル拡張子診断
 - ・ OS コマンドインジェクション診断
 - ・ ディレクトリトラバーサル診断
 - ・ 権限昇格診断
 - ・ パラメータ書き換え診断
 - ・ その他 Web アプリケーション固有の問題の診断

7.2 テスト計画の策定

テスト方針、品質指標、開始及び終了条件、テスト実施体制、テスト方法(利用するツール等を含む)、テストデータ、テスト環境、テスト運営方法等について記述したテスト計画書を作成し、IPA の承認を得ること。

7.3 テスト方法

- (1) システムテスト
 - ① システムテストは、構築したシステム環境の正常稼働、及び開発したアプリケーションが本書に基づいた要件を満たすことを担保するために実施する。
 - ② システムテストに伴って発生するアプリケーションの修正や設定変更等の作業を行うこと。また、テスト終了時にシステムテスト報告書を作成すること。
 - ③ システムテスト工程で発見された不具合等については、システムテスト工程完了時までに対応を完了すること。
- (2) 受入テスト、ペネトレーションテスト
 - ① 受入テストは、IPA がテスト仕様書を作成し、これに基づいて実施する。請負者は、IPA の作業支援を行うこと。
 - ② 受入テストにおいて納入物件の全部または一部に不合格が生じた場合は、直ちに必要な修復を行うこと。
 - ③ テスト実施結果を取りまとめる作業に協力すること。
 - ④ テスト時に使用した一時ファイル等の不要な資産は、テスト終了後に請負者が削除すること。また、設定等を見直し、システムの稼働が可能な状態とすること。

7.4 テストデータ

- (1) テストで使用するデータが存在するときは、テスト計画書に使用するデータの種類等を記載し、使用したテストデータをテスト結果とともに IPA に提示すること。
- (2) テスト終了時には、テスト時に使用した不要なデータ、ユーザ ID 等が存在しない状態であること。
- (3) テスト終了時には、テスト時に使用した不要なプロセス及びサービス等は、運用開始までに完全に停止すること。

8 移行に関する要件

システム導入前に実施している業務データについてもシステム導入後のデータと同じように扱える状態にする必要がある。しかしながら、アカウント情報については機密性が高いものが多くあることから、容易に移行できる手段及び手順の提供をすること。なお、移行手順及び移行環境に関しての情報セキュリティ要件は、「5.3.2 セキュリティ要件」の各要件を遵守すること。コンテンツの移行方法やスケジュール等については、以下の要件を満たす「コンテンツ移行計画書」を作成し、IPA の承認を得ること。

- (1) 本番環境へのリリース及びデータの移行に伴うシステムの停止（利用者が本システムの各機能を利用できない状態を指す）は可能な限り短時間とし、停止時間は最大でも 48 時間以内（移行に失敗した場合の切り戻しに要する時間を含む）とすること。

9 保証要件

- (1) 納品時において納入物件が設計したとおりに動作することを保証すること。
- (2) 納入物件に関わる技術的な問題（導入時に使用していない機能や、バージョンアッププログラムを含む）で、設計書等により判別がつかない事象が発生した場合に、速やかに対応し事象を解決することができる技術情報の提供体制を構築すること。
- (3) 納入物件に関するセキュリティパッチ及びアップデートの適応について、速やかに IPA に情報提供するとともに、システムが正常動作することを保証すること。
- (4) JVN（Japan Vulnerability Notes）、JVN iPedia の活用等により、IPA に対し本システムのセキュリティリスクに関する情報提供を適宜かつ速やかに行うこと。
- (5) 設計書に基づいた保証基準を保証期間開始前に作成し IPA に承認を得ること。
- (6) システム障害発生等によるサービスの停止に際し、迅速な対応を行うこと。また、業務継続上問題がない程度の障害である場合においても、IPA と協議の上、承認された対応策を適用すること。
- (7) 運用・保守や障害対応の結果、成果物の内容に変更が生じた場合は、都度再納入すること。
- (8) 下記項目については保証の範囲外とする。
 - ・ 利用者側の故意により問題が発生した場合。
 - ・ 納入後に請負者以外が行った機能追加等の改修及び改造部分に関する問題である場合。ただし、問題の切り分けについては請負者の範囲とする。
 - ・ 納入物件に含まれる、請負者または第三者が従前から保有する知的財産権が含まれている物件のバージョンアップ等により保証対象範囲の変更が必要となった場合。
 - ・ 保証の対象外であることを、保証期間開始前に IPA と合意した項目の場合。
- (9) 保証期間における役割分担については、表 11 に示す。
 - ・ IPA：リスクマネジメント部クラウドサービス評価グループ システム管理者
 - ・ 運用保守業者：「ISMAP ポータルサイト及び制度運営支援システムの 2023 年度以降保守・運用支援業務」の請負業者
 - ・ 請負者：本調達で受託した請負業者

