

インターネット接続系システム基盤更新業務委託仕様書

第1章 総則

1 業務名

インターネット接続系システム基盤更新業務委託

2 目的

本業務は、総務省が示す「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（令和6年10月版）」に則り、「 α モデル」のネットワーク構成を堅持しつつ、LGWAN 接続系端末から安全かつ利便性の高いインターネット利用環境を整備し、以下を実現することを目的とする。

- (1) インターネット閲覧環境の安全性向上
- (2) Web 会議環境（ブラウザ版：Microsoft Teams / Zoom / Webex 等）の整備
- (3) ファイル無害化による安全なデータ受渡し
- (4) 利用者利便性向上
- (5) 管理者の運用負荷軽減
- (6) 将来的な α' モデル・SSE/SWG 高度化を見据えた拡張性確保

3 業務の範囲

本業務の範囲は以下のとおりとする。

- (1) インターネット接続系システム基盤の設計・構築
- (2) 機器・ソフトウェア・ライセンスの調達・納入・設置
- (3) 既存システムからのデータ・設定移行及び初期設定等
- (4) 動作確認・受入試験の実施
- (5) 利用者・管理者向け操作説明・研修
- (6) 契約期間中の運用保守
- (7) 各種ドキュメント（設計書・操作マニュアル等）の作成・納品

4 契約期間

本業務の契約期間は、契約締結日から令和13年9月30日まで（地方自治法第234条の3に基づく長期継続契約）とする。

なお、業務は導入期間・保守期間に分けて管理する。

- (1) 導入期間 : 契約締結日から令和8年9月30日まで
- (2) 稼働開始日 : 令和8年10月1日
- (3) 保守期間 : 令和8年10月1日から令和13年9月30日まで

5 履行場所

たつの市役所（たつの市龍野町富永 1005 番地 1）

第2章 現行システムの概要

6 現行構成の概要

現行のインターネット接続系システムは、αモデルに基づく三層分離構成（マイナンバー利用事務系・LGWAN接続系・インターネット接続系）を採用しており、LGWAN接続系端末からのインターネット利用は、インターネット接続系に設置したサーバ群を経由する画面転送型リモートデスクトップ方式を採用しており、現行の主要構成は以下のとおりである。設置場所はすべて本庁舎電算室である。

(1) サーバ構成

既設サーバ	台数	導入時期
リモートデスクトップサーバ	1	平成28年度
セッションホストサーバ	4	平成28年度
リモートデスクトップデータ保存サーバ	1	平成28年度
FileZen（ファイル受渡し）	1	平成28年度
ADサーバ	2	平成28年度
SMTPサーバ	1	平成28年度
メールリレーサーバ	1	平成28年度

※上記は現行システムの主要構成を参考として示したものであり、本業務においてサーバの流用は行わない。現行システムは本業務完了後も一定期間引き続き稼働する。

(2) ファイル受渡し・無害化

インターネット接続系からLGWAN接続系へのファイル受渡しには、FileZen（ソリトンシステムズ製）を使用している。ただし、CDR（Content Disarm and Reconstruction：コンテンツ無害化・再構築）処理機能は有していないため、アップロードできるファイルの拡張子をPDFや画像ファイル等に制限している。本業務では、CDR機能を有するファイル受渡し・無害化システムを新規構築し、現行システムと置き換えるものとする。

(3) ネットワーク機器

L2スイッチ及びUPS（無停電電源装置）については、いずれも保守期限を迎えている。

第3章 調達要件

7 基本方針

以下の基本方針に従い、システムを構築すること。

(1) α モデルの堅持

LGWAN 接続系とインターネット接続系の分離を維持し、インターネット側の脅威が LGWAN 接続系に波及しない構成とすること。

(2) 安全性と利便性の両立

セキュリティを確保しつつ、利用者が通常業務を円滑に行えること。

(3) 運用負荷の軽減

管理者の日常運用・障害対応が効率的に行えること。

8 インターネット分離・閲覧機能要件

以下の要件をすべて満たすこと。

(1) ネットワーク分離

- LGWAN 接続系端末からインターネットを安全に利用できる分離方式を採用すること。
- 分離方式は、仮想ブラウザ方式（画面転送型）又はセキュアブラウザ方式（専用ゲートウェイ経由型）のいずれかとする。
- インターネット側で端末へサイバー攻撃がされた場合でも、LGWAN 接続系へ影響が及ばない構成とすること。
- セッション終了時にブラウザ環境がリセット・削除される機能を有すること。

(2) クリップボード制御

- インターネット接続系と LGWAN 接続系間のクリップボード経由のデータ転送を双方向で制御できること。
 - コピー完全禁止
 - テキストのみ許可
 - 画像のみ許可
 - テキスト・画像ともに許可

