

「子どもの健康と環境に関する全国調査
(エコチル調査)」に係るデータ管理システム一式
要件定義書(案)

第1版

環境省

目次

1. 用語の定義	1
2. スケジュール要件定義	2
2.1. 調達計画	2
2.2. 概要	2
3. 業務・機能要件定義	3
3.1. システム化要件	3
3.2. システムの利用者	3
3.3. 汎用パッケージソフトウェアの利用要件	4
3.4. 情報信頼性コントロール要件	4
4. システム方式要件定義	5
4.1. システム全体構成要件	5
4.1.1. システム化方式	5
4.1.2. システム全体構成	5
4.2. 性能要件	7
4.3. 信頼性要件	7
4.3.1. 信頼性に関する指標、目標値	7
4.3.2. 可用性	7
4.3.3. 機密性	7
4.3.4. 完全性	8
4.3.5. 拡張性	8
4.3.6. システムの中立性	8
4.3.7. 復旧性	9
5. 情報・データ要件定義	9
5.1. データボリューム一覧表	9
6. ユーザーインタフェース要件定義	10
6.1. 画面一覧	10
6.2. 帳票一覧	10
6.3. 画面設計規約	10
6.3.1. 表示内容	10
6.3.2. 画面遷移	11
6.4. 帳票設計規約	11
7. 外部インタフェース要件定義	12

7.1. 連携対象システム一覧	12
8. ネットワーク要件定義	12
8.1. システム全体構成イメージ	12
8.2. 回線と接続方式	12
8.2.1. 調達予定の回線	12
8.2.2. 接続方式	13
8.3. LAN 要件	13
8.3.1. 方針	13
8.3.2. 効率性要件	13
8.3.3. LAN 信頼性要件	13
8.3.4. LAN 構築要件	14
8.4. その他ネットワーク要件	14
8.4.1. 方針	14
8.4.2. 効率性要件	15
8.4.3. 信頼性要件	15
8.4.4. 構築要件	15
9. ハードウェア要件定義	16
9.1. 共通要件	16
9.2. サーバ	16
9.2.1. サーバ機能一覧	16
9.2.2. サーバ共通要件	17
9.2.3. Web サーバ	17
9.2.4. アプリケーションサーバ	18
9.2.5. DB サーバ	18
9.2.6. 文書管理サーバ	18
9.2.7. メールサーバ	19
9.2.8. 運用管理サーバ	19
9.2.9. 認証サーバ	20
9.2.10. DNS サーバ	21
9.3. ストレージ等	21
9.3.1. ストレージ装置	21
9.3.2. 外部交換装置	21
9.4. ネットワーク関連機器	21
9.4.1. スイッチ	21
9.4.2. ルータ	21

9.5. 各監視用機器、セキュリティ用機器	22
9.5.1. ファイアウォール装置	22
9.5.2. IDS（侵入検知システム）	22
9.6. 業務用機器（PC、プリンタ等）	22
9.6.1. 運用管理用端末（データセンター）	23
9.6.2. 運用管理用端末（コアセンター）	23
9.6.3. 業務用端末（コアセンター）	23
9.6.4. 保守端末（コアセンター）	23
9.6.5. ユニットセンター用端末	23
9.6.6. プリンタ	23
9.6.7. OCR	23
9.6.8. バーコードリーダー	23
9.7. ハードウェア拡張性要件	24
10. ソフトウェア要件定義	24
10.1. 共通要件	24
10.2. ソフトウェア要件	25
10.2.1. サーバ共通ソフトウェア要件	25
10.2.2. Web 系（DMZ）サーバソフトウェア要件	25
10.2.3. 侵入検知サーバソフトウェア要件	25
10.2.4. 認証サーバソフトウェア要件	26
10.2.5. 運用管理サーバ要件	26
10.2.6. 端末共通ソフトウェア要件	28
10.2.7. 業務用端末ソフトウェア	29
10.2.8. ユニットセンター端末ソフトウェア	29
11. 情報セキュリティ要件定義	30
11.1. 共通要件	30
11.2. 権限	30
11.3. 情報セキュリティ対策	30
11.3.1. 主体認証機能	30
11.3.2. アクセス制御	31
11.3.3. 権限管理機能	31
11.3.4. 証跡管理機能	31
11.3.5. 保証のための機能	32
11.3.6. 暗号と電子署名（鍵管理を含む）	32
11.3.7. セキュリティホール対策	32

11.3.8.	不正プログラム対策	33
11.3.9.	サービス不能攻撃対策	33
11.3.10.	踏み台対策	33
11.3.11.	不正アクセス対策	33
12.	設計・開発要件定義	33
12.1.	設計・開発実施計画の作成	33
12.2.	設計・開発実施体制	34
12.3.	設計・開発スケジュール	36
12.4.	開発環境の整備	36
12.5.	開発方法	36
13.	テスト要件定義	37
13.1.	テスト実施計画の作成	37
13.2.	テスト実施体制と役割	37
13.3.	テストスケジュール	37
13.4.	テスト環境	37
13.5.	テスト方法	37
13.6.	テストデータ	38
13.7.	受入テストの支援	38
14.	移行要件定義	38
14.1.	システム移行	38
14.2.	業務移行	39
14.2.1.	教育	39
14.2.2.	教育訓練実施体制と役割	39
14.2.3.	教育訓練スケジュール	39
14.2.4.	教育訓練環境	39
14.2.5.	教育訓練方法	39
14.2.6.	教育訓練用教材の開発	39
14.2.7.	教育訓練用教材の評価	40
14.2.8.	教育訓練の実施報告と評価	40
15.	運用・保守要件定義	40
15.1.	運用・保守体制と役割	40
15.1.1.	体制と役割	40
15.1.2.	主な業務内容	40
15.1.3.	運用範囲	42
15.1.4.	その他運用保守体制に関する事項	42

15. 2. 運用業務要件	43
15. 2. 1. 業務内容一覧	43
15. 2. 2. 運用ドキュメント	46
15. 2. 3. 運用・保守業務時間とシステム稼働時間	47
15. 2. 4. 障害対応	47
15. 2. 5. セキュリティ対応	47
15. 2. 6. その他	47
15. 3. データ管理要件	48
15. 3. 1. バックアップ要件	48
15. 4. システム運用・保守施設	48
15. 4. 1. システム運用・保守業務の作業場所	48
15. 4. 2. データセンター運用業務の作業場所	48
15. 5. 保守業務要件	48
15. 5. 1. 主な業務内容	48
15. 5. 2. 保守範囲	49
15. 5. 3. 保守業務時間	49
15. 6. ソフトウェア保守要件	49
15. 6. 1. ソフトウェア保守対象	49
15. 6. 2. ソフトウェア保守について	49
15. 7. ハードウェア保守要件	50
15. 7. 1. ハードウェア保守対象	50
15. 7. 2. ハードウェア保守について	50
15. 8. データセンター要件	51
15. 8. 1. 基本要件	51
15. 8. 2. 設備要件	52

○別添資料

- 別添 1 プロセス一覧
- 別添 2 機能情報関連図(DFD)
- 別添 3 業務フロー
- 別添 4 業務記述書
- 別添 5 機能一覧
- 別添 6 画面一覧(例)
- 別添 7 帳票一覧(例)
- 別添 8 データボリューム一覧表
- 別添 9 権限マトリクス(例)

1. 用語の定義

「子どもの健康と環境に関する全国調査(エコチル調査)」に係るデータ管理システム一式 要件定義書(以下、「本要件定義書」という。)および別添資料に記述する主な用語を表 1-1 に示す。なお、以下の定義は、本要件定義書および別添資料で用いるための定義であり、今後、用語の利用方法等に変更が行われる可能性がある。

表 1-1 用語の定義

用語	定義
運用管理用端末	本システムの運用管理を行う目的でコアセンター、及びデータセンター内に設置する端末。
運用担当者	ヘルプデスク業務を実施する運用・保守事業者。
運用・保守事業者	本システムに係るソフトウェア、ハードウェア、ネットワーク、データセンタの運用、及びソフトウェア、ネットワークの保守業務を受注した事業者。
解析	コンピューターを用いて行う統計処理のこと。
環境試料	参加者の住環境において、曝露するあるいは曝露する危険性のあるすべての化学物質。曝露源としては、大気、室内空気、建築物、飲料水と生活水、食事、流域水、土壌、玩具、家具など我々が接するほとんどすべてのものに及ぶ。
完全同意撤回	参加者が過去に遡ってエコチル調査への協力を撤回すること。撤回後、収集された全てのデータ、試料等が削除される。
協力医療機関	ユニットセンターが協力を呼びかけて参画する地域の医療機関。
協力中止	参加者がその時点からエコチル調査への協力を撤回すること。
業務用端末	データの出力、分析等の目的で利用される、またはデータの入力等の目的で利用されるコアセンター内に設置する端末。
検査会社	採取された試料について検査・分析を行う外部の機関。
コアセンター	独立行政法人国立環境研究所に設置される本調査全体のとりまとめを行う機関。本システムの運営、各試料の保存・分析、ユニットセンターの管理、支援、参加者からの問合せ対応を行う。
コールセンター	参加者への各種問合せ対応を行う、コアセンターに設置される機関。
個人情報	個人に関する情報であり、当該情報に含まれる情報(氏名、住所、生年月日、その他記述等)により特定の個人を識別することができる情報。
参加者	エコチル調査に登録され、継続的にデータ収集、あるいは試料採取に協力する妊産婦、夫、およびその子供(リクルート時は胎児)のこと。
システム管理者	本システム利用者の権限、認証履歴、データ操作の履歴等の管理を行うコアセンター内の担当者。
システム利用者	ユニットセンター、及びコアセンターにて本システムを利用する者。
質問票調査	10 万人を対象に全国統一で実施する質問票を用いた調査。協力医療機関内で記入する場合と、参加者が自宅で記入したものを返送してもらう場合を想定している。
詳細調査	10 万人の中から抽出された一部の参加者を対象に実施される調査。
試料	エコチル調査で収集される生体試料および環境試料。
試料採取用キット	試料の採取に利用される検査用のキット。
生体試料	血液、尿、爪、毛髪、唾液、頬粘膜、臍帯、臍帯血、胎盤、胎脂、胎便、母乳などで分析・保存を目的として生体から採取されたもの。
精度管理	本調査では、試料採取準備時から試料分析時までの汚染の有無を確認するトラベルブランク等を想定している。
設計・開発事業者	本システムの設計・開発業務を受注した事業者。
長期保存施設	生体試料、環境試料等を長期間保存するための施設。
データセンター	エコチル調査で収集されたデータを蓄積・管理する施設。
同意	調査対象地区の妊産婦が、エコチル調査への参加に同意すること。

用語	定義
ニュースレター	調査状況、データ解析結果等の公表を目的として、参加者に対し定期的を送付される文書。
ブランク試料	試料採取から分析開始までの試料の汚染具合、分析機器の分析精度を確認するために精度管理で使用する試料。
ヘルプデスク	本システム利用者への問い合わせ対応やシステムの監視、障害対応受付等、運用・保守事業者が実施する業務。コアセンター内に設置する想定である。
ポータルサイト	調査関係者間で情報の共有、発信、管理をする機能、及び参加者が、個人情報、その他調査関連情報について確認、各種申請をする機能を持つウェブサイト。
メディカルサポートセンター	アウトカムの測定に関する手順の作成支援、調査に関わる医療関係者への指導及び支援を行う機関。
ユーザ	⇒「システム利用者」を参照。
ユニットセンター	地域において本調査のとりまとめを行う機関。全国 15 箇所程度を想定。
リクルート	研究参加者を探すこと、声かけ、同意取得、登録するまでの一連の作業。
連結可能匿名化	必要な場合に個人を識別できるよう、個人を識別することができる情報の全部又は一部と、符号又は番号の対応表を作成する方法による匿名化。
連結不可能匿名化	個人を識別ができないよう、個人を識別することができる情報の全部又は一部と、符号又は番号の対応表を作成しない方法による匿名化。
ID	(詳細決定後、記載。)
OCR	手書き文字や印字された文字を光学的に読み取り、予め記憶された認識パターンとの照合により文字を特定し、文字データを入力する装置。
OCR 帳票	OCR で読み取るための入力帳票。

2. スケジュール要件定義

2.1. 調達計画

本システムに係る調達は、以下の通りとする。

調達番号	調達件名
業務A	平成22年度「子どもの健康と環境に関する全国調査(エコチル調査)」に係るデータ管理システムの構築に関する調達支援およびプロジェクト管理業務
業務B	平成22年度「子どもの健康と環境に関する全国調査(エコチル調査)」に係るデータ管理システムの設計・開発等業務
業務C	平成22年度「子どもの健康と環境に関する全国調査(エコチル調査)」に係るデータ管理システムの賃貸借業務
業務D	平成22年度「子どもの健康と環境に関する全国調査(エコチル調査)」に係るデータ管理システムに関するネットワーク構築および運用・保守業務

2.2. 概要

「子どもの健康と環境に関する全国調査(エコチル調査)」に係るデータ管理システム一式(以下、「本業務」という。)の全体スケジュール概要を図 2-1 に示す。

- 1) 本システムの運用開始は平成 23 年 1 月を目途とする。



図 2-1 スケジュール概要

3. 業務・機能要件定義

3.1. システム化要件

本システムのシステム化要件については、本仕様書別添資料 1.「プロセス一覧」、別添資料 2.「機能情報関連図(DFD)」、別添資料 3.「業務フロー」、別添資料 4.「業務記述書」、別添資料 5.「機能一覧」を参照のこと。

