真岡市情報セキュリティ強靭性向上
リニューアル業務委託　仕様書

令和３年１２月

真岡市　総合政策部　情報政策課

目次

1　委託仕様

1．1　業務名称

真岡市情報セキュリティ強靭性向上リニューアル業務

1．2　契約期間

契約締結日から令和４年１２月３１日までとする。

1．3　履行場所

真岡市役所、二宮コミュニティセンター、その他行政出先機関（１９箇所）および小中学校（２７校）

1．4　提案上限額

構築限度額　４２，８４５，０００円（税込）

① 上限額は上記契約期間終了までに要する額とする。

② 上限額は予定価格を示すものではなく、企画内容の規模を示すためのものである。

③ 提案上限額を超える額で提案した事業者は失格とする。

④ ソフトウェア・ハードウェアについては令和４年９月から５年間の運用を予定している。保守、運用支援について月額を提示すること。なお、保守は別途契約とし、構築分の契約は、保守分の契約を確約するものではない。

⑤ 機器費用は、令和４年９月からの５年リースとし、別途契約とする。プロポーザル時にリース対象経費を提示すること。

1．5　委託内容

本仕様書「2　要求仕様」に従い「1．7　作業内容・納品成果物」に記載する事項を行う。

1．6　スケジュール

令和４年９月３０日までに運用を開始できるように、設計・構築業務、動作確認を行うこと。

1．7　作業内容・納入成果物

1．7．1　作業内容

作業内容について、以下の通り、全体管理業務、設計業務、構築・移行業務、運用・保守業務の４種類に分類する。

（1）管理業務

作業実施計画書の作成、進捗管理、品質管理、関連事業者との連絡調整・

課題管理等を実施し、プロジェクトの包括的な管理を行うこと。

（２）設計業務

要件を確認し、具体的なサービスや機器を決定した上で設計を行うこと。具体的な要求仕様については「２．４．２　設計業務要件」に記載する。

（３）構築・移行業務

要件を確認し、安定したネットワークの稼働を行うこと。また、県 SC への接続・移行を行うこと。具体的な要求仕様については「２．４．３　構築・移行業務要件」に記載する。

（４）運用・保守業務

要件を確認し、ハードウェア、ソフトウェアの保守および障害発生時の迅速な対応、マニュアルの整備、発注者の教育等、万全の体制を構築すること。具体的な要求仕様については、「２．４．４　運用・保守業務要件」に記載する。

１．７．２　成果物

本業務において調達をした機器・ソフトウェア（OS、アプリケーション）等について、市が指定する時期までに、関連するドキュメントを作成し納品すること。

（１）管理ドキュメント

工程管理表、スケジュール表、課題管理表、議事録など

（２）設計ドキュメント

基本設計書、詳細設計書、構築図など

（３）構築・移行ドキュメント

IP アドレス一覧表、設定値記載の設定仕様書、ラック搭載図、機器接続図、機器設定ファイルなど

（４）運用・管理ドキュメント

操作手順書など

１．８　基本事項

（１）本調達において提案された企画提案書については、本仕様書の付属資料として契約を構成する文書の一部とし、本委託の対象業務に含むものとする。
ただし、業務の目的達成のために修正すべき事項がある場合は、受注者と発注者の協議により契約締結段階において項目を追加、変更または削除できる。協議が整った場合に、予定価格の範囲内で、発注者と随意契約により委託契約を締結するものとする。

（２）受注者は本調達にかかる費用一切を含むものとして契約すること。そのため、本委託契約の履行に係る作業場所及び作業機器等並びにハードウェアおよびソフトウェア等の作業環境は、受注者側の負担で用意するものとする。また、本調達により現行のネットワークの設定変更費用および一時的に発生するすべての費用も見積額に含めること。

（３）本仕様書の記載事項に疑義が生じた事項は、対応について発注者と協議を行うこと。なお、これらの事項が業務委託に付随して必要となる事項である場合には、速やかに発注者と協議を行い、受注者は必要な作業を実施すること。
（４）受注者は本業務委託の遂行に当たっては、関連する法令、条例等を順守しなければならない。
（５）企画提案書に記載された事項が履行できなかったときは、契約金額の減額または損害賠償請求等を行うものとする。

