

次期産業標準策定システム更改に係る
移行開発業務
要件定義書

令和7年5月27日

経済産業省

イノベーション・環境局 基準認証政策課

基準認証調査広報室

目次

1. 業務要件	1
1.1 システム方式に関する事項	1
1.1.1 次期 e-JISC システムサービスの範囲	1
1.2 業務実施手順	1
1.2.1 業務の範囲	1
1.3 規模に関する事項	3
1.3.1 利用者数及び想定アクセス数	3
1.3.2 データ量	3
2. 機能要件	3
2.1 機能に関する事項	3
2.2 データに関する事項	4
3. 非機能要件	4
3.1 性能に関する事項	4
3.1.1 応答時間	4
3.1.2 スループット（単位時間当たりの処理件数）	4
3.2 信頼性に関する事項	5
3.3 拡張性に関する事項	5
3.4 ソフトウェア等に関する上位互換性	6
3.5 中立性に関する事項	6
3.6 継続性に関する事項	6
3.6.1 バックアップの方針	6
3.6.2 災害への対応方針	7
3.7 情報セキュリティに関する事項	7
3.7.1 情報セキュリティ対策要件	7
3.7.2 ログの取得及び管理	9
3.8 情報システム稼働環境に関する事項	10
3.8.1 稼働環境に関する要件	10
3.8.2 クラウドサービスに関する要件	10
3.8.3 サーバ・ストレージ要件	11
3.8.4 ソフトウェア要件	11
3.8.5 ネットワーク要件	15
3.9 テストに関する事項	15
3.10 移行に関する事項	16
3.11 引継ぎに関する事項	16
3.12 SLA 管理	17

1. 業務要件

1.1 システム方式に関する事項

次期e-JISCのシステム方式は以下のとおり。

- ① 次期e-JISCを稼働させるために必要なソフトウェア、ネットワーク等の環境は、「次期e-JISCシステムサービス」として原則現行e-JISCのシステム構成、及びアプリケーションを踏襲した上で構築及び提供すること。
- ② 次期e-JISCシステムサービスの実現方式は、次期e-JISCの稼働に支障を来さないことを前提にモダン化する方針とし、「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」（令和5年9月29日 デジタル社会推進会議幹事会決定）が定める要件を遵守するものとする。なお、本ガイドラインにおいて、クラウドサービス提供事業者の実施が望まれる事項及びクラウドサービスの関連情報に記載されている事項について、実施できない範囲を明示すること。
- ③ 受注者は、クラウドサービスにおいて、一定のセキュリティレベルが確保されていることの保証として、クラウドサービスに対する情報セキュリティ監査報告書の内容及び取得、維持している各種認定・認証制度の基準等について事前に確認すること。

1.1.1 本調達範囲

次期e-JISCシステムサービスの範囲を以下のものとする。

- ① 次期e-JISCの動作に必要なオペレーティングシステム（OS）を含めたソフトウェアやそのライセンス、及び各種クラウドサービス
- ② 次期e-JISCに係る環境の設計、構築、テスト、移行に係る役務

1.2 業務実施手順

1.2.1 業務の範囲

e-JISCでは、産業標準化法に関する以下「表 1 e-JISCの関連業務」に示す業務を電子化及び支援するための機能を提供している。

表 1 e-JISCの関連業務

業務名称	業務内容
JIS 等の 制定・公示・公開等に関する業務	産業標準化業務計画の作成、JIS 原案及び類似の技術文書である TS（標準仕様書）/TR（標準報告書）原案の作成支援・受理、PD の公表、JISC の審議調整、JIS 制定等の付議、意見受付公告、主務大臣への答申、公示・公開、審議委員・原案作成団体対応等の組織運営に係る業務
JIS マーク制度に係る業務	JIS マーク制度に基づき登録認証機関情報、認証取得者情報の管理、認証報告の報告・受理、各種統計情報の集計、公開情報

	管理、判定委員会の管理及び業務連絡機能による情報管理に係る業務
JISC のホームページに係る業務	JIS 等の策定に関する情報（JIS・TS/TR）の検索・表示（閲覧ユーザの利用情報登録、変更、パスワード変更機能あり）、作業計画・作成状況及び PD の表示、意見受付公告の一覧の表示、登録認証機関とその事業所の検索と情報表示、認証取得者の検索と表示、JISC の審議に関する開催情報、配布資料の表示

