令和８年度

情報提供等記録開示システム
バックエンド機能の追加開発業務一式

別添２　要件定義書（案）

令和８年１月

デジタル庁

1. 業務要件定義 3
1.1. 業務実施手順 3
1.2. 業務の規模 9
1.3. 業務実施の時期・時間 9
1.4. 業務の実施等 9
1.5. 業務観点で管理すべき指標 9
1.6. 情報システム化の範囲 10
1.7. 業務の継続の方針等 10
1.8. 情報セキュリティ対策の方針等 10
2. 機能要件定義 11
2.1. 機能に関する事項 11
2.2. 画面に関する事項 12
2.3. 帳票に関する事項 12
2.4. データに関する事項 12
2.5. 外部インタフェースに関する事項 12
3. 非機能要件定義 14
3.1. ユーザビリティ及びアクセシビリティに関する事項 14
3.2. システム方式に関する事項 18
3.3. システム規模に関する事項 20
3.4. 性能に関する事項 22
3.5. 信頼性に関する事項 23
3.6. 拡張性に関する事項 24
3.7. 上位互換性に関する事項 25
3.8. 中立性に関する事項 25
3.9. 継続性に関する事項 26
3.10. 情報セキュリティに関する事項 29
3.11. 情報システム稼働環境に関する事項 31
3.12. データマネジメントに関する事項 33
3.13. テストに関する事項 34
3.14. 移行に関する事項 40
3.15. 引継ぎに関する事項 43
3.16. 教育に関する事項 44
3.17. 運用・保守に関する事項 44

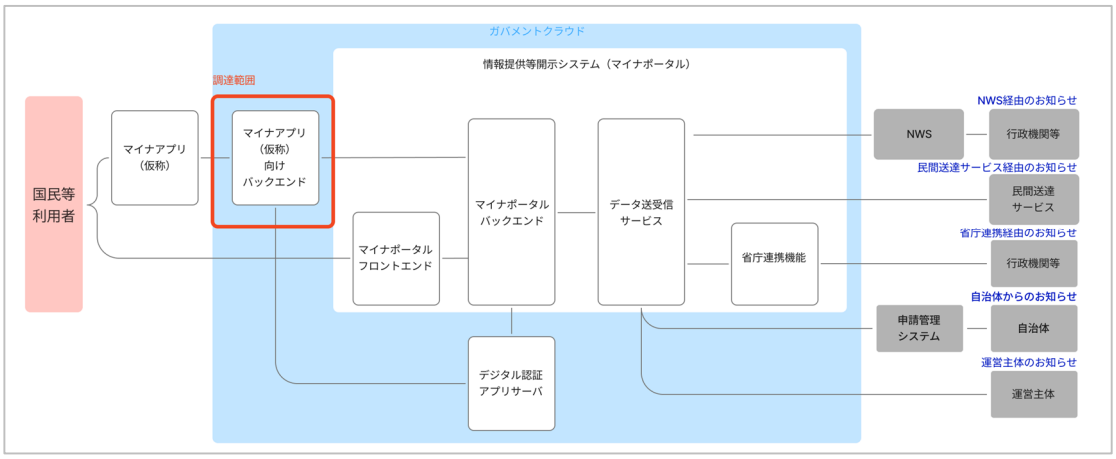
1. 業務要件定義

1.1. 業務実施手順

(1) 業務範囲

本業務の調達範囲を「図表 1 調達範囲」に示す。本調達は、マイナアプリ（仮称）向けのバックエンド機能を新規構築するものである。

図表 1 調達範囲



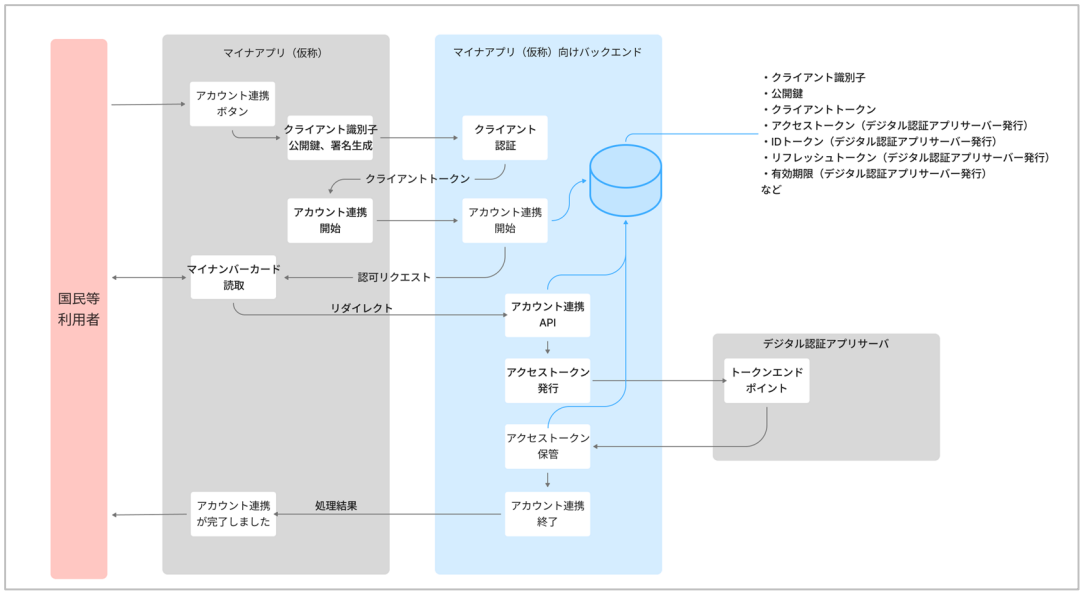
(2) 情報システム化範囲

情報システム化の範囲を以下に示す。なお、本記載は現状の想定であるため、主管課へのヒアリング等を実施の上、必要に応じて最適な処理フローを提案すること。

ア　アカウント連携

マイナアプリ（仮称）から、初回接続時にアカウント連携を行う。なお、アカウント連携可能な端末は 1 利用者につき 1 台とする。

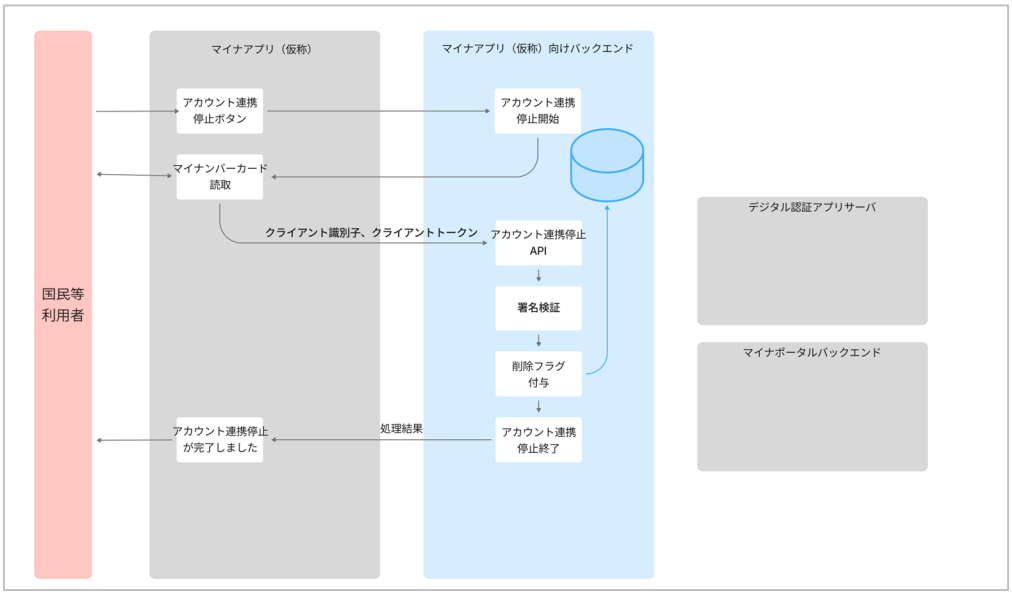
図表 2 アカウント連携



イ　アカウント連携停止

マイナアプリ（仮称）とのアカウント連携を停止する。

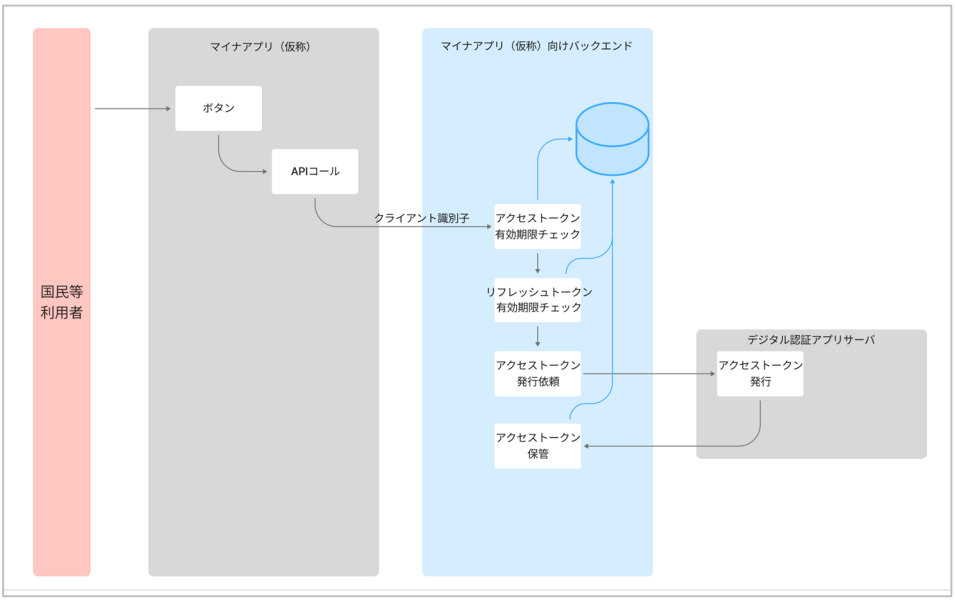
図表 3 アカウント連携停止



ウ　アカウント連携更新

マイナアプリ（仮称）から API がコールされた際に、アクセストークンの有効期限が切れていた場合、リフレッシュトークンの有効期限内であれば、自動的にデジタル認証アプリサーバから新しいアクセストークンを取得する。

