新潟市インターネット仮想環境
構築業務委託仕様書

令和４年１１月

新潟市総務部情報システム課

目　次

新潟市インターネット仮想環境構築業務

1. 業務内容

1.1 業務の名称

新潟市インターネット仮想環境構築業務（以下「本業務」という。）

1.2 委託期間

契約締結の日から令和５年２月２８日まで

1.3 本業務の目的

新潟市（以下、「本市」という。）は、平成 29 年より総務省の求めるネットワーク三層分離に対応するため、個人番号利用事務系、LGWAN 接続系、インターネット接続系に環境を分離している。

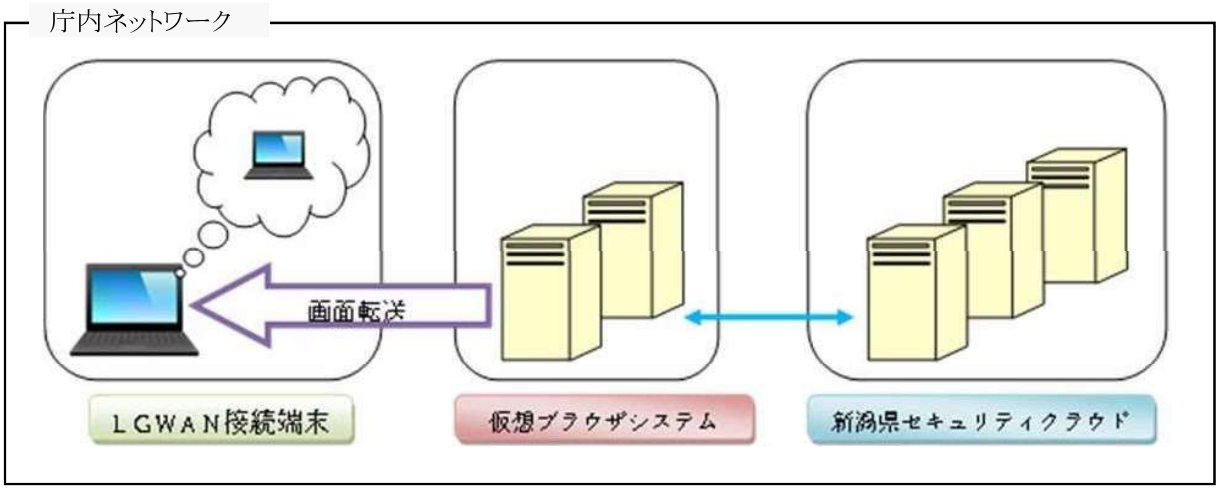
本業務では、インターネット接続系を仮想環境上で構築し、画面を LGWAN 接続系に転送することで、業務の利便性の向上を図っている。平成 29 年 3 月より運用開始し機器のリース期間が終了するため、インターネット環境を見直し、再構成することを目的として実施する。

1.4 構築する環境の概要

本業務は、ＬＧＷＡＮ接続系とインターネット接続系を分割するにあたり、ＳＢＣ方式（サーバＯＳベース）の仮想化技術を用いて構築し、ＬＧＷＡＮ接続系端末は、転送された画像配信によって各種操作を実現するものとする。以下に全体概要図を示す。

受託者は、これらの内容を考慮して本業務を遂行すること。

全体概要図



1.5 業務の範囲

本業務の範囲は、以下の（1）から（3）のとおりとする。

本業務の位置づけとして、本書に記載の仕様書に基づき、「新潟市インターネット環境構築業務委託契約書」（以下「本契約書」という。）により、本市と受託者間で委託業務契約を締結する。

また、運用・保守業務は令和５年３月１日から、本業務受託者との随意契約により実施することを想定している。

(1) プロジェクト管理

受託者は、本業務のプロジェクト管理（プロジェクト実施計画、進捗管理、品質管理、課題／リスク管理、変更管理等）を行い、本業務を円滑に進め、高品質な成果物を作成すること。

(2) システム設計・開発

① 本業務の要件定義、基本設計、詳細設計、プログラム開発、他システムとの連携、試験（単体試験・結合試験・総合試験）を行うこと。なお、事前に本市環境下で仮想環境を構築し、動作確認を行っているため動作確認時の設定内容及びテスト結果を別途提供する。