なお、当該資料は本要件定義書作成時点での想定であるため、基本設計時に別添資料 1～9 の検討事項の検討を行い、必要に応じて追加・修正を実施し、最終化すること。

3.2. システムの利用者

本システム利用者について表 3-1 に示す。なお、下表は本要件定義書作成時点での想定であるため、基本設計時において変更が生じる可能性がある。

表 3-1. システムの利用者

拠点	拠点数・世帯数	1 拠点及び1世帯あたりの想定利用者数(人)	想定利用者数(人)
コアセンター	1	30～40	30～40
メディカルサポートセンター	1	10～20	10～20
各ユニットセンター	15	20～30	300～450
協力医療機関	300	5～10	1,500～3,000
各研究者	200	1～5	200～1,000
各家庭	100,000	3 程度	300,000

3.3. 汎用パッケージソフトウェアの利用要件

パッケージソフトウェアの使用は可能であるが、本システムで使用するパッケージソフトウェア(ライブラリを含む)は、以下の条件を満たしていること。

- 1) 本システムで使用するパッケージソフトウェアは、一般に販売された実績を有し、本調達用の専用製品では無いこと。
- 2) 本システムで使用するパッケージソフトウェアの使用ライセンスは、販売実績を有する複数事業者(開発メーカを含む事も可)から購入可能であること。なお、上記複数事業者は本システムで使用するパッケージソフトウェアを使用したシステムの構築実績を有し、かつ構築業務を受託可能であること。
- 3) 本システムで使用するパッケージソフトウェアの保守ライセンスは、複数事業者(開発メーカを含む事も可)から購入可能であること。なお、上記複数事業者は、保守業務を受託可能であること。

なお、本調達でカスタマイズされたソフトウェアは、全て調達仕様書の「6.1 著作権等の取扱い」の記載に従うこと。

3.4. 情報信頼性コントロール要件

以下のような情報信頼性コントロール方法を適切に整備し、システム機能に対する情報の信頼性を確保すること。特に、本システムでは手作業でデータを入力する場合も想定されるため、入力チェック、フォーマットチェック、合理性チェック等によりデータの正確性を担保すること。

- 1) データの網羅性コントロール方法
必要とされる全てのデータが重複することなく処理され、保管されるかを判断する。
- 2) データの正確性コントロール方法
データが正確に入力され、処理後データが正しく書き込まれるかを判断する。
- 3) データの正当性コントロール方法
データ保管時に、承認された情報のみが適切なテーブルに保管されるかを判断する。

4) データの継続性コントロール方法

適切なテーブルに正しいデータが継続的に保管されているかを判断する。

4. システム方式要件定義

4.1. システム全体構成要件

4.1.1. システム化方式

エコチル調査に係る業務の定義、システムの在り方について検討を行い、以下の方針を考慮したシステムを構築する。

1) エコチル調査の円滑な実施

- (1) システムの設計・開発からテストまでを短期間で実施する必要があるため、効率的かつ効果的に設計・開発を行うこと。
- (2) ネットワークの回線数、サーバ性能、ディスク容量等は最小構成とし、将来的な業務量の伸び率に応じてネットワークの回線数、サーバ性能及びディスク容量等を拡張できるようなネットワーク構成、ハードウェア構成とすること。
- (3) ユーザインタフェース設計等において、利用者の要望を整理し、利便性に優れたシステムを構築すること。

2) 適正な情報管理の実施

- (1) システムアーキテクチャの柔軟な変更を可能にするため、特定の事業者や技術等に依存しないシステム構成とすること。
- (2) システムの信頼性、可用性、機密性、完全性、拡張性を十分に勘案した上でシステムを構築すること。

4.1.2. システム全体構成

本システムの全体構成イメージ及び概要を図 4-1、表 4-1 に示す。

全体イメージ

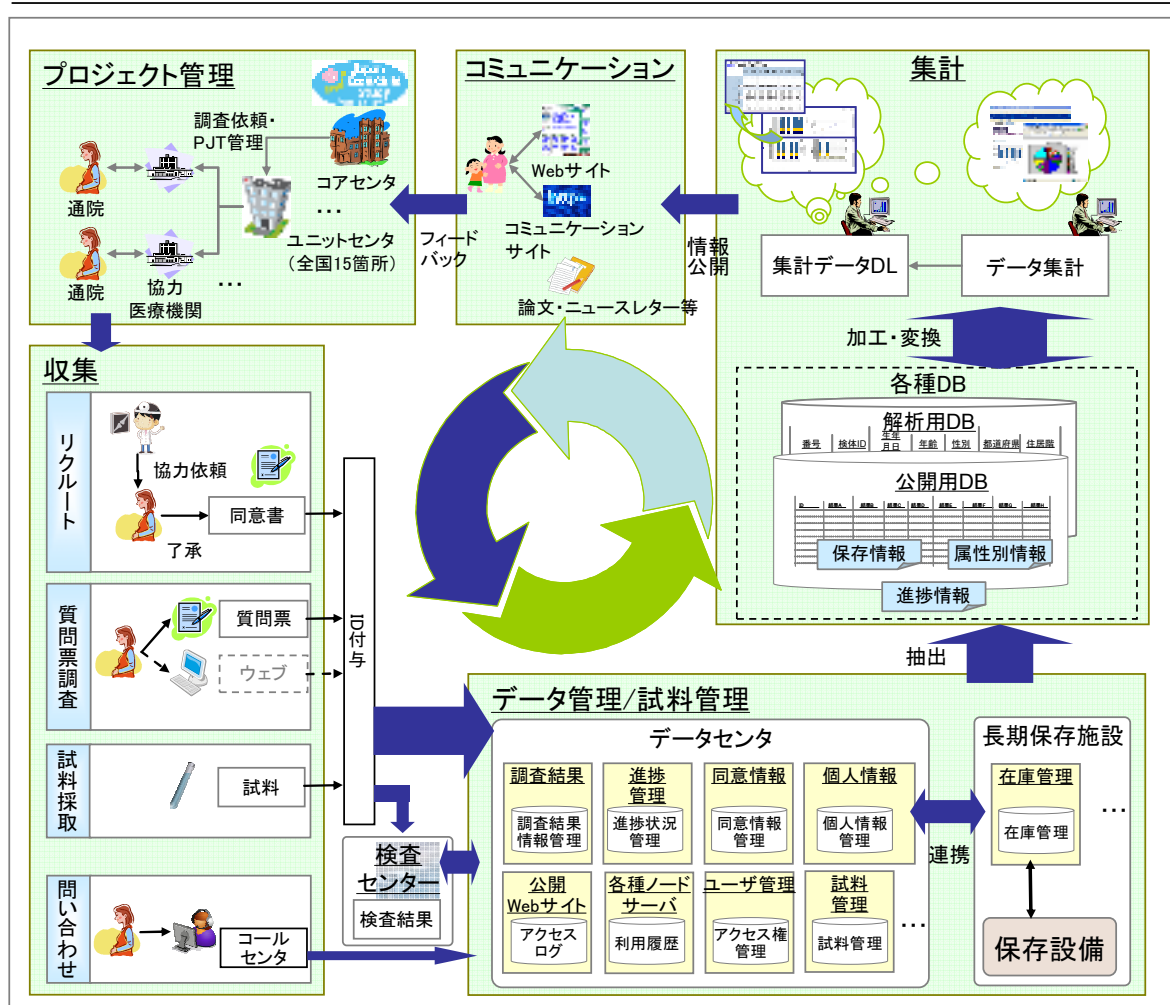


図 4-1 本システムの全体構成イメージ

表 4-1 本システムの全体構成概要

機能	内容
収集	参加者に対してエコチル調査の説明・協力依頼を行って同意を得た場合、参加者に対する各種調査を実施し、質問票、診察記録票等によるデータ収集、採取により試料の収集を行う。
データ管理	収集された各データ(個人情報、診察記録票情報、調査結果情報、及びその他データ)を管理する。データは電子化されデータセンター内で保存される。
試料管理	収集された試料を保管する。試料は長期保存施設等に保管される。
集計	収集されたデータの集計、及び外部の集計ツールを用いたデータ解析を実施し、レポートを作成する。
コミュニケーション	Web サイト及びニュースレター等により、参加者に対し分析結果等の情報公開を行う。
プロジェクト管理	エコチル調査全体の進捗管理、参加者の管理等を行う。

4.2. 性能要件

「3.2.システムの利用者」において示されている利用者数を想定し、業務遂行に際して支障のないレスポンスを確保すること。また、各業務処理のピークにおいてもレスポンスやスループットの極端な低下を招かないように、十分な処理性能を確保するための方法について検討を行うこと。

4.3. 信頼性要件

4.3.1. 信頼性に関する指標、目標値

システムの信頼性に関する目標値は、表 4-2 の通りとする。なお、下表は本要件定義書作成時点での想定であるため、基本設計時に変更される可能性がある。

表 4-2 信頼性に関する指標、目標値

項目		内容	備考
稼働率		99.0%以上を目標とする。	定期保守による計画停止時間はサービス時間から除く。
目標復旧水準	目標復旧時間	業務に支障のない時間内とする。	
	目標復旧地点	障害直前の完了トランザクションまでとする。	日次バックアップを利用したりカバリを想定
	目標復旧レベル	復旧後、全ての業務が遂行可能となっている状態であることとする。	

4.3.2. 可用性

システムの可用性については、以下のような基本要件や観点を考慮して検討を行うこと。また、目標稼働率、目標復旧時間を満たす障害設計、可用性の検討を行うこと。

- 1) システムを構成するハードウェア、ソフトウェア等は、製品としての動作が十分に保証・確認されたものを用い、システム全体が安定して動作すること。
- 2) 障害の局所化を図るため、クラスタリング等の複数台によるサーバ機器の冗長構成、ハードディスク装置の RAID 構成、ネットワーク機器の冗長構成等を採用可能なこと。
- 3) 停電時、UPS(無停電電源装置)の利用により、業務が復旧するまでの十分な期間、システム稼働を維持できること。

4.3.3. 機密性

本システムは、参加者からの個人情報を取り扱うため、機密性の高いシステムとなるよう考慮すること。

1) ネットワーク利用による脆弱性回避

ネットワークを介してデータ連携を行うため、情報漏洩の危険性に対し十分な対策を施したネットワークを構築し、機密性を確保すること。

2) データアクセス制限

データアクセス可能なシステム利用者を適切に管理し、許可されたシステム利用者だけが情報にアクセ

スすることができるよう機密性を確保すること。

4.3.4. 完全性

本システムでは参加者からの個人情報を取り扱うため、以下の要件を満たした完全性の高いシステムとなるよう考慮すること。

1) 誤操作によるデータ消去への対応

誤操作を行った場合にも、安易にデータが消去されてしまうことがないよう、必要な措置を講ずること。

2) データの二重化

情報の保全性を確保するため、情報の二重化および日次バックアップの取得を実施するシステム設計とすること。

3) ログの出力

システム利用者におけるデータの登録、変更、削除等の操作について履歴の管理を行えるようにし、ログのレベル設定を可能にすること。また、システムの運用中に何らかの障害・トラブル等が発生した際に、その原因が追求可能となるよう必要なログの蓄積、解析、出力を可能にすること。

4.3.5. 拡張性

本システムが対象とするエコチル調査は長期に渡るため、調査業務の変更等に伴い、調査項目の追加、入力装置の変更、新規機能の追加等のシステム要件が変更される可能性がある。従って、システム機能のモジュール化によるシステムの拡張性・再構築が可能であること。本要件定義書作成時点において、将来導入を検討されている要件は以下の通り。

1) 画像データの保存

2) 録画映像の保存

4.3.6. システムの中立性

本システムの中立性要件を以下に示す。

1) ハードウェア、ソフトウェアの中立性

特定の製品や技術に依存することなく、標準的な技術で信頼性の高いハードウェア、ソフトウェアを選定すること。

将来にわたって予想される仕様変更、システム更改、増設、システム移行時に、特定の事業者の製品、技術に依存することがないようなシステム設計・開発を行うこと。

2) 設計技法の中立性

本業務における設計にあたっては、特定の事業者の設計技法に偏ることのない標準的な設計技法を用いること。

3) ドキュメントの中立性

本業務で使用するドキュメント類が第三者にもわかりやすく作成されていること。

4.3.7. 復旧性

システムの復旧性については、以下の要件や「15. 運用・保守要件定義」を考慮して検討を行うこと。また、目標稼働率、目標復旧時間を満たす障害対応策、可用性の検討を行うこと。

- 1) 障害対策として、障害の影響を受けたデータは、障害直前のトランザクション完了の状態に戻すことを可能とすること。なお、バックアップについては「15.3 データ管理要件」を参照のこと。
- 2) 本システムが連携する他システムの停止時において、当該他システムと関係しない機能は、サービスが継続されること。

5. 情報・データ要件定義

本システムでは、表 5-1 に掲げるデータの管理を想定している。主要なデータの流れは、別添資料 2.「機能情報関連図 (DFD)」を参照のこと。なお、これらは本要件定義書作成時点での想定であるため、基本設計時に再整理した上で確定すること。

表 5-1 本システムの情報・データ概要*

No	情報・データ名	情報・データ概要
1	同意情報	参加者のエコチル調査への同意状況を管理する。
2	個人情報	参加者の個人情報を管理する。
3	調査結果情報	質問票調査および詳細調査にて収集された情報を管理する。
4	診察記録情報	カルテに記入された参加者の診察結果を管理する。
5	検査結果情報	検査会社にて実施された試料の検査結果を管理する。
6	解析結果情報	調査結果情報、診察記録情報、検査結果情報の解析結果を管理する。
7	試料管理情報	コアセンター内長期保存施設にて保管される生体試料、および環境試料の入出庫状況、ステータス情報を管理する。
8	在庫管理情報	ユニットセンター内にストックされている試料採取用キットの在庫状況を管理する。
9	進捗管理情報	エコチル調査全体の進行状況、各参加者の調査のステータス情報、参加者への謝礼支払い状況を管理する。
10	アクセス権管理	本システム利用者のアクセス権限に係る情報を管理する
11	ID管理情報	(詳細決定後、記載する)
12	文書管理情報	エコチル調査業務で使用される全ての文書を電子化し管理する。