表 11 保証期間における役割分担

分類	項目	内容	IPA/運用 保守業者	請負者
管理	インシデント管理	異常または中断、劣化させる事象の発生から訂正までの管理 過去実績の調査・解決策の情報収集、対応策の決定	△	◎
	問題管理	インシデントが問題（障害）であった場合の具体的な訂正	△	◎
	変更管理	システムの変更	△	◎
	リリース管理	本番環境へのリリース	△	◎
	構成管理	システムへの変更に関する履歴等の管理	△	◎
	定期報告	システム稼働状況や運用・保守作業等の定期報告	△	◎
製品保証	ハードウェア製品	故障部品の交換等	△	◎
	ソフトウェア製品	更新セキュリティ対応	△	◎
システム保証	監視	運用状況の監視、データ収集	△	◎
	点検	機器・部品等の定期的な点検	△	◎
	バージョンアップ	セキュリティパッチ等のテスト及びシステムへの組み込み	△	◎
	設定変更	ハード・ソフトの設定値変更	△	◎
	バージョン管理	補修、仕様変更等の管理	△	◎
教育	利用者教育（外部）	監査機関、クラウドサービス事業者向けの操作マニュアルの作成及びメンテナンス	△	◎
	利用者教育（内部）	業務実施者、業務管理者、システム管理者向け操作マニュアルの作成及びメンテナンス	△	◎
業務運用と利用者支援	ユーザ管理	利用者 ID の追加、削除、更新等	◎	-
	マスターメンテ	業務データ管理	◎	-
	問合せ対応	利用者からの質問への回答	◎	○
	ログ分析	システムが出力するログのエラー検知、分析等	△	◎
問題の解決	障害対応	システム障害の復旧作業等	△	◎
	障害原因調査	システム障害の原因追求と問題点の切り分け	△	◎
	不具合補修	問題点の解消（プログラム改造、部品交換、バージョンアップ）	△	◎

△：承認または確認 ◎：主担当 ○：一部担当 -：該当しない

10 プロジェクト管理要件

10.1 プロジェクト管理業務

- (1) プロジェクト計画書（方針、作業アプローチ、条件、WBS、計画スケジュール、体制、品質及びリスク管理方法、課題管理方法等）を契約後 2 週間を目途に作成し、作業開始前に IPA の承認を得ること。
- (2) プロジェクト計画書には、プロジェクトの効果目標や要求事項、要求との関係、各種テストによる効果目標や要求事項の達成、要求の実現可能性等について記載すること。

10.2 スケジュールの策定

本開発範囲における詳細スケジュールを策定すること。策定における条件は以下のとおり。

- (1) 工程の開始・終了が明確であること。想定している工程は以下に示すとおりであり、これ以外に必要と考える工程がある場合には追加で記載すること。
 - 基本設計工程
 - 詳細設計工程
 - 製造工程
 - 単体テスト工程
 - 結合テスト工程
 - システムテスト工程
 - 受入れテスト及び稼働準備工程
- (2) IPA が作業のボリュームを把握して機構内の手続きや作業に係る要員計画を作成できるよう、IPA 側の作業項目（要件のヒアリングや承認行為、受け入れ試験等）と実施時期について記載すること。
- (3) マイルストーンについては以下を想定する。詳細は、IPA と協議の上決定することとする。
 - キックオフ
 - 仕様凍結宣言
 - 工程終了／次工程開始宣言（工程毎）
 - 本番稼働承認