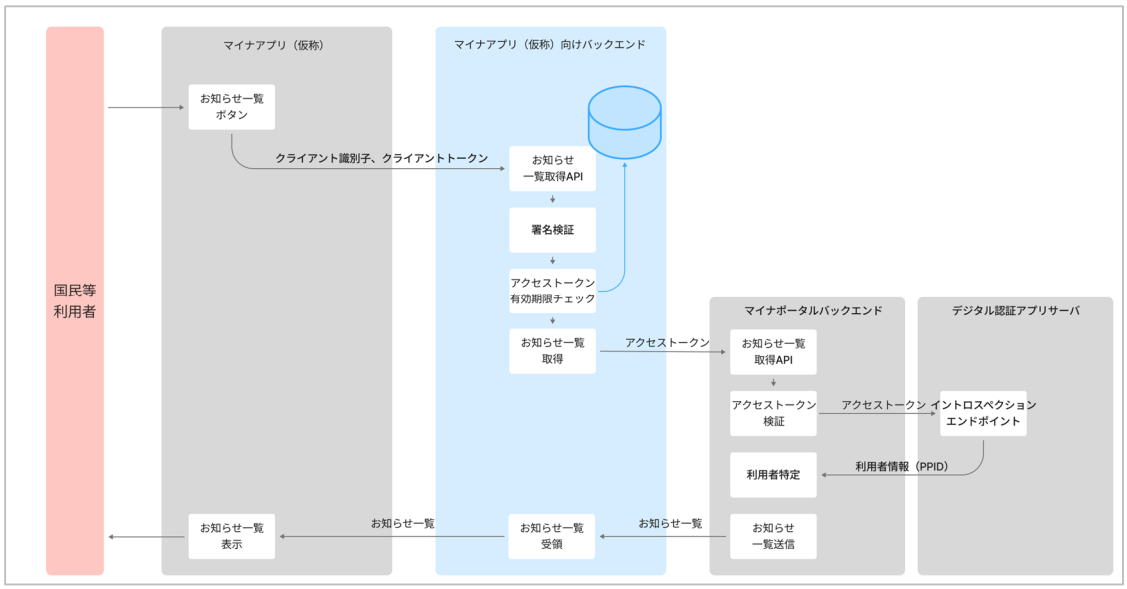
図表 4 アカウント連携更新



エ　お知らせ一覧取得

マイナポータルバックエンドからお知らせ一覧を取得し、マイナアプリ（仮称）に連携する。

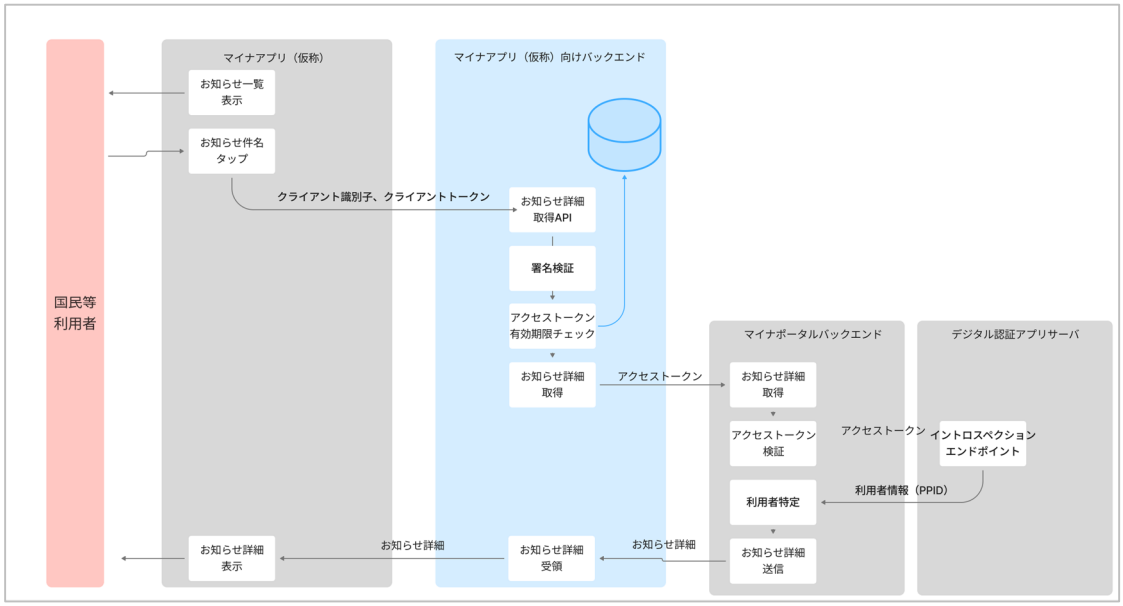
図表 5 お知らせ一覧取得



オ　お知らせ詳細取得

マイナポータルバックエンドからお知らせ詳細を取得し、マイナアプリ（仮称）に連携する。

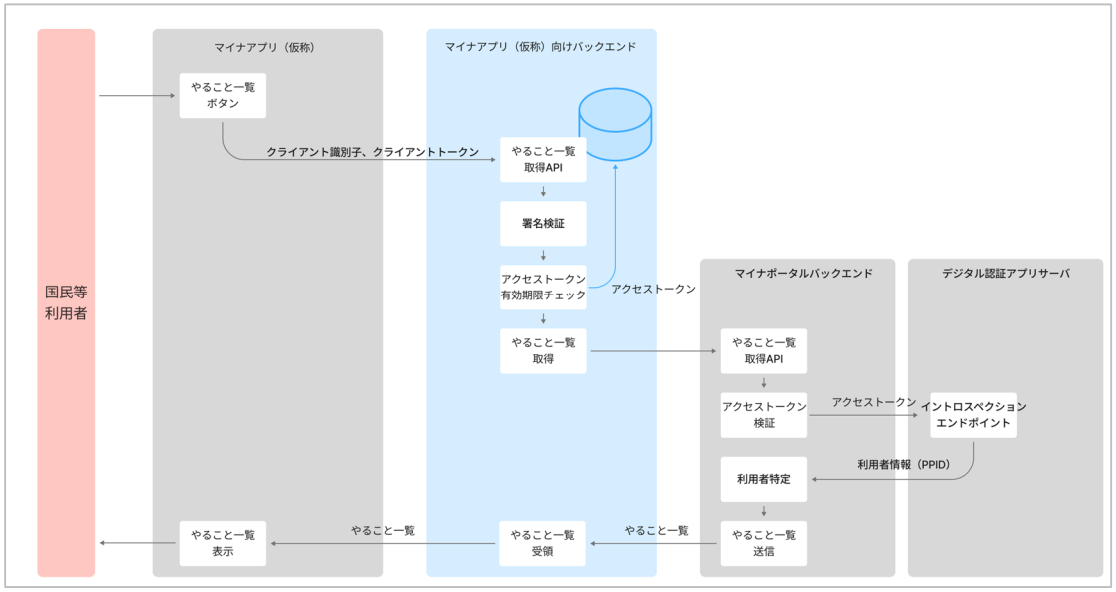
図表 6 お知らせ詳細取得



カ　やること一覧取得

マイナポータルバックエンドからやること一覧を取得し、マイナアプリ（仮称）に連携する。

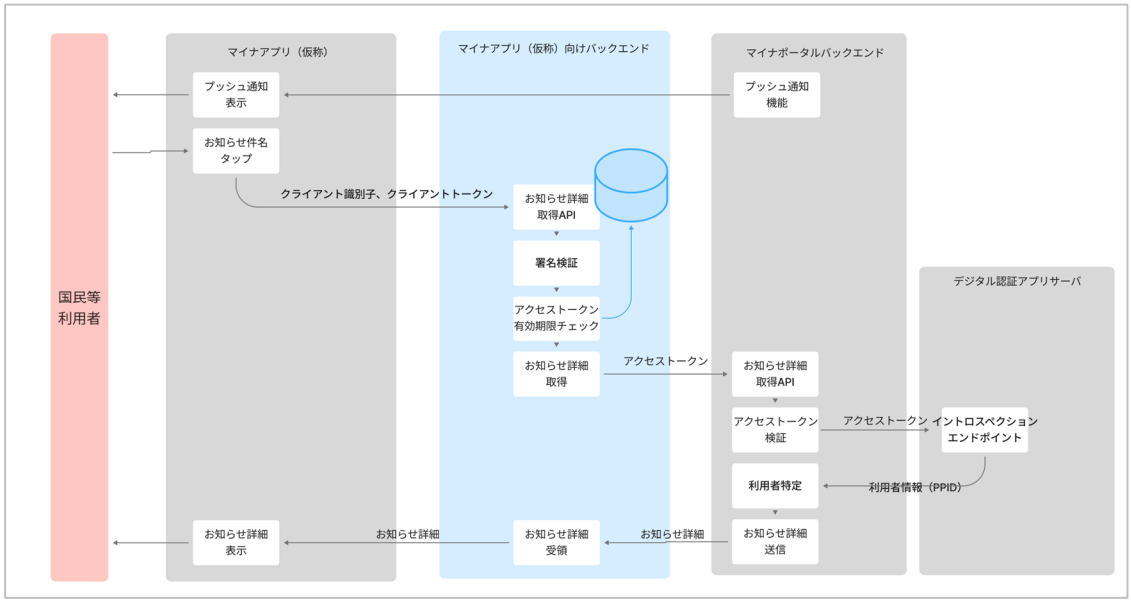
図表 7 やること一覧取得



キ　プッシュ通知機能

マイナポータルバックエンドからのプッシュ通知をマイナアプリ（仮称）に連携する。

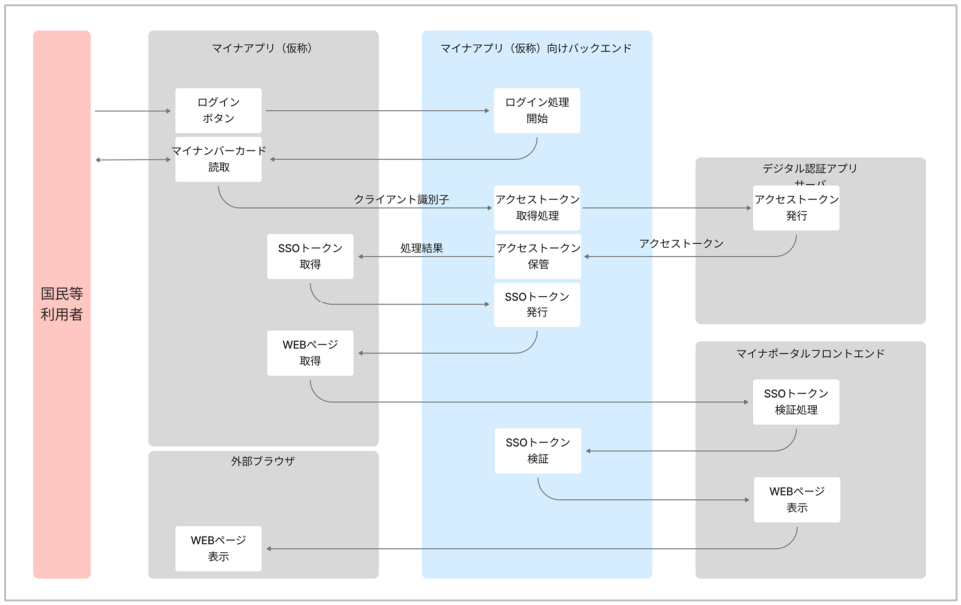
図表 8 プッシュ通知機能



ク　マイナポータルへの SSO 機能

マイナポータル（WEB サイト）へのログインに必要な認証を行い、WEB ページにリダイレクトする。

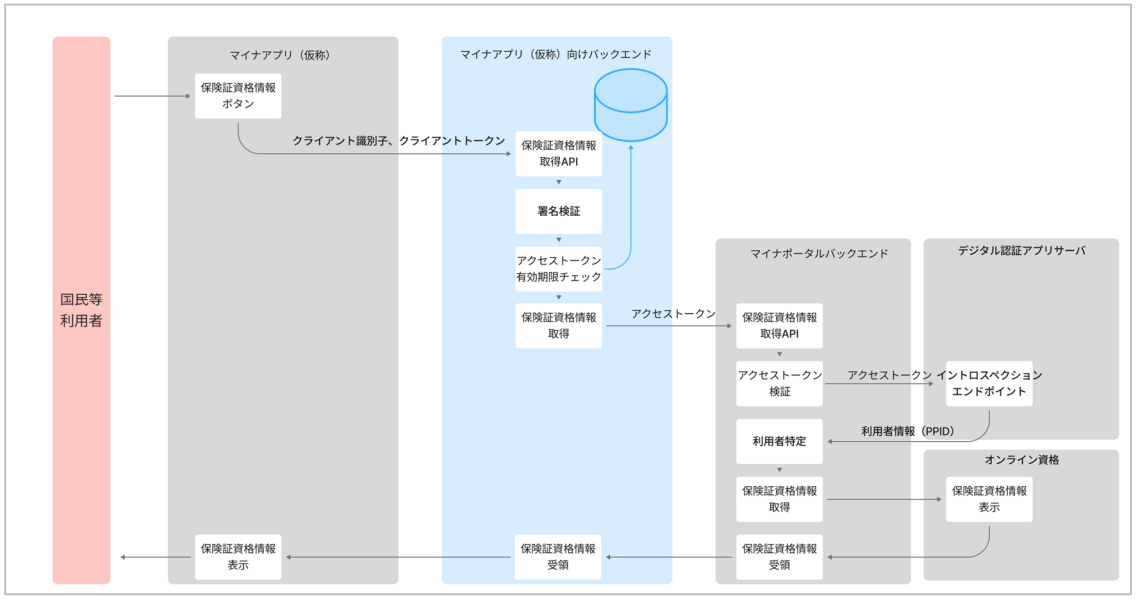
図表 9 マイナポータルへの SSO 機能



ケ　保険証資格情報取得機能

マイナポータルベックエンドから保険証資格情報を取得し、マイナアプリ（仮称）に連携する。

図表 10 保険証資格情報取得機能



(3) 業務の実施に必要な体制

本システム関連業務の実施に現段階で想定する体制について「図表 11 業務の実施体制」に示す。

図表 11 業務の実施体制

項番	実施体制	業務概要	補足
1	マイナアプリ（仮称）向けバックエンド担当 ※受託者含む	マイナアプリ（仮称）向けバックエンドに関する、要件定義、開発、運用等を行う。	—
2	マイナアプリ（仮称）担当	マイナアプリ（仮称）に関する、要件定義、開発、運用等を行う。	—
3	マイナポータルバックエンド担当	マイナポータルバックエンドに関する、要件定義、開発、運用等を行う。	—
4	デジタル認証アプリサーバ担当	デジタル認証アプリサーバに関する、要件定義、開発、運用等を行う。	—
5	工程管理支援事業者	マイナポータルの開発全般に関する、工程管理支援を行う。	—

(4) データ量

2025 年のお知らせ件数を「図表 12 お知らせ件数」に示す。なお、マイナアプリ（仮称）及びマイナポータル、関連システムの利用範囲の拡大に伴い、データの範囲と種類、容量が拡大する可能性もあることを、あらかじめ留意すること。

図表 12 お知らせ件数

項番	項目	対象月	件数	開封件数	開封率
1	運営主体お知らせ	2025 年 1 月	171,740,450	8,489,402	4.94%
2		2025 年 2 月	86,927,740	3,502,272	4.03%
3		2025 年 3 月	-	-	-
4		2025 年 4 月	-	-	-
5		2025 年 5 月	89,854,775	1,624,568	1.81%
6		2025 年 6 月	180,837,484	840,590	0.46%
7	NWS 経由と省庁連携機能経由のお知らせ	2025 年 1 月	3,496,810	1,184,356	33.87%
8		2025 年 2 月	7,301,139	3,121,659	42.76%
9		2025 年 3 月	15,501,696	5,228,346	33.73%
10		2025 年 4 月	3,987,281	1,342,127	33.66%
11		2025 年 5 月	1,406,815	317,054	22.54%
12		2025 年 6 月	1,891,466	316,508	16.73%

1.2. 業務の規模

本システムで実現する業務で想定される規模について、以下に示す。なお、本システムで実現する業務は、本システム及びマイナアプリ（仮称）の機能拡張後に新しく開始される予定である。以下の内容についても、過去の業務実績等に基づく値ではなく、本調達時点の想定に基づく値である点に留意すること。

(1) サービスの利用者数及び情報システムの利用者数

本サービスの利用者について、マイナポータルを利用開始し利用者フォルダを開設した利用者のうち、マイナアプリ（仮称）からマイナポータル連携開始を実施した利用者とする。マイナアプリ（仮称）については、令和 8 年度リリース予定のため利用者は不明である。

利用者フォルダ開設数：約 8,014 万ユーザー（令和 7 年 9 月時点）

(2) 処理件数

2025 年のお知らせ件数は「1.1(4)データ量」のとおりである。

1.3. 業務実施の時期・時間

(1) 業務の実施・提供時間

本システムについては、主管課の責任のもとで運用・保守事業者が運用作業を実施する。なお、本システムのサービス提供時間、運用時間、システム障害時の対応については以下のとおりである。