② 本仕様書に基づいて設計すること。

③ 本業務範囲（ここでいう本業務の範囲内とは、仕様書で定義する業務範囲の他に業務遂行中に発注者と受託者で協議し決定した業務内容や成果品を含む）についてその一部又は全部が履行されない場合、速やかに原因を究明し無償で対応を行うこと。外部的原因がある場合はそれを速やかに報告し、本市と協議の上で対応を決定すること。

④ 開発及び各試験に必要となる作業場所、機器、消耗品、通信等（本市が別途調達する機器及びその当該機器と不可分な OS 等既製ソフトウェアは除く）に係る費用については、受託者の負担とする。

(3) システム導入と運用・保守準備

① 別途調達済みハードウェア等(別紙「インターネット環境仮想化基盤　機器明細」)へ、必要なソフトウェア（別紙「インターネット環境仮想化基盤　ソフトウェア明細」）をインストールし、本番稼働に必要な設定作業を行うこと。

② サーバーは OS 起動前にどの画面遷移中に起動しなくなったか動画で確認が可能な事で障害の早期発見することを可能とするため、過去 3 回以上の動画での起動キャプチャ記録を保存、再生可能な機構を有していることから、運用時の障害の早期解決を図れるようにすること。

③ プラグインのサポート切れのリスクや脆弱性の観点から、サーバーの管理機能はHTML5に対応し、JAVA などのインストールを伴わず WEB ブラウザ上で管理すること。

④　IPMI2.0 に対応したリモート管理用コントローラを搭載し、OS の状態に依存せずにネットワーク経由でのサーバーの管理/制御（電源管理、仮想コンソール/仮想メディア）が設定可能とすること。また、専用のネットワークポートを設定すること。

⑤　BIOSやファームウェアについて意図しない、もしくは悪意ある変更から保護するため、それらのバージョンアップや設定変更を行おうとした際に警告または禁止すること。また、その機能はシステムを再起動することなく有効化・無効化出来るよう設定すること。

⑥　サーバーのセキュリティ強化のために使用しない USB ポートは無効化すること。また、ポートの無効化と有効化はシステムを再起動することなく設定可能とすること。

⑦　BIOS イメージおよび OS イメージに破損または悪意ある改ざんの疑いがある場合の早期復旧のために、サーバーの内蔵機能による正常なイメージへの復旧設定を行うこと。

⑧　仮想化集約されたサーバーの高負荷に備え、CPU の熱を効率的に冷却し、パフォーマンスの向上と故障率低減を実現するため、搭載された PCIe カードを認識して最適な冷却設定を行い運用負荷を軽減させること。

⑨　メンテナンス性向上のため、機器のシリアル番号を確認できるよう引き出し式の情報タグ等を確認し、サポートへの問い合わせを行うこと。

⑩　庁内の関連部署との調整に必要な資料作成の支援を行うこと。

⑪　本システムは市全職員が利用することから、同等規模以上の構築実績を有すること。

⑫　本システムの構築において、別紙「インターネット環境仮想化基盤　ソフトウェア明細」に示す仮想ソフトウェアのサポート体制を構築し安定稼働させること。

⑬　本業務において構築した環境が円滑に運用されるための必要な設定を行い、マニュアル（運用マニュアル、操作マニュアル）を作成・整備すること。

⑭　本業務を進めるにあたり現行システムの設定等のデータ移行が必要な場合、データ移行に係る費用を含めること。費用については下記に問合せすること。

現行システム運用業者：㈱BSN アイネット　連絡先：025-242-2921

⑮　仕様に記載がない事項であっても、本市及び現行システム運用保守業者と協議の上、本業務を円滑に進めること。

1.6 スケジュール

本業務及び関連部分に係るスケジュール概要を下記に示す。

年度・月 / 項目	令和４年			令和５年		
	10 月	11 月	12 月	1 月	2 月	3 月
業者決定						
構築業務（設計・構築・テスト）		設計	構築・テスト			
稼働					仮稼働	本稼働

2. 業務の基本要件

2.1 基本方針

本業務の基本方針は、以下のとおりとする。

(1) 基本要件

① 庁内のネットワーク状況、既設の各種システム及びサーバーの稼働形態、端末性能などを考慮し、利用者の視点のみならず、運用担当者の視点からも利便性や運用の容易性を極力損なうことなく、費用対効果を最大化できるよう、最適なシステム構成とすること。