10.3 プロジェクト体制

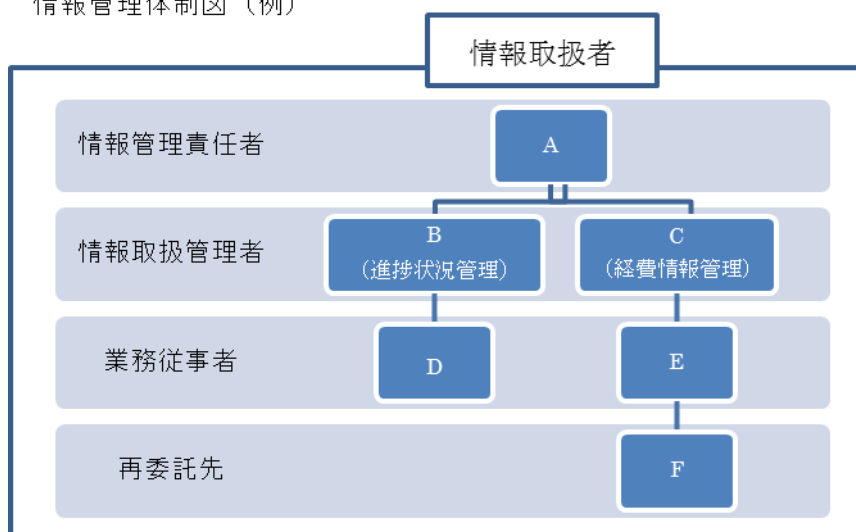
- (1) 組織またはプロジェクトメンバーは、以下の要素技術に関して理解していること
 - Service Now CSM 製品に関する技術知見
 - ServiceNow と gBizID との認証連携
 - AWS KMS を用いた ServiceNow の暗号鍵の管理
 - AWS SES と ServiceNow のメール送信連携
 - SVF Cloud for ServiceNow を用いた帳票出力
 - ServiceNow と Box との連携
- (2) 組織またはプロジェクトメンバーは、類似システム（電子申請システム等）の開発経験を有すること。
- (3) プロジェクト体制図を作成し、プロジェクトメンバーの主担当作業、所有資格、保有スキル、関与度合い等を記載すること。
- (4) プロジェクトメンバーや担当作業に変更が生じる場合、その旨をリスク分析結果とともに IPA に報告すること。
- (5) プロジェクトマネージャとして、情報処理の促進に関する法律に基づき実施される情報処理技術者試験の以下の何れかの区分に合格し、3 年以上の実務経験を有している者を、配置すること。
 - プロジェクトマネージャ試験
 - ITストラテジスト試験

- ・ システムアーキテクト試験
- 或いは、上記と同等以上の資格、若しくは同等以上と認められる実績を有する者を配置すること。
- (6) セキュリティ管理者として、情報セキュリティに関する知識及び技能を有する者を配置すること。情報処理安全確保支援士であることが望ましい。
 - (7) 利用するクラウドサービスの設定、カスタマイズについて、十分な知識や経験を有する要員が体制に含まれていること。
 - (8) 下記の資格を有する要員が体制に含まれていること。
 - ・ ServiceNow Certified Implementation Specialist - Customer Service Management
 - ・ ServiceNow Certified Application Developer
 - ・ ServiceNow Certified System Administrator
 - ・ AWS Certified Solutions Architect - Professional
 - ・ AWS Certified Sysops Administrator - Associate
 - (9) WBS を作成し、作業工程毎の作業内容、作業担当者、作業期間、工数、要素成果物、レビュー方法、リスク、開始、終了条件及び進捗計測基準等を明確にすること。
 - (10) 定期的に進捗状況等に関して報告書を作成し、IPA に報告すること。
 - (11) 情報管理体制について、以下に記載する事項を遵守すること。
 - ① 請負者は、本事業で知り得た情報を適切に管理するため、次の履行体制を確保し、IPA に対し「情報セキュリティを確保するための体制を定めた書面（管理体制図）」及び「情報取扱者名簿」（氏名、個人住所、生年月日、所属部署、役職等が記載されたもの）を契約前に提出し、担当部門の合意を得ること。（住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当部門から求められた場合は速やかに提出すること。）なお、情報取扱者名簿は、業務の遂行のため最低限必要な範囲で情報取扱者を掲載すること。