ア　サービス提供時間

本システムは計画停止を除き、24 時間 365 日サービスを提供できること。

イ　運用時間

運用・保守業者の運用時間は平日（土日及び祝日、年末年始を除く）の 9 時から 17 時までとする。ただし、情報システムの監視は 24 時間 365 日行うこと。

夜間や休日におけるシステム障害時の連絡体制については、運用時間と同等の体制を維持することは求めないが、障害の重要性に応じた機動的な体制を提案すること。

ウ　システム障害時の対応

システム障害時は復旧を優先し、一次対応を速やかに実施すること。障害の原因究明・恒久的対策についても速やかに実施し、結果を主管課に報告すること。

1.4. 業務の実施等

本システムは国民等利用者がインターネットに接続可能な任意の場所から利用するものである。

1.5. 業務観点で管理すべき指標

本システムでは業務観点での指標を設けないが、「3.5(1)可用性要件」及び「3.9 継続性に関する事項」に記載する指標を達成すること。

1.6. 情報システム化の範囲

本調達の範囲は、「1.1(1)業務範囲」に示す範囲である。

1.7. 業務の継続の方針等

本システムの継続に関しては「3.9 継続性に関する事項」に記載する対策を講じること。

1.8. 情報セキュリティ対策の方針等

本システムの情報セキュリティ対策に係る具体的な要件は、「3.10 情報セキュリティに関する事項」を参照すること。

2. 機能要件定義

2.1. 機能に関する事項

(1) 機能一覧

本調達で要求する主要な機能を「図表 13 機能一覧」に示す。詳細な機能構成は、要件定義工程にて主管課と協議の上決定すること。

図表 13 機能一覧

項番	機能名	概要
1	マイナポータル連携機能	マイナアプリ（仮称）からマイナポータルへの初回接続時に、デジタル認証アプリサーバより、アクセストークン・リフレッシュトークン等を取得する機能
2	マイナポータル連携更新機能	マイナアプリ（仮称）からの API アクセス時に、アクセストークンの有効期間をチェックし、アクセストークンが期限切れの場合は、リフレッシュトークンの有効期間内であれば、デジタル認証アプリサーバより、新しいアクセストークンを取得する機能
3	マイナポータル連携停止機能	マイナアプリ（仮称）とマイナポータルの連携を停止する機能
4	お知らせ一覧取得機能	マイナポータルバックエンドから、お知らせ一覧を取得し、マイナアプリ（仮称）へ連携する機能
5	お知らせ詳細取得機能	マイナポータルバックエンドから、お知らせ詳細を取得し、マイナアプリ（仮称）へ連携する機能
6	やること一覧取得機能	マイナポータルバックエンドから、お知らせ詳細を取得し、マイナアプリ（仮称）へ連携する機能
7	プッシュ通知機能	最新のお知らせがある場合、マイナポータルバックエンドからプッシュ通知を受け取り、マイナアプリ（仮称）へ連携する機能
8	マイナポータルへの SSO 機能	マイナアプリ（仮称）からマイナポータルへアクセスする際に、マイナンバーカードでの認証を行い、WEB サイトへリダイレクトする機能
9	保険証資格情報取得機能	マイナポータルベックエンドから保険証資格情報を取得し、マイナアプリ（仮称）に連携する機能
10	お知らせ・やること配信状況管理機能	お知らせ・やることの配信状況や、開封率などのサービスの利用状況を可視化する機能

(2) 今後の機能追加を踏まえた構成

本調達で要求する機能ではないが、将来的にマイナアプリ（仮称）の機能が拡充されることを想定し、本システムの機能追加が容易に行える構成とすること。なお、拡張性については、「3.6 拡張性に関する事項」も参照すること。

2.2. 画面に関する事項

本システムは、マイナアプリ（仮称）向けのバックエンドシステムであり、画面を作成する想定はない。

2.3. 帳票に関する事項

本システムは、マイナアプリ（仮称）向けのバックエンドシステムであり、帳票（紙帳票、PDF 等の電子帳票の双方を指す）を作成する想定はない。

2.4. データに関する事項

本システムは、マイナアプリ（仮称）向けのバックエンドシステムであり業務データを管理する想定はない。マイナアプリ（仮称）と通信するためのユーザーデータと、認証情報を管理する認証データを管理する想定であるが詳細は設計工程で主管課と協議の上で対応すること。

2.5. 外部インタフェースに関する事項

本システムの外部インタフェースに関する要件を以下に示す。なお、一部のインタフェースは機能要件の変更に合わせて修正が必要になることが想定される。新たに追加となった機能への対応を含め、外部インタフェースの修正が必要になる場合については、設計工程で主管課と協議の上で対応すること。なお、インタフェースについてはAPI 連携を原則とすること。

(1) 外部インタフェース一覧

本システムは、「図表 14 外部インタフェース一覧（想定）」に示す他の情報システム等と連携する。なお、外部インタフェース一覧における記載内容は現在の想定である。設計工程において、連携先システム担当と調整の上、決定すること。

なお、デジタル認証アプリサーバの仕様については、デジタル庁開発者サイト（https://developers.digital.go.jp/）に公開されているため、こちらも参照すること。

図表 14 外部インタフェース一覧（想定）

項番	外部インタフェース名	外部インタフェース概要	相手先システム	送受信区分	送受信データ種別	送受信タイミング
1	アカウント連携 API	マイナアプリ（仮称）とマイナポータルの連携を開始する	マイナアプリ（仮称）	受信	API（REST）	リアルタイム
2	アカウント連携停止 API	マイナアプリ（仮称）とマイナポータルの連携を停止する	マイナアプリ（仮称）	受信	API（REST）	リアルタイム
3	お知らせ一覧取得 API	マイナアプリ（仮称）へお知らせ一覧を連携する	マイナアプリ（仮称）	受信	API（REST）	リアルタイム
4	お知らせ一覧取得 API	マイナポータルバックエンドからお知らせ一覧を取得する	マイナポータルバックエンド	送信	API（REST）	リアルタイム
5	お知らせ詳細取得 API	マイナアプリ（仮称）へお知らせ詳細を連携する	マイナアプリ（仮称）	受信	API（REST）	リアルタイム
6	お知らせ詳細取得 API	マイナポータルバックエンドからお知らせ詳細を取得する	マイナポータルバックエンド	送信	API（REST）	リアルタイム
7	やること一覧取得 API	マイナアプリ（仮称）へやること一覧を連携する	マイナアプリ（仮称）	受信	API（REST）	リアルタイム
8	やること一覧取得 API	マイナポータルバックエンドからお知らせ詳細を取得する	マイナポータルバックエンド	受信	API（REST）	リアルタイム
9	プッシュ通知 API	マイナアプリ（仮称）へプッシュ通知を連携する	マイナアプリ（仮称）	送信	API（REST）	リアルタイム
10	プッシュ通知 API	マイナポータルバックエンドからプッシュ通知を取得する	マイナポータルバックエンド	受信	API（REST）	リアルタイム
11	保険証資格情報取得 API	マイナアプリ（仮称）へ保険証資格情報を連携する	マイナアプリ（仮称）	送信	API（REST）	リアルタイム
12	保険証資格情報取得 API	マイナポータルバックエンドから保険証資格情報を連携を取得する	マイナポータルバックエンド	受信	API（REST）	リアルタイム
13	トークンエンドポイント	デジタル認証アプリサーバへアクセストークン等の発行を依頼する	デジタル認証アプリサーバ	送信	API（REST）	リアルタイム

3. 非機能要件定義

3.1. ユーザビリティ及びアクセシビリティに関する事項

本調達では、UI の作成は予定していないが、必要な場合は下記要件を参照の上開発を行うこと。

(1) 本システムの利用者の種類、特性

本システムの利用者の種類、特性について、「図表 15 本システムの利用者の種類、特性」に示す。

図表 15 本システムの利用者の種類、特性

項番	利用者区分	利用者の種類	利用イメージ	特性
1	利用者	【国民等利用者】 利用者（マイナンバーカードの有効な署名用電子証明書を保有しており、スマホ用電子証明書の発行を希望する国民）	マイナアプリ（仮称）を用いて、マイナポータルのサービスを利用する。	スマホの操作に不慣れな利用者も想定されるため、分かりやすいユーザーインタフェースを考慮する必要がある。
2		【任意代理人】 本人からの委任を受け、本人に代わって利用者としてサービスを利用するもの。	利用者に代わり、マイナポータルのサービスを利用する。	スマホの操作に不慣れな利用者も想定されるため、分かりやすいユーザーインタフェースを考慮する必要がある。
3	システム運用担当者	本システムの運用管理担当者	本システムの運用管理に当たり、必要に応じて本システムの操作を行う。	パソコンの操作について、事務作業等に係る一定の知識・スキルを有する。

(2) ユーザビリティ要件

「図表 15 本システムの利用者の種類、特性」に示す役割・業務内容に基づき、各利用者の特性を十分に留意する。また、利用者が想定する流れに沿った操作手順、画面遷移、画面レイアウト、帳票レイアウト等とする。また、サービスのユーザーインタフェースについては、デジタル庁が提供するデザインシステム（https://www.digital.go.jp/policies/servicedesign/designsystem/）を活用して設計すること。

図表 16 ユーザビリティ要件

項番	ユーザビリティ分類	ユーザビリティ要件
1	画面の構成（直感・シンプル）	・ 利用者が何をすればよいか直感的に理解できるデザインにすること。 ・ 無駄な情報、デザイン、機能を排したシンプルでわかりやすい画面にすること。
2	画面の構成（フォント及び文字サイズ）	・ 十分な視認性のあるフォント及び文字サイズを使用すること。 ・ 画面サイズや位置を変更できること。 ・ 一度に膨大な情報を提示して利用者を圧倒しないようにすること。
3	画面の構成（マルチデバイス対応）	・ スマホ、タブレット端末により本システムを利用する利用者を想定し、これら端末の特性を考慮した画面にすること。 ・ レスポンシブデザインにより、PC、タブレット端末、スマホ等の利用環境を問わず、同一の情報をグリッドレイアウト等の適切なレイアウトにより表示できるようにすること。
4	画面の構成（表示/非表示）	・ 情報の優先順位をつけ、重要度の低い情報、特定の利用者層に対して提示する情報は、利用者が必要に応じて表示/非表示を切替え可能とする等の工夫をすること。
5	画面の構成（クリックやチェックができる箇所）	・ 画面上でクリックやチェックができる箇所とできない箇所の区別を明確にすること。 ・ タップ操作が可能なタブレット端末やスマホの場合は、タップ操作の結果（どの部分をタップしたのか）を適切にレスポンスできること。
6	画面遷移	・ 利用者が次の処理を想像しやすい画面遷移とすること。 ・ 無駄な画面遷移を排除し、シンプルな操作とすること。
7	画面表示・操作の一貫性（統一）	・ 機能、用語、レイアウト、操作方法は統一すること。

項番	ユーザビリティ分類	ユーザビリティ要件
8	画面表示・操作の一貫性（視認性）	・ 必須入力項目と任意入力項目の表示方法を変えるなど各項目の重要度を利用者が認識できるようにすること。 ・ 見やすさを考慮し、画面のフォントサイズを決定すること。 ・ 画面ごとに異なるフォントを使わないこと。
9	操作方法のわかりやすさ	・ 無駄な手順を省き、使いやすく、利用者が効率的に作業できるようにすること。 ・ 利用者が操作しやすい手順にするため、画面上の情報項目を上から下へ、左から右へ流れる順番に配置すること。 ・ 利用者の操作を軽減できるよう、画面の初期表示時、入力項目、選択項目等に適切な既定値を設定すること。
10	操作方法のわかりやすさ（操作説明）	・ 原則としてマニュアルを参照しなくても操作できるようにすること。
11	操作方法のわかりやすさ（Tab キー）	・ Tab キー等による画面上のフォーカスの移動順序について、利用者が操作しやすい順序となるようにすること。
12	操作方法のわかりやすさ（画面遷移）	・ 利用者が同じ情報の入力や操作を何度も行う必要がないよう、画面が遷移しても情報がその後の手順に反映されるようにすること。 ・ 利用者の手間を軽減するため、利用者の手順に即した画面遷移に留意し、可能な限り不要な画面遷移を行わないようにすること。
13	操作方法のわかりやすさ（マルチデバイス対応）	・ スマホ、タブレット端末等の狭い表示領域、タッチインタフェースでも効率的に作業できる操作性を実現すること。
14	指示や状態のわかりやすさ	・ ユーザーインタフェース及び UX に関する一般的に使われているデザイントレンドを取り入れ、アイコン・図表のグラフィック表現を適切に適用すること。 ・ 本システムが処理している内容や状況を、利用者が把握できるようにすること。
15	指示や状態のわかりやすさ（外部ドメインへの遷移）	・ ドメインを異にする他の Web サイトへの遷移を行う際は、離脱メッセージを表示する等、利用者が認識できるようにすること。
16	メッセージ出力	・ 利用者に分かりやすいメッセージとすること。 ・ 必要に応じて、登録・変更・削除等の操作を行う場合には、確認画面等で表示し、利用者の注意を促すこと。 ・ 処理時間がかかる操作では、処理中であることが分かるようにすること。
17	メッセージ出力（次の操作）	・ 指示メッセージは、次操作が具体的にイメージできるようなメッセージ出力を行うこと。
18	エラーの防止と処理	・ 利用者が操作や入力を間違えないデザインや案内を提供すること。
19	エラーの防止と処理（エラー防止）	・ 利用者の誤操作を想定し、入力チェック機能によりエラーを防止すること。 ・ 入力値が選択できる場合には、プルダウンメニュー等を活用し、極力キーボード入力操作をなくすこと。
20	エラーの防止と処理（エラーメッセージ）	・ エラーメッセージは、その内容が分かりやすく表示されるとともに、利用者が何をすればよいかを示すこと。
21	エラーの防止と処理（エラー表示と解決策）	・ 入力内容の形式に問題がある項目については、利用者がその都度該当項目を容易に見つけることができるようにすること。 ・ エラーが発生した時は、利用者が迷わずに問題解決できるよう、操作の続行に必要な選択肢を利用者が適切に理解できるようわかりやすく提示すること。 ・ 入力内容の形式に問題がある項目については、それを強調表示する等、利用者がその都度その該当項目を容易に見つけられるようにする。
22	エラーの防止と処理（確認画面）	・ 必要に応じて、登録、更新、削除等の処理の前に確認画面を用意し、利用者が行った操作や入力のやり直し、取り消しがその都度できるようにすること。 ・ 重要な処理については、事前に注意喚起し、利用者の確認を促すこと。
23	エラーの防止と処理（画面遷移）	・ 入出力の過誤があった場合、次の画面へ遷移しないこと。
24	エラーの防止と処理（情報保持）	・ タブレット端末等、屋外での使用を考慮し、電波受信状況の悪い場所においても操作不能とならないよう工夫すること。
25	ヘルプ	・ 利用者が必要とする際に、ヘルプ情報やマニュアル等を容易に参照できるようにする。 ・ ヘルプやマニュアル等についても、利用者が必要な情報を容易に検索できるようにする。