(3) ブックマーク機能

- 利用者が業務上よく利用する Web サイトをブックマーク（お気に入り）として登録・利用できること。セッション終了後もブックマーク情報が保持されること。

(4) Web 会議対応

- ブラウザ版の Microsoft Teams、Zoom、Cisco Webex が利用可能であること。
- Web 会議利用に必要な音声（マイク・スピーカー）、カメラ、画面共有機能が動作すること。
- 複数ユーザーが同時に Web 会議を利用できる十分な性能・同時接続数を確保すること。
- インターネット接続系のブラウザ上において、Word・Excel・PowerPoint・PDF 等のファイルをプレビュー表示（読み取り専用）できること。

(5) URL フィルタリング・アクセス制御

本市が既設する URL フィルタリングシステムと連携し、業務上不要な Web サイトへのアクセスを制限できること。(現行製品：i-Filter (デジタルアーツ社製))

(6) ログ管理

- 利用者の Web アクセスログ (日時、接続元、URL、通信量等) を記録・保存すること。
- ログの保存期間は 1 2 ヶ月以上とし、検索・出力が可能であること。

9 ファイル無害化転送機能要件

以下の要件をすべて満たすこと。

(1) 無害化処理方式

- インターネット接続系と LGWAN 接続系間の双方向のファイル受渡しに際し、CDR 技術によるファイル無害化処理を行うこと。
- マクロ、スクリプト、埋め込みオブジェクト等の潜在的脅威要素を除去し、安全なファイルとして再構築の上、双方向のファイル受渡しができること。
- 無害化後もファイルのレイアウト・内容が可能な限り維持されること。
- 無害化処理はファイル転送時に自動で実施されること。
- 転送可否及び無害化レベルは管理者が設定できること。

(2) 対応ファイル形式・サイズ

- Microsoft Office 文書 (Word・Excel・PowerPoint)、PDF、画像ファイル等を含む、できる限り広範な形式に対応すること。
- 業務上必要なファイルサイズに対応できること。

(3) ファイル受渡し操作性

- 利用者が LGWAN 接続系端末から直感的な操作 (ドラッグ&ドロップ、ワンクリック等) でファイルを受け渡せること。

(4) ログ管理

- ファイル受渡しの操作ログ (日時、利用者、ファイル名、処理結果等) を記録・保存すること。
- ログの保存期間は 1 2 ヶ月以上とし、検索・出力が可能であること。

(5) 承認フロー

- 必要に応じて、管理者による承認を経てファイルを受け渡す承認フロー機能を有すること (又は設定により有効化できること)。

10 認証基盤 (Active Directory) 要件

以下の要件をすべて満たすこと。

(1) Active Directory 構成

- インターネット接続系専用の Active Directory (AD) を構築すること。
- グループポリシーにより、端末設定・セキュリティポリシーを一元管理できること。

(2) アカウント管理

- ユーザーアカウントの追加・変更・削除・無効化が管理者コンソールから実施できること。

- パスワードポリシー（文字数・複雑性・有効期限等）を設定できること。

(3) アカウント移行

- 既存 Active Directory のユーザーアカウント（約 770 名）を参照し、新システム用 AD へのアカウント初期設定を行うこと。

(4) 既存認証基盤との連携

LGWAN 接続系で使用している既存の PC 起動認証基盤との連携が利用できることが望ましい。なお、現行環境では SmartOn（ソリトンシステムズ製）及び Active Directory による認証を使用している。

(5) ログ管理

- 認証ログ（ログイン成功・失敗、アカウントロック等）を記録・保存すること。
- ログの保存期間は 1 2 ヶ月以上とし、検索・出力が可能であること。

11 アンチウイルス要件

以下の要件をすべて満たすこと。

- 本システムを構成するサーバにアンチウイルスソフトウェアを導入すること。
- ウイルス定義ファイルの自動更新機能を有すること。
- 検知・隔離・対応ログを保存し、管理者が確認・出力できること。
- ログの保存期間は 1 2 ヶ月以上とすること。

12 メール中継 (MTA/SMTP) 要件

以下の要件をすべて満たすこと。

(1) メール中継 (MTA)

- インターネット接続系におけるメールの送受信を中継する MTA 機能を有すること。
- 既存メール無害化システムとの連携が可能であること。(現行製品:m-Filter (デジタルアーツ社製))
- LGWAN 接続系メールシステムとの連携（メール転送・中継）が可能であること。
- SMTP over TLS (STARTTLS 又は SMTPS) に対応すること。