【確保すべき履行体制】

 - ・ 契約を履行する一環として契約相手方が収集、管理、作成等した一切の情報が、IPA が保護を要しないと確認するまで情報取扱者名簿に記載のある者以外に伝達または漏えいされないことを保証する。

情報管理体制図（例）



※情報管理体制図に記載すべき事項は、下記のとおり。

- ・ 本業務の遂行にあたって保護すべき情報を取り扱う全ての者。（再委託先も含む。）
- ・ 本業務の遂行のため最低限必要な範囲で情報取扱者を設定し記載すること。
- ・ 情報管理規則等を有している場合で上記例を満たす情報については、情報管理規則等の内規の添付で代用可能とする。

情報取扱者名簿（例）

		(しめい) 氏名	個人 住所	生年 月日	所属 部署	役職	パスポート 番号及び国 籍（※4）
情報管理責任者（※1）	A						
情報取扱管理者（※2）	B						
	C						
業務従事者（※3）	D						
	E						
再委託先	F						

※1 請負者として情報取扱の全ての責任を有する者。必ず明記すること。

※2 本業務の遂行にあたって主に保護すべき情報を取り扱う者ではないが、業務の進捗状況等管理を行うなど、保護すべき情報を取り扱う可能性のある者。

※3 本業務の遂行にあたって保護すべき情報を取り扱う可能性のある者。（再委託先も含む）

※4 日本国籍を有する者、及び法務大臣から永住の許可を受けた者（入管特例法の「特別永住者」を除く。）以外の者は、パスポート番号及び国籍を記載。

※5 個人住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当部門から求められた場合は速やかに提出すること。

- ② 本業務で知り得た一切の情報について、情報取扱者以外の者に開示または漏えいしてはならないものとする。ただし、IPAの承認を受けた場合はこの限りでない。
- ③ ①の情報セキュリティを確保するための体制を定めた書面または情報取扱者名簿に変更がある場合は、予めIPAへ届出を行い、同意を得なければならない。
- ④ 本業務に従事する全ての者の経歴（氏名、所属、役職、学歴、職歴、業務経験、研修実績、専門知識や知見、母国語及び外国語能力、国籍等）がわかる資料を提出すること。
※経歴を提出しない者の人件費は計上不可とする。
- ⑤ IPAから提供した資料またはIPAが指定した資料の取扱い（返却・削除等）については、IPAの指示に従うこと。業務日誌をはじめとする経理処理に関する資料については適宜保管すること。

10.4品質及びリスク管理

- (1) 品質保証に関する計画の立案、管理及び改善のため、品質計画書を作成すること。
- (2) 品質計画の立案、検証及び品質改善策の検討と実施を管理する体制を確保すること。
- (3) 品質確保に関する各種取り組みが計画通り実施されていることを確認し、定期的にIPAへ報告すること。
- (4) 基本設計、詳細設計、各種テスト等の各工程完了時には、品質評価結果をIPAに報告し、承認を得ること。
- (5) 受入れテスト終了時に、プロジェクトの品質管理結果を記載した品質管理報告書を提出すること。
- (6) プロジェクトの遂行に影響を与えるリスクを識別し、その発生要因や発生確率、影響度及び管理方法等について定期的に具体的な分析を行うこと。
- (7) 分析結果を記載した報告書等により定期的にIPAへ報告すること。