*表 5-1 には記載されていないが、調査段階において、画像・動画データの管理を行う想定であるため、基本設計時に要件を確定させること。

5.1. データボリューム一覧表

各データのデータボリュームに関する要件は、本要件定義書別添資料 8.「データボリューム一覧」を参照のこと。

データサイズは、リクルート初期の調査票のデータサイズを基準に 1 日のデータ処理量の最大値を概算

で想定した数値を使用する。

ハードウェア性能(サーバ性能、ディスクサイズ)の見積もりに関しては、業務量の概算見積をベースとして見積もることとする。

なお、当該別添資料は、本システムで使用される予定の画像・動画情報等について算出根拠に含まれていないため、基本設計時に再整理した上で確定すること。

6. ユーザーインタフェース要件定義

6.1. 画面一覧

画面機能については、本要件定義書別添資料 6.「画面一覧(例)」を参照の上、要件を満たすこと。なお、当該別添資料は本要件定義書作成時点での想定であるため、画面機能、画面名は基本設計時に再度検討した上で確定すること。画面名から機能や処理内容、画面遷移が容易に想像できるよう視認性・操作性を考慮すること。

6.2. 帳票一覧

帳票については、本要件定義書別添資料 7.「帳票一覧(例)」を参照の上、要件を満たすこと。なお、当該別添資料は本要件定義書作成時点での想定であるため、帳票の内容、および帳票名は基本設計時に検討した上で確定すること。システム利用者にとって利便性のよい帳票となるよう工夫すること。

6.3. 画面設計規約

本システムの画面表示の内容および画面遷移について、デザイン、操作性など、利便性の観点から設計時に考慮すべき基本的な要件を以下に示す。

6.3.1. 表示内容

画面の表示項目、レイアウト等を設計する際に考慮すべき基本となる要件を以下に示す。

- 1) システム利用者が直感的に画面操作できるよう、視認性・操作性に関して工夫すること。
- 2) 表示する情報は簡潔にすること。例えば、関連する情報は、一画面内で参照できるような画面構成とすること。
- 3) アイコンなどは判り易くなるよう工夫すること。ただし、画像で示すことが難しい内容であれば文字で表現すること。
- 4) データ登録、更新および削除を行う操作については必ず確認画面を表示する等、誤操作が生じないように考慮すること。
- 5) 入力項目に対する数値チェック、暦日チェック等の基本的なバリデーションチェックは画面上にて行うこと。
- 6) エラーおよび警告のメッセージは、システム利用者に誤解のないようシステム全体で統一し、問題点と解決方法がわかるように配慮すること。
- 7) 入力画面と出力される帳票については、各画面・帳票名称や項目名称をシステム内で統一すること。
- 8) 処理に時間のかかる操作は、システム利用者が端末の処理状況を把握できる表示とすること。(例えば、「処理経過の表示」ダイアログや「処理中」メッセージ等。)

6.3.2. 画面遷移

画面遷移を検討する際に考慮すべき基本となる要件を示す。

- 1) システム利用者が次の画面遷移を容易に想像できる遷移となるよう工夫すること。
- 2) システム利用者が処理すべき内容を把握できる遷移となるよう工夫すること。
- 3) 誤操作の防止を含め、入力内容確認等のメッセージ画面を効果的に適用すること。
- 4) システム利用者の職務権限を反映したパーソナライズ化された画面表示と、それによる画面遷移を提供すること。

6.4. 帳票設計規約

本システムから出力される帳票について、設計時に考慮すべき基本要件を以下に示す。

- 1) システム利用者にとって利便性のよい帳票となるよう工夫すること。
- 2) 帳票の行数は、最適な行数を帳票ごとに定めることとする。
- 3) 帳票の文字は、タイトル文字・内容文字等に区別して、それぞれフォントおよびサイズを規定することとする。
- 4) 帳票出力を行う際には、事前に画面上でプレビュー表示ができ、確認後出力できるようにすること。
- 5) 帳票名称については、利用者の誤解が生じないようにシステム内で統一すること。
- 6) 利用者が円滑に帳票出力できるよう、一連の画面操作の流れの中で帳票出力ができるよう工夫すること。

7. 外部インターフェース要件定義

7.1. 連携対象システム一覧

本システムにおいては、システム間連携は想定していない。

8. ネットワーク要件定義

8.1. システム全体構成イメージ

図 8-1 に、本システムの構成概要を示す。なお、下図は本要件定義書作成時点での想定であるため、基本設計時に変更される可能性がある。

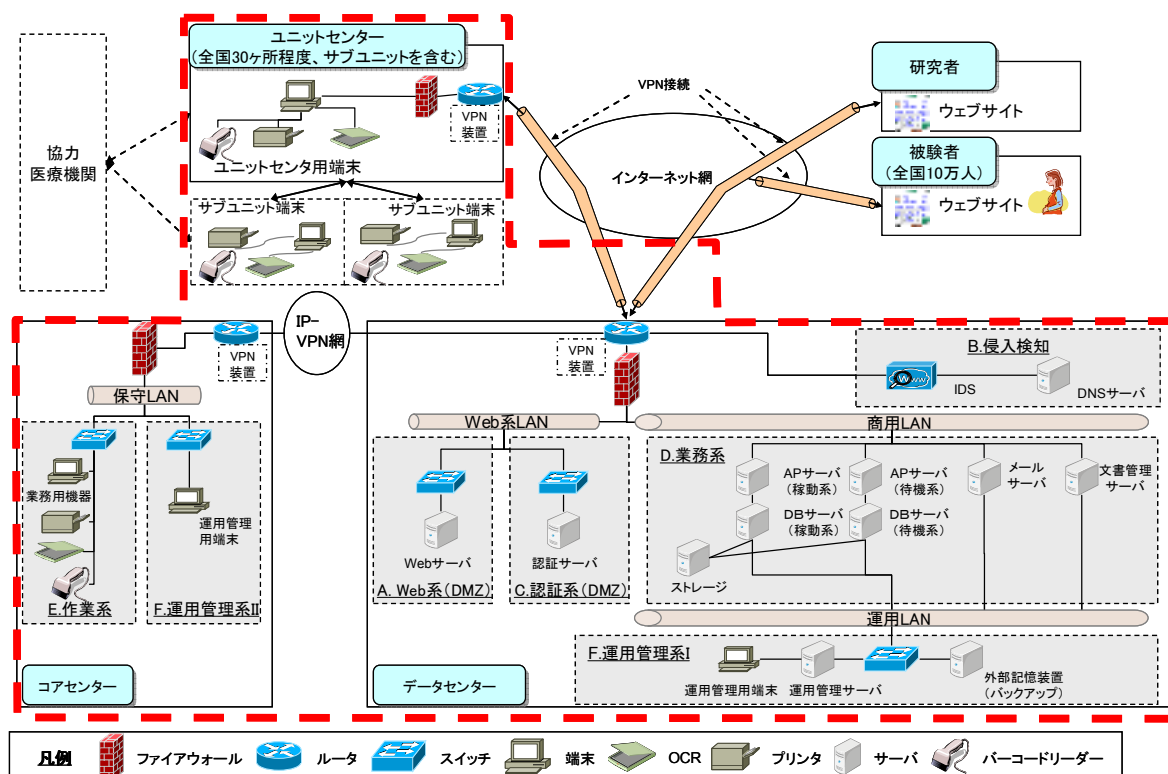


図 8-1 システム概要図

8.2. 回線と接続方式

8.2.1. 調達予定の回線

- 1) データセンターとコアセンター間の接続のため、通信キャリアの提供する IP-VPN 網の調達。
- 2) データセンターからインターネット網へ接続するため、通信キャリアが提供するインターネット接続サービスの調達。

8.2.2. 接続方式

- 1) 参加者、研究者、ユニットセンターとデータセンター間をVPN・SSLやその他の接続方式を用いて接続する。

8.3. LAN 要件

本要件定義書における LAN とは、コアセンター内・データセンター内に構築される LAN を指すものとする。なお、詳細は図 8-1 システム概要図を参照のこと。

8.3.1. 方針

LAN の構築を行うにあたり、以下の方針を適用する。

- 1) プロトコルは、TCP/IP を使用すること。
- 2) IP アドレスは、IPv4 を使用すること。
- 3) 基幹となるネットワーク機器は、冗長化構成とすること。
- 4) 省スペース、省電力設計の機器を使用すること。
- 5) 実績のある機器を用い、安定した稼動を実現すること。
- 6) 運用管理用端末(コアセンター)と、業務用端末(コアセンター)は、データセンターに配置される本システムと同一ネットワークに配置したい為、VPN 接続とし、100Mbps～1Gbps の帯域で、セキュア化された回線を確保すること。
- 7) ネットワーク機器は、国際標準及び業界標準に準拠しており、特定のハードウェア又はベンダーの規格に依存しないこと。ネットワーク機器において、適切なセキュリティ対策が講じられていること。

8.3.2. 効率性要件

LAN の構築にあたり、効率性の要件を以下に示す。

- 1) 伝送速度

LAN の伝送速度においては、拡張性および十分な伝送速度を考慮すること。

- 2) ポート数

LAN のポート数においては、拡張性および十分な数を考慮すること。

8.3.3. LAN 信頼性要件

LAN の構築にあたり、信頼性の要件を以下に示す。

- 1) 機器の信頼性

ルータ、スイッチ等のネットワーク機器においては、実績のある機器を用いること。

- 2) 冗長化の考慮

本システムの基幹となる箇所においては、信頼性を高めるため冗長化構成とし、障害によるシステムダウンが生じないように考慮すること。但し、業務処理に影響しない機器は対象外とする。

8.3.4. LAN 構築要件

LAN の構築にあたり、構築要件を以下に示す。なお、以下の要件は本要件定義書作成時点の想定であるため、仕組みや機能の詳細は、基本設計時において再整理した上で確定すること。

- 1) 本システム LAN 構成については、図 8-1 システム論理構成図を参照のこと。
- 2) 本システムのネットワーク基盤について以下の機能を提供すること。

- (1) スイッチ機能

スイッチとは、本システムのネットワークにおいて、回線およびパケットのスイッチングに使用する機器である。

- ① コールドスタンバイ構成とし、一方に障害が発生して停止しても、迅速な復旧が可能な構成とすること。

- (2) ルータ機能

ルータとは、本システムに各機関のネットワークを接続するために使用する機器である。

- ① コールドスタンバイ構成とし、一方に障害が発生して停止しても、迅速な復旧が可能な構成とすること。

- (3) 外部ネットワーク接続

- ① 各ネットワーク機器におけるポート数等は今回調達する全機器を接続可能な数量とすること。
当該項目は、基本設計時に決定することとする。

- (4) IPv6 対応

IPv6 対応可能な機器を選定すること。

- 3) データセンター内 LAN、コアセンター内 LAN 及びその間の接続は、Ethernet 方式とし、通信プロトコルは原則 TCP/IP とすること。
- 4) SNMP 等のネットワーク監視プロトコルに対応し、システム管理に必要な情報を収集可能となっていること。

8.4. その他ネットワーク要件

本要件定義書におけるその他ネットワークとは、コアセンター・データセンターの外部のネットワークを指すものとし、各ユニットセンター、研究者、及び参加者とコアセンターを接続するものとする。なお、詳細は図 8-1 システム概要図を参照のこと。尚、参加者が利用する端末およびネットワーク回線については、制御できないためその他ネットワーク要件の定義対象外とする。

8.4.1. 方針

ネットワーク構築を行うにあたり、以下の方針を適用する。

- 1) その他ネットワークにおいては、帯域予約(QoS:Quality of Service)機能を採用し、本システムに

対する伝送帯域を確保すること。

- 2) ユニットセンターとコアセンターを接続する回線のセキュリティレベルに関して、一般的な銀行と同程度のセキュリティレベルを確保すること。通信の暗号化(SSL 通信)を行うこととし、接続回線のセキュア化は必須とはしない。
- 3) 各拠点間での通信は、IP アドレスを指定して行うこととする。
- 4) 必要なセキュリティレベルは、ネットワーク提供ベンダーと協議し、適切な技術を用いること。
- 5) 機器の採用においては、障害発生時の対処方法を十分に考慮すること。
- 6) 省スペース、省電力設計の機器を提供すること。
- 7) 実績のある機器を用い、安定した稼動を実現すること。

8.4.2. 効率性要件

その他ネットワーク構築を行うにあたり、効率性の要件を以下に示す。

1) 帯域の見積もり

現時点では 100Mbps を想定しているが、ネットワークの帯域の見積りは、基本設計時に再度実施し、確定すること。

2) 機器の性能

その他ネットワーク構築に用いる機器は、帯域の見積もりを考慮した機器を提供すること。

8.4.3. 信頼性要件

その他ネットワーク構築にあたり、信頼性の要件を以下に示す。

1) 機器の信頼性

ルータ、スイッチ等のネットワーク機器においては、実績のある機器を用いること。

2) 冗長化の考慮

一般回線を使用することを想定しているため、考慮しない。

8.4.4. 構築要件

その他ネットワーク構築にあたり、構築要件を以下に示す。なお、以下の要件は本要件定義書作成時点の想定であるため、仕組みや機能の詳細は、基本設計時に確定すること。

1) 接続機能

(1) IPv6 対応

IPv6 対応可能な機器を選定すること。

※「IPv6」に関する基本遵守事項

(2) IPv6 移行がもたらす脆弱性対策

- ① 情報システムセキュリティ責任者は、情報システムに IPv6 技術を利用する通信(IPv6 通信という。)の機能を導入する場合には、IPv6 移行機構が他の情報システムに情報セキュリティ上

