三豊市不正持出し対策システム構築及び保守運用業務
仕様書

三豊市総務部総務課デジタル推進室

令和６年４月

第 1 章　目的

本市においては、情報セキュリティ強靭性向上モデルに対応した三層分離を実施しており、LGWAN 接続系ネットワーク（以下「LGWAN 系 NW」という。）及び LGWAN 系 NW と分離されたマイナンバー利用事務系ネットワーク（以下「マイナンバー系 NW」という。）を運用している。これらのネットワークについては、三豊市情報セキュリティポリシーに基づき情報セキュリティ対策を実施しているところであるが、運用に当たっては不正持出し等の出口対策について課題がある。

そのため、市の目指す運用ができる不正持出し対策システム（以下「対策システム」という。）を構築することにより、情報セキュリティ対策の更なる強化を行い、ひいては市が所有する市民情報を守ることを目的とする。

第 2 章　業務の概要

1　業務内容

⑴　環境構築業務：対策システムの構築及び本稼働

⑵　保守運用業務：構築した対策システムの保守・運用（6 年）

2　入札額

入札額は、環境構築費及び 6 年間の保守運用費を含めた上限額とする。

項　目	備　考
環境構築費	対策システム構築期間に必要となる全ての経費
保守運用費	6 年間（月額×72 か月分で算出すること。）

※落札者は、業務ごとの価格に関する内訳書を作成し、市に提出すること。

3　納入期限

令和 7 年 3 月 31 日まで【環境構築業務】

4　支払方法

⑴　環境構築費：一括払い

⑵　保守運用費：年間一括払い

（上記支払い方法を基本とし、落札事業者と協議の上定める。）

5　担当課

三豊市総務部総務課デジタル推進室

連絡先：0875-73-3000

第３章　契約

１　契約期間

⑴　環境構築：市の指定する日から令和７年３月 31 日まで

⑵　保守運用：本番稼働の日（令和７年１月１日を予定）から令和 12 年 12 月 31 日まで（６年）

なお、保守運用に関する契約については、「地方自治法施行令第 167 条の 17」及び「三豊市長期継続契約を締結することができる契約を定める条例第２条第２号」の規定による長期継続契約を締結するものとする。このため、翌年度以降の歳出予算における減額又は削除があった場合、市はこの契約を変更し、又は解除することができる。

２　契約不適合責任

受注者は、納入した製品の種類、品質又は数量に関して契約の内容に適合しないものは、手直し又は取替えの義務を負うものとする。

３　秘密保持

⑴　受注者及び受注者の使用人並びに再委託された場合の再委託先及びそれらの使用人は、業務の履行に関して知り得た情報を機密情報として取り扱い、他の目的に使用し、又は第三者に開示し、若しくは漏えいしてはならない。

⑵　受注者は、本件を履行するため市の個人情報を取り扱う場合は、個人情報の保護に関する法律（平成 15 年法律第 57 号）及び関連例規並びに別記１の個人情報取扱特記事項を遵守しなければならない。契約期間満了後も、同様とする。

⑶　受注者は、本件を履行するため市の情報資産を取り扱う場合は、三豊市情報セキュリティ条例（平成 18 年条例第 13 号）及び関連例規並びに別記２の情報セキュリティに係る特記事項を遵守しなければならない。契約期間満了後も、同様とする。