１．９　機密保持

（１）本業務委託の従事者に、知り得た秘密を他人に漏らさないことを誓約した書類を作成させ、発注者へ提出すること。
（２）本業務委託の実施に必要な関係資料を本業務委託以外に使用しないこと。また、第三者に提供しないこと。
（３）関係資料を無断で持ち出さないこと。複写または複製をしないこと。
（４）本業務委託の実施または管理に関して事故が発生した場合は、直ちに報告すること。
（５）発注者が提供する資料は原則として貸し出しによるものとし、本業務委託が完了したときは、直ちに関係資料を返還すること。
（６）本業務委託が完了した時点において関係資料の複写物または複製物があるときは、当該複写物または複製物を直ちに引き渡すこと。ただし、引き渡すことが適当でないと認められる場合は、複写または複製に係る情報を消去すること。
（７）本業務委託の従事者に対し、本業務委託に関して知り得た個人情報の内容をみだりに他人に知らせ、または不当な目的に利用してはならないこと、個人情報の違法な利用及び提供に対して罰則が適用されること、その他個人情報の保護に関して必要な事項を周知させ、個人情報の保護が徹底されるように指導すること。

１．１０　再委託

受注者は受注業務の全部または一部を第三者に再委託することはできない。受注業務の一部を再委託する場合は、事前に再委託する業務、再委託先を発注者に報告し、承認を受けること。

受注者は機密保持等に関して、本調達仕様書が定める受注者と責務を再委託先業者にも負うよう必要な措置を実施し、発注者に報告し、承認を受けること。

受注者が発注者の承認を得て第三者に業務委託しても、最終的な責任は受注者が負わなければならない。

なお、再々委託は基本的に認めない。

１．１１　作業条件等

（１）受注者は、契約締結後速やかに業務に着手しなければならない。
（２）発注者との連絡窓口、連絡手段および情報共有方法については、事前に発注者と協議の上、決定すること。

（３）作業の実施日時および方法等については、発注者と十分に打ち合わせを行うこと。
（４）本業務委託に必要な作業環境は、受注者が用意すること。
（５）受注者は、本調達仕様書の対象業務及び利用する技術に関する十分な知識、理解および経験のある作業者を配置し、従事させること。
（６）受注者は、本業務委託の遂行にあたり、発注者の関係機関、事業者との間で生じる各種調整事項について、積極的に協力・調整を行うこと。特に、現行ネットワーク導入業者や行政情報システムを含む個別システム導入事業者及び回線事業者とは、作業において密接なかかわりがあるので、十分な事前確認・調整を図ること。

１．１２　その他

（１）受注者は関連業者を含め、全体管理、構築・移行、障害対応、保守等の各業務において、発注者に事前に承認された役割について、責任を持って実施すること。
（２）サーバ室には停止が許されない重要な業務システムが稼働している。業務システムを構成するサーバやネットワーク機器の運用に支障を与えないよう、十分注意の上、作業すること。
（３）既存の機器の設定変更等で対応できる部分はできる限り活用し、過大な設備投資とならないようにすること。

２　要求仕様

２．１　構築方針

自治体においては、情報システム・ネットワークを三つのセグメント（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）に分離・分割すると同時に、インターネット接続系においては、都道府県と市区町村が協力し、原則、都道府県単位でインターネット接続口を集約する、「自治体情報セキュリティクラウド」によりセキュリティ対策を行っている。

本市においても平成２８年１０月に、いわゆる「三層の対策」によりネットワーク分離を完了し現在まで運用をしている。

令和２年５月に「自治体情報セキュリティ対策の見直しについて」が公表され、効率性・利便性を向上させた、新たな「三層の対策」のモデルが提示された。本見直しでは、従来型の強靭化モデルについて必要な改善を行ったモデル（αモデル）を基本形としながらも、インターネット接続系に業務端末・システムを配置した「新たなモデル」（βモデル）も選択可能とされた。

本市では、従来のセキュリティレベルを維持できるαモデルを基本系としながらおも、クラウド・バイ・デフォルト原則やテレワーク等にも対応可能なよう、十分な安全性が担保されている外部サービスには LGWAN 端末から直接アクセス（ローカルブレイクアウト）が可能な構成とする。

また、本調達により構築するシステムを次期システムと記載する。

２．２　基本要件

以下に掲げる事項を基本要件とする。なお、本用件は構築の基本部分を記載したものであり、目的達成のため有用であると思われる事項を提案に含めること。

２．２．１　環境調査

（１）ネットワークの運用者及び保守業者等と協力し、接続対象であるネットワークのシステム構成等を事前調査すること。

・マイナンバー利用事務系ネットワーク

・LGWAN 接続系ネットワーク

・インターネット接続系ネットワーク

なお、調査の結果、本事業遂行にあたり、既存環境の設定変更が必要な場合は、設定変更に係る費用を今回の構築費用に含めること。

また、配線工事が必要となる場合は、今回の構築費用に含めること。

電源工事が必要となる場合は、本市が別途行うので必要な容量、回路等を提示すること。

（２）ハードウェア機器は提案事業者の提案とするが、以下の要件を満たしていること。なお、既存ラック内のマウントスペースは 36 ユニット分、電源容量については 20A×２回路を確保している。