- の脅威を及ぼすことを防止するため、必要な措置を講ずること。
- ② 意図しない IPv6 通信の抑制と監視。
- ③ 情報システムセキュリティ責任者は、IPv6 通信を想定していない通信回線に接続される本システムおよびネットワーク機器に対して、IPv6 通信を抑止するための措置を講ずること。

9. ハードウェア要件定義

9.1. 共通要件

ハードウェアの共通要件を以下に示す。なお、ハードウェア要件については本要件定義書作成時点の想定であり、ハードウェアの仕様等については、基本設計時に詳細を決定すること。

- 1) 「4 システム方式要件定義」に示されている各種要件に則すること。
- 2) サーバ等の物理的な機器構成については、信頼性、拡張性、性能など各種要件を考慮し、機能の統合、分離などを行うことにより適切な数量を提供すること。また仮想化技術を使用した機能の提供を可とする。この場合には仮想化技術について詳述すること。
- 3) システムアーキテクチャとして、柔軟で拡張性の高いシステム設計が行えるようにすること。
- 4) ハードウェア要件に特に記載されていない機器についても、「3 業務機能要件定義」などに記載された要件を実現するために必要な機器については、提案の上、提供すること。
- 5) 新システムにおいて提供する各機器について、環境への配慮から可能な限り省電力対応機器であること。
- 6) 端末、プリンタ、ルータ、スイッチ等執務室内に設置する機器については、静音性(騒音対策)、省エネ性(発熱量対策)を最大限考慮すること。
- 7) ラックに関しては、新規調達機器が収納可能なラックを用意すること。

9.2. サーバ

9.2.1. サーバ機能一覧

本システムで使用されるサーバは、表 9-1の機能を持つ。基本設計時に設計開発事業者がサーバの物理構成を再検討し、決定すること。

表 9-1 サーバ機能一覧

サーバ名	主な機能概要
Web サーバ	・コアセンター、ユニットセンター、研究者、参加者にポータルサイト機能を提供する。 ・調査実施機関に同意書、各種診察記録票、各種調査票、各種検査結果の登録・検索機能等を提供する。
アプリケーションサーバ	・同意書、各種診察記録票、各種調査票、各種検査結果の登録・検索処理等の機能を提供する。

	・データを利用した集計機能を提供する。
DB サーバ	・同意書、各種診察記録票、各種調査票、各種検査結果のデータベースへの登録・検索処理等の機能を提供する。 ・ユニットセンターから登録された各種データをデータベースに格納・保存し、一元管理する。 ・本システムの運用に必要な各種データや設定を保存・一元管理する。
文書管理サーバ	・各種調査で利用する文書を電子媒体の形で保管する。
メールサーバ	・コアセンターからユニットセンター、研究者、参加者への連絡、情報共有、案内等を送信するためのメール送信機能を提供する。
運用管理サーバ	・本システムの稼働状況の管理機能を提供する。
認証サーバ	・本システム利用者を認証するための機能を提供する。
DNS サーバ	・ネットワーク上のクライアントを認証する機能を提供する。

9.2.2. サーバ共通要件

新システムを構成する主要サーバについては、下記要件に加え、「4 システム方式要件定義」および「9 ソフトウェア要件定義」の各種要件に則し、最適な構成を提案すること。

1) オペレーティングシステム要件

- (1) マルチプロセッサに対応すること。
- (2) マルチユーザーに対応し、システム利用者ごとにシステムリソースへのアクセス権の設定が可能であること。
- (3) 特に指定のない限り、最新の修正モジュールを適用すること。

2) CPU 要件

- (1) SMP (Symmetric Multi Processor) に対応すること。
- (2) CPU の故障時に自動的に当該プロセッサを切り離す機能を有すること。

3) メモリ要件

- (1) 業務が正常に稼働するのに十分な容量を搭載すること

4) OS 要件

- (1) 汎用性が高いこと。
- (2) 実装する各ソフトウェアの動作を保証すること。
- (3) 本システムにおいて動作を保証すること。
- (4) 操作制限等、セキュリティポリシーを設定できること。

9.2.3. Web サーバ

Web サーバは、Web ベースのインタフェースを提供する。本サーバは、アクセスが集中するサーバである

ため、アクセス数の増加等にもなった負荷の増加に対応可能となるよう、機器の拡張性が容易となる構成とすること。次に掲げる機能を有した Web サーバを搭載すること。

- 1) SSL 等による通信経路の暗号化が可能なこと。
- 2) 可能な限り、マルチプラットフォームで稼動すること。

9.2.4. アプリケーションサーバ

アプリケーションサーバは、業務に関するアプリケーションを提供する。本サーバは、アクセスと業務処理が集中するサーバであるため、クラスタリング構成を考慮するとともに、アクセス数の増加等にもなったサーバ負荷の増加に対応可能となるよう、機器の拡張が容易となる構成とすること。

9.2.5. DB サーバ

DB サーバは、業務上で発生した各種データをデータベースで管理する。本サーバは、本システムで扱うデータを集約しているため、クラスタリング機能と RAID 機能を利用し、信頼性を重視した構成とすること。データアクセスの処理能力によっては、業務全般に影響を及ぼす可能性があるため、可用性を十分に考慮すること。データの改ざん、情報漏えい、盗難に備えること。

データベース機能においては、大容量のデータを管理し、及び操作する利便性を考慮して、原則、RDBMS を推奨する。RDBMS については、以下の機能を有すること。ただし、XML データの管理及び操作に係る部分については、必ずしも RDBMS である必要はない。

- (1) スタンバイデータベースに対してトランザクション単位で変更を適用し、速やかに切り替え可能なスタンバイ機を構築可能なこと。
- (2) 行レベルでのアクセス制御機能を有すること。
- (3) データアクセスのキャッシュとして、複数のバッファプールを作成できること。また、複数種類のページサイズに対応可能であること。
- (4) 自動バックアップ及び自動メンテナンス機能を有すること。
- (5) 可能な限り、XML データと他 RDB のデータを単一の言語で操作可能であること。
- (6) 可能な限り、マルチプラットフォームで稼動すること。
- (7) インデックスデータを利用した高速な検索が可能であること。

9.2.6. 文書管理サーバ

文書管理サーバは、紙媒体の文書において、電子文書として管理・保存を行うための機能を提供する。本サーバは、クラスタリング機能と RAID 機能を利用し、信頼性を重視した構成とすること。データアクセス処理能力に関しては、業務に影響を及ぼしかねないため、可用性を十分に考慮すること。データの改ざん、情報漏えい、盗難に備えること。

9.2.7. メールサーバ

システム利用者間でのメール送信を行うためのメールサーバとしての機能を提供する。詳細については基本設計時に確定すること。

9.2.8. 運用管理サーバ

運用管理サーバは、本システムの運用管理において必要になる次の機能を有すること。

1) 機器及びイベント監視機能

- (1) システム全体を一元的に監視できるように統合コンソール機能を提供すること。
- (2) 監視対象のサーバはマルチプラットフォームをサポートしていること。
- (3) ネットワーク上の各機器の稼動状況を監視し、障害発生時には管理コンソール上に通知及び表示できること。
- (4) サーバ上のログファイルを定期的に参照し、システム管理者に通知すべき情報を抽出し、イベントとして管理コンソール上に通知できること。
- (5) サーバ上のプロセスの稼動状況を監視し、プロセスダウン障害発生時には管理コンソールに通知されること。
- (6) サーバ上の性能情報(CPU 使用率、ディスク使用率、メモリ使用率など)を監視し、設定した閾値を越えた場合、管理コンソール上に通知・確認できること。また、サーバの性能情報を収集し、グラフ表示で確認できること。
- (7) 障害イベントの通知により、規定の対応処理を自動的に実行する機能を有すること。
- (8) イベント情報はデータベースに格納し、一定期間保存が可能であること。また、データベースに蓄積されたイベント情報はコマンド等の手段で必要に応じて取り出すことができること。
- (9) 各運用担当者の役割に応じて、統合コンソールへ表示・通知されるイベントが限定されていること。

2) セキュリティパッチ配布機能

- (1) 手動配布及びあらかじめ指定したスケジュールに従った自動配布の双方に対応すること。
- (2) 配布時に使用するネットワーク帯域を制限可能なこと。
- (3) ネットワークの負荷を考慮し、差分配布・分割配布が行えること。
- (4) 配布の一時中断及び再開が可能であること。また、配布対象のファイル群の送信中に通信エラーが発生した場合、送信途中のファイルから送信を再開すること。
- (5) 配布の前後に、指定した処理を配布先あるいは配布元で実行することが可能であること。
- (6) 配布対象のサーバはマルチプラットフォームをサポートしていること。

3) バックアップ管理機能

- (1) 管理対象のサーバは、マルチプラットフォームをサポートしていること。
- (2) 業務 LAN へのデータ転送負荷軽減のために SAN を利用したバックアップが行えること(LAN-Free Backup)。
- (3) 同パス同名ファイルのバックアップを複数世代保管が行えること。
- (4) 保管ポリシーから外れた不要バックアップデータの自動削除が行えること。
- (5) 保管領域の有効利用のため、データ圧縮機能をサポートしていること。
- (6) 管理コンソールの起動時にユーザーID による認証が行われ、運用管理者以外のシステム利用者に操作を許可しないこと。また、運用管理者の役割に応じて、操作・参照の範囲が限定されており、役割以外の操作・参照が行えないように機能が制限されること。その設定は、上級運用管理者といった上位の役割のシステム利用者でのみ行え、容易に変更されないようになっていること。
- (7) バックアップ後のデータが、他者に容易に覗き見ることができないような構造で保管されること(独自のフォーマットによる書込みを行い、認証後以外は参照できない等)。
- (8) データの送受信において、データの暗号化機能をサポートしていること。
- (9) バックアップデータの管理情報は障害対策のため二重化できること。
- (10) ファイアウォールや NAT を使用したネットワークに対応できること。

4) ジョブ管理機能

- (1) 管理対象のサーバは、マルチプラットフォームをサポートしていること。
- (2) 異なる OS 上で稼動するジョブ同士を連携させる機能を有すること。また、スケジュール間の相互依存関係を設定できること。
- (3) ジョブネットの作成・設定、ジョブの制御・監視はサーバ側で行い、管理対象側はジョブを実行するエージェントを搭載すること。
- (4) また、ジョブ・スケジュールをあらかじめエージェントに転送することで、ノード障害・ネットワーク障害が発生しても確実にジョブを実行できること。
- (5) あらかじめ設定したルールに従って、ジョブスケジューリング管理を行えること。
- (6) スケジュールの基準として複数のカレンダーを作成できること。
- (7) ジョブの実行状況を統合コンソール上で確認できること。
- (8) セキュリティ機能及び監査機能を有すること。

9.2.9. 認証サーバ

次に掲げる機能を有したアクセス管理ソフトウェアを搭載すること。

- (1) 認証用ユーザーレジストリは、標準技術を採用した LDAP サーバであること。
- (2) Web アプリケーションに対する統合された認証とアクセス制御を提供すること。
- (3) システム利用者の追加、アクセスコントロール定義変更等の管理操作を実施するインタフェース

として、GUI 及び CLI を提供していること。

(4) SSL 等の暗号化機能を持ち、Web ブラウザ、Web サーバ及びアプリケーションサーバとの通信を暗号化できること。

(5) 可能な限り、マルチプラットフォームで稼動すること。

9.2.10. DNS サーバ

ネットワーク上のクライアントを認証するサーバとして動作すること。

9.3. ストレージ等

大容量のデータ蓄積、各種メディアの交換、およびデータのバックアップを行う機器とする。

9.3.1. ストレージ装置

業務上に生成される各種情報や画像等を集約し、データベースに格納する機能を提供する。本装置は、業務データを保持する機器で、RAID 構成により信頼性を重視した構成とする。また、大規模データの保存や操作をする上で十分な容量及び性能を有していること。

9.3.2. 外部交換装置

各種メディア（フロッピーディスク、CD）等記録媒体とのデータ交換機能を提供する。本装置は、大量のデータを一定時間内で行う機器で、可用性を重視し、十分な処理能力を持たせた構成とすること。

9.4. ネットワーク関連機器

ネットワーク関連機器は、各機器間のネットワーク接続を中継する機能を行う機器とする。

9.4.1. スイッチ

コアセンター内のネットワークを束ねた1階層目のスイッチ、1階層目に接続される2階層目のスイッチ等、コアセンター内、データセンター内の通信トラフィックを束ねる機能を提供する。本装置は、設置箇所においては、コールドスタンバイ構成とし、一方に障害が発生して停止をしても、迅速な復旧が可能な構成とすること。

9.4.2. ルータ

LAN 間及び LAN と外部ネットワーク間の通信を中継し、通信先に応じて最適経路の選定を行う機能を提供する。本装置は、設置箇所においては、コールドスタンバイ構成とし、一方に障害が発生して停止をしても、迅速な復旧が可能な構成とすること。

9.5. 各監視用機器、セキュリティ用機器

9.5.1. ファイアウォール装置

IP アドレスおよびポート番号を用い、ネットワークの接続相手を制限し、不正アクセスを防止する機能を提供する。本装置は、WAN の接続箇所、コントロールゾーン (DMZ; DeMilitarized Zone)、および内部ネットワーク接続箇所等に設置すること。機器の障害による本システムおよび業務に及ぼす影響を最小限に抑える必要があるため、機器の多重構成によって信頼性を重視した構成とすること。