また、各業務に関連する要件は「表 2 業務の範囲」に記載のとおりである。

表 2 業務の範囲

要件種別	要件項目	記載	概要
上記 3 業務に係る要件	性能要件	3.1	応答時間や処理件数等に係る要件
	信頼性要件	3.2	稼働率やそれを考慮した冗長構成等に係る要件
	拡張性要件	3.3	負荷に応じたリソースの変更や、将来的な環境拡張に係る要件
	互換性要件	3.4	e-JISC で使用するソフトウェア、ミドルウェア、OS のバージョンアップ等に係る要件
	中立性要件	3.5	オープンな規格の利用やベンダーロックインの回避等に係る要件
	継続性要件	3.6	バックアップ・リストアや災害対応等に係る要件
	セキュリティ要件	3.7	e-JISC に適用すべきセキュリティ対策やログの取得に係る要件
	情報システム稼働環境に関する事項	3.8	e-JISC を構成するハードウェア/ソフトウェアを含めた稼働環境に係る要件
その他の要件（更改・移行対応関連）	テスト要件	3.9	移行に伴い実施すべき各種テストに係る要件
	移行要件	3.10	e-JISC 全体もしくは構成するサービスの移行に係る要件
	引継ぎ要件	3.11	現行事業者からの引継ぎ、及び次期運用事業者への引継ぎに係る要件

1.3 規模に関する事項

1.3.1 利用者数及び想定アクセス数

次期e-JISCの利用者数、想定アクセス数、主な利用時間帯は「表 3 利用対象、想定アクセス数、主な利用時間帯」のとおり。

表 3 利用対象、想定アクセス数、主な利用時間帯

利用者※	拠点	人数	想定アクセス数 (件数/日)		主な利用 時間帯
			平均	ピーク数	
一般利用者	不特定多数	不特定多数	130,000	190,000	24 時間
内部利用者	1	150	100	150	平日 8 時-19 時
外部利用者	900	300	70	300	平日 8 時-19 時

※各利用者の定義は以下のとおり。

- ① 一般利用者：インターネット経由でのJISCホームページの利用者
- ② 内部利用者：JIS等の策定及びJISマーク制度の業務を行う担当職員
- ③ 外部利用者：内部利用者以外の次期e-JISCの利用者

1.3.2 データ量

次期e-JISCにおける主要な情報のデータボリュームの一覧は「表 4 データボリューム一覧」のとおり。

表 4 データボリューム一覧

No.	区分		データ量
1	データベース	総テーブル数	約220テーブル
2		総レコード数	約6,500,000件
3		総データ量	約3.3GB
4	ファイル	総ファイル数	約460,000件
5		1ファイル当たりの平均容量	約630KB
6		1ファイルの最大容量	約2150MB
7		総データ量	約288GB

2. 機能要件

2.1 機能に関する事項

次期e-JISCにおいては、パブリッククラウド上で稼動する現行システムを、可能な限りモダン化したうえで、現行システムで提供している全ての機能を継続して提

供することを前提とする。現行システムの機能については資料閲覧にて確認すること。

加えて、「次期産業標準策定システム更改に係る移行開発業務 調達仕様書」内“情報システムに求める要件に関する事項”に記載の要件を踏まえ、業務改善に資する機能を提案すること。

2.2 データに関する事項

データの観点においても、次期e-JISCは現行システムで保有しているデータを引継ぐ必要があるため、データベースの情報を全て移行し、正常に参照・更新等の操作が可能であることを前提とする。

3. 非機能要件

3.1 性能に関する事項

次期e-JISCの性能要件は以下のとおり。

3.1.1 応答時間

「次期産業標準策定システム更改に係る移行開発業務」においては「表 5 応答時間」に記載のとおり応答時間を要件としている。次期e-JISCシステムサービスでは、これを満たすため以下を実施すること。

- ① リクエスト伝送及び結果伝送に係るネットワーク、サーバ処理に遅延が発生しないようネットワーク及びサーバリソースを設定すること。
- ② 監視サービス等を利用してレスポンスタイムを定期的に測定すること。
- ③ 測定結果を分析し、ネットワークの遅延を原因とする目標値の劣化が発生した場合は、設定等の調整を行うこと。

表 5 応答時間

No.	設定対象	指標名	目標値	応答時間達成率
1	オンライン処理応答時間	レスポンスタイム	定常時：5 秒以内 ピーク時：10 秒以内 ※ただし、業務用サイトにおいて帳票作成処理等を行う場合は除く。	90 パーセント マイル
2	バッチ処理時間	-	2 時間（翌日のオンライン処理開始時刻の遅延とならないこと）	-

