令和８（2026）年度生成 AI を活用した児童相談所業務支援システム設計・開発・導入業務委託仕様書

本仕様書は、栃木県（以下「甲」という。）が発注する生成 AI を活用した児童相談所業務支援システム設計・開発・導入業務（以下「委託業務」という。）を受託する者（以下「乙」という。）の業務について、必要な事項を定めるものである。

１　基本事項

（１）業務名

生成 AI を活用した児童相談所業務支援システム設計・開発・導入業務

（２）背景・目的

児童相談所における虐待対応件数の逓増及び複雑化に伴い職員の量的・質的な業務負担が増加しており、従来の業務プロセスでは対応が困難になってきている。また、若手職員割合の増加とともに職員の専門的スキルの蓄積が必ずしも十分でないことや、面談及び虐待通告対応に起因する長時間労働等により、職員のモチベーションの低下や離職等の悪循環が生じている。

このため、児童相談業務の効率化により事務負担の軽減を図り、相談援助活動に注力することで、児童虐待事案等に迅速かつ的確に対応できるよう、生成ＡＩを活用した業務支援システム（以下「本システム」という。）を導入する。

（３）契約期間

契約締結日から令和９年３月 31 日まで

２　業務の概要

（１）本システムの概要

本システムは、以下のア～ウの特徴をもったものとする。

ア　児童相談所システム※（以下「児相システム」という。）内に保存されている児童記録等データ及び関係法令等の読込

※児童相談所システム：児童相談所における児童相談情報管理や通知書及び帳票の出力等を行うシステム。

イ　過去事例の出力

ウ　こどもの処遇に係る対応案及び指定した情報（以下「処遇案等」という。）の出力

（２）導入箇所

栃木県保健福祉部こども政策課

栃木県中央児童相談所

栃木県県南児童相談所

栃木県県北児童相談所

（３）委託業務スケジュール

内容	時期
契約	令和８年９月下旬
システム開発・ネットワーク構築	令和８年 10 月～令和９年２月上旬
試験稼働	令和９年２月中旬～２月下旬
システム運用開始	令和９年３月上旬～

（４）調達範囲

ア　要件定義

イ　導入作業、マスターデータ設定（利用者情報等）等

ウ　システムテスト

エ　運用テスト

オ　運用保守要件定義

カ　その他上記に関する業務

（５）納入成果物

乙は、以下の成果物を納入すること。

なお、パッケージソフトの標準機能に係る設計等、開示が不可能なものについてはこの限りではない。

ア　事業計画書、実施報告書等

乙は、以下の書類を Word、Excel、PowerPoint 等により作成して甲が指定する日までに電子データを甲へ提出し、承認を得ること。

項番	成果物	説明
1	事業計画書	委託業務を行うにあたっての体制、スケジュール、進め方等を記載したもの（試験計画含む）
2	設計書	本システムの機能一覧、システム構成図、マスタデータ定義等について記載したもの
3	マニュアル	本システムの利用者用の操作手引書及び管理者用の操作・運用保守マニュアル

イ　ライセンス

本システムに必要なライセンスは乙が用意すること。

３　システム要件

（１）基本要件

ア　本システムへの指示内容の入力、出力及び情報の連携は児相システムと API 連携することにより実施し、児相システム内の操作により本システムを使用可能であること。

なお、本仕様書は本業務で実現すべき要件を示すものであり、実装上の詳細仕様及び実現方法については本業務契約締結後の要件定義及び基本設計工程において、甲乙及び関係事業者との協議により決定するものとする。

イ　児相システム利用者が児相システムアカウントの情報により、本システム内で２（１）

の操作を行えること。

ウ　２（２）に示す導入箇所における本システムを利用する職員（以下「本システム利用者」という。）が設定された利用者アカウント毎に児相システムのアカウント情報を基にログインできる機能を有すること。また、複数の利用者アカウントが同時に本システムにログインし利用できること。