9.5.2. IDS (侵入検知システム)

攻撃パケットや成りすまし等、外部からの攻撃を検出し、サービス拒否攻撃 (DDOS) や不正侵入を排除する機能を提供する。機器の障害による本システムおよび業務に及ぼす影響を最小限に抑える必要があるため、機器の多重構成によって信頼性を重視した構成とすること。

9.6. 業務用機器 (PC、プリンタ等)

業務用機器 (PC、プリンタ、OCR 等) は、業務システムへのアクセス、OCR 帳票の読み取り、および帳票の印刷等、本システムを利用するにあたり、必要な機能を提供する機器とすること。

機器の設置場所、設置台数に関しては、コアセンター、ユニットセンター、およびシステム運用・保守事業者それぞれの体制との関係もあるため、基本設計時以降、あるいはシステム運用・保守事業者の調達時に検討し、決定すること。

表 9-2 各拠点に設置予定の機器と台数(()内は検討中)

設置場所	拠点数	機器の種類	各拠点毎設置 予定台数
データセンター	1	運用管理用端末	1
コアセンター	1	運用管理用端末	1
		業務用端末	5
		(保守端末)	(1)
		プリンタ	1
		OCR	1
		バーコードリーダー	1
各ユニットセンター	15	業務用端末	5
		プリンタ	1
		(OCR)	(1)
		バーコードリーダー	1

9.6.1. 運用管理用端末(データセンター)

各サーバの管理およびメンテナンスを行うための機能を提供する。本装置は、業務を行う上で十分な仕様とすること。データの漏えいや盗難に備え、ワイヤーロック等を使用すること。

9.6.2. 運用管理用端末(コアセンター)

各サーバの管理およびメンテナンスを行うための機能を提供する。本装置は、業務を行う上で十分な仕様とすること。データの漏えいや盗難に備え、ワイヤーロック等を使用すること。

9.6.3. 業務用端末(コアセンター)

本システムを利用するための機能を提供する。本装置は、業務を行う上で十分な性能を有すること。データの漏えいや盗難に備え、ワイヤーロックを使用すること。

9.6.4. 保守端末(コアセンター)

本システムの運用に必要なアプリケーション、およびハードウェアの保守作業を実施するための機能を提供する。本装置は、業務を行う上で十分な性能を有すること。データの漏えいや盗難に備え、ワイヤーロックを使用すること。

9.6.5. ユニットセンター用端末

本システムを利用するための機能を提供する。本装置は、業務を行う上で十分な性能を有すること。データの漏えいや盗難に備え、ワイヤーロックを使用すること。

9.6.6. プリンタ

複写帳票印刷機能、大量印刷機能を提供する。本装置は、エコチル調査業務の円滑な処理に係わるための十分な性能を有すること。本装置の性能として、医療機関のラベル印刷に対応すること。

9.6.7. OCR

OCR 帳票の読み取り機能を提供する。本装置は、エコチル調査業務の円滑な処理に係わるための十分な性能を有すること。基本設計時に詳細を検討すること。

9.6.8. バーコードリーダー

バーコードに内在する情報を読み取る機能を提供する。本装置は、業務を行う上で十分な仕様とし、表 9-3 に示すバーコードの読み取りが可能であること。

本要件定義書作成段階では、バーコード、もしくは二次元バーコードどちらかの利用を想定している。本システムで利用するバーコードの種類、サイズ、読み取り内容については、基本設計時に検討し決定すること。

表 9-3 バーコード形式一覧

種類	対応規格
バーコード	Code39、NW-7、JAN、Code128、GS1-128(EAN-128)、Code93、GS1 DataBar(RSS)
2次元バーコード	QRコード、DataMatrix、PDF417、Maxi Code、Veri Code

9.7. ハードウェア拡張性要件

平成 23 年 1 月本システム稼動開始後、徐々に業務処理量が増加することが想定される。業務量が増加した際にも対応可能なように、ハードウェアを拡張できるような構成とすること。

- 1) 「4.3.5. 拡張性」に則していること。
- 2) 予備のプロセッサ及びメモリを搭載し、パフォーマンスを増強させる必要性が生じた際に、必要に応じてシステムを停止することなく、速やかにプロセッサを追加できる機能を有すること。
- 3) 上記に関連して、必要に応じて予備のプロセッサ及びメモリを速やかに起動及び停止できる機能を有すること。
- 4) 将来的なデータ量の増加に備え、ストレージの追加が容易にできる構成とすること。

10. ソフトウェア要件定義

ソフトウェア要件定義は、導入、バージョン管理、およびセキュリティの各要件を考慮した上でサーバ、端末に実装する内容を定義する。なお、本章に記載されている要件は本要件定義書作成段階の想定であるため、詳細な内容については、基本設計時に決定すること。

10.1. 共通要件

「4 システム方式要件定義」に示されている各種要件に則すること。また、以下のソフトウェア共通要件に則すること。本システムにおいて、ソフトウェア要件定義に特に記載されていないソフトウェアについても、「3 業務機能要件定義」に記載された機能を実現するために必要なソフトウェアについては、提案の上、別途提供すること。

1) ライセンス

- (1) 稼動期間全体にわたって、セキュリティホール等に対する情報およびプログラムの修正モジュールが継続的に提供されること。
- (2) ライセンスの規定に従って、必要分の数量を確保できること。

2) 保守要件

- (1) 5 年間のソフトウェア保守サポートが実施可能であること。
- (2) ソフトウェア保守要件については、「15.6 ソフトウェア保守要件」を参照すること。

10.2. ソフトウェア要件

10.2.1. サーバ共通ソフトウェア要件

1) 運用管理エージェント

サーバ機器、ネットワーク機器等の稼動状況等を監視する機能を提供する。

- (1) サーバの稼動状況の監視ができること。
- (2) サーバに実装するアプリケーションのプロセス監視ができること。

2) ウイルス監視エージェント

ウイルス検知、駆除機能を提供する。

- (1) ファイルへのアクセス、保存時にウイルス検知、駆除ができること。
- (2) 設定したスケジュールに基づきウイルスチェックができること。
- (3) ウイルス検知時において、駆除、削除、ファイル拡張子の変更、隔離等、複数の対処方法を選択できること。

3) バックアップエージェント

バックアップ・リストア機能を提供する。

- (1) ネットワークを経由し、バックアップ・リストアを行う。
- (2) 「15.運用・保守要件定義」を満たすこと。

10.2.2. Web 系(DMZ)サーバソフトウェア要件

1) Web サーバソフトウェア

WWW による通信機能を提供する。

10.2.3. 侵入検知サーバソフトウェア要件

1) 不正侵入管理

システムおよびネットワークへの不正侵入の検知、遮断、記録などを管理する機能を提供する。

- (1) 不正侵入検知時において、システム管理者への通知やログ記録を行うこと。
- (2) 不正侵入防御装置のログを収集および管理できること。

10.2.4. 認証サーバソフトウェア要件

1) 認証管理

本システムの利用者の端末に対し、認証許可を与える機能を提供する。

- (1) 認証が行われた各端末(ユニットセンター、システム管理者等)へ認証許可を与えること。

10.2.5. 運用管理サーバ要件

1) データベース管理

データベースの管理機能を提供する。

- (1) リレーショナルデータベース管理システム、または同等の機能を有すること。
- (2) ODBC (Open DataBase Connectivity)ドライバ、JDBC (Java DataBase Connectivity)ドライバ等を有すること。
- (3) 「15.運用・保守要件定義」を満たすこと。

2) システム監視

業務システム、サーバ、ネットワーク等、稼動状況を管理する機能を提供する。

- (1) サーバ、ネットワーク機器の稼動監視を行うこと。
- (2) アプリケーションのプロセス監視ができること。
- (3) サーバ上で稼動する各ソフトウェアおよびアプリケーションのログの監視を行うこと。
- (4) 不正侵入保護管理と連携し、ネットワーク監視を行うこと。
- (5) 監視対象のログの設定、および参照ができること。
- (6) 本システムにおけるキャパシティの監視ができること。

3) ジョブ定義

ジョブ管理に対し、各種ジョブの定義、および設定を行う機能を提供する。

- (1) ジョブ、およびスケジュールの定義、設定が出来ること。
- (2) ジョブの実行順番を設定できること。
- (3) ジョブの実行結果を保存、管理できること。

4) ジョブ管理

各種ジョブの実行制御、および管理機能を提供する。

- (1) ジョブ管理で定義された設定(スケジュール)に従い、自動的にジョブを実行すること。
- (2) ジョブの実行時に失敗した場合、関係者および関連機能へ通知すること。

5) ウイルス管理

(1) 集中管理

ウイルス検知・駆除ソフトウェアの集中管理機能を提供する。

- ① ウイルス対策ソフトウェアのベンダーが提供するサーバより、ウイルス検索エンジンの修正パッチ、およびパターンファイルの最新版をダウンロードし、サーバおよび各端末に実装しているウイルス対策ソフトウェアへ自動適用を行うこと。
- ② サーバおよび各端末のウイルス検索エンジンやパターンファイルの更新状況の管理を行うこと。
- ③ ウイルス検知情報を蓄積および管理し、被害や対応状況を確認できること。
- ④ ウイルス検知時において、通知を迅速に管理者および利用者に迅速に通知すること。

(2) ウイルス検知・駆除

ウイルス検知、および駆除機能を提供する。

- ① ファイルへのアクセス、保存時にウイルス検知、駆除ができること。
- ② 設定したスケジュールに基づきウイルスチェックができること。
- ③ ウイルス検知時において、駆除、削除、ファイル拡張子の変更、隔離等、複数の対処方法をとれること。

6) セキュリティ状況チェック

ネットワーク上の機器からセキュリティに関する情報を収集し、OS 修正パッチや修正プログラムの適用など、セキュリティ対応状況のチェックができること。

7) システムログ管理

次に示すログ情報の収集・分析・履歴管理機能を提供する。

- (1) 本システムへのアクセスログおよび変更履歴、各サーバの OS、アプリケーション等の出力する各種ログ情報を収集できること。
- (2) 各種ログ情報において、分析し、レポートを作成すること。
- (3) 各種ログ情報において、履歴管理を行うこと。

8) バックアップ管理

各サーバのバックアップ・リストア管理機能を提供する。

- (1) 磁気ディスク装置を利用してバックアップ・リストアを行うこと。
- (2) ネットワークを経由したバックアップ・リストアを行うこと。
- (3) システムファイルのバックアップ・リストアを行うこと。
- (4) バックアップ・リストア処理のスケジュール設定と自動実行を行うこと。
- (5) バックアップ・リストアの対象ファイルを設定すること。
- (6) バックアップ・リストア処理の一元管理を行うこと。
- (7) 「15.運用・保守要件定義」を満たすこと。

10.2.6. 端末共通ソフトウェア要件

1) オフィス系

文書作成機能、表計算機能、簡易データベース機能を提供する。

- (1) オフィス系ソフトウェアで作成された文書の読み込み、編集、印刷、書出しができること。

2) Web ブラウザ

Web ベースのユーザーインターフェースを利用することを考慮し、Web ページの閲覧機能を提供する。

- (1) Web ページを閲覧できること。
- (2) 各種ドキュメント(PDF、オフィス系ソフトウェアで作成された文書等)の閲覧ができること。
- (3) 暗号化通信に対応すること。

3) ドキュメント閲覧(PDF 用)

PDF 形式のファイルの内容を表示するための機能を提供する。

- (1) PDF 形式の文書内容を表示できること。

4) 情報収集・配布管理エージェント

機器の OS・修正パッチ・パターンファイル等、各ソフトウェアのバージョンを監視し、最適なバージョンの管理を行う機能を提供する。

- (1) 禁止されているソフトウェアが実装されている機器の接続を制限すること。
- (2) 必要なソフトウェアおよび修正パッチが適用されていない機器の接続を制限すること。
- (3) 必要なソフトウェアおよび修正パッチが適用されていない機器に対し、修正パッチを適用すること。

5) 暗号化

各種データの暗号化機能を提供する。

- (1) 各端末から持ち出しを許可されたデータを外部記憶媒体に保存する場合、ファイルを自動的に暗号化すること。
- (2) 暗号化を行ったデータは、セキュリティポリシーに則った処理(パスワードの入力等)において、復元できること。

6) ウイルス対策エージェント

ウイルス検知および駆除機能等を提供する。

- (1) ファイルへのアクセス、保存時にウイルス検知、駆除ができること。
- (2) 設定したスケジュールに基づきウイルスチェックができること。
- (3) ウイルス検知時において、駆除、削除、ファイル拡張子の変更、隔離等、複数の対処方法を選択できること。

7) 認証ソフト

端末へのアクセスに対し、外部認証装置との連携を取り、認証許可を与える機能を提供する。

10.2.7. 業務用端末ソフトウェア

1) バーコードアプリケーション

バーコードリーダー管理機能を提供する。

- (1) GUI、または Web ベースのユーザーインタフェースを有すること。
- (2) バーコードラベルに含まれる情報を読み込み、データベースへアップロード・格納ができること。

10.2.8. ユニットセンター端末ソフトウェア

1) バーコードアプリケーション

バーコードリーダー管理機能を提供する。

- (1) GUI、または Web ベースのユーザーインタフェースを有すること。
- (2) バーコードラベルに含まれる情報を抽出し、データベースへ格納すること。

