

仕様書

1 概要

本件は、当市が令和3年度に構築した自治体情報セキュリティ強靱化に資するインターネット閲覧システムを保全性の観点から更改するものである。情報セキュリティの確保と円滑な業務の遂行を可能とすることを目的とする。

2 基本事項

- (1) 物品名 インターネット無害化システム
- (2) 納入期限 令和9年2月28日（日）
- (3) 納入方法 指定の場所に設置・設定し、動作を確認すること
- (4) 納入場所 勝山市元町1-1-1 勝山市サーバー室
- (5) 納品物 各システムの設定表
- (6) 付随費用 システムの構築および既設設備との接続に要する費用は本調達に含まれるものとする
- (7) 参加資格 見積参加者は次の認証をすべて取得していること
 - ・ ISMS適合性評価制度に基づく ISMS認証ISO27001認証
 - ・ JISQ15001に準拠したプライバシーマーク使用許諾
- (8) 留意事項 本件は総務省の「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（令和8年3月版）」に規定するαモデルの要件を満たすように構築しなければならないことに留意すること

3 調達物品及び数量

- (1) インターネット閲覧システム 1式
- (2) ファイル無害化システム 1式
- (3) メール無害化システム 1式
- (4) 個人情報検索システム 1式

4 調達物品仕様

以下の要件を満たす物品を納入すること

- (1) インターネット閲覧システム
 - ・ 当市の職員各自が利用する行政事務用端末（Windows 11 Pro）（以下「職員用端末」という）内で論理分離したブラウザ（以下「分離ブラウザ」という）を構成し、端末内でインターネット通信の分離を実施すること。
 - ・ 分離ブラウザのみがインターネットへの通信ができること。
 - ・ 分離ブラウザを導入したことによって、職員用端末で従来行えた操作は全く制限されることなく操作可能であること。

- ・分離ブラウザは利用者が職員用端末上のブラウザと外見で識別できること。
- ・分離ブラウザで取得したデータを、職員用端末のデスクトップやCドライブなどの従来環境（以下「ローカル環境」という）に取り込む際にはファイルの無害化を必須とし、無害化できない場合には取り込みを禁止すること。
- ・分離ブラウザで動作する Web ブラウザは、メーカーが独自に提供するブラウザではなく、Microsoft Edge、Google Chrome が動作可能なこと。Microsoft Edge、Google Chrome の両方がローカル環境にインストールされている場合、分離ブラウザを起動する際に起動する Web ブラウザを利用者が選択できること。
- ・Web 会議の使用に際して、職員用端末に接続されたカメラ、マイク、スピーカー等のオーディオデバイスを分離ブラウザで利用できること。
- ・分離ブラウザと職員用端末のローカル環境でクリップボードの共有の許可不許可の設定ができること
- ・クリップボードの共有は指定したクリップボードのデータカテゴリ別（テキスト、画像、HTML）ごとに、許可/不許可の設定ができること。また、ローカル環境から分離ブラウザへのクリップボード共有のみ / 分離ブラウザからローカル環境へのクリップボード共有のみといった、クリップボード共有の方向を設定できること。
- ・分離ブラウザ上で表示している Web ブラウザ画面を、職員用端末に接続されたプリンターから印刷可能なこと。また、分離ブラウザからの印刷を禁止するかどうか設定を選択できること。
- ・分離ブラウザ上の個人プロファイルを保存できること。保存対象としては、お気に入り/ブックマーク、閲覧履歴、Cookie、パスワード、お支払方法・個人情報、ブラウザの拡張機能が保存可能なこと。
- ・システムによる同時接続数の制限ができること。
- ・管理用コンソールは日本語の GUI で提供されること。
- ・既設資産管理システムまたはドメインコントローラから職員用端末への分離ブラウザのインストール及び各種設定ができること。
- ・部署毎に設定を管理できること。
- ・分離ブラウザで閲覧した Web サイトは既設の資産管理システムにて、いつ、誰が、どのサイト (URL)、どのくらいの時間、閲覧していたかをログとして取得し、確認できること。
- ・分離ブラウザのアクセスログは日時、コンピュータ名、IPアドレス、パス/URL、タイトル、期間が取得できること。
- ・分離ブラウザとファイアウォールとの間に分離ブラウザ用ゲートウェイサーバを設置してファイアウォールから見て通信元が1つになるようにすること。