※ レスポンスタイム

リクエスト開始からリクエスト伝送、サーバ処理、結果伝送等を経て最初の応答・出力開始までに要する時間

3.1.2 スループット（単位時間当たりの処理件数）

「表 3 利用対象、想定アクセス数、主な利用時間帯」を参考に他のネットワーク脅威対策に対する負荷も考慮し提案すること。

3.2 信頼性に関する事項

次期e-JISCの可用性要件は以下のとおり。

- ① 「表 6 稼働率」の稼働率を満たすように、故障が発生してもサービスが停止しない適切な冗長構成とすること。
- ② ある拠点で障害が発生しても別拠点のシステムで継続的な運用が可能になるよう複数の可用性領域での構成とすること。
- ③ データベース機能は、クラスタ構成とし、ホットスタンバイによる障害発生時の待機系への切替えを可能とすること。
- ④ Webサービス提供機能、一般利用者用アプリケーション提供機能をクラスタ構成とし、負荷分散及び障害発生時の縮退運転を可能とすること。
- ⑤ 文書保管機能、データベース機能は、外部ストレージにデータを保管すること。

表 6 稼働率

サービス	サービス提供時間	年間の稼働率※
一般利用者向けサービス	24 時間 365 日	99.9%
内部／外部利用者向けサービス	平日の 8 時～19 時	99.9%
その他	事業者が提供するサーバ、ストレージ等の障害により、翌日のオンライン処理開始時刻の遅延とならないこと	

※年間の稼働率：災害発生時及び計画停止時間を除く

3.3 拡張性に関する事項

次期e-JISCの拡張性に係る要件は以下のとおり。

- ① リソースの一次的な変更及び恒久的な変更に対応するための仕組みを提供すること。
- ② 将来的に利用環境の変更が発生した場合、必要に応じて、CPU、メモリ、ハードディスク、ネットワークの変更、若しくは増設が可能であること。
- ③ 増設を行う際のCPU、メモリ、ストレージについては単位当たりの金額を提示すること。ただし、本調達における金額との大幅な差異は認めない。

3.4 ソフトウェア等に関する上位互換性

次期e-JISCのソフトウェア等に関する上位互換性に係る要件は以下のとおり。

- ① 次期e-JISCの稼働環境であるOS又はミドルウェア等のソフトウェアにおいて、バージョンアップ若しくはセキュリティ問題に起因する変更が発生した場合、変更が次期e-JISCに影響がないことを確認の上、担当職員に報告後、変更作業を行うこと。なお、影響が発生する場合は、担当職員と協議の上、変更の実施タイミング等を調整すること。
- ② 次期e-JISCの稼働環境であるOS又はミドルウェア等のソフトウェアが、バージョンアップ若しくはセキュリティ問題に起因する変更が発生した場合、次期e-JISCのプログラム及びデータは円滑に移行できること。

3.5 中立性に関する事項

次期e-JISCの稼働環境においては、以下の点を考慮すること。

- ① 次期e-JISCの移行及び更改に支障がないよう、特定の事業者及び製品に依存しないシステム構成とすること。
- ② 提供するソフトウェア等は、原則として国際規格及び日本産業規格等のオープンな規格に準拠することを優先する。
- ③ 提供するソフトウェア等は、原則オープンなインタフェースを利用して接続又はデータの入出力が可能であること。
- ④ サプライチェーン・リスクを考慮したサービスの選定を行うこと。
- ⑤ サプライチェーン・リスクを軽減する対策として、「1.1.1 次期e-JISCシステムサービスの範囲」に示す範囲において、不正が発覚した場合に、検査及び追跡調査・排除できる体制を整備すること。

3.6 継続性に関する事項

次期e-JISCにおいては、データバックアップからリストアできることを確保するものとする。

3.6.1 バックアップの方針

バックアップの方針は以下のとおり。

- ① システムデータは、各サーバの正常稼働時の状態をバックアップし、そのデータから障害発生前の状態に戻せるように考慮する。
- ② 業務アプリケーションは、各サーバの正常稼働時の状態をバックアップし、そのデータから障害発生前の状態に戻せるように考慮する。
- ③ 業務データベースは、障害回復に必要な情報データ（各種ログ等）を日々バックアップし、そのデータにてフォワードリカバリにより障害発生前の状態に戻せるよう考慮する。
- ④ 業務データ並びにコンテンツは日々バックアップし、そのデータから障害発生前の状態に戻せるように考慮する。