項番	ユーザビリティ分類	ユーザビリティ要件
26	デザイナーによる UI/UX 検討	・ 本システムで開発するスマホアプリの UI/UX 検討に当たっては、利用者の利用動機に着目し、サービスデザイン思考の観点から検討を行うこと。 ・ UI/UX 検討に当たっては、民間スマホアプリ等の経験を有する専門の UI/UX デザイナーを体制に組み入れること。
27	画面遷移、操作ログ等の分析	・ 運用・保守工程において継続的に UI/UX の改善を検討できるよう、利用者の画面遷移、操作ログ等を分析できる仕組みを整備すること。
28	言語対応	・ 本システムでは、日本語のほか、英語で記述されたコンテンツに対応すること

(3) アクセシビリティ要件

アクセシビリティに関する要件を「図表 17 アクセシビリティ要件」に示す。

図表 17 アクセシビリティ要件

項番	アクセシビリティ分類	アクセシビリティ要件
1	基準等への準拠	・ 広く国民に利用され公益性の高い情報システムであるため、日本産業規格 JIS X8341 シリーズ、「みんなの公共サイト運用ガイドライン」（総務省）に準拠し、以下を前提とすること。 https://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/guideline.html ・ JIS X 8341-3:2016「高齢者・障害者等配慮設計指針－情報通信における機器，ソフトウェア及びサービス－第 3 部：Web コンテンツ」の適合レベル AA に準拠することを目標とする。また、レベル AAA のうち、以下の達成基準についても可能な範囲で適用すること。 ➢ 2.1.3 キーボード（例外なし）の達成基準 ➢ 2.3.2 3 回のせん（閃）光の達成基準 ➢ 2.4.8 現在位置の達成基準 ➢ 3.2.5 要求による状況の変化の達成基準 ・ 注記：本仕様書における「準拠」という表記は、情報通信アクセス協議会 Web アクセシビリティ基盤委員会「Web コンテンツの JIS X 8341-3:2016 対応度表記ガイドライン（令和 3 年 4 月版）」で定められた表記による。 ・ また、スマホ等での操作を行うユーザーが増えていることを踏まえ「Web Content Accessibility Guidelines （WCAG） 2.1」で追加された達成基準についても、可能な範囲で適用すること。 ➢ 1.3.4 表示の向き（レベル AA） ➢ 2.5.1 ポインタのジェスチャ（レベル A） ➢ 2.5.2 ポインタのキャンセル（レベル A） ➢ 2.5.4 動きによる起動（レベル A） ➢ 4.1.3 ステータスメッセージ（レベル AA） ・ デジタル庁が整備する「ウェブアクセシビリティ導入ガイドブック」を参考にすること。
2	指示や状態の分かりやすさ	・ 色の違いを識別しにくい利用者（視覚障がいのかた等）を考慮し、利用者への情報伝達や操作指示を促す手段はメッセージを表示する等とし、可能な限り色のみで判断するようなものは用いないこと。ただし、業務の利用用途から、画面色での振り分けを行うことを予定していることから、適用範囲及び配色については主管課及び関係省庁と協議し、決定すること。 ・ Web ブラウザ等の音声読み上げ機能を活用し、視覚障がいの方でも問題なく利用可能な UI とすること。
3	マルチデバイス対応	・ 解像度及び画面サイズの小さい機種でも、業務継続が可能な UI とすること。 ・ OS の設定でフォントサイズ・表示サイズをそれぞれ最大とした場合でも、業務継続が可能な UI とすること。 ・ スタイルシートを利用しないユーザーと利用するユーザーにおいて得られる情報に差（表示されない文字や画像がある等）がないこと。レイアウトにおいても大きな差がないことが望ましい。

3.2. システム方式に関する事項

(1) システム方式についての全体方針

システム方式についての全体方針を「図表 18 システム方式についての全体方針」に示す。本システムはクラウドネイティブの構成として、「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針（以下、「クラウド方針」という。）」に準拠し、クラウドサービスの提供機能を最大限活用するようデザインされたアーキテクチャとすること。特に、信頼性、拡張性（スケーラビリティ）、継続性等の向上に寄与するクラウドサービスと構成を選定すること。使用する IaaS/PaaS はガバメントクラウドを原則とするが、受託者の提案により SaaS を利用することも許容する。

図表 18 システム方式についての全体方針

項番	観点	全体方針
1	システムアーキテクチャ	・本システムのシステムアーキテクチャはクラウドサービス上に用意される Web アプリケーションから構成される。Web アプリケーションは利用者の端末に追加的なソフトウェアのインストール等を行うことなく、一般に利用されている Web ブラウザで処理を行うものとする。 ・本システムや業務機能等の特性を十分に検討し、クラウドサービスプロバイダが提供するリファレンスアーキテクチャに準拠した形で PaaS、SaaS、IaaS 等の最適なサービスを採用し、情報システムを構築する。 ・クラウドサービスプロバイダが提供するマネージドサービスを最大限活用することを基本とし、アプリケーションの作り込みを削減できる設計とする。特にデータベース、認証、セキュリティ機能や運用管理機能はクラウドサービスが提供する機能を最大限活用すること。 ・クラウドサービスが責任共有モデルとして提供されている前提を踏まえ、クラウドサービスを利用するに当たって必要となる考慮事項について検討を行い、安全かつ効率的に情報システムを構築する。 ・予防的統制と発見的統制を実施すること。また、クラウドサービスを利用するために作成する各種アカウントについては、ガバナンスやセキュリティに係るポリシーを設定の上で、権限管理を確実に行うこと。管理者アカウントについては、多要素認証を必須とすること。多要素認証はハードウェア方式を原則とするが、ソフトウェア方式も許容する。ハードウェア方式の場合は対応するワンタイムパスワード用のデバイスを利用システム側で調達すること。 ・リソース使用量の変動等に柔軟に対応するとともに、コスト削減を図るため、民間クラウドサービスの利用を原則とする。 ・全体構成及び利用するクラウドサービスについては、受託者において移行、引き継ぎ、確実なサービス提供等について問題が生じないことをクラウドサービスプロバイダに応札前に確認し、本調達の要件を踏まえ、確認結果と合わせて適切なものを提案する。
2	アプリケーションの設計方針	・マイクロサービスアーキテクチャ、API、クラウドネイティブ、クラウドサービスのマネージドサービスのみによる構成等、モダン技術を前提として構築する。 ・クライアントサーバ方式、専用端末のシンクライアント（VDI）等の旧来技術は、高コスト化の要因となるため採用しないこと。 ・原則としてバッチ処理を採用せず、リアルタイム処理を基本とすること。バッチ処理が必要となる場合は、その理由について主管課の承認を得た上で採用すること。 ・情報システムを構成する各コンポーネント（ソフトウェアの機能を特定単位で分割したまとまり）間の疎結合、再利用性の確保を基本とする。 ・本システムが取り扱うデータの保管・管理に際して、データの容量、更新頻度、保存期間等を考慮し最適なストレージサービスを選定の上、利用する。またデータの保管・管理方針が変更となった際に、ストレージサービス間でのデータの移行が容易となるよう設計上考慮する。
3	ソフトウェア製品の活用方針	・SaaS については、開発量削減の観点から幅広く優先的に、その利用を検討すること。ただし、ニーズにマッチしているか、開発量削減に貢献するか、セキュリティ対策は十分か、費用対効果は十分に得られるか等を慎重に考慮すること。 ・広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用する。 ・アプリケーションの動作、性能等に支障を来たさない範囲において、可能な限りオープンソースソフトウェア（OSS）製品（ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品）の活用を図る。ただし、それらの OSS 製品のサポートが確実に継続されていることを確認しなければならない。 ・ノンプログラミングによる画面生成等プロトタイピング用のツール等を利用することにより、システムライフサイクルコストの削減等が見込める場合には、積極的に採用を検討する。

(2) クラウドサービスの選定、利用に関する要件

ア　セキュリティ確保のため、本システムで用いるクラウドサービスは、原則として 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を選定すること。なお、例外的に 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ないクラウドサービスを選定する場合は、受託者の責任において、当該クラウドサービスが「ISMAP 管理基準」の管理策基準における統制目標（3 桁の番号で表現される項目）及び末尾に B が付された詳細管理策（4 桁の番号で表現される項目）と同等以上のセキュリティ水準を確保していることものを選定すること。

イ　要機密情報を取り扱うクラウドサービスの選定、利用に関しては、「政府機関等のサイバーセキュリティ対策のための統一基準　（令和 5 年度版）」の「4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）」「4.2.2 クラウドサービスの利用（要機密情報を取り扱う場合）」の内容を遵守すること。

ウ　情報資産を管理するデータセンタの設置場所に関しては、国内であることを基本とする。設置場所の考え方についてはクラウド方針を参照すること。

エ　契約の解釈が日本法に基づくものであること。

オ　クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。

カ　主管課の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。情報資産を国外に設置されるクラウドサービスに保管する際の考え方についてはクラウド方針を参照すること。なお、利用者がアクセス可能な部分を除き、国外から情報資産へアクセスする場合も日本国外への持ち出しに該当する。

キ　障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンタに移管されないこと。

ク　情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。従って、主管課が要求する任意の時点で情報資産を他の環境に移管させることができること。

ケ　クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替え等の対策が講じられていること。

コ　クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。

サ　クラウドサービスに係るアクセスログ等の証跡を保存し、主管課からの要求があった場合は提供すること。

シ　インターネット回線を通じたセキュリティ侵害を防ぐため、インターネット回線とクラウド基盤との接続点の通信を監視すること。

ス　クラウドサービスの提供に関する次のいずれかの認証を取得していること。

- ISO/IEC 27017:2015
- CS マーク（特定非営利活動法人日本セキュリティ監査協会（JASA）のクラウドセキュリティ推進協議会が定めるもの）

(3) 開発方式

ア　開発に当たっては、開発環境等を用意すること。各環境の詳細については「3.11.情報システム稼働環境に関する事項」を参照すること。

イ　UI 設計は UI 設計専用のアプリケーションを利用し随時共有すること。

ウ　API 設計には Open API 設計用のツールを利用すること。

(4) 機器等の設置方針

本システムはクラウドサービスを前提としているため、設置場所についてはクラウドサービスプロバイダの提供する場所となるが、その際は日本国内のリージョンを選択すること。

(5) その他

システム方式に係るその他の要件を以下に示す。

ア　本システムは短期間での機能追加・改善を行うことが想定されており、できるだけ簡潔なアーキテクトかつ簡易な構成とすること。なお、IaaS/PaaS については単一クラウドサービスでの構築を想定している。

3.3. システム規模に関する事項

本システムの規模要件を以下に示す。また、本システムの規模に関する業務要件は、「1.2 業務の規模」を参照のこと。

(1) 規模に関する前提条件

本システムはクラウドサービスを利用して運用されるため、以下の取り組みを行うこと。

ア　運用期間中において利用予定範囲を超過することがないよう、情報システムの縮退を検討するために必要となる情報収集等の仕組み（クラウドサービスの課金状況やリソースの利用量の監視、一定の閾値を超えた場合のアラート処理等）を設けること。定量的に計測したデータについては、ダッシュボード等による状況の可視化を行うこと。また、リソース利用状況に基づいたリソース見直しを行う点に留意し、情報収集の仕組みについても修正可能とすること。

イ　クラウドサービスのマネージドサービスを効果的に活用し、コスト削減を継続的に図ること。原則としてサーバレスの構成を取ることとするが、インスタンスを利用してサーバを立てる場合は、サーバのスペック等を適切な範囲に調整してコスト削減を継続的に図ること。（オートスケールを利用する場合の変更条件・上下限値等を含む。）

ウ　リソース確保の方式（リザーブドインスタンス、スポットインスタンス等）についても検討すること。

(2) データ量

2025 年度のお知らせ件数を「1.1(4)データ量」に示す。お知らせは、特定のタイミングで各機関から発信されるものであり、常時発信されるものではないこと、今後マイナポータルの利用者が増加しお知らせ件数もそれに従い増加することを想定し、スケール可能な設計とすること。

(3) 処理件数

お知らせについては、特定のタイミングで各機関から送信される特性から、最大で必要な処理件数のみを「図表 19 処理件数」に示す。なお、本処理件数は運営主体お知らせの件数をもとに作成しているが、運営主体お知らせは利用者フォルダ開設者全員に送信されるものであり、利用者フォルダ開設者は年々増加しており、最終的にはマイナンバーを持つ人すべてが利用することを想定すること。

図表 19 処理件数

項番	項目	処理件数	補足
1	プッシュ通知件数	12,857,143（件/日）	運用主体お知らせは、利用者フォルダ開設者全員のうち、1週間に分けてプッシュ通知を許可している利用者に送られるため、最大値を記載している
2	アクセストークン発行件数	134（件／秒）	下記条件で処理件数を算出 ・ お知らせの開封率を「15%」 ・ 半数のユーザーが「2 時間の間」にお知らせを確認する
3	お知らせ一覧取得件数	134（件／秒）	
4	お知らせ詳細取得件数	134（件／秒）	

(4) 利用者数

本機能の対象とする利用者は、個人番号を付番された利用を希望する者が対象となるが、現時点では、「住民基本台帳に基づく人口、人口動態及び世帯数（令和 5 年 1 月 1 日現在）」により、利用者数を日本人及び常住の外国人を含めた最大約 1 億 3 千万人と想定する。なお、本機能としての利用者数の最大値は基本設計の段階で、業務要件や業務量、マイナンバーカードの交付状況等を踏まえ決定し、主管課の承認を得ること。また、利用者及び業務量については、現状以下の条件も想定している。

ア　現状の利用者フォルダ開設数は、約 8,000 件であるが、最終的にマイナンバーカードを保有するほとんどの者が利用すると想定する。

イ　利用者は月複数回程度、お知らせややることを確認するために利用するものと想定する。利用者数は、マイナンバーカードの交付枚数等の状況により、大きく変動することが想定されるため、設計に当たっては、柔軟性のある設計とすることが求められる。

(5) 保管データ量・保管期間

本システムに保管するデータ量やデータの保管期間については、要件の整理の中で調査を行い、主管課と協議の上、決定すること。

3.4. 性能に関する事項

本システムの性能要件を以下に示す。下記の性能要件を踏まえて、本システムの業務処理の特徴を考慮し、業務処理のピーク時においてもレスポンスの低下等を招かないように、十分な処理性能を確保すること。

(1) 性能を考慮する対象

ア　性能目標の設定対象

性能目標の設定対象は本システムの Web サーバにリクエストが到着した時点からレスポンスを返す時点までとする。ブラウザ、ネットワーク部分での処理時間に関しては、性能目標の設定対象外とする。