（２）個別機能要件（以下「本システム機能」という。）

ア　各種出力のための学習

(ｱ) 児相システム等に保存されている児童記録等データの読込（情報の連携）

児相システム内に保存されている児童記録等のデータを本システムにて読み込み、イ及びウの機能を実施するにあたって学習し参考にするよう設計すること。

情報の連携についてはAPI連携により定期的（日次）に実施することとする。

(ｲ) 関係法令等の読込

児童福祉法、児童福祉法施行令、児童福祉法施行規則、児童虐待の防止等に関する法律、児童虐待の防止等に関する法律施行令、児童虐待の防止等に関する法律施行規則、児童相談所運営指針その他こども家庭庁等が公表する関係通知・ガイドライン等を、出力時に参照すべき規範データとして読み込むこと。

読込データについては甲が準備し、試験稼働時に読込を実施すること。法令改正時点での改正に係るデータの読込実施は甲が行う。

イ　過去事例の出力

(ｱ) 本システム使用者が入力した内容（プロンプト）に応じ、該当する事例を児相システムから検索すること（プロンプト例：「○○を抱える児童で、○○により養育が困難になった事例を出力して」「市町の児童福祉部門と連携して支援に当たっているケースで、学校とも連携できている事例を出力して」等）。

(ｲ) 入力した内容に該当する事例について、事例の概要を要約して出力すること。

(ｳ) 複数事例出力することとし、入力した内容との該当割合が高い順に並べて出力すること。

(ｴ) 過去事例を要約し出力する際には、以下の要素を必ず含んで出力すること。

ａ　ケース番号

ｂ　ケースにおける家族構成・家族が抱える課題

ｃ　受理から現在（または直近の対応情報）に至るまでの経過

ウ　処遇案等の出力

(ｱ) 本システム使用者が入力した内容（プロンプト）に応じ、児相システムから学習した内容を基に指定した事例における処遇案等を出力すること。（プロンプト例：「ケース番号○○○の処遇案を作成して」）

(ｲ) 以下ａ～ｃの内容を含んだ処遇案を複数出力すること。

ａ　基本情報

(a)ケース番号

(b)児童氏名

(c)生年月日

(d)年齢
(e)所属（学校等）
(f)家族情報（家族構成）
(g)関係者（支援機関等）

b　ケースの概要
(a)主訴（概要及び受理時の相談概要等）
(b)ケース概要（現在または直近の対応情報に至るまでの経過）

c　処遇案
(a)処遇案の概要（児童・家族等への対応等）
(b)利点（メリット）
(c)欠点（デメリット）
(d)現在の課題
(e)関係機関との連携
(f)選定理由
(g)参照法令等

エ　各機能の連携について

本システム機能（ア～ウ）のうち、イ及びウについては本システム利用者が容易に操作できるよう児相システム改修業務受託業者※と連携し設計すること。

※児相システム改修業務受託業者：本システムの導入に伴い本システムとのAPI連携その他必要な改修（本業務の範囲外）を行う事業者で、甲が別途委託契約を締結するもの。本システム操作画面は主に児相システム改修業務受託業者が構築する。

（３）接続要件

ア　本システムは、３（４）イに記載の端末（以下「使用端末」という。）から、児相システムを介して利用するものとする。なお、児相システムは、甲が運用している栃木県共同利用型基盤（別添「栃木県共同利用型基盤環境」参照）上のインターネット接続領域（庁外ネットワークとの接続はない）にあり、職員は庁内ネットワークを介して使用端末から児相システムを利用している。

イ　児相システムと本システム間の通信（児童記録等の送受信等）は、閉域接続により行うものとする。なお、当該閉域接続の構築については４（８）エに定めるとおり、本業務の範囲外とし、別途、ネットワーク構築業務受託事業者が調達及び運用保守を行う。

ウ　児相システムと本システム間のAPI連携方法の詳細については、乙が基本設計等において提示し、甲、児相システム改修業務受託業者及びネットワーク構築業務受託事業者と協議の上決定する。