４　権利譲渡等の制限

受注者は、契約に係る権利又は義務を、市の承認を得なければ第三者に譲渡し、又は承継させてはならない。

５　費用負担

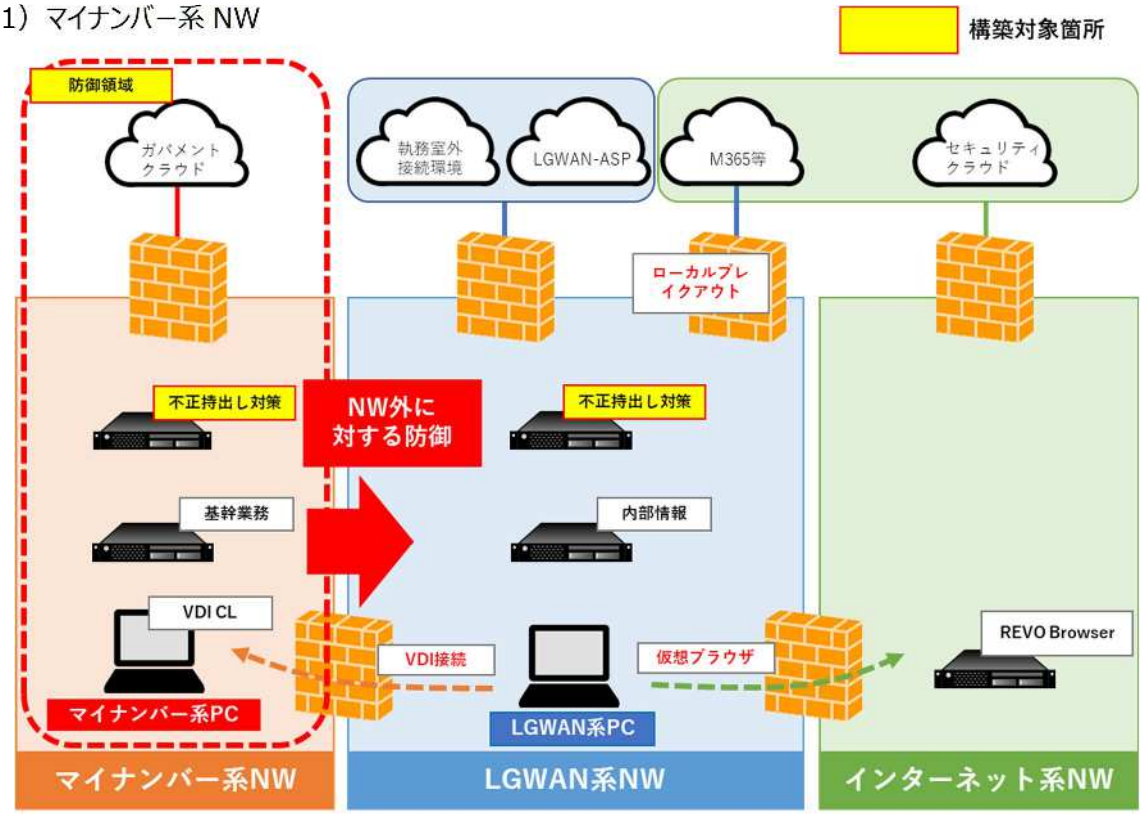
契約の締結に要する費用は、すべて受注者の負担とする。

第４章　業務仕様

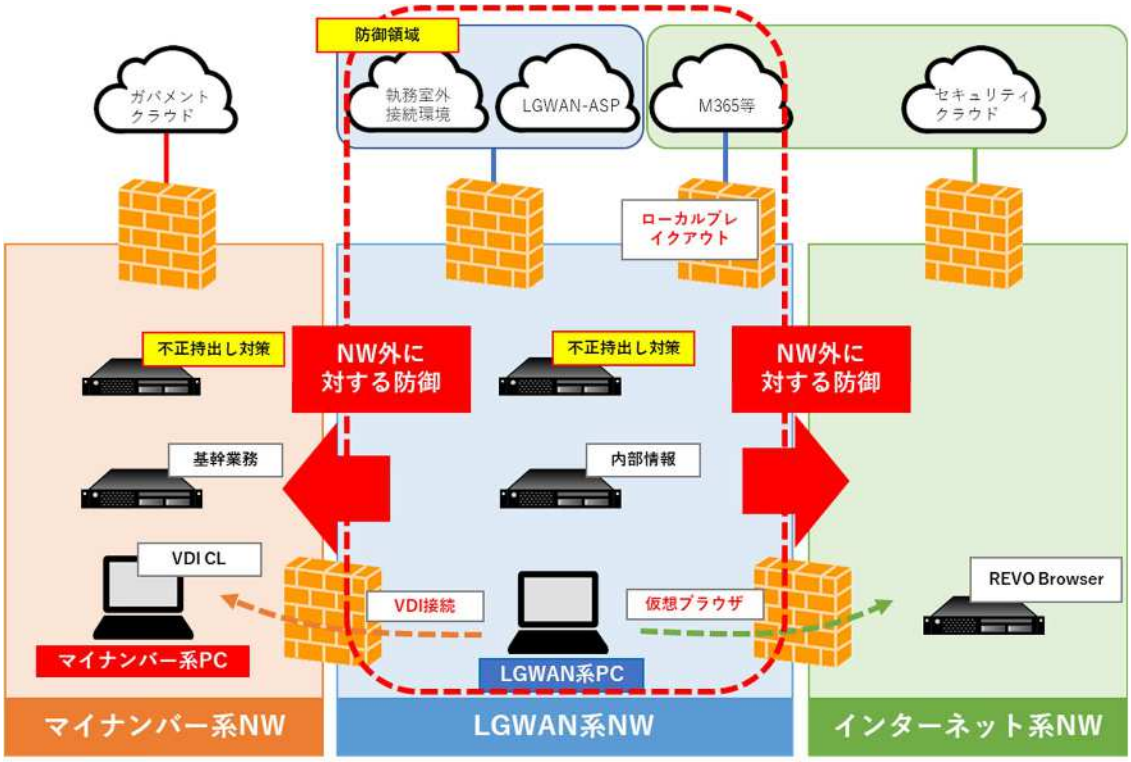
1　対策システムの構成

以下の構成図（案）を基本とし、市既存システム業者及びネットワーク業者との協議の上、決定する。なお、要求仕様を満たすものについて、システム構成の提案を制限するものではない。

（1）マイナンバー系 NW



（2）LGWAN 系 NW



2 対策システムの要件

項 目	要 件
要求機能	対策システムは、ハミングヘッズ株式会社 Security Platform 又は同等以上の機能を持つものとする。（別紙機能要件参照） 構成の例示は以下のとおり。 ① LGWAN 系 NW ＜サーバ側に必要なライセンス＞ ・Sep Server Basic Evolution / SV ・Sep トレーサオプション ・Sep Server イントラネットオプション ・Sep Server エンクリプションオプション ・Sep Server セパレートオプション ＜クライアント側に必要なライセンス＞ ・Sep Client Basic Evolution / SV ・Sep Client イントラネットオプション ・Sep Client エンクリプションオプション ・Sep Client セパレートオプション ② マイナンバー系 NW ＜サーバ側に必要なライセンス＞ ・Sep Server Basic Evolution / SV ・Sep トレーサオプション ・Sep Server イントラネットオプション ・Sep Server エンクリプションオプション ＜クライアント側に必要なライセンス＞ ・Sep Client Basic Evolution / SV ・Sep Client イントラネットオプション ・Sep Client エンクリプションオプション
利用端末	① LGWAN 系 PC（対象端末：870 台） ・CPU：intel Core i5、intel Core i3 ・メモリ：8GB ・OS ：Windows 10 Pro 64bit (15063)、 Windows 10 LTSB 64bit (14393)、 Windows 10 LTSC 64bit (17763) ・資産管理：ハンモック Asset View ・ウイルス対策：ハンモック Asset View Vplus ② マイナンバー系 PC（対象端末：250 台） ・CPU：intel Core i5、intel Core i3 ・メモリ：8GB、4GB ・OS ：Windows 10 Pro 64bit (15063)、