(2) ログ管理

- メール送受信ログを記録・保存すること。
- ログの保存期間は 1 2 ヶ月以上とし、検索・出力が可能であること。

13 ネットワーク機器要件

(1) L2 スイッチ

- 現行の L2 スイッチを更新すること。
- 本調達で構築するシステムを賄える必要ポート数・通信速度 (1Gbps 以上) を確保すること。
- 台数は必要最小限とし、受注者が適切な構成を決定すること。
- VLAN 機能を有し、ネットワークセグメントの分離が可能であること。
- 管理インターフェース (Web GUI 又は CLI) を有すること。

- 保守サポートが契約期間中提供されること。

(2) UPS（無停電電源装置）

- 現行の UPS を更新すること。
- 本調達で更新する機器（物理サーバ・L2 スイッチ等）を接続対象とすること。
- 停電時に接続機器を安全にシャットダウンできる十分なバックアップ時間を確保すること（目安：15 分以上）。
- 自動シャットダウン機能（ソフトウェア連携）を有すること。
- バッテリー残量・異常を管理者へ通知できること。

14 サーバ要件

本システムの稼働に必要なサーバを以下の要件をすべて満たすよう調達・構築すること。

(1) サーバ構成

- システム全体をできる限り少ない物理サーバ台数で構成し、費用対効果の高い構成で構築すること。
- 物理サーバは新規調達とし、既存サーバの流用は認めない。
- 設置場所はたつの市役所本庁舎電算室とすること。

(2) ハードウェアスペック

- 想定ユーザー数・同時接続数に対応できる性能を有すること。
- 参考目安：CPU 8 コア以上、メモリ 32GB 以上、ストレージ 1TB 以上

(3) ストレージ冗長化

- 障害発生時の影響を最小化するため、RAID1 又は RAID5 以上の冗長構成とすること。

(4) 仮想化基盤

- 仮想化基盤は実績のある製品を採用し、採用製品・バージョンを見積内訳書に明記すること。
- 仮想化基盤を採用する場合は、各機能（AD、AV、無害化、MTA/SMTP 等）を適切に分離・配置すること。

(5) 設置要件

- 本業務で調達する機器（物理サーバ・L2 スイッチ・UPS 等）は、市が用意する既設の 19 インチラックに搭載すること。
- ラックへの搭載・配線・電源接続作業を含むこと。
- なお、ラックには十分な空き容量を確保しているが、機器構成に応じた収容可否は受注者が確認すること。

(6) 保守・サポート

- 物理サーバは、保守期間中においてハードウェア保守契約又はメーカーサポートが有効であること。
- 契約期間中の保守サポートが提供されること。

15 同時接続・ライセンス要件

- 職員全員（約 770 名）が本システムを利用できること。また、同時接続数 300 ユーザー以上を保証すること。
- ライセンス形態は問わないが、上記条件を満たすライセンス数・同時接続数の根拠を見積内訳書に明示すること。
- ライセンスの追加・変更が柔軟に対応できること。
- 本業務で導入するすべてのソフトウェア・ライセンス（OS、仮想化基盤、分離システム、ファイル無害化、アンチウイルス、その他関連ソフトウェアを含む）は、保守期間をすべてカバーすること。
- ライセンス期間中、ソフトウェアのバージョンアップ・セキュリティパッチ・定義ファイル更新等が滞りなく適用できること。
- 保守期間の途中でライセンスの更新・追加に係る費用が別途発生しないこと。

第 4 章 非機能要件

16 可用性・信頼性

- システムは 24 時間 365 日稼働を基本とすること。
- 性能・サポートの保証対象時間（コアタイム）は平日 8:30～17:15 とし、時間外・休日においても利用可能であること。
- システムの稼働率は 99.9%以上を目標とし、障害発生時は 4 時間以内の復旧を目指すこと。
- 障害発生時は、速やかに管理者へ通知し、復旧対応を行うこと。

17 セキュリティ要件

- 総務省「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（令和 6 年 10 月版以降の最新版）」に準拠すること。
- 管理者アクセスは多要素認証又は証明書認証等により保護すること。
- システムへの不正アクセスを防止する適切なアクセス制御を実施すること。
- 脆弱性情報を定期的に収集し、必要なセキュリティパッチを適時適用すること。
- TLS1.2 以上（TLS1.3 推奨）の暗号化通信に対応し、HTTP/HTTPS 通信を適切に制御・ログ記録できること。
- システムへのアクセスログを記録・保存し、管理者が監査できること。

18 拡張性

- 将来的な α' モデル（LGWAN 接続系から特定クラウドサービスへのローカルブレイクアウトを可能とするモデル）への移行を見据えた構成とすること。
- SSE（Security Service Edge）、SWG（Secure Web Gateway）等のクラウドセキュリティサービスとの連携・移行が可能な設計とすること。