11. 情報セキュリティ要件定義

11.1. 共通要件

- 1) 本章に示す情報セキュリティに係る要件は、本要件定義書作成時点の想定であるため、仕組みや機能の詳細は、基本設計時に確定すること。
- 2) 「政府機関の情報セキュリティ対策における政策機関統一基準の策定と運用等に関する指針(平成17年9月15日付情報セキュリティ制作会議決定)」を踏まえた「環境省情報セキュリティポリシー(第4版)」に準拠すること。ただし、今後の基準の見直し等によって改定が予想されるので、構築時における最新のものに準拠すること。
- 3) 環境省情報セキュリティポリシーに沿った具体的対策を実施した機器およびソフトウェアを納入すること。
- 4) 本システムは、調査対象者から収集した個人情報等を含む機密性の高い情報を扱うことから、適切な情報セキュリティ対策を講ずること。

11.2. 権限

権限については、本要件定義書別添資料 9.「権限マトリクス」を参照の上、以下の要件を満たすこと。なお、当該別添資料は本要件定義書作成時点での想定であるため、基本設計時に再整理した上で確定すること。

- 1) システム管理者、システム利用者によるデータの参照、更新、実行、削除に関して所属機関、職位等の属性に基づいたきめ細やかな権限の設定を行う機能を設定すること。
- 2) 権限管理を行う機能を設けるために、権限管理を実装している OS、権限管理を行うミドルウェア、又はその他アプリケーション等を導入すること。
- 3) 別添資料 9.「権限マトリクス」の設定値については、システム稼動後も設定の追加・変更・削除が柔軟に実現できること。

11.3. 情報セキュリティ対策

11.3.1. 主体認証機能

本システムの主体認証に係わる要件を以下に示す。

- 1) 利用者が業務システムにアクセスするための端末、およびアプリケーションは、利用者を個別に識別し認証すること。
- 2) システム管理者・運用業務担当者が本システムのサーバ等にアクセスする場合、システム運用者を個別に識別し認証すること。
- 3) 主体認証の方式は、ユーザーID、パスワード、および IC カード等セキュリティデバイスやバイオメトリクスを用いた構成を検討すること。
- 4) 一定期間、休眠状態のユーザーアカウントを利用できないようにすること。
- 5) パスワードは、利用者自身が変更できる仕組みを設けること。
- 6) 一定回数以上のパスワード誤入力を検知した場合、アカウントロックを実施すること。
- 7) 過去に使用したパスワードの利用を、一定世代の間使用不可とすること。

11.3.2. アクセス制御

本システムのアクセス制御機能に関する要件を以下に示す。

- 1) 本システムへのアクセスにおいて、権限のある利用者限定するため、本システムを構成するネットワーク機器、サーバ機器、端末、及びアプリケーションでアクセス制御をすること。
- 2) アプリケーションへの二重ログインを禁止すること。

11.3.3. 権限管理機能

本システムの権限管理機能に関する要件を以下に示す。

- 1) 端末、アプリケーションに対して権限管理を行う機能を設定すること。
- 2) システム管理者に対する権限は、必要な範囲に応じて付与すること。

11.3.4. 証跡管理機能

本システムの証跡管理機能に関する要件を以下に示す。

- 1) システムへのアクセス証跡を取得する機能を設定すること。
- 2) 証跡を取得する箇所および証跡に含める内容(記録する項目、情報の項目等)については、基本設計時に決定すること。
記録する項目には、以下の内容を考慮すること。
 - (1) 利用者による本システムの操作記録
 - (2) システム管理者による本システムの操作記録
 - (3) 本システムに係る端末の操作記録
 - (4) ファイアウォール、IDS(侵入検知システム)等通信回線装置の通信記録
- 3) 証跡を取得することが出来なくなった場合の対応を検討すること。
- 4) 証跡の改ざん、不正消去等の防止を行うこと。
- 5) 証跡の保存期間を定め、保存すること。
- 6) セキュリティ侵害を示す事象を検知した場合、通知する機能を設定すること。

11.3.5. 保証のための機能

本システムの保証のための機能に関する要件を次に示す。

- 1) 主体認証、アクセス制御、権限管理、証跡管理の各機能が有効に機能していることを確認すること。
(脆弱性診断、セキュリティテスト等)
- 2) 本システムを構成する機器やソフトウェアは以下の要件を満たすこと。
 - (1) ファイアウォールおよびIDSは、ISO/IEC15408セキュリティ評価基準の認定を受けていること。
- 3) 本システム稼動時において、導入ハードウェアおよびアプリケーションに関する種別、バージョン情報、すべての設定項目について文書化すること。また、設定項目が正しく設定されていることについて、確認を行うこと。
- 4) 環境省が別途実施する第三者機関によるセキュリティ監査において改善の必要性が指摘された場合には、環境省と相談の上対応すること。

11.3.6. 暗号と電子署名(鍵管理を含む)

本システムの暗号および電子署名に関する要件を以下に示す。

- 1) DMZ(DeMilitarized Zone)に設置するサーバとの通信においては、暗号化を行うこと。
- 2) 暗号技術に関しては、「各府省の情報システム調達における暗号の利用方針」に則ること。公開鍵暗号使用時の鍵長としては 1,024bit 以上とし、共通鍵暗号使用時の鍵長としては 256bit とすること。
独自の暗号化技術は行わないこと。

11.3.7. セキュリティホール対策

本システムのセキュリティホール対策に関する要件を以下に示す。

- 1) 本システムの稼動期間全体に亘り、適切なセキュリティパッチを適用する仕組みを設定すること。
- 2) 「4.3 信頼性要件」を満たすこと。

11.3.8. 不正プログラム対策

本システムの不正プログラム対策に関する要件を以下に示す。

- 1) 本システムの全ての機器(サーバ、端末等)に関して、アンチウイルスソフトウェア等を導入すること。
- 2) 本システムにおいて想定される不正プログラムの感染経路の全てにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施すること。
- 3) 不正プログラムの拡散を防止するための対策を行うこと。

11.3.9. サービス不能攻撃対策

本システムのサービス不能攻撃対策に関する要件を以下に示す。インターネットからアクセスを受ける、通信回線装置又は通信回線を有するシステムについては、サービス提供に必要な通信回線装置が装備している機能をサービス不能攻撃対策に活用すること。

11.3.10. 踏み台対策

本システムの踏み台対策に関する要件を以下に示す。

- 1) 情報システムが踏み台として使われることを防止するための措置を講ずること。
- 2) 情報システムが踏み台として使われた場合の影響が最小となるようにシステムを構築すること。

11.3.11. 不正アクセス対策

外部ネットワークとの接続箇所において、ファイアウォールを導入し、不正アクセスへの対策を行うこと。

12. 設計・開発要件定義

12.1. 設計・開発実施計画の作成

設計・開発事業者は設計・開発実施体制と役割、詳細な作業およびスケジュールに関する設計・開発実施計画を提示し環境省の承認を得ること。

システム設計・構築実施計画には以下の内容が含まれること。

- 1) スコープ管理
- 2) スケジュール管理
- 3) コスト管理
- 4) 品質管理
- 5) リスク管理
- 6) コミュニケーション管理

12.2. 設計・開発実施体制

設計・開発作業を行う要員については、業務に支障をきたさないよう十分な知識が必要である。

- 1) 設計・開発事業者は、統括責任者の指示のもとで、システム設計・開発を行うこと。
- 2) プロジェクト管理者を任命すること。
- 3) 運用プロジェクト管理者を適切な時期に任命すること。
- 4) 全体の実施体制については、体制表を環境省に提出して承認を得ること。
- 5) 役割ごとの主な業務内容については下表を参照すること。
- 6) 設計・開発に必要な課題の解決を行える体制を整備すること。

表 12-1 役割ごとの主な業務内容等

役割	主な業務内容	要員等
総括責任者	プロジェクト全体の管理を行う。	環境省職員が行う。

役割	主な業務内容	要員等
プロジェクト管理者	・プロジェクトが期間内に終結できるプロジェクト作業計画書の策定し、管理を行う。 ・プロジェクトの範囲を明確に定義し、詳細タスク表(WBS)を策定する。 ・プロジェクトの進捗管理および品質管理を行う。 ・総括責任者から設計・開発事業者に対する指示、協議の窓口業務を行う。 ・設計・開発事業者から総括責任者への報告、連絡、相談を行う。 ・調達Aの受注者が行う調達(調達C及び調達D)支援業務を補助する。 ・本システムの稼働開始後のヘルプデスク対応、プログラム改修等、保守業務については、調達Dの受注者が主体的に行うこととするが、当該業務が円滑に実施されるよう、これを支援する。	・システム計画の立案若しくはプロジェクト管理を含むコンサルティングの実務経験を5年以上有する者。 ・以下のいずれかの資格を有する者。 - ア プロジェクトマネージャ(経済産業省) - イ プロジェクトマネジメントプロフェッショナル(米国 PMP)
担当技術者	・システムの設計、構築等に必要な作業を担当する。	・以下のいずれかの資格を有する者。(最低1名) - ア システム監査技術者(経済産業省) - イ ITストラテジスト(経済産業省) ・以下のいずれかの資格を有する者。(最低1名) - ア 情報セキュリティアドミニストレータ(経済産業省) - イ テクニカルエンジニア(情報セキュリティ)(経済産業省) ・以下のいずれかの実績を有する者。 - ア 官公庁に対して、情報システムの要件定義を実施した実績 - イ 官公庁に対して、分離調達が行われ複数の事業者が参画しているプロジェクトにおける、情報システムの設計・開発業務を実施した実績 - ウ 官公庁に対して、全国規模のシステムの設計・開発を実施した実績

役割	主な業務内容	要員等
		エ 医療機関に対するシステム導入業務又は管理業務を実施した実績

7) その他体制に関する事項

- (1) 体制を変更する必要がある場合には、変更内容を記載した書面をもって報告し、事前に環境省の承認を得ること。
- (2) プロジェクト管理者は、平日、開庁時、環境省から連絡を行え、かつ障害対応等を直接指揮できる状態(電話等による運用実施者への指示を含む)にななければならない。ただし、環境省の了解を得て一時的に代理の者がこれを務めることができる。
- (3) 環境省は設計・開発事業者の負うべき責により作業計画に著しい遅れが生じたり重大な問題が発生した結果、環境省の業務に多大な支障を及ぼすと判断した場合、プロジェクト管理者の交代を求めることができる。

12.3. 設計・開発スケジュール

スケジュールについては「2 スケジュール定義」を参照すること。

12.4. 開発環境の整備

システムの構築環境について以下の要件を考慮すること。

1) 開発機器の調達

開発機器の調達は、設計・開発業者により実施し、利用する機器の詳細について環境省との協議の結果承認を得ること。

2) 開発機器の設置場所

開発機器の設置場所については、環境省との協議により詳細を決定すること。

12.5. 開発方法

新システムの設計・開発業務について以下の内容を考慮すること。

1) 将来の保守を見据えた汎用性高いシステム構造

再利用性、拡張性の高いシステム構造にするため、オブジェクト指向設計のアプローチを取ること。

13. テスト要件定義

13.1. テスト実施計画の作成

設計・開発事業者は、テスト作業前にテスト体制と役割、詳細な作業およびスケジュール、テスト環境、テストツール、合否判定基準等に関する試験実施計画を提示し、環境省の承認を得ること。

テスト実施において下記の要件を考慮し実施すること。

- 1) システムが設計通り、且つ要件通りの動作を行うことを確認するため、システム利用者に提供する前に各種(例 単体テスト、結合テスト、性能テスト、負荷テスト、システムテスト、総合テスト、受け入れテスト)試験を必要に応じて実施すること。
- 2) 設計・開発事業者は、試験作業開始前に試験実施計画にもとづく試験の進捗状況、作業上の課題についての管理・報告ルールを提示し、環境省の承認を得ること。設計・開発事業者は、そのルールに沿った管理・報告を行うこと。

13.2. テスト実施体制と役割

1) テスト実施体制

テスト実施体制として「12.2 設計・開発実施体制」を参照のこと。

2) 役割

テストの役割として、システムが仕様通り動作を行うことを確認することにより、システムの品質を保つ重要な役割を担う。

13.3. テストスケジュール

スケジュールについては「2 スケジュール定義」を参照のこと。

13.4. テスト環境

試験を行うにあたって、必要な機器やツールについては、設計・開発事業者において準備すること。

受入テストは本番環境にて実施すること。

13.5. テスト方法

以下の内容について試験を実施し、設計どおりの動作が行われていることを確認すること。また、必要に応じてテスト方法を変更し、工程を追加すること。

表 13-1 実施主体ごとのテスト方法

	実施主体	テスト方法	成果物
--	------	-------	-----

	環境省	事業者		
単体テスト	監理	実施	ホワイต์ボックステスト ・カバレッジテスト (命令、分岐、条件の網羅)	単体テスト仕様書 単体テスト結果報告書
結合テスト	監理	実施	ブラックボックステスト	結合テスト仕様書 結合テスト結果報告書
総合テスト	監理 支援	実施	ブラックボックステスト ・性能テスト ・負荷テスト ・セキュリティテスト ・運用テスト	総合テスト仕様書 総合テスト結果報告書
受入テスト	実施	支援	実施	受入テスト仕様書 受入テスト結果報告書

13.6. テストデータ

環境省は正当な理由があると判断した場合に限り必要なデータ等を設計・開発事業者に提供する。なお、提供されたデータに機密度の高いデータ項目や個人情報に係るデータ項目は取扱いに十分留意すること。場合によってはデータをスクランブル化して利用すること。