	Windows 10 LTSB 64bit (14393)、 Windows 10 LTSC 64bit (17763) ・資産管理：ハンモック Asset View ・ウイルス対策：ハンモック Asset View Vplus
導入先サーバ	市が保有する仮想サーバに対策システムを構築すること。 仮想サーバ 1 台につき許容するリソースは次のとおり。 ・CPU：8 コア ・メモリ：16GB ・ディスク：必要量 ・OS：Windows Server 2019 Standard また、基本ソフトウェアについては、次のソフトウェアの利用が可能である。 ・バックアップソフト：Veritas System Recovery 18 Virtual Edition ・ウイルス対策ソフト：トレンドマイクロ Apex One
基本要件	① LGWAN 系 NW ・マイナンバー系 NW、LGWAN-ASP、インターネット系 NW、電磁的記録媒体及びインターネットを「NW 外」として定義し、「NW 外」に対する防御を行うこと。 ② マイナンバー系 NW ・マイナンバー系 NW 以外の全ての場所を「NW 外」として定義し、「NW 外」に対する防御を行うこと。 ③ 用途ごとの PC モードを設定すること。 ➢ LGWAN 系モード 内部情報システム、グループウェア、ファイルサーバ等（以下「庁内業務システム」という。）を利用して行政事務を行うためのもの ➢ マイナンバー系モード 特定個人情報を取り扱う業務システムを利用して行政事務を行うためのもの ➢ インターネット系モード 管理者がインターネット接続系ネットワークの保守を行うためのもの ➢ 執務室外接続環境モード 特別の理由により執務室外で行政事務を行うときに利用するもの

3 スケジュール

環境構築業務において想定するスケジュールを下表に示す。

表 1 想定スケジュール

スケジュール	R6.4	5	6	7	8	9	10	11	12	R7.1	2	3
契約手続	→	→										
要件定義		→	→									
設計・構築			→	→	→	→	→					
テスト								→	→			
操作研修									→			
展開支援									→	→	→	→
本番稼働										→	→	→

4 設計・構築要件

項 目	要 件
設計・構築事業者	① ISO/IEC27001 による ISMS 認証の国際規格又は同等以上の認証を取得していること。
プロジェクト管理	① 本業務実施に当たり、情報セキュリティを確保し、確実に履行するための実施方法及び管理体制を整備した上でプロジェクト実施計画書にまとめ、市へ提出すること。 ② 全体の進捗及び各工程の詳細な進捗を可視化し、適切に進捗管理を行うこと。 ③ 各工程における決定事項や課題について、市と受注者とで意思疎通を明確にし、課題管理表を作成して報告及び説明を行うこと。 ④ 報告後は速やかに議事録を作成し提出すること。
セキュリティの確保	① 三豊市情報セキュリティ条例その他関連例規の規定を遵守した上で、本業務を進めること。 ② 本業務実施に当たり、責任者、作業に従事する者の氏名並びに所属及び作業場所を特定すること。 ③ 情報資産のライフサイクルに応じて適切な情報セキュリティ対策を講じること。 ④ 受注者は、本業務の全部又は一部の作業を第三者に再委託してはならない。ただし、市の事前承諾を得た場合は、受注者の責任において第三者に再委託できるものとする。 ⑤ 受注者は、市から提供された情報資産が業務終了等により不要になった場合は、確実に返却し又は廃棄すること。

	⑥ 情報セキュリティインシデントが発生した場合は、直ちに復旧作業を行い、原因分析及び対処方法を市に報告すること。
設計・構築	① 要件定義の内容に関する認識に相違が生じないよう、市と要件定義の内容について確認及び調整の上、要件定義を確定すること。 ② 対策システムが正常に動作するよう適切に設計し、端末、仮想サーバ、ネットワーク及びソフトウェアの設定を行い、そのすべての作業に係る設計書、設定手順書等をドキュメントとして市へ提出すること。

5 テスト要件

項 目	要 件
テスト実施計画	① 受注者は対策システムの正常稼働を保証するため、サーバサイドのシステムテスト、ユーザ視点の運用テスト等の必要なテスト項目やテスト方法等を記述したテスト仕様書を作成し、市へ提出すること。
テスト実施	① テスト仕様書に基づき、テストを実施し、全て合格すること。 ② テスト結果は、テスト結果報告書として取りまとめ、市へ提出すること。

6 操作研修要件

項 目	要 件
操作研修	① 管理者を対象とした操作研修を実施すること。研修の内容、方法、スケジュール等についての詳細は、事前に市と協議の上で進めること。
内容	① 管理者向け：Web 管理コンソールの操作方法等
開催回数	① 管理者向け：1 回

