日立市ＤＸ基盤構築事業　仕様書

1　業務の目的

庁内ネットワークは、職員の業務遂行及び市民サービスを支える重要な基盤であり、その構成の在り方によって、業務効率や提供できるサービスの範囲が大きく左右される。

本市では、平成 27 年に策定された国の情報セキュリティポリシーに関するガイドラインに基づき、業務データがインターネットへ流出しにくいネットワーク基盤を、新庁舎への移転時（平成 29 年）に構築し、個人番号利用事務系（以下、「基幹系」という。）、LGWAN 接続系（以下、「情報系」という。）、インターネット接続系を分離するいわゆる三層分離モデル（αモデル）を採用してきた。

一方で、コロナ禍以降、オンライン会議やチャットツールを活用した新しい働き方が急速に普及するとともに、生成 AI をはじめとする高度なインターネットサービスの活用が進展している。こうした社会情勢を踏まえ、国においては、今後の行政事務の遂行においてインターネットの利用が不可欠であるとの判断の下、令和２年及び令和５年に情報セキュリティポリシーの改定を行い、インターネットをより柔軟かつ安全に活用できる新たなＤＸ基盤モデルを示している。

これを受け、県内においては、茨城県をはじめ、県内市町村がＤＸ基盤の構築・検討を進めている状況にある。

本市においても、今後の業務効率化や行政経営改革を一層推進していくためには、インターネットの積極的な活用が不可欠である。特に、電子決裁等の内部事務について、場所を問わず円滑に実施できる環境を整備することは、職員の生産性向上のみならず、限られた人的資源を市民サービスの充実に振り向ける上でも極めて有効である。

こうした背景を踏まえ、市では、国の情報セキュリティポリシーガイドライン改訂版に沿った新たなＤＸ基盤を構築し、庁内ネットワーク環境の見直し・高度化を図ることとした。本件は、その基盤となる庁内ネットワークを再構築し、将来にわたり持続可能な行政運営を支える土台を整備するものである。

2　市の現状・課題

(1)　本庁舎ネットワーク機器の老朽化への対応

本市の本庁舎に設置されているネットワーク機器は、庁舎建設時に導入されたもので

あり、今後、順次メーカー保守期間の終了を迎える状況にある。

保守終了後は、機器故障時の迅速な復旧やセキュリティ上の脆弱性への対応が困難となり、庁内業務の継続性や安定性の確保に支障を来すおそれがある。このため、庁内ネットワークの中核を担う機器について、計画的な更新を行うとともに、将来の業務変化も見据えた基盤全体の再構築が必要となっている。

(2)　庁内パソコン利用環境における機動性の不足

現在の庁内パソコン利用環境は、有線接続を前提とした運用が中心となっており、会議や打合せの都度、会議室への移動に伴う配線作業や接続設定が必要となっている。このため、会議準備に時間を要し、業務の円滑な遂行を妨げる要因となっている。

また、無線通信を利用できるパソコンが限られていることから、会議室等におけるオンライン会議の実施が制約され、場所を問わない柔軟な働き方や迅速な意思決定を十分に支えられていない状況にある。

(3)　内部事務システム利用に係るネットワーク構成上の制約

税務や福祉等の基幹系業務で使用するパソコンから、電子決裁システムや庁内イントラネット等の内部事務システムへの接続が円滑に行えず、日常的な事務処理において非効率が生じている。

加えて、基幹系パソコンからはインターネットを利用することができないため、制度改正時の情報収集や関係資料の確認等において業務の流れが分断されているほか、情報系パソコンと基幹系パソコン間のデータの受け渡しに USB メモリ等の可搬媒体を用いる必要があり、作業効率の低下に加え、情報セキュリティ上のリスクも内在している。

また、こうした環境制約により、財務会計システム等の内部事務システムにおいても、近年活用が進みつつある AI 技術等を業務の効率化や高度化に十分活用できていない状況にある。

(4)　災害時における市民サービス継続手段の不足

原子力災害時における広域避難など、庁舎外での業務実施を余儀なくされる事態を想定した場合、現行の通信環境では、基幹系システムを利用しながら市民サービスを継続するための仕組みが十分に確立されていない。

また、税申告受付等の出張業務を行う際には、専用線の敷設が必要となり、準備に時間とコストを要するなど、迅速かつ柔軟な対応が困難な状況にある。このため、災害時においても市民サービスを継続的に提供できるよう、平時・非常時を問わず、庁外から

安全に基幹系システムを利用可能とする通信手段及び利用環境の整備が求められている。

(5)　国が示す新たな情報セキュリティモデル（α’モデル）への対応

国が示す「地方公共団体における情報セキュリティ対策の新しいモデル（α’モデル）」では、従来のようにLGWANを経由してインターネットへ接続する構成に加え、各拠点から直接インターネットへ接続する「ローカルブレイクアウト（LBO）技術」の活用が想定されており、インターネット通信の効率化やクラウドサービスの円滑な利用が求められている。

しかしながら、本市の現行ネットワーク構成は、LGWAN経由を前提とした設計となっており、α’モデルにおいて想定されているLBO技術を適用した構成に対応していない。このため、今後、クラウドサービスの本格的な活用を進めるに当たり、構成上の制約が生じるおそれがある。