- ⑤ 次期e-JISCにおけるバックアップの実施タイミングについては、「表 7 現行e-JISCにおけるバックアップの実施タイミング」を踏まえ、最適なバックアップの実施タイミング、保存期間等について担当職員と協議の上、決定すること。

表 7 現行 e-JISC におけるバックアップの実施タイミング

対象データ	実施タイミング	世代数	保存期間※1
システムデータ	システムメンテナンス時の作業開始前と作業完了後	2 世代	次々回実行まで
業務アプリケーション	アプリケーション変更時の作業開始前	2 世代 ※2	次々回実行までと作業完了後
業務データ	月次でフルバックアップ (第 1 日曜日 4:00~12:00) 日次で差分バックアップ (毎日 3:00~4:00)	3 世代	3 ヶ月
コンテンツ	月次でフルバックアップ (第 1 日曜日 4:00~12:00)	3 世代	3 ヶ月
ログ	週次でログの切り替えを行う	10 世代	10 週間

※1：保存期間は、全世代での最大期間とする。

※2：1 世代は、メンテナンス前と後の状態のバックアップとする。

3.6.2 災害への対応方針

- ① 次期e-JISCで保持しているデータが消失しないよう、遠隔地でバックアップを保管すること。なお、バックアップの保管先は、300km以上離れた場所とすること。
- ② 災害が発生した場合、遠隔地に構築している次期e-JISC復旧用のシステムで継続して運用できることが望ましい。

3.7 情報セキュリティに関する事項

3.7.1 情報セキュリティ対策要件

次期e-JISCにおける情報セキュリティ対策として、「表 8 情報セキュリティ対策要件」を提供すること。

表 8 情報セキュリティ対策要件

分類	機能	概要
コンテンツ対策	ウイルス対策機能	不正なプログラムがサーバに、ウイルス、ワームその他の不正プログラムの感染及び侵入を防止するため、不正プログラムの検出、隔離、駆除等を行う。
	スパムメール対策機能	無差別・大量に送りつけられる、不要もしくは有害な内容を含む電子メール（スパムメール）を判別し、隔離、破棄等を行う。
	ウイルスゲートウェイ機能	ネットワークパフォーマンスを低下させることなく、ウイルス及びワーム、スパイウェア等に対してネットワークを防御及び添付ファイルに対してスキャンを行う。
	インターネットコンテンツフィルタリング機能	ファイアウォール及び Web サーバで日本国外に割り当てられたアドレス空間からの通信をフィルタリングし、アクセスの遮断等を行う。 ホワイトリスト機能を用いて上記のアドレス空間を一部からのアクセスを許可する。 ただし、アクセス可否の制御の設定変更はアプリケーションから実施予定。
	送信メールフィルタリング機能	送信される電子メールにつき、そのアドレス及び内容、添付ファイル等进行检查し、機密性の確保に違反する内容を含むものに対して、保留、削除、警告、ログ保存等を行う。
ネットワーク脅威対策	ファイアウォール機能	送信元アドレス、送信先アドレス、プロトコルの種類、ポート番号、通信のステータス等の情報に基づき、あらかじめ設定されたルール又はポリシーに従って、通信の許可、遮断等を行う。
	アプリケーションファイアウォール機能	アプリケーションサーバへのネットワーク通信を監視、解析し、不正侵入その他攻撃及び悪用を目的とする通信に対して、遮断、ログ記録等を行う。
	不正侵入検知・防御機能	ネットワーク上の通信の内容及び状態を監視し、侵入もしくは攻撃と判断される通信に対して警告、防止、遮断、ログ記録等を行う。

分類	機能	概要
		また、監視対象となるホストのログ及びコマンドのヒストリから利用状況を監視し、不正アクセスと判断できるアクセス及びファイルの不正改ざんなどの操作を発見した場合に通知等を行う。
	HTTPS 暗号化機能	TLS 暗号化プロトコルと組み合わせることにより HTTP 通信の安全性を向上する。なお、TLS のバージョンは 1.3 を利用すること。
システムセキュリティ	証跡管理機能	システムあるいはネットワークを利用するユーザ（プログラムを含む）のログイン及びログオフを始めたログを管理する。証跡のログは、第三者に不正に利用されないことがないように、アクセス制御、暗号化、改ざん防止、改ざん検出等の措置を講じること。
	改ざん検知防止機能	暗号化及びログ解析等を利用し、Web コンテンツ等の改ざん防止及び検知ができること。
その他	NTP 機能	ネットワークに接続されるサービスが持つ時計について、正しい時刻へ同期。
	DNS 機能	インターネットなどの TCP/IP ネットワーク上でドメイン名及びホスト名と IP アドレスの対応関係を管理。
	納品時のセキュリティ対策	本調達の納品時には、パブリッククラウドサービスにおいて、脆弱性検査が実施可能な範囲を当省に提示した上で、脆弱性検査を実施すること。