・サーバ機器は、既設の 19 インチサーバラックにマウントできること。

・コアスイッチ（L3 スイッチ)、フロア・エッジスイッチ（L2 スイッチ）は、既設のものを使用することを基本とするが、機器の変更・増設等が必要な場合は構築費用に含めること。

（３）環境調査の結果、設定変更等で対応できる部分は、既存機器をできる限り活用し、予備機を含め機器の新設は必要最低限とすること。

（４）県 SC での実施内容を踏まえ、県 SC での対策と本業務におけるインターネットセキュリティ対策を整理し、明確にすること。

２．２．２　ネットワーク分離

既に「２．１　構築方針」に記載した三層の対策によるネットワーク分離は実施済であるが、構築内容を踏まえて必要な設計、設定を行うこと。なお、三つのセグメントは、以下のポリシーにより分離・分割を行うことを原則とする。

（１）マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定 MAC アドレス、 IP アドレス 及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、 その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、インターネット等からマイナンバー利用事務系との双方向でのデータの移送を可能とする。

（２）LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

① インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式
② インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式
③ 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

（３）インターネット接続系

① インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

２．２．３　インターネット接続経路の県 SC 経由設定

現在の本市のネットワーク構成は、行政機関からのインターネットへの接続は県 SC を経由している。令和４年３月に次期県 SC への移行が予定されており、構築期間中の移行が想定される。そのため、次期県 SC 移行に際しては、現在の強靭化システム環境で移行し、本システム稼働時は、次期県 SC への接続を変更する方針とする。

２．２．４　LGWAN 接続系パソコンから安全なインターネットの閲覧

（１）現在 LGWAN 接続系パソコンからインターネット閲覧を行う際は、インターネット接続系セグメント内に構築したサーバの画面転送を行う SBC 方式を採用している。次期システムにおいても、インターネット接続系セグメント内に仮想環境を構築し、LGWAN 接続系パソコンに画面転送のみを行う SBC 方式を基本とする。

（２）SBC サーバの OS は問わないが、安定稼働とセキュリティが担保されていること。

（３）利用者数は現在の情報系パソコンの台数である 700 ユーザとする。インターネット接続に関しては、同時接続数 100 が保証されること。

（４）利用者の特定、利用ログの分析ができること。

２．２．５　パブリッククラウドサービスへのオフロード通信

（１） 十分に安全性が確認されたパブリッククラウドサービス（例：Microsoft365 等）については、LGWAN 接続系 PC から県 SC を経由せずオフロード通信によりアクセスできること。

（２） オフロード通信先のサービスのドメイン情報等を自動更新できること。

２．２．６　ファイル無害化

（１）市民や民間企業等からのメールに添付されたファイルや Web サイトからダウンロー

ドしたファイル（インターネットファイル）については、）危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認した上で LGWAN 接続系セグメントに取り込むことができること。
（２）１ファイル１GB 以上のファイルを登録可能なこと。
（３）インターネット専用パソコンの資産管理、ログ収集などが行えること。なお、現在資産管理ソフトウェアとして SKYSEA Client View を導入しており、同ソフトウェアもしくは同等以上の機能を有すること。

２．２．７　メールセキュリティ対策
（１）本市では、グループウェアの Web メールを利用して、LG.JP ドメインのメールを LGWAN メールおよびインターネットメールとして利用している。
（２）インターネットメールの受信については、リンク無効化、HTML メールのテキスト化等の無害化処理を行ったうえで LGWAN 接続系セグメントのメールサーバに転送し、グループウェアで確認可能なこと。
（３）添付ファイルについては、ファイル無害化システムと連携することにより、自動で隔離し、無害化した上で添付ファイルを取得することができること。
（４）インターネットメールは、インターネット接続系セグメント内において原本を保存し、インターネット接続系パソコンで添付ファイルを含めて受信が可能なこと。
（５）許可をしたアドレスからのメールは、直接原本をグループウェアで受信可能なホワイトリスト機能を備えていること。