このことから、将来的な技術動向等への柔軟な対応を可能とするため、α’モデル等を前提とした通信構成への対応を見据えたネットワーク基盤の整備が必要となっている。

3　業務方針

(1)　本業務は、前項に示した本市の現状及び課題を踏まえ、本市の業務を支えるＤＸ基盤について、安定性及び安全性を確保しつつ、将来的な制度改正や業務変化に柔軟に対応可能な構成とすることを基本方針とする。

(2)　国の指針及び自治体ＤＸの方向性を踏まえ、標準化・効率化及び運用負荷の軽減を図る。

(3)　業務の遂行に当たっては、本市との十分な協議及び情報共有の下、確実かつ円滑な構築・移行を行うものとする。

4　本業務の前提条件及び制約事項

(1)　本市の基幹系及び情報系システムは、既存のセキュリティ対策、運用体制、認証・端末管理方式等が相互に連携した構成となっている。

(2)　本業務は、これら既存構成の全面刷新を目的とするものではなく、現行構成を前提として安定的な運用を継続するための更新・拡張を目的とするものである。

(3)　このため、一部の業務においては、既存構成との互換性、運用継続性及びセキュリティ確保の観点から、仕様書に明示する範囲に限り、特定の方式を指定する。

5　履行期間

契約締結日から令和 15 年 7 月 31 日まで（賃貸借期間を含む。）

なお、各業務内容について個別契約を締結し、契約期間は各契約に準ずるものとする。

6　業務内容

(1)　業務概要

２に示した市の現状及び課題を踏まえ、受託者は次の業務を行うこと。

なお、以下の各業務には、設計・構築に加え、円滑かつ的確な運用を行うために必要な運用支援及び保守対応を含むものとする。

ア　ＤＸ基盤構築事業　設計業務

イ　本庁舎ネットワーク機器更新

ウ　庁内パソコン完全無線化

エ　基幹系転送ネットワーク改善・基幹系インターネット接続システム

オ　基幹系⇔情報系ファイル共有

カ　BCP 対策通信機器整備

キ　α’モデル通信機器整備

(2)　規模

通信量等の積算に用いるユーザー数及び端末数等については、以下を利用すること。

ア　ユーザー数及び端末数

(ｱ)　通常時

ネットワーク系統	ユーザー数	端末数
情報系 （内　本庁舎分）	1120 人 （620 人）	1120 台 （620 台）
基幹系 （内　本庁舎分）	480 人 （360 人）	480 人 （360 人）

(ｲ)　災害発生時（又は、平時の出張業務実施時）

ネットワーク系統	ユーザー数	端末数
基幹系	20 人	20 台

イ　利用する主な業務システム

ネットワーク系統	業務システム	ユーザー数（同時接続数）
情報系	グループウェア	1600 人（1000 接続）
	財務会計システム	1600 人（200 接続）
	人事給与システム	1600 人（200 接続）
	文書管理システム	1600 人（200 接続）
基幹系	住民記録システム、税・福祉関係システム基幹系業務システム	480 人（480 接続）

※　各業務システムは、原則としてブラウザベースのシステムであり、主に画面表示や画面遷移に伴う通信が中心となることから、常時大容量の通信を必要とするものではない。ただし、帳票出力や PDF 等のファイルダウンロード（最大１ファイル 10MB 程度）を行う場合には、一時的に通信量が増加することがある点に留意すること。

ウ　その他各種参考数値等

(ｱ)　外部記憶媒体

登録数	1200 個
主な使途（１処理に要する時間）	基幹系 PC と情報系 PC のデータの受渡し（１処理約５分）
平均利用頻度	基幹系ユーザー１人あたり　３回／日

(ｲ)　現行の基幹系転送ネットワーク

ユーザー数	480 人

※４台の情報系サーバーを、約 480 人のユーザーが同時に共有利用している。サーバーの CPU、メモリ、ストレージ I/O 及びネットワーク帯域が輻輳しやすい構成となっており、リソース競合に起因する処理遅延や接続不安定、障害が発生している。

(ｳ)　広域避難時・出張業務（税申告）※の想定規模

利用端末数	PC15 台、プリンタ４台
利用するネットワーク系統	基幹系、情報系、インターネット系

※出張による税申告支援業務において、1 会場あたりおおむね３日間（計７会場）の運用を行い、会場を移動しながら対応しているが、その都度ネットワーク配線および機器の設置・撤収作業が発生しており、職員の作業負荷が大きい。

7　業務仕様及び技術要件

(1)　DX 基盤構築事業　設計業務

ア　目的

本業務は、本市における DX 基盤構築事業全体について、個別システムや機器更新を部分最適に終わらせることなく、将来的な拡張性、運用性及び情報セキュリティを考慮した全体最適の観点から設計を行うことを目的とする。

イ　業務範囲

本設計業務は、以下に記載する次の全事業を対象とする。

なお、各業務の構築開始前に、設計業務を完了し、市の承認を得ること。

- 本庁舎ネットワーク機器更新
- 庁内パソコン完全無線化
- 基幹系転送ネットワーク改善・基幹系インターネット接続システム
- 基幹系⇔情報系ファイル共有
- BCP 対策通信機器整備
- α'モデル通信機器整備

