要件一覧

１．基本要件

項番	内容
1-1	LGWAN接続系とインターネット接続系の通信経路の分割を行うこと。
1-2	主たる業務端末（LGWAN 接続系端末）から、セキュアブラウザまたはセキュアコンテナ等を起動し、インターネットの情報を参照できるようにすること。
1-3	LGWAN接続系とインターネット接続系の両環境間のファイル通信について、ファイル無害化システムを介して可能であること。 LGWAN接続系からインターネット接続系へのファイル転送については、無害化しない。 インターネット接続系からLGWAN接続系へのファイル転送については、無害化を実施する。
1-4	提案機器での同時接続評価等、動作検証が行われていること（評価項目および評価結果の提供が可能なこと）。
1-5	各システムのサーバ類を本市に設置する場合は、本市指定の19インチラックに設置すること。また、周辺機器類についても同様とする。
1-6	各システムで必要となるサーバ及び無停電電源装置・導入機器のコンソールユニットの他必要な機器は構築費用に含めること。
1-7	運用期間中に必要なソフトウェア等のライセンスについては、本調達の範囲に含めること。
1-8	本システムに関するサーバ・周辺機器類については、本調達の目的と効果について満たすものとし、かつ本仕様書の機能要件を全て満たし、７年間安全な形で運用できる構成にすること。システム利用及び保守と機器保守については運用開始から7年間とする。なお、機器保守にはUPSのバッテリー交換を含む。
1-9	導入する機器、ソフトウェア等については安定稼働の観点から、導入実績があり、契約期間中のサポートが可能であること。また、原則として契約期間中のソフトウェアのバージョンアップ及びパッチ適用は運用業務に含めること。バージョンアップ及びパッチ適用については、本市と協議の上、決定するものとする。
1-10	障害発生時には原因を調査し、システム及び機器を速やかに利用可能な状態に復旧すること。なお、平日（土・日・祝祭日を除く）の8 時30 分から17 時15 分までの間に生じた機器及びシステムの障害復旧については、直ちに対応し、この時間外に発生した障害についても受け付けられる体制とし、緊急性のある場合は市と別途調整の上、直ちに対応を行うこと。
1-11	システム及び機器保守サービスは原則該当機器が設置されている現場で行う「オンサイト保守」とすること。
1-12	ハードディスク返却不要サービスとすること。
1-13	クラウドサービスで提供する場合でHDDを交換等する場合はデータの消去又は破壊証明を提出すること。
1-14	障害復旧のために、機器ファームウェアのアップデートが必要な際は運用業務内で実施すること。その際には事前に検証を行い、本市と対応について協議を行うこと。
1-15	既設ネットワークシステムに影響を及ぼすことが無いように運用保守サービスを提供すること。
1-16	各システムに対して以下のサポートを実施すること。 ① 機器設定に関する技術的支援 ② 運用における技術的支援 ③ 障害発生時の切り分け支援 ④ セキュリティ確保のための技術的支援
1-17	本システムを運用する上で必要な情報の提供に努め、助言を求められた場合は速やかに対応すること。
1-18	システム保守期間終了後、サーバ等のデータは消去し、消去証明書を提出すること。
1-19	賃貸借契約終了後、全て無償譲渡すること。なお、クラウドサービスで利用するものは除く。
1-20	エラー状況があった場合は、システム会社に送付し回答を入手するのではなく、構築委託事業者による一次把握ができること。
1-21	本調達で構築する仮想ブラウザシステムは自治体情報セキュリティクラウドと接続される。
1-22	必要なログおよび設定のバックアップが自動でできること。
1-23	現行システムの課題を解決するためのシステム・機器等を選定すること。