（４）規模・性能要件

ア　規模要件

(ｱ) 想定システム利用者及び想定データ量

導入箇所	想定利用台数	想定利用人数	想定データ量 （出力件数／年） ※過去事例出力及び処遇案出力
こども政策課	５台	５人	100 件
中央児童相談所	40 台	40 人	3,000 件
県南児童相談所	30 台	30 人	2,500 件
県北児童相談所	20 台	20 人	1,300 件

※出力１件あたりのプロンプトの文字数は 100 文字、出力結果は 1,500 字程度を想定。

(ｲ) システム稼働時間

24 時間 365 日（メンテナンスや計画停電等を除く）

イ　性能要件

(ｱ) 以下のシステムの利用環境（各導入箇所における標準仕様）において利用可能なシステムであること。

種別	項目	スペック
使用端末 （一人一台端末）	型名	ThinkPad X1 Carbon Gen9
	CPU	11th Gen Intel(R) Core(TM) i5-1135G7
	メモリ	８ＧＢ
	ストレージ	256GB
	ディスプレイ	14 インチ又は 23.8 インチ
	OS	Windows 11
	ブラウザ	Microsoft　Edge

(ｲ) 本システム機能において、レスポンス時間の目標値は以下のとおりとすること。

a　児相システム等に保存されている児童記録等データの読込

規定しない。

b　過去事例の出力

１分／１回

c　処遇案等の出力

１分／１回

（５）信頼性要件

乙は、本システムの信頼性要件として、以下の項目を遵守すること。

ア　定期メンテナンス等でシステムを停止する必要がある場合は、原則として２週間前までに、甲に対し通知を行うこと。停止時間帯については、可能な限り午前８時 30 分から午後５時 15 分までを除いて設定すること。

イ　障害発生時は、速やかに復旧させること。

また、その状況や復旧の見込み等について、甲に随時知らせること。

ウ　運用時における操作ミス、環境設定ミス、異常動作など様々な脅威からシステム及びデータを保護し、障害発生時の迅速な復旧に努めること。

エ　利用者の操作ミス等によるデータの不整合やシステム障害が発生しない設計・実装を行うこと。

オ　複数の利用者端末からの同時操作等により、処理停止等不具合が起きないよう設計・実装を行うこと。

カ　定期にデータベースのバックアップを行い、複数世代分のバックアップデータを保管すること。また、障害発生等の際、必要に応じてバックアップデータにより復旧させることができるよう設計すること。

（６）拡張性要件

乙は、本システムの拡張性要件として、以下の項目を遵守すること。

ア　利用者やデータ量の増加に対して、プログラムやファイル等の改修なく対応できるよう、データベースやファイル等の容量に余裕を持たせること。

イ　本システム導入後の法改正及び制度改正等による軽微な変更や、本システム機能の改善等に対応できる拡張性を持たせること。ただし、大幅な法改正や制度改正等についてはこの限りでない。

ウ　将来的に想定される本システム更新又は再構築に対応するため、システム移行及びデータ移行に配慮された設計とすること。

（７）情報セキュリティ要件

乙は、導入する本システムの情報セキュリティ要件として、以下の項目を遵守すること。

ア　セキュリティ対策

情報セキュリティマネジメントにかかる国際規格の認証（ISO/IEC27001 など）又はこれと同等の認証を取得しているなど、情報セキュリティ対策が確保されていること。

イ　通信回線対策

(ｱ) 不正通信の遮断

通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。

(ｲ) 通信のなりすまし防止

本システムにおけるなりすましを防止するために、サーバの正当性を確認できる機能を備えるとともに、許可されていない端末、サーバ装置、通信回線装置等の接続を防止する機能を備えること。

(ｳ) サービス不能化の防止

サービスの継続性を確保するため、本システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。

ウ　不正プログラム対策

(ｱ) 不正プログラムの感染防止

不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新

たに発見される不正プログラムに対応するために機能の更新が可能であること。

(ｲ) 不正プログラム対策の管理

本システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること。

エ　脆弱性対策

(ｱ) 構築時の脆弱性対策

本システムを構成するソフトウェアの脆弱性を悪用した不正を防止するため、設計時及び開発時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。