ウ　設計内容

(ｱ)　本市から提示される制約条件及び国の指針を踏まえ、DX 基盤全体の論理構成及び物理構成を設計すること。

(ｲ)　情報系、基幹系及びインターネット接続系の論理分離及びセキュリティ境界を明確にした構成を設計すること。

(ｳ)　端末数の増加、クラウドサービスの利用拡大等を想定し、将来的な拡張が可能な構成を設計すること。

(ｴ)　各事業に共通する設計方針、前提条件及び制約事項を整理し、各個別事業の整合性を確保すること。

(ｵ)　既存環境から新環境への移行にあたり、業務影響を最小限に抑える移行・切替方針を策定すること。

(ｶ)　通信帯域、同時接続数等について、現行及び将来の利用規模を踏まえた要件を整理すること。

(ｷ)　ネットワーク及び主要機器について、冗長化方針及び障害時の復旧方針を整理すること。

(ｸ)　運用体制、役割分担、平常時及び障害時の対応方針を整理すること。

(ｹ)　国の地方公共団体における情報セキュリティポリシーに関するガイドライン及び本市の情報セキュリティポリシーに基づき、必要な対策方針を整理すること。

(ｺ)　国の地方公共団体における情報セキュリティポリシーに関するガイドラインに基づき、本市が実施する情報セキュリティに係る外部監査及び自己点検に対応するため、監査の考え方、実施時期、対象範囲及び必要となる情報（ログ、構成情報、運用記録等）を整理し、監査計画として設計すること。