イ　性能見積もり

本システムのアプリケーション処理時間に係る性能見積りは、以下を考慮する。

- アプリケーション又はコードの起動に要する時間、アプリケーション又はコードの実行時間、データベースアクセスに要する時間に要素分解を行った上で実施すること。
- 各画面・機能等の利用者体験を踏まえた余裕を見込むこと。

(2) 応答時間

目標時間を満たすトランザクションの割合を「遵守率」とし、その目標値を設定すること。ピーク時の遵守率は90%とする（90%以上のトランザクションがレスポンスタイム処理目標時間を満足する性能であること。なお、障害等による縮退運転時並びにネットワーク遅延等の受託者の責によらない遅延は除外する。）

応答時間は、画面を表示するための要求を行った時（ボタン等を押下した時）から画面が全て表示されるまでの時間を指す。応答時間については、関連システムも含めた要件となるため、関連システムとの調整やチューニング、性能テストを適切に行った上で、必要に応じて目標値の見直しを主管課へ提案すること。

目標応答時間：1 秒以内

最大応答時間：3 秒以内

(3) スループット

処理件数については、「1.2(2)処理件数」に示す。

3.5. 信頼性に関する事項

本システムに備える機能の停止等による業務への影響を最低限にとどめるため、クラウドサービスの利用を前提として、以下に示す要件を踏まえ本システムの信頼性を確保すること。

(1) 可用性要件

単一障害点（SPOF）を極力排除するとともに、サーキットブレーカーパターンなども検討し、一律ではなく機能又はセグメントの特性に応じた合理的な提案を示すこと。また、SPOF の発生が避けられない場合においてそれら稼働状況を管理する仕組みを準備すること。

ア　可用性に係る目標値

可用性に係る目標値を「図表 20 可用性に係る目標値」に示す。

図表 20 可用性に係る目標値

項番	指標名	目標値	補足
1	運用時間	24 時間 365 日	以下に該当する時間を除く。 ・　接続回線の計画停止時間 ・　大規模災害等の天災地変に起因する停止時間 ・　連携する情報システムやクラウドサービス又は通信ネットワークの障害・計画停止・緊急メンテナンス等に起因する停止時間 ・　本システムのメンテナンスによる計画停止時間
2	稼働率	99.9% 以上	本システムにおける稼働率を以下の計算式により定義する。 稼働率＝年間実稼働時間／年間予定稼働時間 x 100 当該計算式において、年間実稼働時間は「利用者が本システムを利用可能な時間の合計」、年間予定稼働時間は「年間稼働時間（24 時間 365 日）から計画停止時間及び大規模災害による停止・縮退時間を除いた時間の合計」とする。

イ　可用性に係る対策

本システムの可用性を確保し、前述に示した稼働率を遵守するため、以下に示す要件に基づく対策を行うこと。

- クラウドサービスの利用を前提として、本システムを構成するサーバ、ネットワーク機器及びネットワーク経路を冗長化し、単一障害点（SPOF）を回避すること。
- クラウドサービスの利用を前提として、フェールソフトの観点から、障害が発生したコンポーネントを切り離すことによりシステム全体を停止せずに運用可能とすることを考慮する。そのために各種障害発生時の影響を回避又は局所化し、原則として自動縮退運用に対応すること。
- 本システムに係る運用・保守上の人的ミスに起因する障害が本システムの可用性に影響を与える事態を未然に防止するため、「3.17 運用に関する事項」及び「3.18 保守に関する事項」を踏まえ、適切な手順書を整備すること。また、定型的なオペレーションは自動化すること。

(2) 完全性要件

以下に示す要件を踏まえ、本システムの完全性を確保するための対策を行うこと。

ア　クラウドサービスの利用を前提とし、以下の対策を講ずること。

- コンポーネントの故障に起因するデータの減失や改変を防止する。
- 異常な入力や処理を検出しデータの減失や改変を防止する。

イ　システム運用中に障害・トラブル等が発生した際に原因追求が可能となるよう、操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログ等を取得・保管し、必要な時に出力可能とすること。ログの出力に当たっては、環境（本番環境、検証環境等）別に出力するログのレベル（ERROR、WARNING、INFO、DEBUG 等）の設定を可能とすること。なお、ログの保管期間は 5 年間とする。

3.6. 拡張性に関する事項

(1) 性能及び機能の拡張性

ア　基本方針

本システムの利用率の増加、データ量の増加等により、利用資源の規模・性能を拡張する必要が生じた場合に備え、可能な限り性能の拡張を柔軟に行えるよう、設計・開発を行うこと。また、将来の制度改正等により機能を拡張する必要が生じた場合に備え、容易に機能追加・変更を行えるよう、設計・開発を行うこと。

イ　マネージドサービスなどの活用

本システムはクラウドサービスを利用する想定としている。本システムの構築に当たっては、当該クラウドサービスのマネージドサービスなどを可能な限り活用することにより、処理能力等の動的調整を実現することとし、業務量及び処理能力の拡張性については特段の拡張性要件を定義しない。

ウ　機能の追加

機能の追加や、新たな機能開発の必要が生じることが想定されることから、将来開発する機能も含めた機能間の連携が十分に図られるようにすること。

本システムは、連携業務アプリケーションとの一層の連携など、拡張性を備えた情報システムであることが求められる。連携機能等の拡張が必要になった際に拡張が容易となるような構成をとること。

エ　コンポーネントの再利用性・拡張性

アプリケーションやインフラの設計に当たっては、将来の拡張時に効率良く対応ができるように、設定情報の外部化や一元化、機能の共通化等に努めること。特にスマホアプリについては、様々な利用者が広く利用することが想定されるため、特定のスマホ端末、OS のバージョン、ミドルウェア等に可能な限り依存しない設計とすること。

オ　モニタリングと定期的な報告

本システムの運用に当たっては、定期的な運用報告において定期的にサーバコア数やディスク、メモリ、ネットワークの帯域などの使用状況等を確認すること。またリソースの増加の必要性が見込まれる場合は、リソースの増強の必要性の有無を判断できるような形で主管課に報告を行うこと。

カ　割り当て変更

業務量の増加減に伴い、これらリソースの割り当てを動的に行えるようにし、主管課の指示に基づきリソースの割り当てを変更すること。

3.7. 上位互換性に関する事項

(1) 上位互換性

クラウドサービスの活用を踏まえ、OS、サーバソフトウェアのバージョンアップ又は変更に備え、本システムを構成する。

ア　クラウドサービスのバージョンアップ

本システムの構成にクラウドサービスのマネージドサービスを採用する場合、軽微なバージョンアップについては自動適用を前提とする。大規模なバージョンアップについては、アプリケーションへの影響を事前に精査し、適用を検討すること。

イ　OS 等への依存

原則特定バージョンへの依存は避けること。なお、やむを得ず OS、ミドルウェア等の特定バージョンに依存する場合は、その利用を最低限とすること。

ウ　クライアント端末の更新

クライアント端末が更新され、OS や Web ブラウザとして新しいバージョンのものを利用する場合も、業務運営に極力支障が生じないよう計画されたシステム構成とすること。

(2) 業務分担

本システムを構成する機器・ソフトウェアの更新、バージョンアップの必要性が生じた場合は、各事業者がそれぞれの担当範囲において影響調査、対応策の検討を実施することとしている。

ア　アプリケーション保守事業者は、業務アプリケーションへの影響調査、対応策の検討を実施する。

イ　運用事業者は、システム基盤の影響調査、対応策の検討を実施する。

ウ　機器・ソフトウェアの更新、バージョンアップの対象が持ち込みソフトウェアの場合は、運用事業者が実施する影響調査、対応策の検討を機器・ソフトウェア賃貸借・保守事業者が支援する。

3.8. 中立性に関する事項

(1) オープンな標準的技術又は製品の採用

本システムを構成するサーバ、ソフトウェア、アプリケーションとして、市場で広く利用されている製品群及びクラウドサービスが提供する標準的なサービスを除き、原則として特定事業者の技術に依存しないオープンな技術仕様に基づくものを選択すること。

ア　データの可搬性の担保

データの可搬性の担保に当たっては、以下の要件を満たすこと。

- 本システム内のデータについては、原則として XML や CSV 等の標準的な形式で取り出すことができるものとすること。
- パッケージ製品から抽出されたデータであっても、移行データフォーマットや移行データの権利は主管課に所属すること。
- 技術的な理由により、提供することが難しいデータ項目がある場合には、代替案を提示することが可能であること。
- 移行用データが満たすべき制約（移行データのデータフォーマットやスキーマなどの要件も含む）をドキ

ュメントに取りまとめること。ドキュメントについては、本システムの業務要件を理解しているユーザーであれば理解できるように記述すること。なお、システム運用期間中に該当ドキュメントの内容に変更が生じる場合は継続して改定を行い最新化できること。

・ 移行データに関する文字コード等は以下に従うこと。

- 取り扱う日本語文字集合の範囲： JIS X 0213
- 文字コード： ISO/IEC 10646
- 文字の符号化形式： UTF-8

イ オープンソースソフトウェア（OSS）活用

ソフトウェア又はアプリケーションについてフレームワークを活用する場合は、可能な限りオープンソースソフトウェアとして提供されているフレームワークを選定すること。

ウ オープンなインタフェースの活用

本システムを構成するサーバ、ソフトウェア等は、原則として仕様が公開された API 等のインタフェースを選定すること。

3.9. 継続性に関する事項

本システムの停止等に際しても必要最低限の業務を継続（又は回復）するため、以下に示す要件を踏まえ、本システムの継続性を確保すること。

(1) 継続性に係る目標値

以下に、機能停止等の原因となる事象の規模に応じて継続性に係る目標値を示す。なお、連携するマイナポータルバックエンドシステム及びデジタル認証アプリサーバの障害・計画停止時は、本システムの継続も困難になることから、連携するシステムの復旧後、速やかに復旧を行うこととする。

ア 予測可能な障害発生時

予測できる障害（一時的な過負荷等）については、あらかじめ業務停止を回避するための対策を講ずること。また、単一障害発生時は業務停止せずに処理継続可能であること。

イ 業務停止を伴う障害発生時

予測困難な事象により業務停止を伴う障害が発生した場合の目標復旧時間（RTO）、目標復旧レベル（RLO）及び目標復旧時点（RPO）を「図表 21 継続性に係る目標値（業務停止を伴う障害発生時）」に示す。

図表 21 継続性に係る目標値（業務停止を伴う障害発生時）

項番	目標復旧時間（RTO）	目標復旧レベル（RLO）	目標復旧時点（RPO）
1	2 時間以内	通常どおりのサービスレベルに復旧	停止前の最新バックアップ状態へ復旧（ただし、アーカイブログを取得しているデータは障害発生時点への復旧を可能とする。）

ウ 大規模災害発生時

インターネット等通信インフラが被災しておらず、発災前と同様の通信環境が確保されていることを前提として、大規模災害による業務停止が発生した場合の目標復旧時間（RTO）、目標復旧レベル

（RLO）及び目標復旧時点（RPO）を「図表 22 継続性に係る目標値（大規模災害発生時）」に示す。

図表 22 継続性に係る目標値（大規模災害発生時）

項番	目標復旧時間（RTO）	目標復旧レベル（RLO）	目標復旧時点（RPO）
1	24 時間以内	通常どおりのサービスレベルに復旧 （機能面は通常レベル、性能面では通常の半分のレベルの復旧とする）	停止前の最新バックアップ状態へ復旧（ただし、アーカイブログを取得しているデータは障害発生時点への復旧を可能とする。）

(2) 継続性に係る対策

本システムの継続性要件を実現するために、以下の対策を講じること。

ア 冗長化

各構成要素について、故障等を検知した際、クラウドサービスの利用を前提として自動的に予備の環境へ切替える等、適切に冗長化を行い、特定の部分の障害によりシステム全体が停止してしまうようなSPOF（単一障害点）を極力排除するよう、設計時に配慮すること。

イ 災害対策

災害対策環境の事前準備等によるシステム上の対策及び非常時の運用体制や切替え手順の整備等による運用上の対策を行うことで、業務継続を可能とすること。

災害発生後に本番環境が正常に稼働できる場合は、災害対策環境から切り戻しができるよう連携先システムと調整しておくこと。

ウ アベイラビリティゾーン

アベイラビリティゾーン（以下「AZ」という）については、マルチ AZ によって複数の AZ をまたいだシステム冗長化を実現し、可用性を高める方針とする。しかし頻繁に AZ 間の通信が発生するアプリケーションについては、AZ 間のレイテンシが増幅し性能に影響を与える可能性がある。これらの性能面の影響を評価できるよう、設計・開発期間中の早い段階で性能面の影響を評価し、必要に応じてアプリケーション改修等の手段で性能改善への対応方針を確立すること。

エ データバックアップ

・ バックアップ対象

データバックアップに当たっては、本システムの稼働に必要な全データを復旧可能とすることを前提として、外部組織から再入手可能なデータの有無を含め、保全対象を精査し、復旧時に必要となるデータを過不足なく保全対象に含めることができるようにすること。なお、クラウドサービスのマネージドサービスを利用することで自動的にバックアップを取得できる部分はあるが、オペレーションミスやアプリケーションのバグ等に起因するデータ破壊に対しても破壊前の時点まで遡れるように、バックアップの実施方法について配慮すること。

・ バックアップ頻度

バックアップの取得間隔は、原則日次とする。ただし、障害発生時点への復旧が必要なデータについては、復旧に用いる PITR : Point In Time Recovery/Restore を保存する等の対応を行うこと。

・ 保存期間

万一の障害発生に備え本システムの稼働に必要な全データを復旧可能とするとともに、過去のシス

テム処理に問題が発生した場合に原因分析を可能とすることを目的として、日次のバックアップについては、30 日分のデータをバックアップとして保持すること。

・ アクセス権限

バックアップしたデータの保管場所にはアクセス権限を付与し、管理者以外がアクセスできないようにすること。

・ データの隔地保管

「3-2-1 ルール」（2012 年に US-CERT（米国のコンピュータ緊急対応チーム）が提唱）に示されている「データはコピーして 3 つ保有（プライマリー1 つ、バックアップ 2 つ）、2 種類の異なる記録媒体に保管、コピーのうち 1 つは遠隔地に保存」という方針を十分に理解した上で、データのバックアップについて万全を期した対応を行うこと。クラウドサービス上のスナップショットやレプリカだけではこの要件に十分対応できないので、バックアップとして永久増分と重複排除を積極的に活用し、ISMAP 管理基準が求める暗号化を行った上で、別リージョンのオフサイトに隔地保管すること。