(ｲ) 運用時の脆弱性対策

運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、本システムを構成するソフトウェアの更新を効率的に実施する機能を備えるとともに、本システム全体の更新漏れを防止する機能を備えること。

オ　ログ管理

(ｱ) ログの蓄積・管理

本システムに対する不正行為の検知、発生原因の特定に用いるために、本システムの利用記録、例外的事象の発生に関するログを蓄積し、甲が指定する期間保管するとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。

(ｲ) ログの保護

ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能及び消去や改ざんの事実を検出する機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざんの脅威の軽減）のための措置を含む設計とすること。

(ｳ) 時刻の正確性確保

情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、本システム内の機器を正確な時刻に同期する機能を備えること。

カ　不正監視

(ｱ) 侵入検知

不正行為に迅速に対処するため、本システムで送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること。

(ｲ) サービス不能化の検知

サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。

キ　主体認証

本システムは、利用時に児相システムとの API 通信時に主体認証を実施すること。認証方式として API キーその他同等以上の安全性を有する方式とすること。

ク　アカウント管理

(ｱ) ライフサイクル管理

システム利用者のアクセス権を適切に管理するため、本システム利用時に児相システムのアカウント情報を読込み判別する機能を備えること。

(ｲ) アクセス権管理

本システムの利用範囲を利用者の職務に応じて制限するため、本システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。

(ｳ) 管理者権限の保護

本システムにおいて各種定義情報及びアカウント情報の管理等を行う管理者（２（２）におけるこども政策課職員を想定。以下「本システム管理者」という。）による不正を防止するため、管理者権限を制御する機能を備えること。

ケ　通信経路上の情報漏えい防止

(ｱ) 通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信内容を暗号化する機能を備えること。暗号化は適切なアルゴリズムを用いた処理を行うこと。

(ｲ) 端末認証や多要素認証、アクセスコントロール等の措置やインターネットVPN等の活用など、セキュリティ対策を実施すること。

コ　保存情報の機密性確保

本システムに蓄積された情報の窃取や漏えいを防止するため、アクセスを制限できる機能を備えること。また、保護すべき情報を本システム利用者が直接アクセス可能な機器に保存できないようにすることに加えて、保存された情報を暗号化する機能を備えること。

サ　保存情報の完全性確保

情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。

シ　情報の物理的保護

情報の漏えいを防止するため、記憶装置のパスワードロック、暗号化等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。

ス　侵入の物理的対策

物理的な手段によるセキュリティ侵害に対抗するため、本システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。

セ　ウイルス対策

使用するサーバにはアンチウイルスソフトを導入し、適宜ウイルスチェックを実施すること。

ソ　データセンター要件

本システムに入力された情報、出力した情報及びフィードバックや利用状況等については、日本国内のデータセンターで管理され、日本の裁判管轄、法令が適用されること。

タ　本システム利用終了後のデータ削除

本システム利用終了時には出力データ、アカウント情報等をはじめとした本契約に関わ

る全ての情報を復元不可能な状態に削除し、データ削除報告書を提出すること。

チ　構成装置の処分

委託業務で使用した本システムの構成装置が処分される際に、セキュリティを保った対応が行われること。

ツ　本システム外利用の禁止

本システムに入力された情報、出力した情報及びフィードバックや利用状況等については、本システム内での学習・改善にのみに使用することとし、システム外での利用・学習を行わないこと。

テ　その他

「栃木県情報セキュリティ基本方針」、「栃木県情報セキュリティ対策基準【秘密】」及び「クラウドサービス利用手順（第2.0版）【秘密】」に準拠し、適切なセキュリティ対策を実施すること。

（８）障害対策（事業継続対応）

ア　本システムの構成管理

情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の本システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する情報）を管理し、運用開始後の最新の構成情報及び稼働状況の管理を行うこと。

イ　本システムの可用性確保

サービスの継続性を確保するため、本システムの各業務の異常停止時間が復旧目標時間として１日を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。また、稼働率の目標を９９％とすること。