エ　成果物

(ｱ)　DX 基盤全体構成図

(ｲ)　各事業に係る設計書（概要設計レベル）

(ｳ)　運用設計書（役割分担、平常時・障害時対応）

(ｴ)　監査計画書（外部監査及び自己点検に係る対象範囲、実施時期、確認項目の整理方針、必要資料の整理等）

(2)　本庁舎ネットワーク機器更新

ア　目的

本庁舎に設置されている情報系及び基幹系ネットワーク機器について、老朽化への対応及び安定的なネットワーク運用を実現するため、機器の更新及び付随作業を行う。

イ　機能要件

(ｱ)　情報系及び基幹系ネットワークについて、コア、サーバー、フロア各階層のスイッチを更新すること。

(ｲ)　更新後のネットワークにおいて、VLAN、IP アドレス及びルーティング設定を適切に行い、現行業務を継続できること。

(ｳ)　切替作業において、業務影響を最小限に抑えた手順で実施できること。

(ｴ)　全職員がストレスなく業務を行えるネットワーク環境を構築すること。

ウ　非機能要件

(ｱ)　性能

10GbE 対応ポートを備え、将来的な通信量増加に対応できること。

(ｲ)　可用性

コアスイッチは冗長構成とし、機器障害又は回線障害が発生した場合においても、

単一障害点を排除し、業務継続が可能であること。

(ｳ) 運用保守

・ 保守期間は 84 か月とし、平日午前 9 時から午後 5 時までのオンサイト保守を受けられること。

・ ネットワーク機器の稼働状況、ポート利用状況及びトラフィック状況を把握できること。

・ 障害発生時において、影響範囲の特定、原因分析及び復旧対応を迅速に行える運用体制を確保できること。

・ 設定変更、機器交換及び構成変更について、管理者が計画的かつ容易に実施できること。

・ 構成図、設定内容、切替手順及び運用手順等のドキュメントを整備し、継続的で属人化しない運用が可能であること。

(ｴ) セキュリティ

・ ネットワーク機器の管理アクセスについては、適切な認証方式を用い、管理者権限を厳格に制御できること。

・ 不要な通信や不正なアクセスを防止するため、ポート制御、VLAN 制御等のネットワークレベルのセキュリティ対策を講じられること。

・ 設定変更履歴及び管理操作ログを取得・保管し、事後的な確認に対応できること。

(ｵ) 監視

・ 本業務で構築したネットワークについて、24 時間 365 日、監視ツール等を用いた稼働監視を行うこと。

・ 監視内容は、死活監視・ハードウェア監視を基本とすること。

・ 事前の協議で設定した閾値を超えた場合、監視ツール等から、市及び受託者へ即時メール通報すること。

・ 監視状況、監視結果について管理画面等を用いて確認できること。

(ｶ) その他

認証及びアクセス制御については、現行の「Account＠Adapter」との互換性を確保すること。

(3)　庁内パソコン完全無線化

ア　目的

本庁舎内の全てのパソコンを無線化し、場所を移動しても作業やオンライン会議を行うことができる環境を整備し、事務効率化と移動作業の負担軽減を図る。

イ　機能要件

(ｱ)　無線 LAN を用いて、本庁舎内の業務端末（情報系及び基幹系）が安定的に業務システムへ接続できること。

(ｲ)　本庁舎内であれば、利用場所の変更に伴う設定変更を必要とせず、職員がストレスなく業務を行えること。

ウ　非機能要件

(ｱ)　性能

全職員が同時に接続した場合においても、業務に支障を来すことのない十分な通信性能を確保できること。

(ｲ)　可用性

無線コントローラ等は冗長化され、単一障害時にも通信を継続できること。

(ｳ)　運用保守

・　管理システムにより、アクセスポイントの稼働状況、接続状況及び障害の有無を一元的に把握・管理できること。

・　電波干渉や通信品質の低下が発生した場合に、原因の特定及び設定変更等の対応を迅速に行える運用体制を確保できること。

・　アクセスポイントの増設、移設又は設定変更について、業務影響を最小限に抑えつつ、管理者が容易に対応できること。

・　障害発生時において、影響範囲の把握、原因分析及び復旧対応を円滑に実施できること。

・　構成図、設定内容及び運用手順等のドキュメントを整備し、継続的かつ安定した運用が可能であること。

(ｴ)　セキュリティ

・　利用端末は、職員が業務で使用する市の管理下にある端末に限定し、端末認証を必須とすること。

・　無線通信については、強固な暗号化方式を採用し、通信内容の盗聴及び改ざん

を防止できること。

・　不正な端末接続やなりすましを防止するため、利用者認証及び端末認証を組み合わせたアクセス制御を実施できること。

・　不正アクセスポイントや異常な通信を検知し、管理者が把握・対応できる仕組みを有すること。

・　セキュリティ設定の変更履歴及び接続ログを取得・保管し、必要に応じて確認できること。

(ｵ)　監視

・　本業務で構築したネットワークについて、24 時間 365 日、監視ツール等を用いた稼働監視を行うこと。

・　監視内容は、死活監視・ハードウェア監視を基本とすること。

・　事前の協議で設定した閾値を超えた場合、監視ツール等から、市及び受託者へ即時メール通報すること。

・　監視状況、監視結果について管理画面等を用いて確認できること。

(4)　基幹系転送ネットワーク改善・基幹系インターネット接続システム

ア　目的

基幹系パソコンからの情報系業務システム（グループウェア、電子決裁等）及びインターネット接続について、安全性と効率性を両立した通信環境を整備する。

イ　機能要件

(ｱ)　基幹系と他のネットワーク間の通信経路を明確に分離し、制御できること。

(ｲ)　情報系業務システムやインターネットを、職員がストレスなく利用できること。

(ｳ)　簡易に運用管理が行えるシステムを提供すること。

ウ　非機能要件

(ｱ)　性能

情報系業務に影響を与えない通信遅延水準等を確保できること。

(ｲ)　可用性

通信回線及び装置は冗長構成とし、単一障害点を排除できること。

(ｳ)　運用保守

・通信状況、接続状況及びトラフィック量等を継続的に把握・監視できること。

・不正通信検知や事後確認を目的として、通信ログ及び接続履歴を取得し、一定期

間保管できること。

・障害発生時において、影響範囲の把握、原因特定及び復旧対応を迅速に行える運用体制を確保できること。

・利用者数の増減や通信条件の変更等について、管理者が容易に設定変更を行えること。

・市職員の運用管理において、専門的な作業を極力必要としない運用負荷の低い構成であること。

(ｴ) セキュリティ

・ 基幹系と情報系及びインターネット間の通信について、通信経路及び通信内容に応じた厳格なアクセス制御を実施できること。

・ 不正通信、異常なトラフィック又は不審な挙動を検知し、管理者が把握の上、遮断等の対応を行えること。

・ マルウェア感染や情報漏えいにつながる通信を抑止するため、通信内容又は通信先に基づくセキュリティ対策が講じられること。

・ 通信ログ及びセキュリティイベントログを取得・保管し、インシデント発生時に追跡・分析が可能であること。

・ セキュリティポリシーの変更履歴を管理し、運用上の統制が確保されること。