10.5 課題管理

プロジェクトで発生した課題については、その内容、発生日、担当者、検討状況、検討結果及び解決日等の必要情報を一元的に管理すること。

- (1) 定期的に課題対応状況を監視し、解決を促す仕組みを構築すること。
- (2) 課題発生時には、速やかに IPA に報告し対応策を検討すること。

10.6 コミュニケーション管理

- (1) 請負者の責任者と IPA により編成されるプロジェクトの意思決定・承認機関を編成し、プロジェクト上発生し得るリスクや発生した課題、是正要求、変更管理は、全て当該機関に報告され、協議、意思決定するものとする。
- (2) プロジェクトで実施すべき会議について、内容、出席者、開催頻度、提示情報及び報告様式等を定義し、プロジェクト計画書に記載した上で開催することとする。
- (3) 各会議において議事録を作成し、IPA に提出の上承認を得ること。
- (4) 定期報告事項については、報告の頻度と時期を定めること。少なくとも、月次での進捗報告を行うこと。
- (5) IPA に提出する報告様式は、現状と計画との差異、今後の予測、及び対応策等が盛り込まれており、状況を把握でき各種判断を容易に行えるものであること。
- (6) プロジェクト関連情報の作成、収集、配布、共有及び蓄積等の一連のプロセスに関してルールを策定し、プロジェクト計画書に記載すること。
- (7) プロジェクト早期に、成果物の予測ボリュームやレビュー担当者、レビュー予定期日を定義したレビュー計画を策定すること。

11 開発範囲

11.1 作業範囲

- (1) 本書で記述する要求事項を満たすサービス、ソフトウェアの開発に係る、以下の作業を行うこととする。
 - 基本設計作業
 - 詳細設計作業
 - 製造作業（アプリケーション作成、システム環境構築等）
 - 単体テスト実施
 - 結合テスト実施
 - システムテスト実施
 - 受入れテスト支援、稼働準備支援
- (2) 利用者（業務実施者、業務管理者、システム管理者）、申請者向けの操作マニュアルを作成すること。
- (3) 本書で記述するシステム開発に関するプロジェクト管理、課題管理、リスク管理等のプロジェクト推進に関する作業を行うこと。
- (4) 納入物件、及びプロジェクト管理に関するドキュメント（課題管理表、議事録等）作成を行うこと。

11.2 環境

開発用 PC、及び作業場所については請負者にて用意すること。

なお、受入れテストは、IPA が所有する PC を利用して実施する。

11.3 成果物

納入する成果物の一覧を、表 12 表 12 に示す。各種ドキュメントは、各工程の進捗に併せて提出すること。

なお、下記に示す以外のドキュメント（プロジェクト進行に伴う報告書、議事録、課題管理票、管理台帳、連絡票等）についても、適宜 IPA に提出すること。

表 12 成果物

No.	工程	成果物	提出時期／備考	数量
1	基本設計	基本設計書	基本設計終了時	1 式
2		プロジェクト計画書	契約後 2 週間を目途	1 式
3	詳細設計	詳細設計書	詳細設計終了時／パッケージ製品等を利用した場合は個別に変更した範囲のみ	1 式
4		品質計画書	製造開始前	1 式
5		テスト計画書	テスト開始前	1 式
6	製造	ソースコード 実行プログラム	受入れテスト終了時／パッケージ製品等を利用した場合は個別に変更した範囲のみ	1 式
7	単体テスト	単体テスト仕様書兼結果報告書	単体テスト終了時（単体テスト仕様書は単体テスト開始前）／パッケージ製品等を利用した場合は個別に変更した範囲のみ	1 式
8	結合テスト	結合テスト仕様書兼結果報告書	結合テスト終了時（結合テスト仕様書は結合テスト開始前）	1 式
9	システムテスト	システムテスト仕様書兼結果報告書	システムテスト終了時（システムテスト仕様書はシステムテスト開始前）	1 式
10	受入れテスト/稼働準備	操作マニュアル	受入れテスト開始前	1 式
11		品質管理報告書 保証基準	受入れテスト終了時	1 式
12		コンテンツ移行計画書	移行作業前	1 式