（９）サプライチェーン・リスク対策（不正プログラム等対策）

本システムの構築において、甲が意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。

(10) 利用者保護

ア　情報セキュリティ水準低下の防止

本システム利用者の情報セキュリティ水準を低下させないように配慮した上で本システムを提供すること。

イ　プライバシー保護

本システム利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。

(11) 試験要件

ア　基本方針

(ｱ) 本書で示す各種要件が満たされており、十分な品質が確保されていることを確認する試験を行うこと。

(ｲ) 試験に使用するデータは、甲が準備したものを用いること。その際、実際の運用に準

じた試験とすること。

イ　作業要件

(ｱ) 本番運用に準じた環境（以下「試験環境」という。）において、本システム機能が本書の内容および操作マニュアルどおりに動作することを、甲所属の本システム利用者（以下「試験実施者」という。）が確認すること。

(ｲ) 試験は、原則として試験実施者が主導して実施し、乙は試験環境の提供、操作支援、不具合対応及び結果の記録を行うこと。

(ｳ) 試験の実施方法は、オンライン会議等の遠隔方式による実施を含み、乙の現地常駐を必須としない。ただし、児相システムとの連携確認等、遠隔では確認困難な事項については、甲乙協議の上、必要な方法で確認すること。

(ｴ) 本書の情報セキュリティ要件を満たしていることを確認すること。

ウ　不良修正の扱い、原因の究明

試験中に不良が認められた場合には、その原因について調査・分析し、対応すること。

エ　試験稼働（利用者による操作確認）試験期間中、試験実施者が、操作マニュアルに基づき、業務に即したシナリオで本システムを自主的に操作し、画面・操作・出力結果等に問題がないことを確認できること。

乙は、試験実施者からの問合せに応じ、必要に応じて操作説明及び不具合対応を行うこと。

4　作業要件

（1）作業の体制及び方法

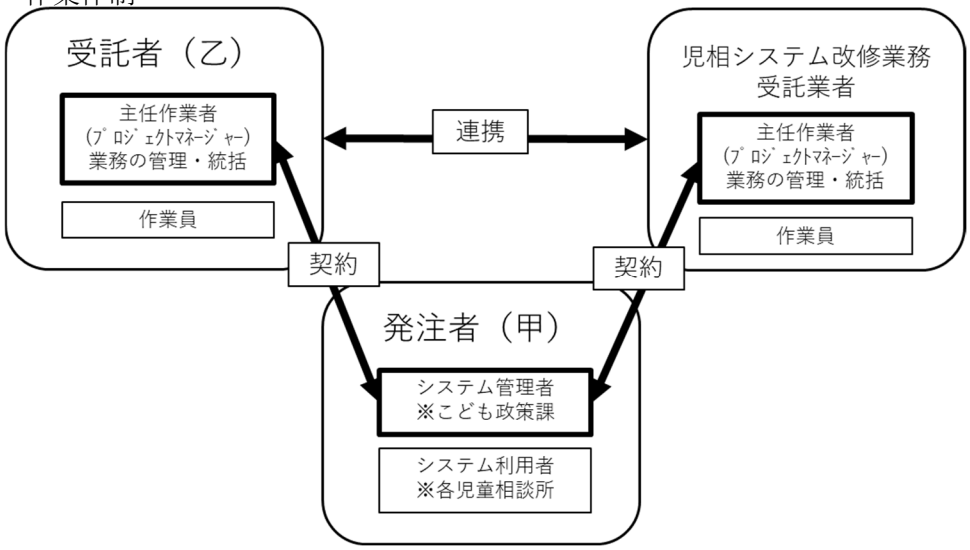
ア　必要となる資格

(ｱ) 乙は、過去５年以内に国又は地方公共団体のシステム設計・開発の履行実績を有すること。

(ｲ) 乙は、ISMS 又はプライバシーマークを取得している者であること。

(ｳ) 主任作業者は、IPA が公表している IT スキル標準Ｖ３のレベル４相当以上の能力を有し、かつ、本業務に係る情報システムの設計、開発、構築、運用又は保守を技術的に統括できる者を選任すること。