② 必要に応じて現地での調査や打合せを行い、設計に反映させること。

③ 三層分離環境の安全性担保および「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」遵守の観点から、インターネット接続系セグメントに設置する仮想サーバマシンに対して、接続元端末から仮想化技術によりアクセスし、転送された画面を操作する方式とすること。また、所属単位で公開アプリケーション、公開デスクトップの設定を行えるようにすること。

④ システム提供形態はオンプレミス型の構成とする。なお、別途調達済の機器等を本市が指定するデータセンター内のサーバーラックに設置すること。

2.2 機能要件

(1) システム構成

① 本システムが稼働するための必要リソースを搭載した物理サーバーを 8 台構築すること。

② インターネット環境仮想化の RDSH サーバーが稼働する仮想化基盤の物理サーバ 8 台を HCI により統合しリソースの有効活用を実現すること。

③ インターネット環境仮想化基盤は VMware vSphere Enterprise で仮想化し、VMware vCenter Server Standard で管理を行うこと。

④ インターネット環境仮想化基盤の ActiveDirectory サーバーを 2 台(物理サーバ 1 台と仮想サーバ 1 台)を構成すること。なお、ここで構築する ActiveDirectory は、既存のドメインにドメイン参加させ、昇格させてプライマリドメインコントローラを構築するものとする。

⑤ 利用者総数(延べユーザー数)は約 6,500 ユーザーとする。仮想端末接続に関しては、同時接続数約 1,000 が保証されよう構築すること。

⑥ インターネット環境仮想化基盤のサーバー、物理サーバー等の管理ポートは、KVM スイッチに収容し、KVM モニタより機器の操作ができるように設定すること。

(2) 仮想基盤に関する要件

① 仮想基盤を VMware vCenter Server Standard で一元管理すること。

② ハードウェアの監視サーバーを導入すること。

③ KMS 認証を通じて Windows ライセンス認証を簡便に行えるようにすること。

④ 仮想サーバマシンの展開時に使用するマスタイメージは、要件ごとに 1 つのみを運用すること。また、ユーザーアカウントに応じて要件の異なる任意の仮想端末群 (プール) の割り当てを可能とすること。

⑤ 構成及び運用簡素化の観点から、仮想化基盤全体で仮想スイッチを単一の仮想スイッチで構成し、仮想ネットワーク設定を GUI から一括して構成・管理可能とすること。

⑥ 仮想端末が稼働する物理ホストに障害が発生した際に、異なる物理ホスト上で仮想端末が再起動されることで、ダウンタイムを最小化すること。なお、再起動する仮想端末の優先順位を設定すること。

⑦ 特定の仮想化サーバーに負荷が集中し、そのサーバー上で稼働する仮想端末のサービスレベルが低下する場合、自動的に異なる仮想化サーバーへ一部の仮想端末を稼働させたまま移行するよう設定すること。なお、移行する際には、仮想端末グループを指定することで、特定の仮想端末の組み合わせを同一のホスト上に移行させる設定や、同一のホストに移行させない設定をすること。

⑧　メンテナンス時など、運用におけるサービス停止の影響を最小限とするために、仮想端末を停止せずに、サーバーノード間で仮想端末の移動が可能とすること。また同様に仮想端末を停止せずに、仮想端末が稼働するストレージ領域の移動が可能とすること。

⑨　追加クラスタソフトウェア等を利用せずハイパーバイザーのみで、8 つの vCPU を持つ仮想端末を二重化しフォールトトレラントを構成すること。

⑩　他の仮想端末のリソース消費による性能影響を回避するために、仮想端末にて利用可能な CPU およびメモリのリソースの予約（確保するリソースを任意の数値で定義）や制限（割り当てるリソースの上限値を任意の数値で定義）を設定すること。

⑪　運用性向上の観点から、仮想化管理ソフトウェアから GUI で一括して仮想化ソフトウェアの管理、設定が行えるようにすること。また、仮想化基盤のタスクやイベント、リソース情報、および運用管理において必要となるログ情報の取得すること。