7 保守運用要件

項 目	要 件
ヘルプデスク	① 平日の 9 時から 17 時まで（可能であれば 8 時 30 分から 17 時 15 分までの開庁時間）の対応とし、電話、メール等での問い合わせに対応すること。
保守運用	① 運用における課題等が発生した場合は、課題管理表を作成し、市と受注者とで協議を行うこと。また、対応履歴を蓄積すること。 ② 運用中にシステム不具合、トラブル等が発生した場合は、保守報告書を作成し、報告及び説明を行うこと。 ③ 対策システムのハードウェア及びソフトウェアに障害が発生した場合の保守体制を明確にし、即座に対応が可能なこと。 ④ ソフトウェアのバージョンアップやメンテナンスに対応すること。
セキュリティ	① 対策システムは、ウイルスやマルウェア等に対する対策が適切に講じられていること。また、管理する機器、ソフトウェア等に関してセキュリティパッチやソフトウェア等の更新が公開された場合は適用判断を速やかに実施し、必要性のあるものについては速やかに対応すること。

	② サーバログ（システムログ、アプリケーションログ、セキュリティログ等）を取得し、最低 1 年間保管すること。 ③ 障害時等にシステムを復旧できるようバックアップを実施すること。

8 成果物

本業務における成果物を以下に示す。これ以外に本業務において必要と考えられる成果物がある場合は、提案すること。

なお、成果物は全て電子データで納入すること。

表 2 成果物一覧

項 目	成果物名	納入期限	要 件
環境構築	プロジェクト計画書	プロジェクト開始時	・業務実施方法 ・実施体制 ・セキュリティの確保に関する事項 ・その他事項
	進捗状況報告書	適時	・進捗状況 ・課題管理
	議事録	適時	・議事内容、決定事項
	テスト仕様書	テスト開始時	・テスト項目 ・テスト方法
	テスト結果報告書	テスト完了時	・テスト結果
	各種設定資料	運用テスト時	・確定した要件定義 ・設計書、設定手順書
	操作マニュアル	運用テスト時	・ユーザ向け操作マニュアル ・管理者向け運用、保守マニュアル ・その他必要となるマニュアル等
	保守計画書	令和 6 年 12 月 28 日	・保守内容
保守運用	保守報告書	適時	・保守作業報告
	課題管理表	適時	・課題管理

9 特記事項

・情報セキュリティインシデントが発生した場合は、当該インシデントの公表を必要に応じ行う場合がある。

・三豊市情報セキュリティポリシーに準拠した情報セキュリティ対策の履行が不十分と見なされるとき又は本業務に係る情報セキュリティインシデントが発生したときは、必要に応じて市の行う情報セキュリティ対策に関する監査を受け入れること。

・本業務委託に関し、三豊市情報セキュリティポリシーが遵守されなかったことにより、市又は第三者に損害を与えたときは、その損害を賠償しなければならない。再委託先においても同様とする。