・ バックアップツール

バックアップ対象、頻度、バックアップデータへのアクセス権限及び保存期間といったバックアップポリシーを一元的に管理できる機能を持った、クラウドサービスプロバイダが提供するバックアップサービスをできるだけ利用すること。なお、個別データの復旧にはデータベース等の PITR：Point In Time Recovery/Restore を実現できることが望ましい。

オ システムバックアップ

クラウドサービスのマネージドサービスにおけるバックアップ機能を有効に活用すること。なお、インスタンスを利用してサーバを立てる場合のバックアップ方式は、バックアップ＆リストア、コールドスタンバイ、ウォームスタンバイ、マルチサイトの 4 つのディザスタリカバリ方式のうち、目標復旧時間から考えて、コールドスタンバイ以上の構成を想定している。

「図表 21 継続性に係る目標値（業務停止を伴う障害発生時）」及び「図表 22 継続性に係る目標値（大規模災害発生時）」に示す RTO、RLO、RPO を満たすようにすること。

3.10. 情報セキュリティに関する事項

(1) セキュリティ対応方針

セキュリティ要件を決定するためのシステム特性や特に対処すべきセキュリティリスク、セキュリティ対応方針を「図表 23 本システムのおけるセキュリティ対策方針」に示す。

図表 23 本システムのおけるセキュリティ対策方針

項番	分類	概要
1	原則	・ 「政府機関等のサイバーセキュリティ対策のための統一基準」、「デジタル庁情報セキュリティポリシー」に準拠した情報セキュリティ対策を講ずること。なお、「デジタル庁情報セキュリティポリシー」は非公表であるが、「政府機関等のサイバーセキュリティ対策のための統一基準」に準拠しているので、必要に応じ参照すること。「デジタル庁情報セキュリティポリシー」の開示については、契約締結後、受託者がデジタル庁に守秘義務の誓約書を提出した際に開示する。 ・ セキュリティ対策については、高度化/大規模化するサイバー攻撃等に対応するため、多層防御やサイバーレジリエンス強化といった原則に基づいて要件を定義する。
2	システム特性（概要）	【システムの利用者】 ・ 本システムは国民向けサービスであり、利用者数は現時点で約 8,000 万人である。 【システムで取り扱う情報】 ・ 個人情報は取り扱われる ・ 要配慮情報に相当する情報や特定個人情報は取扱われない 【利用環境・ネットワーク構成】 ・ 利用者はスマホアプリからインターネットを介して当該 Web システムにアクセスし、ログインして各種機能を使用する ・ システム管理者はインターネット VPN を介して本システムにアクセスし、システム管理を実施する ・ マイナポータルバックエンドシステムやデジタル認証アプリサーバなどと接続する 【その他】 ・ 本システムはマイナポータルの機能をスマホアプリから利用するものであり、システム停止により甚大な影響が発生することから、可用性に関しても機密性、完全性と同等に高いレベルで担保する必要がある
3	優先的に対処すべきセキュリティリスク	【優先的に対処すべきセキュリティリスク】 ・ 外部からの不正アクセスにより、本システムの個人情報が漏洩する。 ・ サービス妨害を目的とした攻撃等により本システムが長時間停止する。
4	セキュリティ対応方針	【セキュリティ要件のベースライン】 ・ 本システムにおいては、セキュリティ要件を過不足なく導出するため、NCO の提供する SBD マニュアルをセキュリティベースラインとして利用する 【優先的に対処すべきセキュリティリスクへの対応方針】 ・ 上記の優先的に対処すべきセキュリティリスクについては、多層防御の観点で発生確率を抑えるとともに、発生時の範囲を極小化するような対策を実施する。 ・ 外部からの不正アクセス対策として不正ログイン対策、脆弱性対策を徹底するともに、攻撃やインシデントの兆候を早期検知できるような仕組みを導入する。 ・ サービス妨害を目的とした攻撃対策については、L3～L7 層で対策可能な仕組みを導入する。 【その他セキュリティリスクへの対応方針】 ・ ・上記以外のセキュリティリスク（内部不正や人為的ミス等に起因するもの、サプライチェーンに起因するもの等）についても発生時影響は看過できないことから、予防的な対策だけでなく早期検知するための対策を実施し、リスクを低減する。

(2) セキュリティ要件

上記のセキュリティ対応方針に基づき、「別添 3 情報セキュリティに関する事項」に本システムにおけるセキュリティ要件を記載する。

受諾者は、開発の各工程において、本セキュリティ要件に則ってセキュリティ対策がもれなく実装されていることを検証する方法を定め、要件のトレーサビリティを確保することが求められる。

開発工程以降、セキュリティ対策を具体化する過程でセキュリティ上の懸念が発生した場合は、本要件のみに縛られず、必要に応じて追加のセキュリティ対策を講じること。また、デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」の記載内容（要求事項、実施内容、重要なセキュリティ対策の考え方）に従い、各工程でのセキュリティ対応状況について抜け漏れを確認して是正すること。加えて、デジタル庁「政府情報システムにおける脆弱性診断導入ガイドライン」の 4 付録 A を参考に情報システムの脆弱性が作りこまれないように留意すること。

3.11. 情報システム稼働環境に関する事項

クラウドサービスの構成、ハードウェアの構成、ソフトウェア製品の構成、ネットワークの構成、施設・設備要件等について記載する。

(1) システム構成

受託者は、設計・開発及び運用・保守に用いる環境としてクラウドサービス上に構築する「本番環境」、「検証環境」及び「開発環境」の 3 種類を利用すること。

本番環境及び検証環境は、デジタル庁が用意するガバメントクラウド上に構築し、開発環境は受託者が用意するものとする。

設計・開発及び保守作業は、原則として「検証環境」及び「開発環境」で行った上で、「本番環境」にリリースし、運用作業を行うこと。環境の構成や利用方法の詳細は、主管課と協議の上決定すること。

なお、システム構成については可能な限りクラウドサービスのマネージドサービスを活用することを前提に受託者の提案によるものとする。

(2) クラウドサービス構成

ア クラウドサービスの要件

クラウドサービスの要件については、「3.2.システム方式に関する事項」の「(1)システム方式についての全体方針」、「(2)クラウドサービスの選定、利用に関する要件」を参照すること。

イ クラウドサービス構成

本システムは可能な限りマネージドサービスを活用すること。なお、速やかに本番同等の環境を構築できるように、インフラの設定は Infrastructure as Code にて構成し、環境変更時にはその変更をメンテナンスできるようにすること。

(3) ハードウェア構成

本システムでは、クラウドサービス外に準備するハードウェアは想定していない。

(4) ソフトウェア構成

本システムの構築に当たっては、可能な限りクラウドサービス提供のサービスを活用すること。また、いずれのソフトウェアについても、原則として最新バージョンを適用すること。

(5) ネットワーク構成

本システムのネットワーク構成については本システムの設計・開発時に決定する。以下の点に留意すること。

ア 連携先システムとのネットワークについては、閉域網（専用線、広域イーサネット、IP-VPN 等）で接続し、外部からの侵入を物理的に防ぐこと。

イ 敷設する回線で本システムに固有のグローバル IP を要する場合、適切なグローバル IP アドレス数を同時に用意すること。

ウ クラウド上に論理的に隔離された仮想閉域ネットワークを構築すること。

(6) 施設・設備要件

本システムはクラウドサービス上に構築するため、施設・設備要件はない。

(7) 利用端末の要件

本システムで動作保証の対象とする利用端末は、マイナアプリ（仮称）に依存することになるが、現時点では未確定のため現行のマイナポータルアプリの対応機種（https://services.digital.go.jp/mynaportal-app/）を参考とすること。

3.12. データマネジメントに関する事項

本システムのライフサイクル全般を通じて、保有するデータ品質の維持・向上やデータの適正な利活用等を実現するため、以下に示す要件を踏まえ本システムのデータマネジメントを実施すること。

(1) データ管理体制の明確化

システムで扱うデータの種別ごとに管理主体（管理する組織、担当者等）や役割の設定を主管課と共に行い、データ毎の管理責任を明確化すること。

(2) データの標準化

データの相互運用性を高めるため、以下の点に留意すること。

ア　マスターデータは、広範囲に共通利用できるデータから選定すること。マスターデータを独自に作成する場合は、関連する分野でも共通利用できるように設計上の配慮を行うこと。

イ　コード値については、国際標準、業界標準など、広範囲に共通利用されているものを採用すること。コード値の標準化については、「コード（分類体系）導入実践ガイドブック」（デジタル社会推進標準ガイドライン DS-463-1）を参考とすること。

ウ　本システムだけでなく、関連分野全体でのデータ流通を促進するという大局的な視点も踏まえて、ステークホルダーとの連携、調整を主管課と共に行うこと。

(3) データに関するドキュメントの一元的管理

本システムの運用・保守にあたってデータに関する一元的管理が行えるように、データに関する各種設計書等のドキュメントを内容的に独立した構成とすること。

(4) オープンデータ化を容易にする設計

本システムが扱うデータのうち、オープンデータとして対外的に公開することが有意義と考えられるものについては、公開要否を主管課が検討することを支援する。また、オープンデータとして公開するデータについては、オープンデータ・バイ・デザインの考え方に基づき、機械判読性の高いデータにする、Web-API により処理できるようにする、データを抽出しやすいデータベース構造にする等の対応を設計段階から十分に検討し、実装すること。

(5) データに関する運用情報の管理

システム障害等が発生した際に迅速な原因分析が行えるように、データに関するログ機能を充実させること。

また、サービス・業務の運営状況に関する指標や本システムの利用状況等のデータを適時に把握できる機能を組み込み、取得したデータに基づいて本システムの継続的な改善を行うとともに、サービス・業務改革（BPR）が行えるようにすること。

(6) データの機密性定義に応じた設計

データの機密性に応じたセキュリティを確保するため、データ配置やアクセス管理方法について設計段階から十分に検討し、実装すること。

(7) データ品質の継続的改善

データ品質に起因するシステム障害や不具合を防止し、データの利活用を推進するため、データ品質の定期的な棚卸と不備・不具合の改善を行うこと。

3.13. テストに関する事項

本システムのテストに関する要件を「図表 24 テスト要件」に示す。なお、品質管理の観点から必要に応じて主管課が指定する専門チームがテストに参加することもあるため、受け入れること。また、テストデータやテストに関連する情報の提供にも協力すること。

図表 24 テスト要件

項番	分類	要件
1	テスト工程の定義	・ 本システムでは調達仕様書に記載の通り、以下のテストを実施する。 (1) 単体テスト (2) 結合テスト (3) 総合テスト (4) 受入テスト
2	テスト環境	・ 本番環境に加え、テストを実施するための環境（開発環境・検証環境等）を整備すること。 ・ テスト環境については、連携先システムと接続して行う外部連携テストが実施可能な環境として整備するほか、同時並行的な開発に対応できるように複数のテスト環境を整備すること。 ・ 開発スケジュールを踏まえ、効率化を考え、各環境を流用するなど検討すること。
3	テスト計画書	・ 各テスト工程の開始時に、以下の内容を定義したテスト計画書を作成し、主管課の承認を得ること。 ➢ テスト計画書の目的と位置付け ➢ テストの目的、概要 ➢ 対象範囲 ➢ テストスケジュール ➢ テストの観点 ➢ テスト実施体制、役割分担 ➢ テスト実施手順 ➢ テスト環境 ➢ テストシナリオの概要 ➢ 工程開始条件、工程終了条件 ➢ 使用するテスト自動化ツール ➢ 成果物一覧 ➢ テスト結果に係る定性・定量評価の方法（テスト密度、バグ検出密度等） ➢ 進捗管理 ➢ 品質管理 ➢ 不具合管理 ・ 受託者は、本業務を実施する各過程においてテスト計画書の内容に変更が生じる場合、変更箇所及び内容について主管課の承認を得ることを条件として、テスト計画書を適切に更新すること。 ・ 情報セキュリティの観点から必要なテストがある場合には、テスト項目及びテスト方法を定め、これに基づいてテストを実施し、その実施記録を保存すること。 ・ 受託者は、テストに係る管理要領を共通化し、各テスト工程において、原則として同一の管理要領を適用するようにすること。各テスト工程に応じて部分的に異なる管理要領の適用を必要とする場合は、その適用差分のみ「テスト計画書」に記載すること。 ・ 機能一覧を基準として欠陥の相対的な発生確率と欠陥顕在化時の相対的な影響度について、それぞれ高・中・低の 3 段階で評価することにより、本システムの品質リスクを分析し、その結果を踏まえてテストケースの数や質に変化をつけるリスク・ベース・テストを適用すること。
4	テスト仕様書	・ 本システムの各テスト工程の開始前に、テストシナリオ、テスト項目等を記載したテスト仕様書を作成すること。 ・ 各テスト工程のテスト項目は、設計書等の記述内容を網羅的に確認できるよう作成すること。 ・ 各テスト工程に応じたテスト技法を適用すること。 ・ テスト項目は、品質を確保するために十分なテスト項目を定義すること。また、テスト計画の策定時に定めた定性・定量評価方法を満たすよう作成すること。 ・ 受託者においてレビューを徹底し、上記要件を満たしたテスト仕様書となっているかを確認すること。