3.7.2 ログの取得及び管理

次期e-JISCに係る情報収集及び予兆の検知、トレーサビリティ確保を目的として、「表 9 ログの取得及び管理」にあるログの取得及び管理を行うこと。

ログは世代管理を行い各サーバのディスク内に保存する。なお、障害発生のため取得できなかったログについての保証は求めない。

表 9 ログの取得及び管理

対象		取得、管理するログ
サーバ	オペレーティングシステム (OS)	認証ログ、操作記録、SYSLOG、エラーログ
	ミドルウェア	認証ログ、操作記録、アクセスログ、エラーログ
	アプリケーション	アクセスログ、バッチログ
ネットワーク		通信記録、アクセスログ、操作記録
リモート管理		認証ログ、操作記録、アクセスログ、エラーログ

3.8 情報システム稼働環境に関する事項

3.8.1 稼働環境に関する要件

次期e-JISCの稼働環境は、以下の要件を満たすものを提案すること。なお、現行e-JISCに係る設計書等は、資料閲覧時に確認すること。

- ① 3階層モデルを採用すること。
- ② ファイアウォール機能によりインターネット及び内部ネットワークから隔離された区域 (DMZセグメント) を設け、Webサーバ等、インターネットに公開するサーバを設置すること。
- ③ 所定の稼働率を満たすために必要なサービスを冗長化すること。
- ④ Webサービス提供機能、一般利用者用アプリケーション提供機能等の高負荷が想定されるサーバ等は負荷分散を行うこと。
- ⑤ アプリケーションの保守及びソフトウェアのバージョンアップ等を検証するための試行環境を設置すること。
- ⑥ 試行環境のサーバ構成については、保守及び検証が可能であれば、統合することも可とする。
- ⑦ 試行環境は、本番環境と同等又は下位の性能のサーバ等を用いること。
- ⑧ 現行e-JISCの詳細な設計書等は、資料閲覧時に確認すること。

3.8.2 クラウドサービスに関する要件

次期e-JISCの稼働環境として、以下の要件を満たすものを提案すること。

- ① ISMAP等クラウドサービスリストからクラウドサービスを選定すること。
- ② 情報資産を管理するデータセンタの物理的所在地が日本国内であり、5年以上の運用実績があること。
- ③ 当省の指示がない限り、一切の情報資産について日本国外への持ち出しが

行われなないこと。

- ④ 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。
- ⑤ クラウドサービスの利用に関連して生じる紛争は、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。
- ⑥ 契約の解釈が日本法に基づくものであること。
- ⑦ 情報資産の所有者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。
- ⑧ 当省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。
- ⑨ 情報資産が残留して漏えいすることがないように、必要な措置を講じられていること。

3.8.3 サーバ・ストレージ要件

次期e-JISCで利用するサーバ及びストレージに係る要件は以下のとおり。

① サーバに係る要件

次期e-JISCを構成するサーバに係る共通要件は以下のとおり。

- (ア) 24時間運転が可能なこと。
- (イ) 構築後に必要なソフトウェアのインストールが可能なこと。
- (ウ) 各機能のメモリ、ハードディスク等に関する情報については、資料閲覧で確認の上、次期e-JISCが稼働できるよう検討し提案すること。

② 外部ストレージに係る要件

データベース機能及び文書管理機能で利用する外部ストレージに係る要件は以下のとおり。

(ア) ディスク装置

データ格納領域として、合計 3TB 以上の実効容量を持つボリュームを確保すること。

3.8.4 ソフトウェア要件

「次期産業標準策定システム更改に係る移行開発業務 調達仕様書 表2 システムサービス対象機能」を実現するために必要となるソフトウェア、及びそのサポートライセンスを提供すること。なお、構成については、現行e-JISCのシステムを踏襲した上で次期e-JISCのシステムを構築すること。

その他、以下の要件を満たすこと。

- ① 以下のソフトウェアについては、ソフトウェア及びバージョンに指定があるため、資料閲覧で確認すること。また、当該ソフトウェアについては、初期インストール及び設定作業を行うこと。
 - (ア) オペレーティングシステム