イ　作業体制



（２）運用保守作業要件

乙は、本システムの運用に関する計画、手続、評価における以下の作業を実施すること。

ア　運用計画の作成

運用支援作業に対する操作、問合せフロー、障害対応フローを作成すること。

イ　運用手順書の作成

運用操作マニュアル、問合せフロー、障害対応フローとして作成すること。

ウ　運用評価・改善

運用計画に基づき、定期的に運用結果を評価すること。

また、システム環境のチューニングを含む運用改善案を作成し、甲の承認の上、運用改善を実施すること。

エ　運用保守関連文書の作成方針

運用計画、運用手順書、問合せフロー、障害対応フロー等の運用保守関連文書は、乙が保有する標準テンプレートを基礎として作成し、本システムの構成・運用体制に合わせて内容を調整したものを納入すること。

ただし、本仕様書に定める事項を満たすことを条件とし、甲の業務実態に即した内容とすること。

オ　その他

乙は、リモートアクセス保守に際しては端末を限定するなど「栃木県情報セキュリティ対策基準【秘密】」及び「クラウドサービス利用手順（第2.0版）【秘密】」を遵守すること。

（３）マスターデータ設定

ア　本システムの運用開始に必要なマスターデータ（利用者情報等）の設定を行うこと。

イ　マスターデータの内容の作成・提供は甲、本システムへの設定及び設定内容の確認は乙が行うものとする。

ウ　マスターデータの項目、提供方法、設定手順その他詳細は、甲乙協議の上、設計書等に定めること。

（４）サポート体制

ア　作業時間

月曜日から金曜日（祝日、年末年始（１２月２９日～１月３日）を除く）の午前９時から午後５時（途中、１時間の休憩を含む）までを基本とし、運用保守を実施する。ただし、障害発生等の緊急事態には、甲と乙が協議の上、対応すること。

イ　対応

乙は、運用支援、保守業務を遂行するための体制を整備するものとする。

また、障害発生時の緊急事態に対応するため、可能な範囲内において甲と乙が常時連絡を取り合える体制を敷くこと。

ウ　インシデント管理

本システムに発生したインシデント（システムの不具合、機器の故障、エラー、警告メッセージの発生など）を検知した場合は、以下のとおり対応を実施すること。

(ｱ) 過去のインシデント情報を検索し、対策方法がある場合、回答又は解決方法を実施す

ること。ただし、システムへの侵入、ウイルス感染等、セキュリティに関するインシデントである可能性がある場合は、速やかに甲に報告すること。

(ｲ) 過去のインシデント情報を検索し、対策方法がない場合、緊急度、優先順位、影響範囲等を考慮して、問題管理にエスカレーションすること。

(ｳ) 発生したインシデント、その対応内容及び対応結果について記録を作成し、一元的に保管及び管理すること。

エ　問題管理

インシデント管理からエスカレーションされてきた事象について、速やかに甲に報告するとともに、以下のとおり、トラブルとして対応を実施すること。

(ｱ) 乙は、内容を確認し、関連事業者との責任分界点に従って「一次切り分け」として問題を切り分けること。問題の切り分けに当たって必要があれば、関連事業者に調査を依頼すること。

(ｲ) 障害の切り分け後、障害の該当箇所を担当している関連事業者に対して、原因の特定と問題解決に向けた対処を依頼すること。

(ｳ) 取得済みバックアップデータからのリカバリや手動による縮退運転移行等復旧作業をすること。

(ｴ) 障害が復旧するまで、作業内容を監理し、復旧したことを確認すること。早急に根本的解決ができない場合、甲の了承を得た上で、一時的な対応を実施すること。かつ、恒久的な解決策を策定又は関連事業者に依頼すること。