5	テストの実施	・ 作成したテスト項目に基づきテストを実施すること。 ・ テストを実施する際は証跡を取得すること。証跡の納品対象については別途主管課と協議の上決定すること。 ・ 受託者は証跡等に代表されるテストの成果物のレビューを徹底し、テスト項目に基づきテストを実施しているか確認する。想定外のテスト結果となった場合は、本システムの欠陥であるか、想定結果が誤りであるか等、原因を明らかにした上で必要な対応を行うこと。 ・ 欠陥を検知した場合は、その原因を明らかにした上で、原因を解消すること。 ・ 検知した欠陥について修正を行った場合は、修正対象機能について回帰テストを実施すること。 ・ 主管課において、再テストが必要と判断した場合、受託者は再テストの計画を作成し、主管課の承認を得た上で、定められた期限内に再テストを実施すること。また、類似バグを抽出するため、必要に応じて強化テストを実施すること。
6	テストデータ	・ 総合テスト及び受入テストにおいて実データを使用する必要がある場合は、実データの取得申請を条件として、実データの使用を許可する。なお、疑似データの作成に当たり、実データの匿名化、符号化等を行う場合は受託者の作業とする。 ・ 取得した実データは、適切に保管・管理すること。 ・ 受入テストにおいて作成したテストデータは、システム切替え実施前までに、検証環境等のデータも含め削除すること。 ・ 機密性の高いデータ項目や個人情報に係るデータ項目は、マスキングした上で使用すること。
7	対応状況の報告	・ テストの進捗としては、テスト実施済項目数や信頼度成長曲線等の定量的なメトリクスの推移を示すことにより、テスト進捗状況、不具合検出状況及び不具合対応状況を報告すること。 ・ 受託者は、主管課からのテストの進捗状況や品質等に対する指摘に対し確実に修正すること。 ・ 結合テスト・総合テストでの報告書には、ソースコードメトリクスを取得し、テスト結果及び品質指標とともに、主管課に報告すること。 ・ 受託者は、各テスト工程に応じたテスト計画内容について主管課に説明し、各テスト工程における最初のテスト開始予定日の遅くとも 1 週間前までに主管課の承認を得ること。
8	テスト完了報告書	・ 各テスト工程の完了に当たっては、テスト完了報告書を作成し、主管課の承認を得ること。また、完了に当たっては以下をすべて満たすこと。 ➢ すべてのテスト項目が完了していること。 ➢ テスト結果について、定性評価及び定量評価（テスト密度、バグ検出密度等）により評価を行うこと。 ➢ テストで発生したすべての障害が、当該テスト工程内で解消されていること。 ➢ 外的要因等により次工程への申し送り事項が発生した場合は、対応方針、対応時期等を明確にした上で、主管課の承認を得ること。
9	テストの自動化	・ 各テスト項目のうち、反復的にテストを実施するものについては、自動化することを原則とする。そのために、必要となるテストツールについては、新規に作成するか、既存のツールを活用すること。 ・ UI のテスト、受入テスト等、テストの自動化に馴染まないものについては、自動化対象外とする。ただし、自動化対象外とすることについて、主管課の承認を得ること。
10	将来時点の仕様変更	・ OSS を適用する部分を除き、将来時点の仕様変更への対応を柔軟にする観点から、テスト駆動開発、ソースコードに対する静的解析及びリファクタリングにより、クラスや関数構造をシンプルに保つこと。
11	構築時の脆弱性対策	・ ネガティブテスト、ファジング、フォルト・インジェクション等の障害注入テスト手法を活用し、エラー処理や例外処理に係る脆弱性に対処すること。 ・ 品質保証、フォレンジック及びインシデント・レスポンスの観点から、問題原因を把握するために必要な例外情報をログに出力するようにすること。 ・ 設計・開発段階の早期からセキュリティを検証すること。

(1) 単体テスト

単体テストは、本システムにおける最小の実装構成要素（関数、メソッド等）に着目し、ソースコードの確からしさを確認することを目的とするコードベースの単体テストと、UI を含む単機能のテストにより構成する。現時点で想定する単体テストの要件を以下に示す。

ア　本システムにおける最小の実装構成要素の動作を検証するために必要となるテストコードを作成し、コードベースの単体テストを実行すること。また、テストコードは、テスト対象とする実装構成要素に関するソースコードを記述する前に記述するようにすること。

イ　単体テストの結果は、必要に応じて数値的指標等（ステップ数あたりの試験項目数、試験消化率等）をもって報告すること。以下に示す事項については、あらかじめ主管課に提示すること。

- 単体テストのスケジュール
- テスト環境（テストを実施するハードウェア、ソフトウェアの構成、テストツール等）の概要
- 合否判定基準　等

ウ　単体テスト実施時は、テスト結果を検証するための証跡を採取すること。

エ　単体テストは、原則として開発環境において実施すること。

(2) 結合テスト

結合テストは、本システムの構成要素（アプリケーション機能、ソフトウェア、ハードウェア等）に着目し、各要素の連動又は協調動作に関する設計の欠陥を検出することを目的として行う。現時点で想定する結合テストの要件を以下に示す。

ア　結合テストの観点として以下を想定する。

図表 25 結合テストの主なテスト観点

項番	テスト種別	概要
1	システム基盤テスト	構築した本番環境及び検証環境の確認を行う。現時点で想定するシステム基盤テストの要件を以下に示す。 ・　環境設計において作成したリソース定義コードを実行し、本システムのインフラストラクチャを構成する環境及び仮想資源を構築すること。 ・　構築した環境及び仮想資源が正しく動作するか、動作確認テストを実施すること。 ・　クラウドサービスが提供するツールによって実行可能なテストコードを作成すること。 ・　動作確認テストの結果、何らかの異常またはエラーを確認した場合、実行したリソース定義コードに原因が作り込まれていないか、必要な見直しを行うこと。 ・　問題修正後、該当する環境または仮想資源について、再構築と動作テストを再度実施すること。
2	外部連携テスト	外部システムとの連携部分の確認を行うため、以下を実施する。 ・　疎通テスト：本システムと外部連携システム間で必要な通信の疎通が通ることを確認する。 ・　異常系テスト：想定しうるエラーを発生させ、エラーメッセージ等の確認をする。また必要な対処を行うように修正する。 ・　バリエーションテスト：インタフェースによる動作と必要なバリエーションの確認を行う。 ・　運用観点テスト：正常時、異常時の運用に関する動作を確認する。異常時の対応として、エラーメッセージやログ等を基に、運用事業者が運用業務を行えることを確認すること。

イ　テスト対象機能について同値分析、境界値分析、原因結果分析を行い、その結果を踏まえてテストケース、テスト項目を設定し、アプリケーション機能相互間の接合に不具合が無いことを検証すること。

ウ　状態遷移マトリクスを踏まえ、本システムに備えるユーザーインタフェースについて、仕様どおりに操作可能か、誤った操作をした場合も適切なエラーメッセージが表示されるか等の操作確認を行うこと。

エ　状態遷移マトリクスを踏まえ、アプリケーションコンポーネントが備える API に対して境界値テストを行い、境界及び状態遷移を網羅すること。

オ　結合テストに用いるテストデータには、テストケース、テスト項目を踏まえた疑似データを作成して使用すること。

カ　結合テスト実施時は、テスト結果を検証するための証跡を採取すること。

キ　結合テストは、原則として開発環境または検証環境において実施すること。

(3) 総合テスト

総合テストは、機能仕様及びアーキテクチャに由来する欠陥を検出することを目的として行う。現時点で想定する総合テストの要件を以下に示す。

ア　総合テストの観点として「図表 26 総合テストの主なテスト観点」を想定する。

図表 26 総合テストの主なテスト観点

項番	テスト種別	概要
1	業務運用テスト	・ 業務の実施手順や業務で取り扱うデータを基に様々なシナリオ・データのバリエーションを作成し、本システムを用いて業務、機能を確認する。 ・ シナリオ・データには、日常的に実施する業務や日常的に取り扱うデータだけではなく、月次や年次等の特定のタイミングでしか発生しない業務やイレギュラデータも含めること。 ・ ユーザーの誤操作や予期しない現象を契機としたシステム障害が発生しないことを確認することを目的として異常系のテストケースも含めること。
2	ユーザビリティ/アクセシビリティテスト	利用者にとっての主観的な利用品質を計測する。現時点で想定するユーザビリティ/アクセシビリティテストの要件を以下に示す。 ・ ユーザビリティ/アクセシビリティテストの計画に当たっては、以下の内容を総合テスト計画書に記載すること。 ➢ テスト目標 ➢ 実施場所及び実施時期 ➢ 具体的なテスト内容 ➢ UX メトリクス ➢ タスクシナリオの開始基準・終了基準 ➢ ユーザビリティ/アクセシビリティテスト実施報告書の構成 ・ 本システムを対象としたユーザビリティ/アクセシビリティテストに必要となる実施施設や環境は、原則として受託者が手配すること。当該施設を利用するに当たって利用料金が発生する場合、受託者は、当該施設の利用料を本業務に伴う設計・開発に係る経費に含めること。 ・ ユーザビリティ/アクセシビリティテストの実施担当者を受託者において選定することとして差し支えないが、当該実施担当者は、調達仕様書「5.2.作業要員に求める資格等の要件」に示す要件を満たす者であること ・ ユーザビリティ/アクセシビリティテストの被験者、人数及び選定方法は、主管課との協議により定めること。ユーザビリティ/アクセシビリティテストの被験者は、最終ユーザーだけでなく、管理者である職員もテスト対象とすること。 ・ ユーザビリティ/アクセシビリティテストにおいてどのようなユーザー補助手段（マニュアル、ヘルプ等）を用意できるか整理すること。 ・ 受託者は、本業務において実施する各ユーザビリティ/アクセシビリティテストについて、客観的な評価を行うため、必要に応じて簡易な映像記録を制作することが望ましい。
3	性能・拡張性テスト	ユーザー数、データ量、リクエスト数、レスポンス等の性能要件を本システムが満たしているか検証する。検証に当たっては、現在の想定だけではなく、今後の予想される増加量も含めて確認する。 短時間で本システムに重い負荷をかけ、本システムが処理量や長時間稼働等のシステム限界に関する性能や拡張の要件を満たしているか確認する。
4	可用性（障害）テスト	疑似的に障害を発生させる等の方法により、本システムのコンポーネントに障害が発生した場合に、どの程度許容して安定動作するか検証する。また、システム障害及びエラー発生時の回復機能等が適切に動作することを確認する。
5	完全性テスト	疑似的に障害を発生させる等の方法により、本システムのコンポーネントに障害が発生した場合に、データの減失や改変がないことを検証する。また、操作ログやアクセスログ等のシステムログが出力されることを検証すること。
6	セキュリティテスト	不正侵入や Web 特有の攻撃への対策、データベースへの不正アクセスなどに対する対策、データの持ち出しに対する対策、マルウェア（ウィルス）対策等のセキュリティ要件を満たしているか脆弱性検査、インシデントレスポンステスト等を実施し確認する。

7	運用・保守テスト	運用・保守作業全般を通して、運用・保守事業者が円滑に日々の業務を実施できることを確認する。 また、運用・保守における正常時、異常時の運用に関する動作を確認し、特に異常時の対応として、エラーメッセージやログ等を基に、運用・保守事業者が業務を行えることを確認すること。

イ　総合テストに用いるテストデータには、本番運用を想定した疑似データを作成して使用すること。

ウ　キーワード駆動テストの適用により、総合テストの効率化を図ること。

エ　システム停止に伴うシステムバックアップやシステム停止、リストア、システム起動等については、受託者が主体的に実施すること。

オ　総合テスト実施時は、テスト結果を検証するための証跡を採取すること。

カ　総合テストは、原則として検証環境または本番環境において実施すること。

(4) 受入テスト

受入テストは、要件に対するアプリケーションの充足性確認を目的として行い、主管課は構築された情報システムが要件定義書に記載した事項を適切に実現しているか、本システムを用いて実際のサービス・業務を正しく実施できるかといった観点でテストを実施する。受入テストに用いるテストデータには、本サービスが原則として公開情報を取扱うことを踏まえ、可能な限り本番環境に近い複製データを使用する。ただし、受入テストの目的を担保可能であることを条件に、疑似データを使用することも可能とする。

受託者は調達仕様書にある通り以下の支援を行うこと。

ア　受託者は、主管課が実施する受入テスト計画書作成作業を支援するために、受入テスト計画書（案）を作成すること。主管課は受入テスト計画書（案）を基にして受入テスト計画書を作成する。なお、受入テストの実施期間は十分に確保したスケジュールとすること。

イ　受託者は、主管課が実施する受入テスト仕様書作成作業を支援するために、テスト項目、使用するテストデータ、合格判定基準等を示した受入テスト仕様書（案）を作成すること。主管課は受入テスト仕様書（案）を基にして受入テスト仕様書を作成する。

ウ　受託者は、主管課及びプロジェクト関係者が受入テスト計画書及び受入テスト仕様書に基づき実施する受入テストの実施支援を行う。

エ　受入テストは、原則として検証環境または本番環境において実施すること。受入テストの実施に当たり、必要に応じて本システムの運転スケジュール、環境設定、テストデータ等の変更を行うこと。

オ　受入テストの実施に当たり、主管課からの質問に対する問合せ対応を行うこと。

カ　受入テストで発生したすべての障害が解消されている、または問題を特定した上で対応策について主管課の承認を得ていること。

3.14. 移行に関する事項

本システムは、新規システムのためデータ移行は想定していないが、本番昇格環境の不要データの削除や初期データの登録、本番稼働のための設定変更等の作業を実施すること。

(1) 移行計画の作成

移行等に関しての計画をまとめた「移行計画書」を作成し、主管課の承認を得ること。「移行計画書」には、「図表 27 移行計画書の記載内容」を含めること。なお、移行計画は本プロジェクト関係者以外の第三者にも容易に理解可能でかつ継承可能な形式で作成すること。