・機器の搬入や設置に係る要件については、市と協議の上決定すること。

・搬入作業の際には、施設等を傷つけることのないよう、万全を期すこと。

・本仕様書記載内容に疑義が生じた場合、また必要な事項が生じた場合は、市と協議の上決定すること。

■別紙（機能要件）

カテゴリ	No.	要件
サーバ	1	仮想基盤上に構築可能なソフトウェアであること。
暗号化・復号化	2	NW内/NW外の定義は管理者により設定可能なこと。 ※NW内の定義は、PCのローカルドライブ、ファイルサーバ及びNAS、業務サーバ等のホスト名・IPアドレス・共有フォルダパス並びに庁内イントラネットのURL（グループウェア、業務システム等）において設定可能なこと。
	3	ファイル暗号化による運用トラブル（ファイル破損、動作の遅延、既存システムへの影響等）を避けるため、PCのローカルドライブ以外のNW内には平文で保存されること。
	4	PCからNW外へのファイル持ち出しは、管理者により許可されたプログラムからのみ持ち出し可能なこと。
	5	NW内に存在する全てのファイルが、NW外であるUSBメモリ等の外部記憶媒体、メールの添付ファイル、Webページへのアップロード、許可外サーバ等に持ち出される際は、ファイル拡張子に依存せず必ず自動的に暗号化され、又は禁止されること。また、暗号化に際し、パスワードの入力が不要なこと。
	6	暗号化されたファイルをNW内に戻したとき、自動的に復号化されること。また、復号化に際し、パスワードの入力が不要なこと。
	7	職員がNW内のファイルを正当にNW外へ持ち出す場合は、持出専用フォルダを経由して持ち出しができること。持ち出すファイルは平文を禁止しパスワード暗号化をかけたZIP形式に強制することも可能なこと。
	8	NW外へのファイル持ち出しにおいては、特定の管理者の承認を得たファイルのみ持ち出し可能な設定ができること（以下「承認機能」という。）。承認を得たファイルにおいても、パスワード暗号化をかけたZIP形式に強制することも可能なこと。
	9	承認に関する申請があった場合は管理者に自動で通知が飛ばせること。また、承認・否認した場合は、申請者に自動で通知が飛ばせること。
	10	承認機能については、本システムの提供機能で実装できること。
	11	AES暗号256bit以上の暗号強度が利用できること。
ローカルドライブ保存制限及び削除	12	PCのローカルドライブにファイルを保存できる領域を、特定の領域(以下、「特定領域」という。）のみに制限可能なこと。
	13	特定領域に保存されたデータは、管理者が指定したタイミングで自動で削除されるよう設定可能なこと。 ※削除タイミングはWindows起動・終了、ログオン・ログオフ、時間・曜日等から選択して設定可能なこと。
	14	管理者が特定のPCに対して、遠隔で特定領域に保存されたファイルの削除命令を発行可能なこと。
アプリケーション起動制限	15	アプリケーションの起動を制限可能なこと。 ※起動の許可・制限は、アプリケーション名、ファイルパス、ハッシュ値の組合せにより設定可能なこと。
IP送信の制御	16	IPプロトコルを使用したデータ送信（書き込み）を制限可能なこと。 ※送信（書き込み）の許可・制限は、アプリケーション名、IP アドレス、ポート番号の組合せにより設定可能なこと。
PCモード定義	17	管理者がPCに適用するセキュリティポリシーをモードとして複数定義でき、利用者が業務に応じてPCでモードを切替可能なこと。
	18	№12～№14の特定領域のみの制限をモードごとに設定可能なこと。
	19	№15のアプリケーションの起動制限をモードごとに設定可能なこと。
	20	№16のIP送信の制限をモードごとに設定可能なこと。
	21	使用できる有線LAN、Wi-Fi のアクセスポイント(SSID)、プロキシ又はVPN をモードごとに設定可能なこと。
	22	指定したパスのファイルに対するアクセスの制御（禁止又は読み取り専用）をモードごとに設定可能なこと。
	23	モード間のクリップボードのデータの制御（破棄又はテキストのみ可）をモードごとに設定可能なこと。
操作性	24	暗号化及び復号化は、職員の意識やITスキルに依存しないよう、職員が新たに暗号化ソフトの使い方を覚えることなく、ファイル作成・コピー・保存・アップロード等の通常操作の延長で、意識することなく自動で行われること。
履歴	25	NW外へのファイル持ち出しに関し、ユーザ名、コンピュータ名、日時、対象ファイル名、操作内容、持ち出し経路等の特定が可能な記録内容であること。
	26	インシデント発生時に、いつ、だれが、何を、どのような手段で、どのような形式で外部に持ち出したかを迅速に追跡できる履歴を取得できること。また、被害状況の把握、原因の追跡を行い、再発防止を講じるための証跡管理が行えること。
	27	承認機能において、誰が、いつ、どのファイルを、どのような理由で持ち出し申請・承認したのかを把握できる証跡を残せること。
	28	記録した履歴について一元管理が可能であること。
運用管理	29	運用管理負荷低減のため、上記要件を単一のソフトウェアで実現すること。
	30	SCCMやログオンスクリプト等の機能を用いて、サイレントインストールやアップデートができる機能を有すること。
	31	Active Directoryと連携して権限設定が行えること。
その他	32	国際標準規格 ISO/IEC15408 EAL3又は同等の第三者認証を取得したソフトウェアであること。