(ｵ) 一連の障害対応を取りまとめ、内容を資料として残し、定期的に問題発生の統計を取り、発生の傾向を分析して、甲に報告すること。

（５）問合せ対応

本システムの問合せ窓口を設け、本システム管理者からの電話またはメール等での問合せに対応すること。電話での対応時間は月曜日から金曜日（祝日、年末年始（１２月２９日～１月３日）を除く）の午前９時から午後５時（途中、１時間の休憩を含む）までを基本とし、メールでの受付は２４時間３６５日とすること。問合せ発生時には以下の作業を実施すること。

ア　問合せの管理問合せ

内容、回答内容、状況を管理すること。

イ　問合せの回答書作成

問合せの内容を確認し、回答書を作成すること。

（６）研修

試験稼働環境下において、甲及び本システム利用者に対し、操作マニュアルに基づいた説明を行うこと。

研修用テキスト及び研修時に使用するダミーデータ等については、乙が用意すること。ダミーデータ等を準備することが容易ではない場合は甲にその旨報告すること。

（７）マニュアル

乙は、本システムの操作運用に関わる以下のマニュアルを提供すること。マニュアルは本システム利用者向けのものと管理者向けのものをそれぞれ提供し、極力専門用語を使用せず

分かりやすい表現で記載すること。やむを得ず専門用語を使用する場合には、注釈等を付けること。また、内容は随時最新の状態に更新し、電子データで常に確認できるようにすること。

ア　利用者用操作マニュアル

本システム利用者用の操作マニュアルとして、各機能単位に操作の手順、入力方法等を明確に記述すること。誤って情報を登録した場合の修正方法等についても記述し、本システム運用開始後の本システムの操作に関する問合せを極力少なくするものであること。

イ　管理者用運用マニュアルシステム（運用保守マニュアル含む）

管理者を対象とした運用マニュアルとして、各種定義情報やユーザー情報等の管理方法、障害発生時の対応方法について記述すること。

（8）その他

ア　サービス利用環境

委託業務に使用する開発環境は乙の負担で準備し、業務期間内は保持すること。

イ　委託業務に係る機器及び使用材料の負担

委託業務の遂行に当たって必要となる運用機器、資材、消耗品等は乙が準備し、それにより発生した費用は乙が負担とする。

ウ　資料提供

乙は、委託業務の遂行に当たり、現行事務にかかわる規程、マニュアル等の資料について、閲覧の必要が生じたときは甲に依頼するものとする。甲は、乙から依頼があり、必要と認めたときは対応する。

エ　本システムの導入に係る児相システムの改修業務及びネットワーク構築業務は本業務の範囲外とし、別途甲が選定する事業者に委託するものとする。乙は、本システムの開発に際しては児相システム改修業務受託業者及びネットワーク構築業務受託事業者と連携し、本システムの円滑な稼働に向けて協力するものとする。