(ｵ) その他

インターネット接続については、現行の「SKYSEA Client View 環境分離　ブラウザ」を継続利用する。

(5) 基幹系⇔情報系ファイル共有

ア 目的

基幹系と情報系間で必要なファイルを、安全かつ効率的に共有できる環境を整備する。

イ 機能要件

(ｱ) 全利用者が、USB メモリ等の外部記憶媒体を介することなく、基幹系ネットワークと情報系ネットワーク間のファイル共有を安全に行えること。

(ｲ) ファイルの受渡し履歴を確認できること。

ウ 非機能要件

(ｱ) 性能

日業業務で利用されるファイルサイズを想定した転送性能を確保できること。

(ｲ) 可用性

障害発生時にもデータ消失を防止できること。

(ｳ) 運用保守

・ 利用者毎の利用状況（送受信回数、ファイル容量等）を把握・管理できること。

・ ファイル共有に係る操作ログ及び受渡し履歴を一定期間保管し、必要に応じて確認できること。

・ システム設定変更や利用者追加・削除等の運用作業を、管理者が容易に実施できること。

(ｴ) セキュリティ

不正なデータ持ち出しを防ぐため、アクセス制御が実施されること。

(ｵ) その他

現行の資産管理システム「SKYSEA Client View」と連携できること。

(6) BCP 対策通信機器整備

ア 目的

災害時等においても、広域避難先等から市の業務を継続できる BCP 対策通信機器を整備する。

イ 機能要件

本庁舎のネットワークを延伸し、パソコンやプリンタを移設するだけで業務を継続できる環境を整備すること。

ウ 非機能要件

(ｱ) 性能

災害時の想定利用シーン（罹災証明書の発行等）に必要な通信品質を確保できること。

(ｲ) 可用性

災害時であっても、本庁舎（サーバー室）の電源が確保されている限り、通信ができること。

(ｳ) 運用保守

・平時において、機器の起動確認、通信確認等の定期的な動作確認を実施できること。

・災害発生時を想定した接続手順及び利用手順を明確化し、職員が円滑に利用できるよう訓練を実施できること。

・機器の設置場所、保管状況及び設定情報を適切に管理し、非常時に速やかに利用開始できる体制を確保できること。

・障害や不具合が発生した場合に、原因の把握及び復旧対応を迅速に行える運用体制を確保できること。

(ｴ) セキュリティ

非常時通信においても情報漏えい対策が講じられること。

(7) α'モデル通信機器整備

ア 目的

特定のインターネットサービスを、安全・快適に利用することができる日立市専用ハイウェイ（ローカルブレイクアウト）を導入する。

イ 機能要件

α'モデルに基づくネットワーク構成を実現できること。

ウ 非機能要件

(ｱ) 性能

- α'モデルにおいて、Microsoft 365 等の各種クラウドサービスを全職員がストレスなく利用できること。
- 各種業務システムと、外部のクラウドサービス（生成 AI を活用したサービスを含む）との連携が可能であること。

(ｲ) 可用性

構成機器を冗長化し、安定稼働できること。

(ｳ) 運用保守

- 将来的なクラウドサービスの追加や利用拡大、職員数の増減等を想定し、ネットワーク構成や通信設定の変更に柔軟に対応できること。変更は、見積額の範囲内で対応すること。
- 通信ポリシー、ルーティング、セキュリティ設定等について、管理者が容易に変更・管理できること。
- 障害発生時において、影響範囲の把握、原因特定及び復旧対応を迅速に行える運用体制を確保できること。

・　構成図、設定内容及び運用手順等のドキュメントを整備し、継続的かつ安定した運用が可能であること。

(ｴ)　セキュリティ

国の地方公共団体における情報セキュリティポリシーに関するガイドラインに準拠した対策が実施されること。

(ｵ)　監視

・　本業務で構築したネットワークについて、24 時間 365 日、監視ツール等を用いた稼働監視を行うこと。

・　監視内容は、死活監視・ハードウェア監視を基本とすること。

・　事前の協議で設定した閾値を超えた場合、監視ツール等から、市及び受託者へ即時メール通報すること。

・　監視状況、監視結果について管理画面等を用いて確認できること。

8　信頼性要件

(1)　可用性

ア　本業務で構築する各システム及びネットワークについて、計画停止及び事前に合意されたシステムメンテナンス時間を除き、年間稼働率 99.9%以上（SLA）の達成を目標とした設計とすること（具体的な SLA の定義、算定方法、免責条件については、下表の SLA 要件のとおり。）

イ　下表の SLA 要件を達成するため、業務に影響を与えるおそれのあるシステム及びネットワーク機器については、冗長化、フェイルオーバー等の対策を講じ、システム停止時間を最小限に抑えられる構成とすること。

(2)　性能・拡張性

ア　利用者数や通信量の増加等に伴う各種機器、回線等の増強について、最小限の業務影響で対応できるよう、システムの拡張性を確保すること。

イ　データ量の増加等により性能が低下しないよう、負荷分散方式等を適切に組み込むこと。

表　SLA 要件

No	区分	概要
1	サービスレベルに関する合意	利用者への継続的・安定的なサービスの提供を円滑に行うため、受託者と市の役割、必要な管理項目とサービスレベル管理指標の目標値及び未達の際のペナルティ等について市と協議の上、SLA として明文化すること。
2		サービスの品質を確保するため、受託者は具体的な SLA の項目や管理指標、目標値について提案すること。
3		SLA の内容については、次の点に留意すること。 ①　受託者との役割を明確にすること。 ②　費用を考慮してサービスレベル管理指標の目標値等を設定すること。 ③　SLA 達成状況を管理し月次で市に報告すること。また、必要に応じサービス内容を改善すること。
4	サービスレベルの内容	SLA を設定する項目及び目標値としては、以下の内容を想定している。 ここでいう「障害」とは、故障やプログラムのバグ等により、一部サービスの停止や著しいレスポンス低下が発生し、業務に支障を来す事象を指すものとする。 ただし、クラウドサービス及び本業務の範囲外となるハードウェア・ソフトウェア・ネットワークに起因する障害については、本 SLA の対象外とする。 また、サービスが停止していない場合であっても、通常時と比較して明らかなレスポンス低下が発生し、複数の利用者から業務に支障が生じている旨の申告があり、当該状態がおおむね 20 分以上継続した場合には、本項における「障害」に該当するものとして取り扱う。 ①可用性 サービス提供期間は 24 時間 365 日とし、計画停止及び事前に合意したメンテナンス時間を除き、稼働率 99.9%を目標とする。 ②障害対応 障害を検知してから 1 時間以内に対応に着手すること。 また、現地での対応が必要と判断された場合は、その必要性を認識してから 4 時間以内に現地へ駆け付け対応を行うこと。 ③目標復旧時点 障害発生時点から遡り、直近 24 時間前の状態へ復旧できること。
5	サービスレベルの評価期間	サービスレベルの評価は、庁内ネットワーク基盤の運用開始後からとする。