２．２．８　オンラインストレージ導入
（１）　ファイル無害化システムと連携することにより、LGWAN 接続系から外部ユーザー（市民、民間企業等）と直接ファイル授受が行えるオンラインストレージサービスを導入すること。
（２）　インターネットからのファイルを取り込む場合は、ファイルの無害化が行えること。
（３）　利用者の特定及びログ分析が行えること。

２．２．９　マイナンバー利用事務系ファイルサーバ更新
（１）マイナンバー利用事務系セグメントで利用している共有ファイルサーバを更新する。
（２）データ領域として１テラバイト以上を有すること。
（３）現サーバ内に保存されている文書ファイル等の移行を行うこと。
（４）マイナンバー利用事務系セグメント内ドメインコントローラーで設定しているグループ（課単位）でアクセス権を設定することができること。
（５）誤って削除してしまったファイルの復元機能を有すること。

２．２．１０　サーバ・ネットワーク機器の死活監視
（１）インターネット接続系セグメント内のサーバ・ネットワーク機器の死活監視を行う。
（２）定期的に ping 送信をし、応答がない場合は管理者宛にメール等で通知を行うこと。

２．３　調達機器・システム群（例）

本業務において調達する機器及びシステム群（例）を以下に掲げる。なお、現システム構成及び「２．２　基本要件」を踏まえた想定機器及びソフトウェアであり、提案内容によって追加、削除、台数の増減及びクラウドサービスを選択することを可能とする。各項目の括弧内は現在使用しているシステム（OS、アプリケーション等）を参考に記入している。

２．３．１　仮想ホスト

２．３．２に記載するゲストOSをホストする物理サーバ３台構成とする。

２．３．２　ゲストOS

（１）ドメインコントローラー（WindowsServer2012R2、ActiveDirectory×2）
インターネット接続系のユーザ情報、グループポリシー等を管理する。

（２）メールリレーサーバ（RedhatLinuxEnterprise7）
インターネットへの送信メールを県SCのメールサーバに中継する、またインターネットからの受信メールをメール無害化サーバへ中継する。

（３）ファイル無害化システム（LGWAN-ASPサービス）
市民や民間企業等の外部ネットワークから入手したファイルについて、危険因子をファイルから除去した上でLGWAN接続系セグメント内に取り込む。

（４）メール無害化システム（WindowsServer2012R2、m-filter）
インターネットメールをテキスト化しLGWAN接続系メールサーバに転送する。
添付ファイルを含めたインターネットメールの原本を保管する。

（５）インターネットプロキシ（WindowsServer2012R2、i-filter）
インターネット利用の際県SCプロキシサーバへの通信を中継する。
フィルタリング機能によりユーザごと、端末ごとにアクセス制限を行うことができる。

（６）クライアントウイルス対策システム（WindowsServer2012R2、TrendMicroApexOne）
クライアントPCのウイルス・マルウェア対策を行う。

（７）WSUSサーバ（WindowsServer2012R2、WindowsServerUpdateService）
クライアントPCの更新プログラムを管理・配信する。

（８）資産管理システム（WindowsServer2012R2、SKYSEAClientView）
クライアントPCの資産情報管理、ログ管理、リモート保守を行う。

（９）SBCサーバ（WindowsServer2012R2、CitrixXenApp）
画面転送方式によりLGWAN接続系PCでWeb閲覧を行う。

２．３．３　通信機器

（１）　県SC接続用ファイアウォール（Fortigate-200D×2）

インターネット接続系セグメントと県 SC 接続ファイアウォールの間に配置し、インターネットへの通信を制御する。

（２） オフロード通信用ブロードバンドルーター

オフロード通信先のクラウドサービスへ通信を中継する。

なお、通信回線については、別途調達する回線を利用すること。

２．３．４　セグメント間ファイル受け渡しシステム【ファイル無害化システム】

（１）マイナンバー利用事務系－LGWAN 接続系間ファイル受け渡しシステム(FileZEN×2)

・マイナンバー利用事務系セグメントと LGWAN 接続系セグメントの間でのファイルの受け渡しを行う。

・LGWAN 接続系セグメント内のドメインコントローラーによりユーザ認証を行う。

一定期間が経過したファイルを自動的に削除する。

（２）LGWAN 接続系－インターネット接続系間ファイル受け渡しシステム（LGWAN-ASP サービス）

・LGWAN 接続系セグメントとインターネット接続系セグメントとの間でファイルの受け渡しを行う。

・インターネットからのファイルの取込の際は、ファイルの無害化等を行えること。

オンラインストレージサービスと連携し、市民や民間企業等との間でもファイルのやり取りが可能なこと。

・２．３．４（１）と同一のシステムで構成が可能なオプション機能を有すること。

・１ファイル１GB 以上のファイルを登録可能なこと。

２．３．５　大容量ファイル転送・共有システム（LGWAN-ASP サービス）

ファイル無害化システムと連携することにより LGWAN 接続系セグメントから外部ユーザー（市民、民間企業等）と直接ファイル授受が行えるオンラインストレージサービスを導入すること。