(2) ファイル無害化システム

- ・インターネット経由でファイルを職員用端末へ取込む場合にはスクリプト、マクロ及びOLEオブジェクトなどリスクの高い因子について総務省ガイドラインの無害化処理要件を満たしたうえで取り込むこと。
- ・無害化エンジンのソースファイルの拡張子の対応数については、一般に使用される160種類以上であること。
- ・無害化後のファイルの操作性(編集・加工)やアプリケーションの適合性を保持するため、無害化処理前と処理後で75%以上はファイル拡張子が変わらないこと。なお無害化処理についてはファイル構造を解析して、内部構造に含まれるファイル要素も無害化処理して再構成する処理プロセスを要件とし、この処理においてファイル拡張子が維持されること。
- ・無害化に対応していないファイルについては、マルチスキャン処理(複数のマルウェア検査エンジンによるウイルスチェック)を行い、安全判定となった場合に無害化処理はせずにファイルのダウンロードを可能とする制御ができること。
- ・無害化に対応しないファイルに対する危険因子のないことの確認のためのマルチスキャンエンジンについては4つ以上のマルウェアエンジンで検査できること。
- ・ファイルの拡張子だけでなく、ファイルシグネチャーやファイル構造などからファイルタイプを識別できること。また、ファイル構造が正規の仕様と異なる場合はこれを遮断もしくは正規のファイル形式への修正ができること。
- ・無害化に対応していない拡張子や拡張子を改ざんした不正なファイルの転送を遮断、または許可できること。
- ・無害化処理のポリシー設定については、アプリケーション単位にポリシー設定が可能であること。(例:Microsoft Office の場合、Word/Excel/Powerpointなどの単位)。
- ・無害化結果は、そのファイルが持つ要素(Officeファイルの場合、埋め込みオブジェクトやマクロ、ハイパーリンクなど)ごとに確認が可能であること
- ・以下のファイルについてマルウェア検査だけでなく再帰的な無害化処理ができること。

<文書ファイル>

Word (doc, docx, docm)、 Excel (xls,xlsx, xlsx)、 PowerPoint (ppt, pptm, pptx, ppsm)、Word Viewer (rtf)、Visio(vsd)、一太郎文書 (jtd, jtdc)

<画像ファイル>

JPEG (jpg/jpeg)、PNG(png)、TIFF(tiff)、GIF (gif)、BMP (bmp)、ai、ait、heic、Windows Metafile(wmf/emf)

<動画ファイル>

WMV(wmv), MPEG(mpeg), WAV(wav) , MP3(mp3), MP4(mp4), MOV(mov), AVI(avi), WEBM(webm)

<圧縮ファイル>

ZIP (zip), RAR(rar), 7Z(7z), GZIP(gz), XZ (xz), LZH (lzh)

<CAD>

AutoCAD (dwg) ,AutoCAD Drawing Template (dwt),AutoCAD Drawing Standards (dws), SXF Feature Comment (sfc),STEP Data Model (p21), JW CAD(jww), Drawing Interchange Format (dxf)Design Web Format (dwf), 3D Studio (3ds)

- ・無害化対象とする拡張子は、各拡張子ごとに有効／無効が設定可能であること。
- ・無害化装置の保守サポートにあたっては国内に製品担当技術者・サポートセンターがあり日本語での問い合わせの対応が実施できること。
- ・利用者の端末に専用モジュールをインストールせずに、機能を提供すること。
- ・仮想サーバ上でも物理・ベアメタルリソース上と同様の動作が可能であること。
- ・無害化エンジンを動かす実行機能分のサーバ以外に管理サーバ等必要としないこと。
- ・利用ユーザー数の増減によってライセンス費用が変化しないこと。
- ・マルチスキャンの搭載エンジンがエンジンメーカーより提供終了となった場合、追加費用が不要でエンジンが補填されること。
- ・分離ブラウザでダウンロードした際に無害化を行うダイアログが自動的に表示され、ワンクリックで無害化及びマルチスキャンが自動で実施され、職員用端末の事前に設定したフォルダへ転送されること。
- ・分離ブラウザに保存されているファイルについては、分離環境用のエクスプローラーを利用して、同様に無害化及びマルチスキャン実施され、職員用端末の事前に設定したフォルダへ転送されること。
- ・zip ファイル等、圧縮されているファイル、パスワードロックが掛かっているファイルについても対応できること。
- ・無害化せずに原本ファイルの受け渡しを実施する際は、申請承認ワークフローを使用し、申請された原本ファイルはマルチスキャンで安全性が確認された後物理端末側へ転送されること。
- ・申請承認ワークフローはActive Directoryと連携し、ActiveDirectoryに登録されたユーザーで申請することが可能なこと。またワークフローを使用した履歴(ログ)の取得も可能なこと。