⑫　仮想端末（vmdk）単位のポリシー機能により、保護レベル(Raid0、 1、 5、 6 相当)の変更や、QoS の設定を行うこと。

(3) バックアップに関する要件

①　インターネット環境仮想化サーバーをバックアップ装置へバックアップするよう設定すること。

(4) セキュリティ対策

①　新潟県セキュリティクラウドにて実装されるセキュリティ機能（メール無害化、ファイル無害化等）を利用するため、仮想端末は、新潟県が準備するセキュリティ機能との接続を充分考慮した設計とすること。

②　仮想端末のセキュリティリスクに対応するため、未知の不正プログラム対策(Endpoint Detection and Response（以下、「EDR」という。)）を導入・設定すること。。また、ウイルススキャン時の負荷が、業務に影響を与えないように設計すること。なお、EDR では単一のエージェントでカーネルモードでの端末のログ収集、パターンマッチングでのマルウェア対策のどちらも実施すること。

③　画面転送・印刷・音声の通信に開放するポートは必要最低限とすること。

④　仮想端末から接続元端末にインストールされているプリンタに印刷できるように設定すること。この際、圧縮によりネットワーク帯域の消費を抑えること。

⑤　接続元端末のディスクを仮想端末側から参照することを禁止すること。

⑥　インターネット環境仮想化基盤では、インターネットからのランサムウェア等の高度な脅威から防御するため、分散ファイアウォールを導入・設定すること。

⑦　ハイパーバイザーに組み込まれたネットワーク仮想化機能による分散ファイアウォールを利用し、同一セグメント内の仮想端末間の通信制御を可能とすること。

⑧　一元的なセキュリティポリシーの管理を実現するため、分散ファイアウォールを適用する対象として、仮想端末やリソースプール等のオブジェクトに紐付けてルールの作成を行うこと。

⑨　ファイアウォールルールをタグや仮想端末名、OS 名に紐付けて作成すること。

⑩　仮想端末が稼働したまま別の物理ホストに移動した際、その仮想端末に関連する分散ファイアウォールのルールがそのまま適用されるように設定すること。

⑪　単一の IP アドレスを使用する仮想デスクトップや仮想アプリケーションに対してユーザー毎に異なるファイアウォールルールを適用できるように設定すること。

(5) 運用管理機能の構築

①　仮想サーバーマシンの稼働状態やリソースの監視ができるように設定すること。

②　サーバーのハードウェア監視ができるように設定すること。

③　ハードウェアの性能情報（CPU 負荷、メモリ使用量など）を集計しグラフ表示できるように設定すること。

④　ハードウェア異常発生時にメール通知できるように設定すること。

⑤　複数の仮想サーバーマシンを一括で起動/シャットダウンできるように設定すること。

⑥　仮想端末で使用するマスタデータおよび、仮想端末管理系サーバー群のシステムファイルおよび各ログなどは、必要に応じて随時バックアップを取得できるように設定すること。

⑦　仮想端末へのアクセスログ（接続ユーザー・接続日時・接続した仮想端末等）を取得するとともに、取得したログを１年間保管できること。また当該ログを退避する仕組み・手順を用意すること。

(6) 仮想デスクトップ機能に関する要件

①　Web 閲覧をするため、仮想デスクトップ上のインターネット接続ブラウザとして Microsoft Edge を使用可能と設定すること。Office ソフト等による編集作業等は基本的に行わないが、下記図表 2.2 に示すアプリケーションについてインストールを行うとともに操作がスムーズに行えるようサイジング等各種設定を行うこと。また、その他のアプリケーションが必要となった際は、本市と協議のうえ、導入すること。いずれのソフトウェアも、インストール時点で最新のバージョンを導入すること。

【図表 2.2 仮想端末インストールアプリケーション一覧】

項目	アプリケーション
Web ブラウザ	Microsoft Edge
ドキュメントビューワー	Adobe Acrobat Reader DC DocuWorks Desk 一太郎ビューア
圧縮解凍ソフト	7-zip
オフィススイート	LibreOffice
仮想デスクトップエージェント	VMWare Horizon Agent （インターネット閲覧環境への接続用）

② 仮想デスクトップの動作 OS は Windows ベースとすること。

③ 1 つの Windows サーバーに複数人がセッション接続し、仮想アプリケーションのウィンドウ（公開アプリケーション）のみ、もしくは仮想デスクトップ（公開デスクトップ）のイメージを、接続端末に画面転送する SBC(RDSH)方式を実現すること。