２．３．６　マイナンバー利用事務系ファイルサーバ（WindwsServer2012R2）

マイナンバー利用事務系セグメント内で文書ファイル等を保存する。

２．３．７　その他関連機器等

（１） バックアップサーバ

・各サーバのディスクイメージ、データ等をバックアップする。

・障害発生時にバックアップからリストアする機能を有すること。

（２） 無停電電源装置（UPS）

・各サーバ、通信機器に対して電源供給を行う。

・停電時にサーバを自動シャットダウンさせる機能を有すること。

（３） 時刻同期（NTP）サーバ

・県 SC の NTP サーバから時刻情報を取得し、インターネット接続系セグメント内

のクライアントにサービスを提供すること。

（４） 死活監視システム（Zabbix アプライアンス）
・インターネット接続系セグメント内のサーバ･ネットワーク機器の死活監視機能を有すること。

（５） LCD コンソール及びコンソールスイッチ

（６） その他、目的を達成するために必要と思われるものがあれば調達に含めること。

２．４　委託内容に関する要件

２．４．１　全体管理業務要件

（１）調達する業務範囲は、本調達に関する契約期間にわたるすべての作業工程における業務全般とする。

（２）発注者から指導、助言を受けた際は、速やかに対応すること。

（３）本調達仕様書に示す以外で、全体管理業務を円滑に行うために必要となる作業があれば受注者が行うこと。

２．４．２　設計業務要件

（１）既存環境（機能・サービス）を十分に理解し、機能要件に従ったうえで、ネットワーク・サーバ環境を含むシステム全体の構成設計、機能設計、セキュリティ設計、移行設計、運用設計を行うこと。特に、ネットワーク間の特定通信に関しては、業務に必要な通信のみを許可し、不要な通信は全て遮断する。

（２）システム全体とは、ネットワークに関しては、本調達以外の機器群・出先接続・学校接続・LGWAN 接続・県 SC への接続を前提としたインターネット接続を含めた本市全体を指し、サーバ環境としては、本調達外の機器群を含めたサーバ・クライアント環境とする。

（３）設計に際し、事前環境調査も含めること。既存詳細情報（設定情報等）については、業者決定後別途案内とする。

２．４．３　構築・移行業務要件

本業務の提案・検討・調整結果から必要となった機器を調達、納品すること。設計内容に従い、構築及び移行作業を行うこと。本調達外の機器群に対しても設定変更などが発生する際は、本市立ち合いの上、既存導入業者、保守業者とも調整し、本業務に含めること。

（１）構築範囲

①ネットワーク分離・分割設定
②インターネット接続経路の県 SC 経由設定
③LGWAN パソコンから安全なインターネット閲覧環境の構築
④パブリッククラウドサービスへのオフロード通信環境の構築
⑤ファイル無害化システムの構築
⑥メールセキュリティ対策システムの構築
⑦オンラインストレージの導入

（２）作業内容

①機器の調達、搬入、設置作業

②機器等の設定、構築作業

③機器等の調整作業

④通信ケーブル、電源ケーブルの敷設、接続作業

⑤動作確認・テスト

⑥その他、目的達成のために必要な作業

（３）移行要件

①安定した稼働、業務継続性に影響することなく安全で確実な作業をすること。

②移行準備時、テスト実施時、移行作業時、運用開始時の日程および手法の具体的な提示については、発注者と調整のうえ、事前にすること。

２．４．４　運用・保守業務要件

（１）運用業務要件

①本調達で導入するすべてのサーバ機器、通信機器等について、操作手順書等を整備し納品すること。

②ソフトウェアの設定変更等、柔軟な運用ができるようマニュアル等を整備し納品すること。

③本市では、年度末の人事異動に合わせ複数システムの設定変更を職員で行っている。本調達におけるシステムで人事異動に伴う設定変更が必要な際は、既存システムと連携し設定変更を行うなど、運用面での負担軽減に配慮すること。

（２）保守業務要件

①障害やセキュリティインシデント発生時の対応窓口、対応方針を明確にしておくこと。

②保守対応時間については原則以下のとおりとする。

曜日：月曜日から金曜日（祝祭日等休業日は除く）

時間：9：00～17：30