- (イ) 全文検索機能
 - (ウ) データベース機能
 - (エ) データベース管理機能
 - (オ) PDF閲覧・変換機能
 - (カ) 電子メール・メーリングリスト機能
 - (キ) Webサーバ機能
 - (ク) APサーバ機能
 - (ケ) アプリケーション開発/実行環境
- ② 導入時においては、原則として最新の修正モジュールを適用すること。
 - ③ 脆弱性等の対応が必要な場合に備え、修正モジュールの提供サポートが受けられる環境であること。
 - ④ 日本語データを扱うことが可能なこと。また、受注者側が利用するものについてのユーザインタフェースは原則日本語とし、日本語版が提供できない場合は、日本語版ユーザマニュアル等を提供すること。
 - ⑤ 国内における商用での納入実績があること。
 - ⑥ 各個別機能に関するソフトウェアの要件は以下のとおり。
 - (ア) 電子メール・メーリングリスト機能に係る要件
 - (1) SSL 等による通信経路の暗号化が可能であること。
 - (2) サーバ証明書には、政府認証基盤（GPKI）を利用すること。
 - (イ) DNSサーバ機能に係る要件
 - (1) 内部ネットワーク用に DNS サーバ機能を提供すること。
 - (ウ) NTPサーバ機能に係る要件
 - (1) 基準となる時刻に使用するサーバ等の時刻を同期する機能を提供すること。
 - (2) 基準とする時刻は日本標準時（JST）が望ましい。
 - (エ) 改ざん検知機能に係る要件
 - (1) システムに行われた不正な変更を検知及び通報する機能を提供すること。
 - (2) 正規の変更（更新、削除及び追加）と不正な変更を判別できるよう設計及び設定を実施すること。
 - (3) 判別の基準等を設計するために必要な情報はアプリケーション開発等事業者を確認すること。
 - (4) 設計した情報を当該機能に設定すること。
 - (オ) 不正アクセス防止機能に係る要件
 - (1) 外部ネットワークからの侵入及びコンピュータ内部からの外部ネットワークへの不正な通信を検知、遮断する機能を提供すること。
 - (2) 次期 e-JISC のネットワーク及びコンピュータへ不正に侵入されるのを防御する機能を提供すること。

(カ) ウイルス対策管理機能に係る要件

- (1) サーバ内のウイルスを検知し、駆除する機能を提供すること。
- (2) メールに対するウイルス検知及びメール情報の漏えい防止機能を提供すること。
- (3) ポリシーファイルの更新による新種ウイルスの検出・駆除が可能であること。
- (4) ポリシーファイル及びパターンファイルの最新化を実施すること。
- (5) スパイウェア及びフィッシング等に対するゲートウェイセキュリティを提供すること。
- (6) 以下の機能に導入すること。
 - ・ 電子メール・メーリングリスト機能
 - ・ Webサーバ機能
 - ・ PDF閲覧・変換機能
 - ・ APサーバ機能
 - ・ データベース機能
 - ・ データベース管理機能
 - ・ バックアップ機能
 - ・ システム運用管理機能

(キ) バックアップ管理機能に係る要件

- (1) 次期 e-JISC と同程度の規模に対応したバックアップとリカバリが可能であること。
- (2) データベースのオンラインバックアップが取得できること。

(ク) ファイアウォール機能、統合脅威管理機能に係る要件

- (1) ファイアウォール機能が、アクセス制御、認証、ネットワークアドレス変換 (NAT) 等の機能を有し、プライベートネットワークの保護が可能であること。
- (2) 内部ネットワークアドレスの外部流出防止機能を提供すること。
- (3) アクセスが許可されているかどうかのユーザ認証によるアクセス制御機能を提供すること。

(ケ) 不正アクセス監視機能 (IPS/IDS) に係る要件

- (1) 外部接続からの不正アクセスを検知し、アクセスを遮断する機能を提供すること。
- (2) 不正アクセスの監視及び遮断状況等の監視を提供すること。
- (3) シグニチャベースのパターン・マッチング検出が可能であり、ネットワーク型の IPS/IDS であること。