図表 27 移行計画書の記載内容

項番	項目	補足
1	主管課及び各事業者の移行実施体制と役割	・ 移行作業は、受託者が主体となり実施するものとする。
2	移行に係る詳細な作業及びスケジュール	・ 受託者は、主管課に最終的な移行スケジュールを提示し、確定した内容を移行計画に反映させること。
3	移行対象 ※必要な場合	・ データ名称、保管環境、容量、など
4	移行環境／移行方法／移行ツール	・ 移行可能期間の制約も踏まえた上で、一括移行、差分連携等の手法を組み合わせて、円滑に移行が行えるように留意すること。 ・ 業務停止に当たっては、主管課に対して移行に係る時間や制約条件等を報告し、事前に十分な調整を行うこと。 ・ 移行方式は、原則として一括移行（or 複数回の分割移行）とする。
5	移行作業、移行に伴い発生する各種設定を行うための各種手順書・マニュアル	・ 移行する際の移行手順及び、機能改修のリリースに係る移行手順を作成し、主管課の承認を得ること。具体的な移行方法や手順は、主管課との協議の上で確定し、必要に応じて手順やツールの操作方法等に関するマニュアル等を受託者が作成すること。 ・ 移行手順は、本システムと連携するシステムにも影響があることを踏まえ、主管課経由で調整等を実施した上で作成すること。
6	移行判定基準	・ 移行開始時に満たすべき移行判定基準を定めること。なお、移行判定基準には以下を含め詳細は主管課と協議の上決定すること。 ➢ 計画した全てのテストケースを消化し、摘出された全ての障害（バグ、不具合等を含む）が除去されていること。仮に除去されていない障害がある場合は、その対処方針が明確となっていること。 ➢ 移行計画書及び移行リハーサルの結果が適正であること。 ➢ 切り戻し基準や切り戻し手順書を定めており、主管課の承認を得ていること。 ➢ 稼働後の運用準備が整っていること。
7	連携先の外部システム	・ システム移行に当たっては、関連システム関係者と連携すること。その際、システム連携の現状を把握し、本システムへの移行に伴うテスト計画を作成し、テストに向けた事前合意形成を行い、テストフェーズでも進捗管理、課題管理を行って、テスト結果の取りまとめを行うこと。その際に、必要な資料等の作成を行うこと。
8	移行リハーサルの実施場所（システム環境）	・ 移行リハーサルについては、必要に応じて、関連システム関係者と調整の上、検証環境及び本番昇格環境で実施すること。 なお、移行リハーサルにおいて本番昇格環境を利用しない場合は、可能な限り本番昇格環境に近い環境を準備した上で移行リハーサルを実施すること。

移行計画書に加えて「図表 28 計画の種類」の計画も作成すること。

図表 28 計画の種類

項番	計画の種類	概要
1	移行リハーサル計画	移行の設計内容、データ移行用サーバ及び移行用インポートサーバの設計内容、連携業務 AP の接続切替え方法、移行リハーサルにおける方針、スケジュール、実施体制、実施手順、検証方法等を定めたもの
2	移行（本番）計画	本番移行時の方針、スケジュール、実施体制、実施手順、作業結果判定方法、移行作 業時のセキュリティ対策等を定めたもの

(2) 移行データ準備・提供

データ移行作業が必要となった場合は、受託者は移行対象データの分析を行い、データ・クレンジング等の加工作業が必要であるか確認の上、主管課に報告すること。

(3) 移行設計

受託者は、「移行計画書」を踏まえ、以下の点に留意して移行設計書を作成の上、主管課の承認を得ること。

ア システム移行、データ移行、稼働の方式を設計すること。

イ 本番移行等、各移行作業に関しての見込み時間を記載すること。その際は、部分的なデータを送信して所要時間を計測するなど、必ず事前に計測を行い、本番移行の見込み時間の妥当性を証明すること。

(4) データ移行サーバ・ツールの開発

データ移行が必要な場合は、「移行設計書」の内容に基づき、データ移行ツールの開発及びテストを実施すること。なお、既製のソフトウェア製品の機能をそのまま利用してデータ移行を実施する場合は不要であるが、利用には主管課に報告の上、承認を得ること。

なお、移行対象データに対し、データ・クレンジング等の加工作業が必要な場合は当該作業を実施すること。

(5) 移行リハーサル

システム移行、データ移行のリハーサルでは以下の点に留意すること。

ア 移行リハーサル設計書及び移行リハーサル手順書の内容を最終確認し、関連システム担当者と最終的な意識合わせを行うこと。

イ 関連システム側に設定変更等を依頼する場合は、依頼書を準備し、期間的な余裕を持って、主管課経由で依頼すること。

ウ 受託者は、移行リハーサルの実施後、移行に係る作業手順、作業時間見積もり等を評価し、「移行リハーサル結果報告書」を作成すること。また、その内容について主管課に説明し、承認を得ること。

エ 移行計画書及び移行手順書に問題がないことを検証するため、最低 1 回以上移行リハーサルを実施すること。
なお、移行リハーサル実施後における使用データの扱い（移行リハーサル後に使用データを削除等）についても検討すること。

オ 受託者は、移行リハーサルの結果として移行リハーサルの結果を分析し、本番移行に向けた課題などを明確にすること。

カ　作業品質に改善及び再検証を要する問題点を確認した場合、必要に応じて移行リハーサルの再実行を検討すること。

キ　受託者は、主管課の指示がある場合、修正した移行リハーサル計画書及び移行リハーサル手順書を基準として移行リハーサルを再実行すること。

ク　受託者は、移行リハーサル評価結果に基づき、本番移行までに解決を要する課題について整理すること。

(6) 移行判定

主管課は、移行開始判定を目的とした会議を招集し、「（2）　移行計画の作成」にて定めた移行判定基準を満たしているか確認した上で、移行判定を行う。

受託者は、主管課が移行判定を適切に実施できるよう、報告には「（2）移行計画の作成」に記載した移行判定基準を満たしているか分かるような情報を含めること。

(7) 本番移行

本番移行では以下の点に留意すること。

ア　本番移行に向けて、移行リハーサルの実施結果を元に移行計画書及び移行手順書を修正すること。また、その内容について主管課に説明し、承認を得ること。

イ　移行計画書には、チェックポイントを設定し、作業の進捗度と経過時間などを元に、切り戻しの判断基準を設けること。

ウ　受託者は、本番移行及び稼働に係る作業過程において作成する提出物及び成果物の内容について、主管課に説明を行い、承認を得ること。

エ　受託者は、本番移行に伴う作業状況について、事前にチェックポイントを設定し、適切なタイミングで主管課に報告すること。万一、作業の実施中に不具合等を生じた場合は、速やかに主管課に報告するとともに、必要な対応を行うこと。

オ　受託者は、本番移行開始判断を受け、稼働のための作業を実施し、本番稼働を開始すること。

カ　受託者は、稼働関連作業の完了後、本システムの稼働状況を確認すること。

キ　移行リハーサル、本番移行の実施結果を「移行結果報告書」として取りまとめ、主管課の承認を得ること。

(8) 稼働判定

主管課は、サービスインを判断（稼働判定）する。その際、受託者は、本番環境への移行の実施結果が適正であり、新しい情報システムへ切り替えても業務に支障が生じないことを主管課が判断するための資料を提出すること。

3.15. 引継ぎに関する事項

本システムの運用は、別途調達する本システムの運用・保守事業者が実施する予定である。現時点で想定する引継ぎ要件を以下に示す。

(1) 引継ぎ計画書の作成

本システムの関連事業者に対する引継ぎの開始前に、本システムの引継ぎに係る引継ぎ対象、引継ぎ体制、引継ぎ内容、引継ぎ方法、引継ぎスケジュール、理解度確認方法、完了条件等を記載した「引継ぎ計画書」を作成し、主管課の承認を得ること。

(2) 引継ぎ方法

ア 受託者は、「引継ぎ計画書」に従い、十分な時間的余裕を持って、必要な運用引継ぎを行うこと。その際は、引継ぎ対象者の理解度を確認し、必要な場合には、「引継ぎ計画書」に記載したスケジュール等の変更を行うこと。

イ 本システムは、その保守や将来の拡張等の業務を他事業者に引き継ぐことが可能であること（引き継ぎのために必要となる各種ドキュメントを整備する等）。第三者による保守性を向上させるため、成果物等は標準的に利用されているドキュメント作成ソフトウェアを用い、編集可能な形式で納品すること。

ウ ドキュメントには設計結果のみを記載するのではなく、設計根拠等も明示し、検討経緯を可視化すること。

エ 期間内に引継ぎが完了しない場合は、原則として受託者の責任と負担において引継ぎを完了すること。

オ 連携先システムである、マイナアプリ（仮称）及びマイナポータルバックエンドの運用保守事業者に対しては、必要となる知識等について引継ぎを行うこと。

(3) 引継ぎ対象

本システムの引継ぎ対象を「図表 29 本システムの引継ぎ対象」に示す。なお、引継ぎに際しては主管課の指示に基づき書面又は電子媒体で行うこと。

図表 29 本システムの引継ぎ対象

項番	引継ぎ期間	引継ぎ先	引継ぎ内容	引継ぎ手順	補足
1	令和９年２月～ 令和９年３月	本システムの運用・保守事業者	・ ソースコード（テスト・構成管理・環境構築等に利用するコード含む） ・ 開発環境に必要となる各種ツール ・ 各種設計書・ドキュメント類 ・ 運用課題（管理簿） ・ 仕様課題（管理簿） ・ インシデント状況（管理簿） ・ 連携業務アプリケーション対応状況（管理簿） ・ ヘルプデスク作業 ・ 各種運用・保守作業 ・ その他成果物一式 （クラウドサービスの管理に必要なアカウントや鍵情報、また IaC（Infrastructure as Code）に基づくシステム構築・管理等に係る構成管理ファイル等情報を漏れなく含む）	受託者は、引継ぎ計画書の内容に基づいて、引継ぎ作業を行う。	―
2	令和９年２月～ 令和９年３月	関連システム（マイナアプリ（仮称）、マイナポータルバックエンド）の運用保守事業者	API 利用ガイド、API リファレンス等	受託者は、引継ぎ計画書の内容に基づいて、引継ぎ作業を行う。	―

(4) クラウドサービスを利用する場合の引継ぎ

本システムでは、本調達の契約期間終了後も、クラウドサービスの契約期間終了前に契約の延長又は他の引継ぎ先事業者（運用・保守事業者を想定）への引継ぎ等を行うことで、クラウドサービスをそのまま継続利用することを想定している。引継ぎに際しては、必要に応じて引継ぎ先事業者及びクラウドサービスプロバイダとの間で書面による契約等を行い、しかるべく管理者権限の引渡し等を行うこと。

(5) 引継ぎ結果報告書の作成

引継ぎ作業の完了時に、本システムの、他事業者等への引継作業の実施結果について記載した「引継ぎ結果報告書」を作成し、主管課へ報告を行うこと。

3.16. 教育に関する事項

本システムでは、UI の構築は行わないため、教育訓練は想定していないが、システムの概要説明資料や API 利用ガイド、API リファレンス等の資料は作成すること。

3.17. 運用・保守に関する事項

(1) 運用・保守計画

運用・保守の設計で検討した内容を踏まえて、以下の要件が含まれる形で運用・保守計画書及び運用・保

守実施要領の確定版を作成すること。なお、本システムの運用保守は、本調達の受託者と別途契約する想定である。

図表 30 運用・保守計画書の記載内容

項番	項目	補足
1	作業概要	・ 監視、運用・保守作業の対象範囲、管理対象、作業概要等を記載する。
2	作業体制に関する事項	・ 運用・保守業務を実施するための体制について、管理体制図、本件受託者の要員（責任者、作業者、役割分担）、連絡手段等について記載し、全体的な運用管理体制を明確にすること。
3	スケジュールに関する事項	・ プロジェクト計画書及び調達仕様書に基づき、運用・保守を行う上で基本とする作業内容、関係するほかの作業工程、そのスケジュール等について記載すること。 ・ 日次、週次、月次等の定型的な業務について、作業内容を記載すること。 また複数回発生した非定型業務の報告及びその定形業務化（手順書の作成等）の提案を含めること。 ・ 年次の作業内容には、運用業務の中で発生した運用上の課題、作業量の多い作業等について整理報告し、その改善（例えば自動化等）の提案を行う作業、システム運用継続計画の見直し作業、運用・保守計画書の見直し作業を含めること。
4	成果物に関する事項	・ 運用・保守業務にて納品する成果物の内容、担当者、納品期限、納品方法、納品部数等について記載する。
5	運用・保守形態、運用・保守環境等	・ 運用において採用する運用形態（オンサイト、リモート等）、運用にて利用する環境（本番環境、検証環境、研修用の環境等の有無）等を記載すること。
6	管理対象	・ 受託者は本業務で開発するシステム及びドキュメントについて保守を行うこと。
7	クラウドサービスの利用	・ 運用作業、運用手順及び運用管理用のソフトウェアも含め、可能な限り統一化を図るとともに、自動化された機能及びクラウドサービスが提供する機能等を利用し、運用に係る役務を可能な限り効率化すること。 ・ 利用しているクラウドサービスの機能や性能等に変更が発生した場合、受託者側でクラウドサービスの変更に伴う開発中システムへの影響を確認し、本システムの改修が必要な場合は、原則対応すること。ただし、改修規模が大きい又は影響範囲が広い場合は主管課と協議の上対応を検討・実施すること。
8	サービスレベル	・ 運用・保守業務で達成目標とするサービスレベル項目及びサービスレベルを主管課が協議の上、決定すること。 ・ 運用におけるリソース使用状況に基づき、毎年のリソース計画を策定する。月間の運用実績を評価し、達成状況が目標に満たない場合はその要因の分析を行うとともに、サービスレベル達成状況の改善に向けた対応策を提案すること。
9	その他	・ 上記に掲げる事項のほか、運用・保守を行う上での前提条件、時間、予算、品質等の制約条件等について記載する。

図表 31 運用・保守実施要領の記載内容

項番	項目	補足
1	コミュニケーション管理	・ 運用・保守業務を実施する上で必要となるコミュニケーション手段について、会議体（会議体 名称、開催目的、開催スケジュール、出席者、報告内容等）、インシデント発生時 の報告ルート等について記載し、効率的かつ円滑なコミュニケーションを実現すること。
2	体制管理	・ 運用・保守に携わる事業者における作業体制の管理手法等について記載する。
3	作業管理	・ 運用・保守作業及びその品質の管理手法等について記載する。
4	リスク管理	・ 運用・保守における作業を阻害する可能性のあるリスクを適切に管理するため、リスク認識の手法、リスクの管理手法、顕在時の対応手順等について記載すること。
5	課題管理	・ 運用・保守において解決すべき問題について、発生時の対応手順、管理手法等について記載すること。
6	システム構成管理	・ 運用・保守における情報システムの構成（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、施設・区域、公開ドメイン等）の管理手法等について記載すること。
7	変更管理	・ 運用・保守により発生する変更内容について、管理対象、変更手順、管理手法等について記載すること。
8	情報セキュリティ対策	・ 平常時のセキュリティ運用として、継続的な脆弱性管理、構成管理及び変更管理を行い、不正アクセス等のセキュリティ脅威に対する監視運用を行うための具体的な方法を記載すること。 また、セキュリティインシデント発生に備えた体制や手順、発生時の被害極小化、速やかなサービス復旧を行うための具体的な方法を記載すること。