- ユーザー数増加・機能追加に対応できる拡張性を有すること。

19 性能要件

- 通常業務時において、Web ページの表示・ファイルのダウンロード等が実用的な速度で動作すること。
- Web 会議（Teams / Zoom / Webex 等）が映像・音声ともに安定して利用できること。
- ファイル無害化処理は、通常業務で使用するファイルサイズ（目安：10MB 以下）において、30 秒以内を目標とし、最大 60 秒以内に完了すること。

第 5 章 移行・導入要件

20 移行要件

以下の要件をすべて満たすこと。

- 本業務において、現行インターネット接続系システムから新構築システムへの切り替えを行うこと。なお、機能移行の対象は既存メール中継（MTA）の設定・ルーティング情報とし、移行計画（スケジュール・手順・リスク対策）を提示すること。
- 現行メール中継（MTA）の機能・設定を新システムへ適切に引き継ぎ、移行前後でメールの送受信に支障が生じないよう必要な設定をすべて実施すること。なお、送信ドメイン認証（SPF・DKIM・DMARC）についても適切に設定すること。
- ユーザーアカウントについては新システム用 AD への初期設定として実施すること。
- 移行作業は、業務への影響を最小限とする時間帯・方法で実施すること。
- 本番移行前にリハーサルを実施し、課題を事前に解消すること。
- 移行後の設定内容の整合性を検証し、結果を市に報告すること。
- 移行前後の動作確認を実施し、市の承認を得てから本番切替を行うこと。
- 本番切替後、一定期間（目安：2 週間以上）は現行システムとの並行稼働又は切り戻し可能な状態を維持すること。

第 6 章 運用保守要件

21 保守対応

- 保守期間中、システムの安定稼働を維持するための定期保守・障害対応を実施すること。
- 障害対応時間：平日（8:30～17:15）内での一次対応（リモート）は 1 時間以内に開始すること。
- 機器故障等によりオンサイト対応が必要な場合は、連絡受付後 2 時間以内に現地へ駆けつけ対応を行うこと。
- 復旧対応は 4 時間以内を目標とすること。
- 障害発生時は、速やかに市担当者へ報告し、原因・対応状況・再発防止策を報告する

こと。

- 保守対応窓口（連絡先・担当者）を契約時に明示し、変更時は速やかに市へ通知すること。

22 定期報告

受注者は、以下の要件をすべて満たすこと。

- 毎月、システム稼働状況・障害発生状況を市へ報告すること。
- 四半期ごとに、セキュリティインシデント・脆弱性対応状況等を含む総合報告を市へ行うこと。
- 脆弱性情報・セキュリティ情報を収集し、対応が必要な場合は速やかに市へ報告すること。

23 ドキュメントの納品

以下のドキュメントを納品すること。

No.	ドキュメント名	納品時期
1	システム設計書（基本設計・詳細設計）	構築完了時
2	ネットワーク構成図	構築完了時
3	機器・ソフトウェア一覧	構築完了時
4	導入したソフトウェアのライセンス証書・構成内容を一覧化した資料	構築完了時
5	操作マニュアル（利用者向け・管理者向け）	稼働開始時
6	試験仕様書・試験結果報告書	検収時
7	移行計画書・移行結果報告書	移行完了時
8	運用手順書	稼働開始時
9	障害対応手順書	稼働開始時

※上記ドキュメントは、システム変更・更新の都度最新版に改訂し、市へ提供すること。

第7章 見積要件

24 見積書記載事項

見積書は以下の項目別に内訳を明示すること。

- (1) 機器費（サーバ、L2 スイッチ、UPS 等）
- (2) ソフトウェア・ライセンス費（各ソフトウェア・ライセンス費用）
- (3) 構築費（設計・構築・移行・試験）
- (4) 運用保守費（年額・保守期間合計）
- (5) その他（研修費、ドキュメント作成費 等）

第8章 その他

25 情報セキュリティの遵守

受注者は、本業務の遂行にあたり、たつの市情報セキュリティポリシーを遵守し、業務上知り得た情報を第三者に漏洩しないこと。また、業務終了後も同様とする。

26 関係事業者との連携

- 本業務の遂行にあたり、既存ネットワーク・関連システム（URL フィルタリング、メール無害化、PC 起動認証基盤等）の保守事業者との調整・連携が必要な場合は、受注者が主体となって調整を行うこと。
- 連携にあたっては、市が間に入り、必要な調整に協力するものとする。
- 連携に要する作業・費用は、本業務の範囲に含むものとする。

27 疑義

本仕様書に定めのない事項又は疑義が生じた場合は、市と受注者が協議のうえ決定する。