(コ) リモート管理機能に係る要件

- (1) サーバの設定情報の参照及びアプリケーションの障害分析等を実施するために、サービスへ接続する機能を提供すること。

- (2) SSL 等による通信経路の暗号化が可能であること。
- (3) 以下の機能に導入すること。
 - ・ 電子メール・メーリングリスト機能
 - ・ Webサーバ機能
 - ・ PDF閲覧・変換機能
 - ・ 負荷分散機能
 - ・ APサーバ機能
 - ・ データベース機能
 - ・ データベース管理機能
 - ・ 文書保管機能
 - ・ バックアップ機能
 - ・ システム運用機能
- (サ) システム運用機能に係る要件
 - (1) 単一の画面等から、監視機能、性能機能、ジョブ機能及びファイル配布機能の管理ができること。
 - (2) 監視機能
 - ・ ログ監視、SNMP監視、SQL監視、キャパシティ監視、プロセス監視等の監視手段を用いて、ネットワーク、OS、リソース、アプリケーション等の障害及び利用状況等の監視を実施できること。
 - (3) 性能機能
 - ・ CPU、メモリ、ディスク等のリソース利用状況を収集、蓄積及び管理することができること。
 - ・ 収集値をファイル出力又はグラフとして保存可能なこと。
 - (4) ジョブ機能
 - ・ ジョブの定義、任意ジョブからの開始・停止・中断・再開等を行うことが可能なこと。
 - ・ 複数ジョブを任意の順序でまとめて定義・実行が可能なこと。
 - ・ 任意の日付・時間・曜日等にジョブの開始、停止、中断及び再開のスケジュールが可能なこと。
 - ・ ジョブ実行結果を画面表示、メール送信等により通知可能なこと。
 - (5) 仮想化環境上のリソース変更が実施できること。
 - ・ サーバ設定（CPU、メモリの追加／変更、サーバの追加／削除等）
 - ・ ストレージ設定（容量の増減、論理ドライブの追加、ストレージ種別の変更等）
 - ・ ネットワーク設定（ファイアウォールの設定変更、ロードバランサの設定変更、セグメント追加等）
 - (6) 設計情報及び現行運用事業者による設計変更情報等の内容に従い、設定情報の投入、変更を行うこと。

(7) 上記(1)から(6)を満たすシステム運用機能を導入すること。

3.8.5 ネットワーク要件

① ネットワーク構成

次期e-JISCで想定しているネットワーク構成については、資料閲覧で確認すること。

(ア) ネットワークに係る要件

ネットワークに係る要件は以下のとおり。

- (1) インターネットへの接続を行うため、外部接続セグメント、運用管理セグメント等にファイアウォール機能を提供すること。
- (2) インターネットからの不正アクセスを防止するため、不正侵入防止機能を提供すること。
- (3) 一般利用者 Web 機能、内部／外部利用者 Web 機能においてアクセスの負荷分散を行うため、負荷分散機能を提供すること。
- (4) 政府認証基盤（GPKI）のサーバ証明書を利用することし、必要な作業を実施すること。
 - ・ 証明書署名要求（CSR：Certificate Signing Request）の作成を行い、作成された証明書をWeb機能等に導入すること。
 - ・ サーバ証明書の有効期限内に更新を行うこと。
 - ・ 外部公開用サーバにおいてはTLSを利用すること。
 - ・ ネットワーク内のアクセスはTCP/IPを利用すること。

3.9 テストに関する事項

以下のテスト作業を実施すること。

① システムサービステスト作業

- (ア) 性能／信頼性に係るテストを含めたテスト計画を作成し、担当職員と合意すること。
- (イ) システムサービスに係るテスト仕様を作成すること。
- (ウ) システムサービスに係る動作確認を行うこと。
- (エ) アプリケーションの単体テスト～結合テストを行うこと。
- (オ) システムサービス全体が設計通りに動作することをテストすること。
- (カ) 担当職員に対して、テスト結果の報告を行うこと。

② 稼動環境構築作業

- (ア) 受注者は、アプリケーションの初期インストール及び設定作業を行うこと。
- (イ) 性能／信頼性を測定し、必要に応じてのデータベース等のミドルウェアのチューニングを行うこと。

- (ウ) 「テスト計画書」に基づき、アプリケーションテスト工程に使用したデータ等の初期化を行うこと。

3.10 移行に関する事項

次期e-JISCに係る移行作業として、移行計画書に従い、以下を実施すること。

- ① 次期e-JISCのデータ移行は、通常業務を止めないように、現行e-JISCを並行稼働させながら実施するものとする。
- ② Webサイト及びメールを停止せずに移行を実施するために、現行のドメインの移管に係る作業及びDNS切り替えに係る作業を実施すること。なお、契約期間中は当該ドメインを継続して提供すること。
- ③ 現行システムサービス事業者、現行運用事業者が抽出した業務データ等を次期e-JISCインフラ環境に従い格納すること。
- ④ 現行システムに保存されたアプリケーションに係る情報及びアクセス制限に係る設定情報等、現行システムサービス事業者、現行運用事業者から取得し、次期e-JISCインフラ環境に設定すること。
- ⑤ 移行を実施するに当たっては、担当職員、現行システムサービス事業者、現行運用事業者等関係業者と連携の上、移行作業に支障が発生しないようにすること。