④ 接続サーバ側のセッション数に応じて接続先のサーバ負荷分散を行う機能を設定すること。

⑤ 仮想デスクトップおよび仮想アプリケーション環境の管理を効率化するために、マスターイメージからクローン展開が可能であること。

⑥ 運用管理を効率化するため、仮想デスクトップの展開方式は大規模環境での導入実績のある、差分クローン方式とすること。単一障害点を極力削減するため、仮想デスクトップのネットブート方式での展開は認めないこととする。

⑦ Microsoft Edge にて、本市の議会中継が再生可能であり、音声も流れるようにすること。また、一般的な形式によるストリーミング動画が閲覧できるようにすること。

⑧ Microsoft Edge にて、Web 閲覧に必要となるプラグインをインストールしておくこと。

⑨ 仮想端末上の個人設定及びブラウザのブックマーク、Cookie、ダウンロードデータをユーザーごとに保存を可能とすること。なお、ユーザーが保存したダウンロードデータは、一定期間が経過した場合、自動削除するように設定すること。

⑩ ブックマークは接続する仮想端末を提供する仮想サーバマシンが変わっても継続して利用可能とすること。

⑪ アクセスする URL サイトに応じて、ローカルブラウザと仮想化によるインターネット接続用ブラウザのうち、適切なブラウザの起動ができるよう設定すること。

⑫ 接続元端末と仮想端末の間でコピー&ペーストを許可するもの、許可しないものと、その方向についてをクリップボードのデータ形式により設定すること。

⑬ 仮想アプリケーションにおいて、接続元端末で実行されるアプリケーションと区別す

るため仮想アプリケーションのウィンドウに任意の色の枠をつけて認識できるように設定可能とすること。

⑭　仮想端末のアイコンはユーザログイン時にスタートメニューやデスクトップに動的に配布されるよう設定可能なこと。誤ってアイコンを削除・変更した際に、再ログインにて復旧すること。

⑮　仮想端末へ接続しているユーザーが一定時間無操作の場合、自動的にログアウトするよう設定可能とすること

⑯　ネットワーク接続が切れ、仮想画面が消えた場合でも、仮想環境側では作業画面が保持され、一定時間は再接続によって再開できるよう設定すること。

⑰　仮想端末を提供する仮想サーバがウイルスに感染した場合、再起動などにより即時にロールバックできるに設定すること。

⑱セキュリティの観点から、RDP は利用しないこと。

3　開発要件

3.1　作業要件

3.1.1　作業場所

(1) 会議、レビュー

本業務の設計・開発に関する打合せ、進捗会議やレビュー等は、原則として本市が指定する場所で実施すること。

(2) 本業務の設計・開発・試験

受託者事業所内とすること。

(3) 運用試験

本番稼働を想定した試験となることから、作業場所や使用可能な環境については、本市と協議のうえ決定するものとする。

3.1.2 開発機器・使用材料の負担

開発に必要な資材は原則受託者が負担すること。発注者しか知り得ない開発に係わる情報については下記の方法で提供を行う。

(1) 発注者からの貸与物件

開発に必要な物件・資料のうち、返却の必要なもの及び持ち出し禁止条件に該当するものについては、契約書の機密保持事項に従い所定の手続きにより貸与する。

(2) 構築におけるツール

構築作業で使用する各種ツールは、業界標準の汎用製品・国際標準技術を採用したものとするが、止むを得ず提案者独自のツールを利用する場合は、提案書にその理由とともに明記すること。

3.2 機密保持等

3.2.1 機密保持

本業務を遂行するにあたり、「新潟市情報セキュリティポリシー」の内容を遵守するとともに、「新潟市インターネット仮想環境構築業務委託契約書」(以下、「契約書」という) に定める別記「情報セキュリティに関する要求事項」を遵守しなければならない。

3.2.2 貸借資料の届出・管理

本業務の実施に必要となる資料を借用する場合は、必ず届出を行い発注者の許可を得ること。

3.2.3 個人情報及び行政情報の保護

本業務を遂行するにあたり、契約書に定める別記「個人情報取扱特記事項」を遵守しなければならない。

3.2.4 法令などの遵守

本業務の履行にあたっては、関係法令及び本市の条例、規則、要綱などを十分理解すること。なお、本市で定める文書管理規程など、本システムで関連する規程類は、本市のホームページ (https://www.city.niigata.lg.jp/) の例規集及び要綱集に掲載のとおりである