(3) メール無害化システム

- メール無害化処理として、添付ファイルを削除し、URL リンク等の削除を行ったうえで、完全テキスト化する無害化転送機能を有していること。さらに、URL、メールアドレス、電話番号等リンク情報についてはリンク削除に加えて、リンク情報が無効になるように加工されていること。
- ファイル無害化システムと連携し、無害化処理後の添付ファイルを再添付し、内部メールサーバへ転送できること。
- メール無害化処理サーバは、メールの無害化機能に加えて、ユーザの操作性を考慮し、同一システム内にて、メールの原本を保存できる機能を有していること。なお、メール原本を閲覧する場合は、アーカイブ保存形式による都度検索処理をすること無く、一般的なメール BOX 形式で保存されたデータを一般ユーザが容易にアクセス出来るシステムであること。また、原本アクセスの際には、クライアント環境に依存することの無いよう Web ブラウザでのアクセスが可能であること。
- メールが無害化機能に加えて、有事の際の対応として通常の Web メールシステムとして、メールシステムの基本機能を装備されているシステムであること。なお、メールの送信機能については、LGWAN 用のメールサーバで一元管理することも想定し、メール作成の機能を利用できないようにユーザ及びグループ単位で機能を制御できること。
- 無害化転送先の設定は、GUI での登録及び CSV 形式での一括登録を有していること。
- 無害化転送機能については原則、インターネットメールシステムで受信した全件のメールを転送できること。ただし、必要に応じて特定送信元の場合は、転送時に無害化処理を除外する設定による運用が可能であること。
- 無害化転送を行う際には、添付ファイルの内容を即時確認できるように、添付ファイルの内容をテキスト抽出し、転送メール本文にその情報を挿入して、社内メールシステムに転送できる機能を有すること。これにより添付ファイルの確認のために、都度インターネットメールサーバにアクセスをしないように職員の負担を軽減できる機能を有していること。
- LGWAN 接続系のメールサーバに無害化転送処理を行う場合は、転送元メールのヘッダ情報を維持したまま、転送が出来ること。その転送メールに対して、LGWAN 接続系のメールサーバより返信処理をした場合、元の送信者に返信が可能であること。
- LGWAN 接続系のメールサーバに無害化転送をする際には、インターネットメールからの転送メールであると解るように、メールの件名に任意の文字列を挿入

し転送できること。

- ・ 地方自治体において、インターネットメールの無害化転送機能として、当市以上の規模にて長期間の稼働実績のあるシステムであること。
- ・ 一定期間を経過したメールについては、容量管理のため、メールサーバ上より削除できる機能を有していること。
- ・ ユーザアカウント管理については、Active Directory などの認証基盤と連携し、ユーザ追加などのアカウント管理ができること。
- ・ 複数のドメインが管理できるマルチテナント方式のシステムであること。
- ・ 無害化転送したメールに、無害化処理前の原本メールをプレビューすることが出来る URL を挿入し、インターネット閲覧システムから参照できる機能を有していること。
- ・ 受信 BOX に格納された無害化処理前の原本メールを、無害化転送先のメールサーバへオリジナル形式で転送できる機能を有していること。
- ・ ファイルサニタイズ製品との自動連携機能については、パスワード付き ZIP ファイルの解凍を行い、無害化処理後に再添付し、庁内メールサーバへ転送できる機能を有すること。なお、無害化処理ができなかったファイルについては、再添付せずに、メール本文のみ無害化処理を行い、併せて、無害化出来なかった添付ファイル名をメール本文に記述の上、庁内メールサーバに無害化転送を実施できること。
- ・ 既存のインターネットメールサーバ及びメール無害化サーバに保存されているメールデータの移行/取り込みの機能を有しているシステムであること。
- ・ 日本語マニュアルをインターネット上に公開していること。

(4) 個人情報検索システム

- ・ 個人情報を含むファイルを検出するアルゴリズムを有すること。
- ・ 検査可能なファイル形式として Microsoft Word/Excel/PowerPoint、一太郎、DocuWorks、および PDF を含むこと。また、アーカイブ形式として ZIP / Tar / Gzip / 7z / LZH / RAR / bzip2 を全て含むこと。
- ・ 検査条件は任意のグループごとに異なる条件を設定できること。
- ・ 検査対象が PC の場合とサーバの場合、個人情報取扱い部門端末とその他部門端末などで異なる検査条件を設定できることを想定した運用ができること。
- ・ 個人情報として、以下を検出できる辞書を含むこと。
 - 名字（漢字、カナ、ローマ字）
 - 住所
 - 電話番号
 - メールアドレス