3.11 引継ぎに関する事項

以下の引継ぎ作業を実施すること。

- ① 引継ぎ計画の作成
 - (ア) 現行運用事業者からの引継ぎ及び次期e-JISC関係者への引継ぎについて、引継ぎ項目、引継ぎ体制・役割、作業及びスケジュール、引継ぎ結果の評価方法・評価基準等を記載した「引継ぎ計画書」を作成し、担当職員の承認を得て、実施すること。
- ② 引継ぎ作業の実施
 - (ア) 「引継ぎ計画書」に従い、引継ぎ作業を実施すること。
 - (1) 現行システムサービス事業者及び現行運用事業者からの引継ぎ項目の例
 - ・ 次期e-JISCの運用に必要な現行e-JISCの各種設定情報
 - ・ 現行e-JISCの利用に係る各種情報
 - ・ 現行e-JISCのインフラ及びアプリケーションの設計情報
 - (2) 次期 e-JISC 関係者への引継ぎ作業
 - ・ 各種サービスに係る設定情報
 - ・ アクセス件数等、e-JISCの利用に係る各種情報
 - ・ 次期e-JISCの運用に必要なシステムサービスに係る設計情報
 - ・ 次期e-JISCの運用に必要なプログラム情報及びデータ

- ・ 次期e-JISCの運用に係る運用設計書、及び各種マニュアル
- ③ 引継ぎ完了の報告
- (ア) 各引継ぎ計画に従い実施した引継ぎの内容を記載した「引継ぎ作業完了報告書」を作成すること。なお、「引継ぎ作業完了報告書」については、担当職員に報告した上で、承認を得ること。

3.12 SLA管理

次期e-JISCシステムサービスにおけるSLA (Service Level Agreement) を以下のものとする。また、SLAについては「表 10 SLA目標」のとおり。

- ① 本調達においては、担当職員と協議の上、SLAの締結及び順守すること。
- ② 担当職員に対して事前に提出された運用・保守等に係る計画停止時間及び災害発生時等の場合を除き、SLAを遵守できない場合、対応策の検討を迅速に実施し、担当職員の了承を得た上で改善を実施すること。
- ③ 各サービスの監視、測定等を行い、サービスレベルの達成状況を逐次確認、把握すること。なお、監視、測定方法については、担当職員と協議の上、決定すること。
- ④ SLAを満たせない可能性がある場合、速やかに担当職員に報告すること。

表 10 SLA 目標

No.	サービスレベル項目	内容	目標値	その他
1	稼働率①	一般利用者向けサービスの稼働率※ (24 時間 365 日の稼働率)	99.9%	モニタリング及び報告は月次、評価は年次で行うものとする。サービス停止時間は、提供されたシステムサービスに起因する事象により、次期 e-JISC がまったく利用できない状態の時間、若しくは 48 時間以上継続して縮退運転となった場合の 48 時間経過後の時間とする。 なお、担当職員からの依頼によるサービス停止又はサービス提供停止が不可欠な保守メンテナンス（パッチ適用、バックアップ等）による停止は除く。
2	稼働率②	内部／外部利用者向けサービスの稼働率※ (平日 8 時～19 時における稼働率)	99.9%	
3	障害復旧	業務時間内に次期 e-JISC を構成サービスにおいて、機能提供の停止を伴う障害が発生した場合に、障害が発生した時点から機能提供再開までの時間	障害発生から 2 時間以内 (なお、障害の内容により当該目標値での復旧が見込めない場合は、別途担当職員と協議の上、対応すること。)	
4	障害通知	監視対象において障害検知後、当省指定先に通知するまでの時間	45 分以内	障害通知は原則としてメールで行うこと。ただし、緊急時には電話にて通知を行うこと。

※稼働率（年間）の算定式：

$(\text{年間の総[稼働保証時間]} - \text{一年間の総[稼働保証時間]内のサービス停止時間}) \div \text{年間の総[稼働保証時間]}$

※稼働率（月間）の算定式：

$(\text{月間の総[稼働保証時間]} - \text{一月間の総[稼働保証時間]内のサービス停止時間}) \div \text{月間の総[稼働保証時間]}$