4. 成果物

4.1 成果物一覧

4.1.1 設計書・マニュアル等

本業務の成果品として下記図表 4.1.1 に示すドキュメントを作成し納品すること。各ドキュメントの記載事項や納入期限等については、本市の承認を得ること。なお、プロジェクト計画書は契約後直ちに提出すること。

【図表 4.1.1 成果物一覧】

No.	成果物	備考
1	プロジェクト 計画書	作業構成（WBS）、マスタスケジュール、進捗報告書、課題管理表等のプロジェクト管理に必要な各種様式を含むこと。
2	基本設計書	ネットワーク構成図、ハードウェア構成図、ラック搭載図、物理配線図、論理配線図、ソフトウェア構成図等を含むこと。
3	詳細設計書	各種機器、ソフトウェア、システムの設定情報を含むこと。
4	テスト計画書	テスト実施結果報告書を含むこと。
5	操作マニュアル	利用者及び運用担当者がシステムを利用する手順書を画面の画像等を用いて作成すること。
6	保守・運用 マニュアル	運用担当者が平時の運用としてオペレーションが必要となる作業をまとめた資料を作成すること。
7	障害時対応 マニュアル	運用担当者が障害と思われる事象が発生した場合に事象の切り分けや復旧方法などの実施すべきオペレーションをまとめた資料を作成すること。
8	議事録	「３．１．１（１）会議、レビュー」に記載する、打ち合わせ及び進捗報告等の会議における議事録。 会議等実施後５日以内に提出すること。

4.2 納入条件

(1) 納入物の媒体や部数

① 各納品物は、MS-Office 製品を用いて、もしくは PDF 形式で作成のうえ、CD-R などに格納したものを納入すること。なお、各納品物の内容に応じて紙媒体で納入を求めることがある。

② 紙媒体の用紙サイズは日本工業規格 A4 版を原則とし、必要に応じて A3 版を認める。

(2) 納入場所

新潟市総務部情報システム課とする。

5. 教育・研修

5.1 教育・研修

本仕様書の要件に基づいて、以下のとおり職員に対して操作等教育・研修を実施すること。

(1) 職員研修

職員に対してシステム操作マニュアルの作成を行うこと。特に IT 知識の乏しい職員にも理

解できるよう、専門用語を多用せずに画面の画像等を用いて作成すること。

(2) 運用者研修

運用担当者が平常時の際に必要となるオペレーションマニュアルを作成すること。特に年度が切り替わる際に発生する大規模な人事異動の際に対応できるようにバッチファイルやツールの提供やそれに特化した手順書等が必要となる場合は提供すること。

運用担当者が障害と思われる事象を検知した際の切り分け手順及び対応手順をまとめた障害時対応マニュアルを作成すること。

(3) 本稼働開始直後のサポート

本稼働の直後は、利用者より様々な問合せが寄せられることが想定されるため、安定稼働後のサポート体制時よりも細やかな対応が求められる。そのため、必要に応じて現地立会いも想定したサポート体制をとること。

6 その他

6.1 業務評価の特記仕様

本市は、本業務の履行完了など、契約終了後に受託の業務内容について、下記図表 7.1 に示す基準により評価を行い記録の保存を行う。

なお、受託者は評価結果について異議を申立てることはできないものとする。

また、評価結果が契約条件に影響を与えることは一切ない。

【図表 7.1 業務評価基準】

評価	評価基準
A	成果物の品質、納入などで仕様を超える成果があった。
B	通常の指示により仕様どおりの成果を得た。
C	仕様書の他に口頭の指示などにより仕様どおりの成果を得た。
D	担当者が相当程度指導するなどして、なんとか仕様レベルの成果を得た。
E	仕様を達成できなかった。(契約解除など)

6.2 その他

(1) 本調達仕様書に定めのない事項については、発注者と協議のうえプロジェクト計画書で定めることとする。

(2) 本業務について疑義を生じた場合は、速やかに本市と受託者で協議を行い、業務を実施すること。