No	区分	概要
6	サービスレベルの達成状況評価	サービスレベルを設定した項目に対し、実績を運用・保守報告会議で報告し、市と協議の上、サービスレベル達成状況を評価すること。
7		サービスレベルを達成できなかった場合、返金対応等は行わず運用保守費用から相殺すること。
8	改善の実施	サービスレベル目標値が達成できていない場合は、速やかに改善策及び改善実行計画を検討し、市の承認を得た後、改善を実施すること。
9		改善の実施に当たっては、その改善実行ログを取得し、改善の効果、サービスレベル目標値への影響度を分析の上、サービスレベル目標値に達成できる改善がなされるまで月次で報告すること。
10		改善に必要な人的リソースの追加、体制の変更、改善のために必要なシステム・仕組みの導入等に費用がかかる場合は、市と協議の上対応方針と費用負担者を決定し、実施すること。

9　情報セキュリティ及びガバナンス要件

(1)　情報セキュリティ及びガバナンス

ア　本業務の実施に当たっては、国の地方公共団体における情報セキュリティポリシーに関するガイドライン等を踏まえ、情報資産の機密性・完全性・可用性を確保すること。

イ　受託者は、本業務の設計・構築・運用支援に当たり、発注者の情報セキュリティ統制が有効に機能するよう、体制、役割分担、手順等の明確化を支援すること。

(2)　委託・クラウド利用時の責任分担

ア　クラウドサービスを利用する場合においても、情報セキュリティに関する最終責任は発注者に帰属する。責任分担を明確化し、必要事項を整理・説明すること。

イ　受託者は、クラウドサービス提供事業者との責任分担（責任共有モデル）を明確化し、発注者に対し、以下の事項を説明・整理すること。

- 発注者が管理・設定すべき事項
- 受託者が実施する設定・運用事項
- クラウドサービス提供事業者が担う責任範囲

ウ　受託者は、クラウドサービスの利用に当たり国の地方公共団体における情報セキュリティポリシーに関するガイドライン等に準拠したセキュリティ対策が講じられていることを確認し、必要に応じて、発注者に説明資料を提出すること。

(3)　ログ管理及び監査対応

ア　利用者操作ログ、管理者操作ログ、システムログを取得すること。

イ　ログの保存期間、保存方法、参照権限については、発注者と協議の上、適切に定めること。

ウ　受託者は、発注者が実施する情報セキュリティ監査、自己点検及び関係機関からの確認等に対応できるよう、必要なログ、構成情報、運用資料等を適切に整備・提供すること。

(4)　情報セキュリティインシデント対応

ア　情報セキュリティインシデント発生時は、速やかに報告し、初動対応・原因分析・再発防止を支援すること。

イ　情報セキュリティインシデントに関する報告手順、連絡体制等については、運用設計の中で整理し、発注者の承認を得ること。

ウ　攻撃の兆候を早期に把握できるよう、検知及び被害拡大を抑止するための仕組みについて整理し、必要な対応を行うこと。

(5)　ガイドライン改定対応

履行期間中に、国の地方公共団体における情報セキュリティポリシーに関するガイドライン等が改定された場合は、発注者と協議の上、必要な対応を行うこと。

10　作業要件

(1)　プロジェクト管理方針

ＤＸ基盤構築スケジュールを確実に履行するため、プロジェクト管理を徹底すること。

ＤＸ基盤構築作業におけるプロジェクト管理の方針は、次のとおりとする。

ア　受託者は、プロジェクト計画を立案し、市の承認を得た上で構築を進めること。

イ　構築作業における進捗状況や発生した問題等は、随時、市に報告・協議の上、対応方針を策定すること。

ウ　本業務により既存事業者と調整が必要な既存環境の設定変更、各種テスト等の作業に当たっては、関係事業者と連携・協力して実施すること。

(2)　プロジェクト計画書

受託者は、契約締結後、速やかにプロジェクト計画書案を作成し、市へ提出すること。提出されたプロジェクト計画書案を基に市と協議し、プロジェクト計画書として

承認を得た上でプロジェクトを遂行する。作成するプロジェクト計画書には、以下の内容を含めること。

No	記載事項	詳細
1	プロジェクト基本方針	プロジェクト憲章、プロジェクトの実施方針を記載すること。
2	スコープ定義・作業項目定義	・本業務における作業スコープを明確にすること。 ・作業項目を策定し、市と受託者の役割分担を明確にすること。
3	全体工程表	・市が想定する「12　スケジュール」を考慮した工程表を作成すること。 ・マイルストーンを明確にすること。 ・市及び受託者並びに関係者が、いつまでに何をやるのかを明確にすること。 ・各作業項目の開始時期・終了時期を明確にすること。
4	プロジェクト体制・作業員名簿	・体制図を作成して構築体制を明確にすること。 ・各チームリーダを明確にすること。 ・プロジェクト内の業務分担を明確にすること。 ・構築環境、運用環境、構築場所等を明確にすること。
5	工程定義・工程終了条件	各工程の終了条件や成果物、承認者を明確にすること。
6	プロジェクト管理	・スコープ管理を明確にすること。 ・仕様変更管理方針を明確にすること。 ・各工程の進捗管理方針を明確にすること。 ・要員管理方針を明確にすること。 ・課題管理方針を明確にすること。 ・リスク管理計画を明確にすること。 ・セキュリティ管理方針を明確にすること。
7	コミュニケーション管理	コミュニケーション管理の具体的な方策を明確にすること。
8	会議体	本プロジェクト内で開催する会議体を明確にすること。
9	構成管理	・構成管理方針を明確にすること。 ・ファイル名や文書管理番号の規約を明確にすること。
10	品質管理計画	・各工程の品質判定基準を明確にすること。 ・品質情報の収集から分析までの考え方を明確にすること。 ・成果物の検証方法について明確にすること。
11	テスト計画	各テスト工程の目的、検証の観点、実施方法等の概要を記載すること。
12	支給品管理	市からの支給品や借用品の管理方法を明確にすること。