また、テストの結果について、設計・開発事業者は試験結果を「試験報告書」として取り纏め、環境省の承認を得ること。

13.7. 受入テストの支援

設計・開発事業者は運用・保守事業者への受け入れテスト実施の際に受け入れテストを支援すること。

14. 移行要件定義

開発環境・テスト環境から本番環境へのシステム移行が発生するため、移行計画書を事前に環境省に提示し、承認を得ること。

14.1. システム移行

本システムにおいては、開発環境・テスト環境から本番環境へのアプリケーションの移行が発生する。尚、本システムにおいては現行システムが存在しないため、ソフトウェアおよびハードウェアに関する現行システムからの移行作業は発生しない。

14.2. 業務移行

14.2.1. 教育

設計・開発事業者は教育訓練実施体制と役割、詳細な作業およびスケジュールに関する教育訓練実施計画を提示し環境省の承認を得ること。

教育訓練実施計画は以下の要件を満たすこと。

- 1) システムの導入スケジュールに合わせた研修計画を環境省に提示し、承認を得ること。
- 2) 設計・開発事業者は、教育訓練開始前に教育訓練実施計画にもとづく教育訓練の進捗状況や作業上の課題についての管理・報告ルールを環境省へ提示し、承認を得ること。設計・開発事業者は、そのルールに沿った管理・報告を行うこと。
- 3) 教育訓練の目的を明確にし、以下の内容を訓練すること。
 - ① システム運用手順
 - ② ヘルプデスク業務
 - ③ システム利用者への教育

14.2.2. 教育訓練実施体制と役割

- 1) 設計・開発事業者は統括責任者の指示のもとで、教育訓練を行うこと。
- 2) 全体の実施体制については、体制表を環境省に提出して承認を得ること。

14.2.3. 教育訓練スケジュール

スケジュールについては「2 スケジュール定義」を参照すること。

14.2.4. 教育訓練環境

設計・開発事業者は環境省と事前の協議により、教育訓練設備や教育訓練用機器等の必要性の有無等を決定し、承認を得ること。

14.2.5. 教育訓練方法

設計・開発事業者は教育訓練方法を環境省に提示し、承認を得ること。

14.2.6. 教育訓練用教材の開発

設計・開発事業者は教育訓練用教材の開発方法を環境省に提示し、承認を得ること。また、教育訓練用教材については利用者の視点に立った理解しやすい教材を開発すること。現行業務と、エコチル調査で実施予定の業務内容の相違点を明確にしたうえで、トレーニング教材を作成すること。

14.2.7. 教育訓練用教材の評価

設計・開発事業者は評価方法を環境省に提示し、承認を得ること。

14.2.8. 教育訓練の実施報告と評価

設計・開発事業者は教育訓練の実施報告および評価方法を環境省に提示し、承認を得ること。

15. 運用・保守要件定義

15.1. 運用・保守体制と役割

15.1.1. 体制と役割

役割については下表を参照のこと。各役割については兼務を可とする。体制については、業務 D を調達後、決定すること。

表 15-1 役割ごとの体制

役割	
運用総括責任者	
システム運用・ 保守	運用プロジェクト管理者
	運用担当者
	保守担当者
データセンター 運用	運用技術支援管理者
	担当技術者

15.1.2. 主な業務内容

業務内容については下表を参照のこと。各役割、業務内容については兼務を可とする。

表 15-2 役割ごとの主な業務内容

役割		主な業務内容	要員等
運用総括責任者		プロジェクト全体の管理や判断等を行う。	環境省職員が行う。
システム運用・保守	運用プロジェクト管理者	・運用業務の作業計画策定を行う。 ・運用業務の進捗管理、品質管理（サービスレベル管理）、課題管理を行う。 ・運用総括責任者との窓口業務（指示、報告、連絡、協議等）を行う。 ・運用担当者に対して、業務実施に必要な専門知識やノウハウ等についての教育、訓練を行い、必要なスキルを習得させる。 ・設計開発事業者行う保守業務との連絡窓口、作業調整を行う。	・情報処理技術者試験のプロジェクトマネージャ試験合格者であり、かつ業務に必要な知識、業務経験を有する者が望ましい。 ・又は、これと同等の知識、業務経験を有すると認められる者。 ・その他、運用管理業務を円滑に遂行できる IT 知識を有するもの。
	運用担当者	・システム利用者への操作問合わせ対応や定常業務（監視、障害対応受付等）を行う。 ・運用プロジェクト管理者、運用総括責任者等への問題のエスカレーションを行う。 ・運用上の技術的な業務を担当する。	・業務に支障をきたさないように作業を遂行するための知識、業務経験を有する者。
	保守担当者	・本システム稼動開始後のソフトウェア、ハードウェア、ネットワークの保守作業を行う。 ・ヘルプデスク設置、各種障害対応、プログラム改修等を行う。	・業務に支障をきたさないように作業を遂行するための知識、業務経験を有する者。

役割		主な業務内容	要員等
データセンター運用	運用技術支援管理者	・運用業務の作業計画策定を行う。 ・運用プロジェクト管理者との窓口業務（指示、報告、連絡、協議等）を行う。 ・担当技術者、業務実施に必要な専門知識やノウハウについての教育、訓練を行い、必要なスキルを習得させる。	・情報処理技術者試験のプロジェクトマネージャ試験合格者であり、かつ業務に必要な知識、業務経験を有する者が望ましい。 ・ITIL ファンデーション試験合格者であり、かつ業務に必要な知識、業務経験を有する者。 ・システムのソフトウェア、ハードウェアにおけるベンダー認定の上位資格を有する者。 ・又は、上記3つと同等の知識、業務経験を有すると認められる者。 ・その他、運用技術支援業務を円滑に遂行できる IT 知識を有するもの。
	担当技術者	・障害対応の支援、原因解析、根本的対策立案、システムの修正変更など運用業務の支援を行う。	・ITIL ファンデーション試験合格者であり、かつ業務に必要な知識、業務経験を有する者。 ・システムのソフトウェア、ハードウェアにおけるベンダー認定の上位資格を有する者。 ・又は、上記2つと同等の知識、業務経験を有すると認められる者。 ・その他、運用技術支援業務を円滑に遂行できる IT 知識を有するもの。

15.1.3. 運用範囲

運用の対象組織については、「4.2 システムの利用者」を参照のこと。運用対象物については本業務で納入したハードウェア機器およびソフトウェアとする。

15.1.4. その他運用保守体制に関する事項

- 1) 運用担当者、保守担当者及び担当技術者は本システムを熟知したものを従事させるものとし、万全な体制を確保し協力して作業に従事すること。
- 2) 運用担当者と保守担当者は、兼務を可とする。
- 3) 体制を変更する必要がある場合には、変更内容を記載した書面をもって報告し、事前に環境省の承認を受けること。
- 4) 運用技術支援管理者は運用業務時間内に環境省から連絡を行え、かつ障害対応等を直接指揮できる状態（電話等による担当技術者への指示を含む）になければならない。ただし、環境省の了解を

得て、一時的に代理の者がこれを務めることができる。

- 5) 環境省は、システム運用・保守事業者の負うべき責により作業計画に著しい遅れが生じたり重大な問題が発生した結果、環境省の業務に多大な支障を及ぼすと判断した場合、運用プロジェクト管理者、運用技術支援管理者の交代を求めることができる。

15.2. 運用業務要件

15.2.1. 業務内容一覧

作業項目単位の担当業務を以下に記す。

表 15-3 作業項目ごとの担当

項番	作業項目		平日の日中	
			システム運用・保守	データセンター運用
1	運用総括管理		環境省職員が担当する	
2	運用プロジェクト管理		○	○
3	セキュリティ管理		○	○
4	ネットワーク管理			○
5	インシデント管理		○	○
6	問題管理		○	
7	構成管理		○	
8	変更管理		○	
9	リリース管理		○	
10	バックアップ		○	○
11	ヘルプデスク管理		○	
12	サービスレベル管理	サービスレベル管理	○	○
		利用統計		
13	運用ドキュメント管理		○	

1) 運用総括管理

- (1) 運用業務全般について、全体管理や作業方針等の判断を行う。
- (2) システム利用者との調整を行う。

2) 運用プロジェクト管理

- (1) プロジェクトの作業計画策定支援を行うこと。
- (2) プロジェクトの進捗管理、品質管理、課題管理を行うこと。
- (3) 運用総括責任者との窓口業務(指示、報告、連絡、協議等)を行うこと。
- (4) 運用担当者、担当技術者への作業指示および作業管理等を行うこと。
- (5) 運用業務上の問題を管理すること。
- (6) システム利用者との調整支援を行うこと。
- (7) 定例報告会を開催し、運用総括責任者へ運用状況の報告等を行うこと。
- (8) 運用担当者、担当技術者に対して、業務実施に必要な専門知識やノウハウ等についての教育・訓練を行い、必要なスキルを習得させること。
- (9) 運用業務の改善提案を行うこと。
- (10) 運用総括責任者に人事異動があった場合、新任者に対して、必要な研修を実施すること。

3) セキュリティ管理

- (1) セキュリティホールやウイルス情報等の確認を常に行い、システムの情報セキュリティの維持・強化を行うこと。
- (2) 「10 ソフトウェア要件定義」に示す、情報セキュリティ対策に必要な運用業務を行うこと。
 - ① ウイルス対策に必要な運用業務を行うこと。
 - ② 暗号化に必要な運用業務を行うこと。
 - ③ ログオン認証に必要な運用業務を行うこと。
 - ④ サーバ利用制限に必要な運用業務を行うこと。
 - ⑤ 端末利用制限に必要な運用業務を行うこと。
- (3) ウイルス検知等の情報セキュリティ上の問題となる事象について監視を行い、報告および改善提案等を行うこと。

4) ネットワーク管理

- (1) ネットワーク管理機能を用いて、サーバ、ネットワーク、ソフトウェアなどの稼動状況の把握等を行うこと。
- (2) ネットワーク管理機能については、「10 ソフトウェア要件」を参照のこと。

5) インシデント管理

- (1) サービスの中断やサービス品質の低下につながるような事象(インシデント)について、中断時間を最小限に抑えて速やかに回復し、サービスの品質を維持する活動を行うこと。
- (2) 運用・保守事業者、運用技術支援業者は、インシデントの解決策に対して作業分担を行い、実施すること。
- (3) 問合せの履歴管理を行うこと。
- (4) 障害履歴管理を行うこと。

6) 問題管理

- (1) 通常のサービス運用に回復した後、インシデントの根本的な原因の究明を行い管理すること。
- (2) 業務上発生した、システムに関わる問題を管理すること。

7) 構成管理

- (1) ハードウェア、ソフトウェア、すべての運用対象機器の詳細な情報を管理すること。

8) 変更管理

- (1) システムの変更を行う際は変更対象を明確に定義し変更手順の管理を行うこと。
- (2) システムの変更が原因で起こるインシデントを最小限に抑えるため、必要な承認プロセスを確立し細心の注意を払うこと。
- (3) システムの変更を行う際は RFC(変更要求)を作成すること。

9) リリース管理

- (1) 変更管理で承認された RFC に対して、リリース計画を作成し、その実行を管理すること。

10) バックアップ

- (1) バックアップについては「15.3 データ管理要件」を参照のこと。

11) ヘルプデスク管理

- (1) システム利用者からの問い合わせ対応を行うこと。
- (2) 障害対応窓口を行うこと。必要に応じて、担当技術者へ問題のエスカレーションを行うこと。
- (3) 操作マニュアルや FAQ 等の作成、維持管理を行うこと。
- (4) 問い合わせ履歴、障害履歴の管理を行うこと。

12) サービスレベル管理

- (1) 環境省とサービスの品質基準を協議し、サービスレベルの基準を作成すること。
- (2) サービスレベル管理の実施状況および維持状況の報告を運用総括責任者に行うこと。
- (3) サービス状況に関する分析結果および改善提案等を提示すること。

13) 運用ドキュメント管理

- (1) 運用ドキュメントの保守および管理を行うこと。
- (2) 機器に関する操作説明等を実施すること。操作説明等の内容および時期については、環境省と別途協議すること。

15.2.2. 運用ドキュメント

運用ドキュメントは日本語で記載すること。また、運用ドキュメントとしては、以下のものを想定している。

1) 運用開始時に作成し、維持管理を行うもの。

- (1) 運用体制表(組織図、通常・緊急電話連絡網、保守連絡先等)
- (2) 障害対応管理台帳
- (3) ヘルプデスク対応管理台帳
- (4) 環境省の指示にもとづき作成された資料

2) 設計・構築された時点で作成されたものに対して維持管理を行うもの。

- (1) 基本設計書
- (2) 詳細設計書
- (3) 運用設計書
- (4) 操作マニュアル
- (5) 運用手順書
- (6) 環境省の指示にもとづき作成された資料

3) システム運用・保守時に作成し、維持管理を行うもの。これらについては、定期的に提出・報告を行うこととする。

- (1) 作業管理表
- (2) ヘルプデスク対応管理台帳
- (3) 運用定例会議における資料および会議議事録(運用実績・予定、改善提案等を含む)
- (4) 障害報告書(状況、原因、対応方法、再発防止策等)
- (5) 環境省の指示に基づき作成された資料

15.2.3. 運用・保守業務時間とシステム稼働時間

1) 運用業務時間

- (1) 平日午前 9 時から午後 6 時までを運用保守時間とすることを想定とする。
- (2) 土曜、日曜、祝日、年末年始は運用保守時間としないことを想定とする。

15.2.4. 障害対応

1) 障害時

障害対応については、運用保守業務時間に限り常時対応が可能となる体制とすることを想定している。
なお、緊急性の高い対応の障害のみ例外を認めることとする。

2) 不具合対応

障害とはならないが、システムリリース後に不具合が生じた場合は、緊急性と優先度を考慮して対応すること。

15.2.5. セキュリティ対応

1) セキュリティホール対応

ベンダーにより通知されたセキュリティホールに対しては、対応しても問題が無いことを検証した上で、対応をすること。

2) アクセス管理

システム利用者のアクセス権の管理は環境省で任命された担当者のみ設定できること。

15.2.6. その他

1) 新たな運用要員・運用業務受託者に対する引継

体制を変更する必要がある場合には、新たな運用要員・運用業務受託者に対して、業務実施に必要な専門知識やノウハウ等の引継ぎを行う。引継実施にあたっては、以下のような事項を内容とする引継計画書を作成し、環境省の承認を得ることとする。