２．非機能要件

（１）システム構成

項番	内容
2-1-1	導入する各システムは原則、本市サーバ室に設置とするが、可用性・機密性・完全性に加え通信の安定性が担保される場合はデータセンターでの提供も可とする。その場合のデータセンター使用料及び回線費用等は事業者の負担とする。
2-1-2	迅速な業務処理かつ安定的な運用のため、「3.3本案件で導入するシステムの利用者」が利用できるサーバ・機器構成（N台として事業者側で決定）とすること。 ただし、サーバ・機器構成が原因で、システムが遅延する等の影響がある場合、契約の範囲内でN台から増加する等、リソースの対応を行うこと。 ただし、利用数の増等による要因の場合は、別途協議するものとする。
2-1-3	機器に障害があった場合でもシステムの運用が継続できるよう、(N＋1台)の構成とする等、サーバ・機器が1台故障しても、運用が継続できる仕組みとすること。
2-1-4	「3.3本案件で導入するシステムの利用者」に増があった場合でも、ライセンスやリソース追加等の拡張性があり、容易に拡張できる仕組みであること。
2-1-5	必要な機器にはUPSを設置し、停電時の対応を行うこと。
2-1-6	システムの稼働時間は24時間とすること。
2-1-7	各端末にインストール等が必要な場合は本業務の作業範囲に含めること。

（２）セキュリティ

項番	内容
2-2-1	セキュアブラウザまたはセキュアコンテナ利用時に、マルウェア等に万一感染した場合でも、他のユーザに影響がなく、該当ユーザの仮想領域を初期化する等で対応可能なものであること。
2-2-2	導入する各システムは、サポートがあり、セキュリティ対策が実施されているもの。またアップデート可能なもの。
2-2-3	導入する各サーバにウイルス対策ソフトを導入することによる負荷で業務に影響を与えないように設計すること。ただし、アプライアンス等、ウイルス対策ソフトをインストールできない場合は除くが、その場合は別途代わりとなるセキュリティ対策が実施できる製品であること。また、運用期間中のライセンス等費用も金額に含めること。
2-2-4	導入する各サーバの接続ポートは指定できること。

３．機能要件

（１）共通機能（セキュアブラウザ、セキュアコンテナ、ファイル無害化システム共通）

項番	内容
3-1-1	管理用画面があり、機器の設定変更ができること。
3-1-2	管理用画面には、指定された職員のみ庁内ネットワークからアクセスできること。 また、https等安全な仕組みでアクセスできること。
3-1-3	管理画面では以下を確認、操作できること。 ・機器等の稼働状態やリソース（CPU負荷、メモリ使用量など）使用状況 ・設定変更 ・ユーザの追加、削除
3-1-4	機器異常発生時にメール通知が可能であること。
3-1-5	無停電電源装置により、停電時にもシステムを30分は継続して稼働させられること。
3-1-6	停電時には１時間経過後にシステムを正常にシャットダウンできること。
3-1-7	システムファイルおよび各ログなどは、必要に応じて手動バックアップを取得する環境を有すること。
3-1-8	端末またはユーザの接続履歴を記録し、ログとして１年間分を参照可能であること。
3-1-9	ログ機能として以下の情報を記録し、Web GUI の管理画面上で閲覧可能なこと。また、CSV ファイルでのエクスポートも可能なこと。ただし機能上不可の場合は別途提案を認める。 ステータス／ユーザ名／ホスト名／接続時間／終了時間
3-1-10	レポート機能として以下の情報を記録し、Web GUI の管理画面上でグラフィカルに閲覧が可能なと。ただし機能上不可の場合は別途提案を認める。 ユーザ別ログイン回数／最大同時接続数／平均起動時間／エラー回数・率／ CPU 使用率／メモリ使用率／ロードアベレージ／パケット総受信量
3-1-11	無害化サーバ上にユーザー毎のダウンロードフォルダを作成すること。