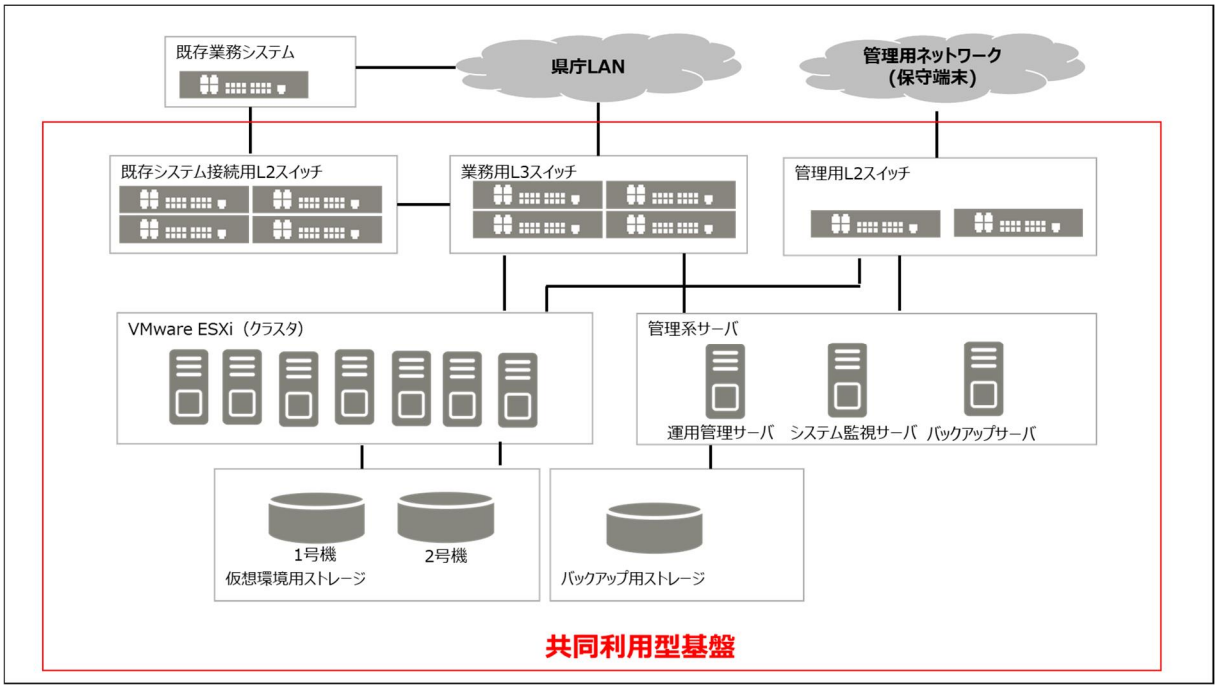
5　その他

この仕様書に定めのない事項については、随時協議すること。

栃木県共同利用型基盤環境

（別添）

ア　概略図



栃木県共同利用型基盤概略図

イ　VMware ESXi（クラスタ）

仮想マシンを稼働させるクラスタ。

７台の仮想サーバで構成されており、ＨＡ機能及びＤＲＳ機能が仮想マシンに適用される。

ウ　仮想サーバ

クラスタ	**構成台数：7 台**		
CPU	メモリ	内蔵ディスク	ネットワーク
インテル® Xeon® Gold 6354 プロセッサー×2 （3GHz、18 コア）	512GB 32GB3200 RDIMM×16	300GB ×3 2.5inch SAS10Krpm/12Gbps	10GBase T×10 Port 1000BASE-T×4 Port

エ　機能

栃木県共同利用型基盤で提供する機能については以下のとおりである。

・バックアップは日次バックアップ7世代を取得する。ただし、データベースの静止点を考慮しないバックアップであるため、必要に応じて業務システム側でデータバックアップを取得すること。

・ファイアウォールは各仮想マシンに実装するインターフェースに対して、VMware NSXによる仮想ファイアウォールを提供する。提供方式はホワイトリストによる通信許可設定を行う。通信に関する設計は業務システムを構築する業者が行い、

設定は県が行う。

・ロードバランサはVMware NSXによる仮想ロードバランサを提供する。提供方式はラウンドロビンによる負荷分散とし、暗号化（SSL通信）は行わない。負荷分散に関する設計は業務システムを構築する業者が行い、設定は県が行う。

・アンチウィルスはTrend Micro Deep Securityにて提供する。定時スキャンのスケジュール設定などスキャンポリシーの設定は一律とし個別変更は行わない。

・データベースはOracle Database Standard Edition 2のライセンスを提供する。インストール作業については、業務システム構築業者で行うこと。

※上記のデータベースソフトではなく、Oracle Database Enterprise Editionが必要な場合や、その他のデータベース製品を使用する場合は業務システム構築業者で用意すること。

オ　システム構築環境

業務システムの構築作業は基本的に以下の手順で行う。

① 県にて払い出した仮想マシンを、業務システム構築業者にて用意する仮想環境に取り込んで構築を行う。ただし、庁内でのシステム開発作業は行わない。

② 構築完了後は、OVF形式のファイルに変化したものを、県に受け渡す。

③ 県にて事前に取り決めた仮想マシンのリソース状況と差異が無いことを確認後、共同利用型基盤に取り込む。

④ 取り込み後は、システム保守室を含む県重要機能室に設置する管理用PCからメンテナンスを行う。