(1) 業務の範囲および内容

引継対象業務の範囲および内容を明確にする。

(2) 管理責任者

運用業務受託者において引継作業を管理するための管理責任者を明らかにする。

(3) 実施担当者

運用業務受託者において、引継対象業務ごとに、引継実施担当者を明確にする。

(4) 引継対象文書

引継対象業務ごとに、運用・保守事業者が整備した文書を明確にする。

(5) 引継方法

引継対象業務ごとの、引継方法を明確にする。

(6) 引継期間

引継対象業務の内容に応じて、引継期間を明確にする。

15.3. データ管理要件

15.3.1. バックアップ要件

- (1) 収集された全てのデータは、差分バックアップ（日次、週次など）とフルバックアップ（稼動開始前、週次など）の定期的な組み合わせによりバックアップが実施され、データセンター内でデータの完全性が確保されること。
- (2) バックアップ媒体は、第三者に不正に利用されないよう、暗号化等により、安全に保存されていること。
- (3) バックアップは深夜時間帯に行うことが望ましい。
- (4) バックアップ対象
 - ① 各サーバ及び NW 機器のシステムファイル
 - ② ログ
 - ③ DB データ
 - ④ その他電子保存文書
 - ⑤ IF ファイル

15.4. システム運用・保守施設

15.4.1. システム運用・保守業務の作業場所

運用・保守事業者が事前に環境省に報告し承認された作業場所とする。

15.4.2. データセンター運用業務の作業場所

運用・保守事業者が事前に環境省に報告し承認された作業場所とする。

15.5. 保守業務要件

15.5.1. 主な業務内容

本業務での作業範囲は次のとおり。

- ① 開発済みのソフトウェアが運用テスト時からサービス開始までに問題なく動作するまでの環境設定
- ② サービス開始までに必要とする今回調達対象となるすべてのソフトウェア、ハードウェアの設定変更等によるチューニング作業
- ③ ソフトウェア、ハードウェアリソースの修正等による環境設定および使用期間中の保守等

15.5.2. 保守範囲

「15.6. ソフトウェア保守要件」、「15.7. ハードウェア保守要件」を参照のこと。

15.5.3. 保守業務時間

1) 保守業務時間

- (1) 「15.2.3. 運用業務時間とシステム稼動時間」と同様の時間帯とする。但し、緊急を要する作業の場合は、運用プロジェクト管理者と作業内容を相談の上、対応すること。

15.6. ソフトウェア保守要件

15.6.1. ソフトウェア保守対象

保守対象ソフトウェアは、本業務で納入するすべてのソフトウェアとする。

15.6.2. ソフトウェア保守について

1) 保守費用の範囲

ソフトウェア保守に関しては以下に留意し、受注金額内で対応すること。

- (1) 保守の実施について、受注期間中は追加費用が発生しないこと。
- (2) 通常の使用状況で障害があった場合についても、作業費用・出張費など追加費用が発生しないこと。
- (3) 代替品の提供時についても、追加費用が発生しないこと。
- (4) 運用・保守事業者内で対応ができない問題が生じ、他社にサポートを依頼する事象が発生した場合においても、追加費用等が発生しないこと。

2) 改善

- (1) ソフトウェアの修正等に伴う機器およびソフトウェアの環境設定変更等を行うこと。
- (2) 環境設定後についても、ソフトウェアの導入・総合試験等の支援を行うこと。

3) 潜在不具合

- (1) 運用・保守事業者は、ソフトウェアのバグ、パッチおよびバージョンアップ等の情報を無償にて速やかに公開し配布するとともに、環境省の指示に従い、機器への導入および動作確認を行い、正常に動作することを保証すること。
- (2) サーバ OS、ネットワーク OS、クライアント OS、ウェブブラウザ、日本語ワープロソフト、表計算ソフト等のソフトウェアのバージョンアップおよびパッチ導入等については、セキュリティホール・バグ等への対応を実施すること。

4) 定期報告

各月ごとの保守の内容および対応実績等について、翌月上旬までに環境省の指定する者に対して報告を行うこと。なお、詳細については環境省と別途協議すること。

15.7. ハードウェア保守要件

15.7.1. ハードウェア保守対象

保守対象機器は、本業務で納入するすべての機器とする。

15.7.2. ハードウェア保守について

1) 窓口対応体制としては、各種問い合わせ、障害全般に対する一本化した窓口を設けること。またクライアントについては、ディスク障害復旧時はリカバリ CD でのリカバリ作業を実施し、納品時の状態へ戻し、ネットワーク接続が可能な状態とすること。

2) 本業務の作業範囲は、次のとおり。

(1) 使用期間経過後の機器の撤去およびディスク内容の消去

(2) 消去の条件は下記のとおり。

- ・ 消去場所: 運用・保守事業者の用意する消去場所にて消去作業を行なうこと。
- ・ 消去方法: ソフト消去にて 2 回以上上書きを行なうこと。
- ・ 証明書: データ消去を実施した証明書を全台数分提出すること。

(3) 機器の撤去時には、設置場所等を設置前と同様の状態に復帰すること。

3) 保守費用の範囲に関しては、以下に留意すること。

(1) 保守の実施について、受注期間中は追加費用が発生することなく、受注金額内で対応すること。

(2) 通常の使用状況で障害があった場合についても、機器費用や作業費用・出張費など追加費用が発生することなく、受注金額内で対応すること。

(3) 運用・保守事業者内で対応ができない問題が生じ、他社にサポートを依頼する事象が発生した場合においても追加費用等が発生することなく対応すること。

4) 改善

(1) 環境省からの求めに応じて、機器増設等の改善についての提案を行うこと。ソフトウェアの修正等に伴う機器およびソフトウェアの環境設定の変更等を行うこと。

(2) 環境設定後についても、ソフトウェアの導入・総合試験等の支援を行うこと。

5) 潜在不具合

運用・保守事業者は、機器に関する技術的な問題点の情報を無償にて速やかに公開し配布するとともに、環境省の指示に従い、機器への導入および動作確認を行い、正常に動作することを保証す

ること。

6) 定期報告

各月ごとの保守支援、保守の内容および対応実績等について、翌月上旬に環境省又は環境省の指定する者に対して報告を行うこと。なお、詳細については環境省と別途協議すること。

15.8. データセンター要件

データセンターに関しては、外部に委託することを想定しており、以下の要件で調達予定である。

15.8.1. 基本要件

- 1) 市場において公正な調達が可能であること。
- 2) 本システムの構築に当たり調達・設置する予定の機器、および設定する回線に事業者等の制約がないこと。
- 3) 本システム構築に従事する各事業者（設計開発事業者、ハードウェア導入事業者、運用・保守事業者等）の入退館及び館内作業が可能であること。

15.8.2. 設備要件

1) 情報セキュリティマネジメントシステム

- (1) JIS Q 27001 又は ISO/IEC 27001 に基づく認証を取得していること。

2) 立地

- (1) 地震、風水害及び落雷等の自然災害による被害の少ない場所に設置されていること。
- (2) 周辺に消防法に定める指定数量以上の危険物製造施設又は危険物貯蔵施設が設置されていない場所に設置されていること。
- (3) 電磁界の被害を受けない場所に設置されていること。

3) 建物

- (1) 震度 6 強の地震に耐える基礎耐震若しくは基礎免震構造であること。
- (2) 出水被害から建物及び情報システムを保護する構造であること。
- (3) 建築基準法に規定する耐火建築物であること。
- (4) 建築基準法、消防法に規定する非常用設備を有すること。
- (5) 避雷設備を有すること。

4) 機器設置室

- (1) 建築基準法に基づく、独立した防火区画であること。
- (2) 火災の予兆を検知できるシステムが設置されていること。
- (3) 新ガス系消火設備を備えていること。
- (4) 水冷方式を採用している場合は、漏水防止策を講じていること。ただし、空冷方式を採用している場合はこの限りではない。
- (5) 機器に対し外部からの電磁波の影響を受けにくい環境であること。
- (6) 当該機器設置室専用の分電盤を室内に準備すること。
- (7) 床構造はフリーアクセス床とし、フリーアクセス床耐荷重 500kg/㎡以上、スラブ床耐荷重 1,000kg/㎡以上であること。
- (8) フリーアクセス床高 600mm 以上であること。
- (9) 保守に必要な空間が確保されていること。
- (10) 導入作業期間の間は、機器を一時的に保管し、設定作業等を実施するための場所(約100㎡)を同一建物内に準備すること。準備する場所は、セキュリティを考慮した場所であること。

5) 電源

- (1) 電力会社から 2 系統以上で受電し、冗長性を確保していること。
- (2) 建物の電源設備の法定点検及び工事の際においても、機器の停電時対策をとる必要のないこと。
- (3) 停電時にシステムを運用するために十分な電源容量を持つ非常用自家発電装置を備えていること。
- (4) 停電時に自家発電装置が安定的に起動するまでの間、瞬断することなくシステムに十分な電力

供給が可能な無停電電源装置を設置していること。無停電電源装置は冗長構成がとられていること。

(5) 自家発電装置の燃料容量は 24 時間以上継続運転が可能であり、その使用中であっても燃料補給にて継続運転が可能であること。

(6) サーバ等と、負荷変動の激しい空調機等の電力系機器等は電源系統を分けてあること。

6) 空調

(1) 24 時間 365 日の自動運転による稼動が可能であること。

(2) 機器設置室内の環境は、温度 $24^{\circ}\text{C} \pm 2^{\circ}\text{C}$ 、湿度 $50\% \pm 20\%$ とすること。

(3) 水冷方式の空調設備の場合には、漏水対策を講じ、漏水の恐れがある場所に漏水センサを設置していること。また、災害時に断水となった場合でも3日間継続運転が可能となる貯水タンクを備えていること。ただし、空冷方式を採用している場合はこの限りではない。

(4) 機器設置室の主要な空調設備機器については、予備器が設置されており、主要機器が故障の場合でも必要な冷却能力を確保できること。

7) セキュリティ

(1) 建物入口から機器設置室までの間において、常駐警備による入退室管理が 24 時間 365 日実施されていること。

(2) 3 段階以上のセキュリティを有し、生体認証による個人レベルでの認証機構又は、有人警備によるセキュリティが施されていること。

(3) 機器設置室の入退出について、設備の運用に従事する人員とそれ以外の人員の入退出管理が明確に区分できる入退出管理の設備等を有していること。また、入退出に関する手順書を有していること。

(4) 機器設置室は、外部から見えない構造になっており、かつ機械設置室に窓がないこと。

(5) 常時利用する入出口には IC カード、生体認証、監視カメラ等の防犯設備を設置していること。かつ、共連れにより入退資格者でない人物が入室できる事を物理的に防止できること。

(6) 監視カメラによる記録を一定期間保存し、受注者側で速やかに画像閲覧できる状態であること。画像の保存期間は、最低1ヶ月間とすること。なお、環境省から画像閲覧を求められたときは、個人情報保護に関する法律(平成十五年五月三十日法律第五十七号)第二十三条(第三者提供の制限)に基づき、速やかに閲覧できる状態であること。

(7) 大型機器類の搬入口では、専用口でデータセンター職員又は警備員立会いの下、入館セキュリティを保つこと。

(8) データセンターのセキュリティゾーン内には、データセンター関係者以外の不特定多数が利用する飲食店などのテナントが入居していないこと。

(9) ラックの個別施錠が可能なこと。

(10) 各設備を常時集中管理及び制御する仕組みを有すること。

(11) 建物及び機械室の人の出入りを遠隔監視する設備が設置されていること。

- (12) 建物及び機械室の防災設備及び防犯設備の作動を遠隔監視する設備が設置されていること。
- (13) 電源設備及び空調設備の稼動状況を遠隔監視する設備が設置されていること。
- (14) 固定電話もしくは構内 PHS 等の通信手段を確保すること。

8) 共用施設

- (1) 共用会議室、洗面所、給湯室が共有設備として利用可能であること。
- (2) 機器の取扱説明書等を保管するための施錠可能なキャビネットを提供可能であること。なお、キャビネットは A4 サイズファイルを保管することのできるもの (H:1800mm x W:800mm x D:400mm) を 5 台程度準備すること。

9) 回線

(1) 基本要件

- ① バックアップ媒体は、オリジナルデータと同時に被災しない場所に保存しておくこと。
- ② 回線稼動は 24 時間とすること。
- ③ 回線稼働率は 99.0%以上を目標とする。
- ④ 回線の帯域は 100Mbps 以上で提供すること。
- ⑤ 緊急性の高い障害は早急に対応すること。
- ⑥ 緊急性の低い障害については環境省と復旧まで期間を協議すること。

(2) 運用

- ① 24 時間 365 日のネットワーク障害受付、故障修理及び復旧ができる体制を有すること。
- ② 通信回線の利用状況、障害等を監視する設備が同一建物内または網内に設置されていること。
- ③ 計画的な工事又は、定期的な保守等に伴いネットワークを停止する場合は、少なくとも、4週間前までに環境省に事前に連絡し、了承を得ること。なお、運用を続けると明らかに障害に至ることがわかっている場合の緊急停止については、環境省と別途協議の上、対応を決めることとし、緊急停止中は、稼働率の停止時間として扱うものとする。