- 生年月日
- マイナンバー（全角表記・半角表記両方に対応すること、区切りなしもしくは4桁ごとのハイフンもしくはスペース区切り表記に対応すること
- ・発注者が指定するキーワードを検査対象として追加設定出来ること。
設定方法は固定キーワードでの定義、および正規表現でのパターン定義の両方が可能であること。
- ・各辞書（検査項目）は、辞書ごとに閾値の指定ができること。
また、AND 検索、OR 検索を任意に組み合わせることができること。
- ・検査結果は、検出したファイルについて、ファイル名をフルパスで取得できること。
また、各辞書で検出された件数を表示し、個人情報の保存数が多いファイルが容易に特定できること。
- ・検査結果は CSV ファイルとして出力できること。
- ・差分検査に対応していること。
2 回目以降の検査は、前回の検査以降に更新、もしくは新規作成されたファイルを検査し、検査時間が短縮できること。
- ・検査結果は、ファイル中の個人情報に該当した箇所を確認できること。
個人情報に該当する文字列だけではなく、その前後の文字列情報と合わせて確認できること。
- ・検査対象 PC および検査対象サーバ上で単独で手動検査が可能であること。
- ・利用に際して管理サーバの構築を必要としないこと。
- ・検査結果を元に、検査対象としたファイルを任意のフォルダに移動させるバッチ処理ができるようにすること。

5 設置・設定作業

（1）インターネット閲覧システム

- ・仮想基盤上の仮想サーバにインターネット閲覧システムを構築
- ・仮想基盤上の仮想サーバに申請承認ワークフローサーバを構築
- ・仮想基盤上の仮想サーバに分離ブラウザ用ゲートウェイサーバを構築
- ・クライアント側に利用するために必要なプログラムの配信
- ・利用するために必要な設定を協議・実施すること
- ・ファイル無害化システムとの連携設定をすること
- ・システム管理者に運用に必要な教育を施すこと

（2）ファイル無害化システム

- ・設定うちあわせ
- ・仮想基盤上の仮想サーバにファイル無害化サーバを構築

- (OSインストール、OS基本設定含む)
 - ・ 設定実施
 - ・ 動作確認
- (3) メール無害化システム
 - ・ 詳細設計 (パラメータうちあわせ)
 - ・ 仮想基盤上の仮想サーバにメール無害化サーバを構築 (OSインストール、OS基本設定含む)
 - ・ パラメータ投入 (設定)
 - ・ 単体試験
 - ・ ファイル無害化システムとの連携パラメータ設定
 - ・ システム管理者に運用に必要な教育を施すこと
 - ・ 稼働切替時の立会い及び翌営業日の立会い
- (4) 個人情報検索システム
 - ・ 仮想基盤上の仮想サーバに検査対象サーバの構築 (ディスク容量は1TB未満とする)
 - ・ 定期的に個人情報判定を実施するためのバッチ処理の作成
 - ・ テストデータを用いた個人情報判定設定の動作テスト
 - ・ インターネット閲覧システムを用いてインターネットにアップロードする際にファイルを検査する仕組みと運用方法についての検討

6 その他

- (1) システムの更改スケジュールについては当市業務に支障が出ない日程を当市担当者と協議のうえ決定すること。
- (2) 仮想基盤上の仮想サーバは新規に構築すること。OSライセンスは、当市が保有するWindows Server 2025または2022を使用すること。
- (3) 既存のIPセグメントの変更は不要と想定しているが、必要が生じる際には下記当市ネットワーク保守事業者にお問い合わせのうえ、費用に含めること。

【問合せ先】 三谷コンピュータ株式会社

公共ソリューション部営業課 小林氏

TEL:0776-67-8004

7 参考商品

本仕様書を作成するにあたり、参考としたメーカー名及び製品名・型番等については下記のとおりである。なお、記載した製品名・型番等の機器に拡張モジュールまたは拡張オプション等を搭載することにより本仕様書記載の仕様を実現している場合があるため、その点を留意すること。

メーカー	製品名	型番等
SKY 株式会社	SKYSEA Client View (GL) ブラウザ環境分離ライセンス	同時接続数：100 利用権：5 年分
OPSWAT	MetaDefender Platform	同時接続数：250 利用権：5 年分
サイバーソリューションズ株式会社	CyberMail-CDR	メールアドレス数：500 利用権：5 年分
三菱電機ソフトウェア株式会社	すみずみ君	利用権：5 年分