11.4スケジュール

想定するプロジェクトの全体スケジュールを、図 7 全体スケジュールに示す。

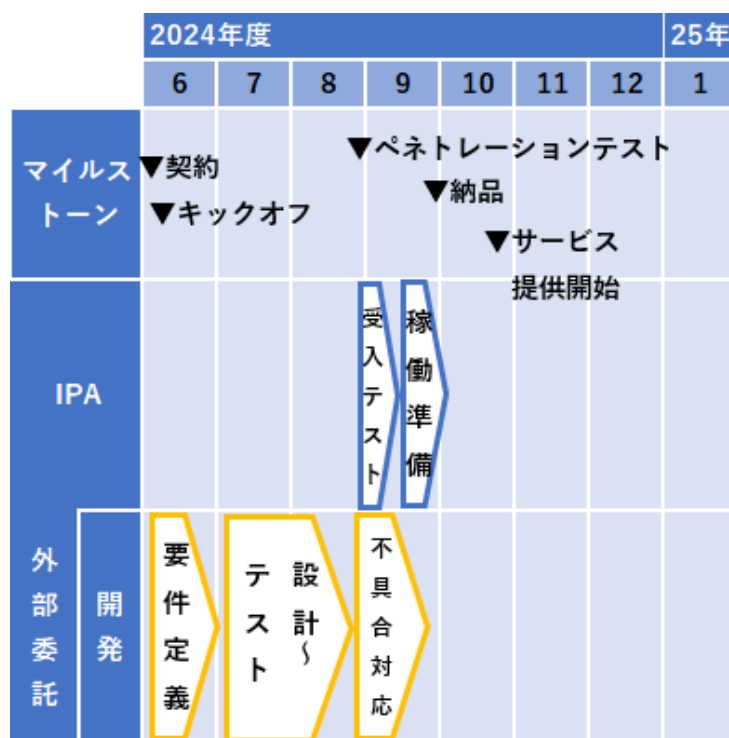


図 7 全体スケジュール

請負者は、稼働に向けた以下の期日を遵守した作業の詳細スケジュールを策定し、プロジェクトを推進すること。

- 受入れテスト開始 : 2024年8月26日
- 最終納品 : 2024年9月30日

11.5納入要件

11.5.1 納入物件及び納入期限

システム納入に係る最終納入期限は、2024年9月30日とする。

納入期限までに、表 12 に記載した成果物のうち以下に示す成果物一式を記録媒体（CD-R、DVD-R等）に格納して1部を納入すること。

なお、記録媒体の形式や紙媒体の要否等の詳細については、IPAの指示に従うこと。

- 基本設計書
- 詳細設計書
- 品質計画書
- テスト計画書
- ソースコード、実行プログラム
- 単体テスト仕様書兼結果報告書
- 結合テスト仕様書兼結果報告書
- システムテスト仕様書兼結果報告書
- 品質管理報告書
- 保証基準
- 研修計画書
- 結果報告書
- 職員向け操作マニュアル
- 申請者向け（クラウドサービス事業者）の操作マニュアル
- コンテンツ移行計画書

11.5.2 納入場所

〒113-6591

東京都文京区本駒込2丁目28番8号 文京グリーンコートセンターオフィス16階
独立行政法人情報処理推進機構

セキュリティセンター リスクマネジメント部 クラウドサービス評価グループ

11.6 検収要件

検収では、本書の条件、項目を満たすか否かにつき検査を行う。また、品質については目的を満たすに十分か否かを判断する。

- (1) システム及びドキュメントについては、原則として公開を前提とした整備が行われていること。
- (2) システム及び成果に関連するソフトウェア、製品等については、それらを特定する名称やバージョンについてドキュメント中に正確に示されていること。
- (3) 品質管理報告書には、責任者の氏名、品質を保証するに足る品質管理方法、品質向上状況、数値化した検査結果が含まれていること。

<留意事項>

- 納入物件については、納入する前にIPAのレビューを受けること。
- 各納入物件に対し、あらかじめ協議して定めた内容を全て満たしていること。また、レビュー後の改訂事項等が反映されていること。
- 検査の結果、納入物件の全部または一部が不合格となった場合には、請負者は必要な補修を行った後、IPAの承認を得て指定した日時までに補修した納入物件を再納入すること。
- 納入物件以外にも、必要に応じて作成した成果物等の提出を求める場合があるため、作成資料等は細心の注意を以て管理し、常に最新の状態を保つこと。

11.6.1 システム構築時

本改修に係る納入物件について、納入を受けた日から30日以内に、本書に基づき検査を実施する。

12 留意事項

本業務を遂行するにあたり留意する事項について、以下に示す。

- 本業務の運営は日本語で行う。また、本書に記載した日付は全て日本の暦を基準とする。
- 本書に記載のない事項については、IPAと請負者で協議の上決定することとする。

— 以上 —