(3)　進捗管理

ＤＸ基盤構築作業にかかる進捗管理は、次のとおりとする。

ア　本業務の全体スケジュールは、市と受託者が共同で作成することとするが、各工程において、それぞれの進捗管理や全体スケジュールの進捗管理は受託者が行うこと。

イ　作業着手前に、本業務のプロジェクト計画書、全体工程表（明細は、工程及び月単位以下）及び最初に着手する工程の詳細スケジュール表（明細は、作業項目及び日単位以下）を作成し、市に提出してその承認を得ること。

ウ　プロジェクト開始後は、プロジェクト計画書等に基づき、本業務の履行管理を行い、ＤＸ基盤整備にかかる業務全般を円滑に遂行すること。

エ　受託者は、月１回程度、本業務全体の進捗に係る会議においては進捗報告書等を提示、説明し、市の承認を得ること。

オ　打合せやレビューにおける決定事項や懸案事項について、受託者は速やかに議事録を作成し市に提出するとともに、その承認を得ること。

カ　受託者は、作業が遅延した場合、遅延した作業の全体スケジュールへの影響評価や、進捗阻害要因の洗い出しと対策の策定を速やかに実施し、会議において市に適時的確に報告すること。

キ　受託者は、進捗を阻害する課題や問題については、課題管理表で管理すること。

(4)　事故対応

受託者は、構築業務全般におけるセキュリティ事故を未然に防止するため、セキュリティ対策計画を策定し、市の承認を得るとともに、関係者等に遵守させること。

セキュリティ事故発生時は、セキュリティ対策計画に則り、迅速に対処を行うこと。

(5)　ドキュメント管理

ＤＸ基盤構築におけるドキュメント管理は次のとおりとする。

ア　受託者は、「15　成果物」に示すドキュメントについて、事前に市と協議を行いながら作成し、最終的に市の承認を得ること。

イ　ドキュメントは、内容が理解しやすく利用しやすいものとし、加筆修正が容易なように、記述方法や構成に留意すること。

ウ　各作業工程の終了時に必要な加筆修正を行い、全てのドキュメント（設計書等）について、常に最新の情報に修正し、バージョン管理すること。

エ　運用開始後において、障害対応等により修正等が生じた場合は、その都度、修正履

歴の管理と差し替えを行い、常に最新の状態を維持すること。

オ　受託者は、運用及び保守を行うために必要となる構築関連資料の整理を行うこと。

なお、基本設計書、詳細設計書等は、運用開始時点で最新の内容に整理すること。

(6)　プロジェクト体制

受託者は、本業務を確実に遂行できる、必要な技量と豊富な経験を有する人員を配置したプロジェクト体制を整備すること。プロジェクト体制は、受託者内において、指揮命令及び伝達が円滑に行うことができる段階的階層構造とし、市の作業状況の確認や問合せに対して適切な対応ができる体制とすること。

また、受託者の本業務に関係する全ての作業従事者は、その権限と責任に応じて、本業務に携わる市職員及び関係事業者と、直接に作業内容の調整、確認、打合せ等を行うものとし、必要かつ十分なコミュニケーション能力を有すること。

受託者は、契約締結後、構築プロジェクト体制案、及び業務従事者一覧を市に提出し、承認を得ること。業務従事者一覧は、氏名、所属組織を明記すること。また、体制変更があった場合は、最新の構築プロジェクト体制、業務従事者一覧を市に提出すること。

(7)　役割分担

構築プロジェクトにおける役割分担は、次の表のとおりとする。

<table>
<tr><th>No</th><th colspan="2">作業内容</th><th>市</th><th>受託者</th></tr>
<tr><td>1</td><td rowspan="4">共通</td><td>プロジェクトの管理（プロジェクト計画書、進捗管理、品質管理、課題管理、リソース管理、コミュニケーション管理、変更管理、構成管理）</td><td rowspan="2">△</td><td rowspan="2">◎</td></tr>
<tr><td>2</td><td>会議体の管理（会議の開催、会議資料の作成、会議録の作成）</td></tr>
<tr><td>3</td><td>事務マニュアル等の見直し</td><td rowspan="2">◎</td><td rowspan="2">○</td></tr>
<tr><td>4</td><td>作業場所（庁内において作業の場合）の調整</td></tr>
<tr><td>5</td><td rowspan="2">設計</td><td>機能要件・非機能要件に関する基本設計書、詳細設計書の作成</td><td>△</td><td>◎</td></tr>
<tr><td>6</td><td>機能要件、非機能要件の提示</td><td>◎</td><td>○</td></tr>
<tr><td>7</td><td>日立市情報セキュリティポリシー改訂</td><td>・α’モデル移行に伴う情報セキュリティポリシー改訂ついての支援</td><td>◎</td><td>○</td></tr>
<tr><td>8</td><td rowspan="2">稼働（準備）</td><td>運用・保守マニュアルの作成</td><td rowspan="2">○、△</td><td rowspan="2">◎</td></tr>
<tr><td>9</td><td>操作マニュアルの作成</td></tr>
</table>

※凡例　◎：主作業 、 ○：作業補助 、 △：確認・承認

11　テスト要件

受託者は、本業務の各システムに求められる信頼性・安全性の水準に応じたテスト及びレビューを市と協力して行うこと。

そのテスト及びレビューにて各システムの機能要件及び非機能要件に対する適合性、要求する機能や、その他要件を適正に達成しているかの客観的な確認に努めること。テストの内容には、詳細要件として設計したグループポリシーやデバイス制御など各端末に適用した設定事項の確認を含むものとする。

テストに当たっては、その実施時期、実施内容、実施方法、テストデータの内容等を記載したテスト計画書を作成し、市の承認を得ること。

また、必要に応じて、適切かつ有効なテストの実施に資する他の方策を提案すること。なお、隣接システムのテストについては市及び既存事業者が実施するが、これに協力すること。

12　運用保守要件

(1)　共通

ア　運用・保守基本方針

本業務の運用・保守にかかる基本方針は次のとおりとする。

(ｱ)　市の負荷軽減に配慮すること。

(ｲ)　既存の運用について、市と協議の上、見直しを図ること。

(ｳ)　実施手順及びルールを標準化し、障害対応・復旧手順、必要に応じて市のシステム管理者向け運用・保守手順を整備すること。

(ｴ)　保守は、原則庁内の端末から本番環境等の各環境にアクセスして作業等を行うこと。ただし、セキュリティが十分に確保できると市が判断した場合には、リモート保守を実施可能とする。リモート保守を提案する場合は、次に掲げる事項に従い、セキュリティを担保した上で、効果的な仕組みとすること。リモート保守を実施する場合は、市に承認を得た上で実施すること。

・　保守に利用するネットワークは専用線又は閉域網とするか、インターネット経由でアクセスする場合は、IPSec や多要素認証等を用いてセキュリティ対策を行うこと

・　保守端末は、市と同等のセキュリティ対策を実施した端末を使用すること。

・　リモート保守の作業場所のセキュリティ対策として、入退室管理、監視カメラ等の対策を行うこと。

・　市職員による作業場所への視察検査に応じること。

イ　運用・保守体制

本業務における運用・保守体制の構築に当たっては、次に掲げる事項を原則とすること。

(ｱ)　運用・保守業務の統括者を配置し、全体の管理を行うこと。統括者は、特別区や市（人口 10 万人以上)、都道府県、官公庁において、全期間又は３年以上の期間に渡り、ネットワーク環境、又はコミュニケーション基盤に関し、NOC、SOC、ヘルプデスク等の統括を含む運用業務全体の指揮命令と管理の実務経験を有すること。

(ｲ)　連絡体制を明確化し、市及び関係者への連絡を円滑、かつ迅速に行える仕組みとすること。

13　スケジュール

各年度の業務内容・スケジュールについては、次の表のとおり。

No.	プロジェクト名	利用開始（予定）	利用終了（予定）	構築期間	賃貸借期間
1	ＤＸ基盤構築事業　設計業務	R8.5.30	R9.3.31	－	－
2	本庁舎ネットワーク機器更新	R8.8.1	R15.7.31	3 ヵ月	84 ヵ月
3	庁内パソコン完全無線化	R8.8.1	R13.7.31	3 ヵ月	60 ヵ月
4-1	基幹系転送ネットワーク改善	R8.12.1	R13.11.30	4 ヵ月	60 ヵ月
4-2	基幹系インターネット接続システム	R8.12.1	R10.9.30	3 ヵ月	22 ヵ月
5	基幹系⇔情報系ファイル共有	R8.12.1	R13.11.30	3 ヵ月	60 ヵ月
6	BCP 対策通信機器整備（１拠点）	R9.10.1	R14.9.30	4 ヵ月	60 ヵ月
7	α’モデル通信機器整備	R9.10.1	R14.9.30	4 ヵ月	60 ヵ月

14　プロジェクト管理

本業務を確実に実施するため、プロジェクト管理方針、実施体制及び全体工程表等を確立し、円滑なプロジェクト管理を実施すること。

15　成果物

(1)　提出書類等

No.	名　称	提　出　時　期
1	業務実施計画書	契約締結後速やかに
2	業務実施体制図	契約締結後速やかに
3	議事録	打合せ終了後、３開庁日以内 ※書式は問わない
4	月次報告書	前月分を翌月１５日まで ※１５日が土日祝日の場合は前日まで
5	各業務に関する完成図書	各仕様書に準ずる
6	業務完了報告書	各業務終了日

(2)　提出方法

紙媒体　１部

電子データ　１部

(3)　納品先

〒317-8601

茨城県日立市助川町 1-1-1

日立市役所　市長公室　デジタル推進課

16　契約について

随意契約により業務委託及び賃貸借に係る契約を締結する。

17　その他

本業務の実施に当たり、本仕様書に明示なき事項及び疑義が生じた場合は、双方協議の上、業務を実施する。

以　上