3-1-12	仮想環境からファイルをダウンロードする場合は上記フォルダに容易な操作で保存できること。
3-1-13	ブラウザのウインドウサイズはユーザが自由に変更できること。ユーザ毎にウインドウズサイズを記憶する機能を有し、次回接続時以降もそのサイズで起動可能なこと。
3-1-14	仮想環境とローカルアプリケーション間でコピー＆ペーストできる機能を有すること。その方向は設定により制御でき、コピー＆ペースト可能な情報はテキスト情報のみに限定出来ること。
3-1-15	仮想環境とローカルアプリケーション間で、コピー＆ペーストを制限した場合でも、仮想環境上内では、コピー＆ペーストできること。
3-1-16	起動時に表示される初期画面（ホームページ等）を指定できる機能を有すること。
3-1-17	日本語Web GUI での管理画面から、各種設定が容易に操作可能であることが望ましい。
3-1-18	ユーザアカウントはCSV での一括登録・変更・削除が可能であること。 不可の場合、人事異動等に柔軟に対応できる仕組みを構築すること。
3-1-19	同時接続数ライセンス方式の場合、指定した時間操作が行われていない場合、その仮想環境を終了させるアイドルタイムアウト機能を有すること。設定は1 分単位で可能なこと。
3-1-20	同時接続数ライセンス方式の場合、操作が行われていてもいなくても、指定した時間でその仮想環境を終了させる強制タイムアウト機能を有すること。設定は1 分単位で可能なこと。
3-1-21	接続時のユーザ認証でAD を参照可能なこと
3-1-22	Webアクセスログ取得のために上位プロキシにユーザ名や IP アドレス情報を付加して送信できる機能を有すること。
3-1-23	導入する各サーバはADと連携が可能であること。
3-1-24	バックアップツールを導入すること
3-1-25	システム及びハードウェア7年保守を提供すること（平日8:30～17:15）
3-1-26	データセンターで提供する場合は上記を参考に十分な環境を提供すること
3-1-27	人事異動の際、登録者の変更作業で人事異動データから変更データを作成し、CSV等で容易に登録できること
3-1-28	CSVファイルを用いたユーザ管理情報のインポート/エクスポートが行えること。
3-1-29	ランチャーが起動する場合は表示領域外から表示させるかタスクバーに表示できること。

（2）セキュアブラウザに求める機能

項番	内容
3-2-1	主たる業務端末（LGWAN 接続系端末）から、セキュアブラウザを起動して、インターネットの情報を参照できるようにすること。
3-2-2	セキュアブラウザ利用には、ID・パスワードを入力させるなど個人を識別する仕組みを持つこと。また、Active Directoryと連動してシングルサインオンできる機能があれば望ましい。
3-2-3	セキュアブラウザとLGWAN接続系端末のブラウザ(MicrosoftEdge、GoogleChrome、Firefox)は個別に独立して起動ができること。 これらについては、操作識別が容易になるようにすること（例：システム画面の外枠を色線で囲む、背景色を変更できる等）
3-2-4	セキュアブラウザのブックマークをユーザー毎に保存が可能なこと
3-2-5	セキュアブラウザのブックマーク、および各設定を管理者でユーザ分を一括変更できること
3-2-6	セキュアブラウザで一般的なストリーミング動画が閲覧できること。 その場合、接続したマイクやスピーカー等が使用でき、音声はユーザ側でＯＮ／ＯＦＦの切替が可能なこと
3-2-7	セキュアブラウザ上で開いたWeb画面やファイルを、LGWAN 接続系のプリンタに送信・印刷する設定が可能なこと
3-2-8	セキュアブラウザ上で、PDFファイルやWord、Excel、PowerPoint等のMicrosoft Officeファイルを閲覧可能であること。
3-2-9	ファイル無害化システムにファイルを送る際は、簡易な操作でファイル無害化システムに送り、ファイル無害化システムにて無害化処理を実施することが出来ること。 無害化されたファイルは、LGWAN端末側から取り出すことができること。
3-2-10	主たる業務端末（LGWAN 接続系端末）からインターネット接続系環境への接続時に暗号化通信を確立できること（その際の暗号化方式は、TLSが一定以上のバージョンである等、サポート期限内であるものとする）

3-2-11	履歴やキャッシュも含め、LGWAN側の他のアプリケーションから参照できないこと
3-2-12	履歴やキャッシュはセキュアブラウザの利用終了時、またはシステムからログアウトするタイミングで消去されること
3-2-13	ユーザ側ではセキュアブラウザに関する設定やアドオンの追加等が実行できないよう制御できること
3-2-14	タブブラウジングが出来ること。
3-2-15	ユーザーによるアドレスバーの直接入力や編集を制限できること。
3-2-16	セキュアブラウザ内検索ができること
3-2-17	Webサイトへファイルのアップロードができること。

（3）セキュアコンテナに求める機能

3-3-1	主たる業務端末（LGWAN 接続系端末）から、セキュアコンテナを起動し、セキュアコンテナ内のブラウザを用いてインターネットの情報を参照できるようにすること。
3-3-2	セキュアコンテナ内のブラウザに求める要件は、（２）セキュアブラウザと同じ。
3-3-3	セキュアコンテナと、ローカル端末については、操作識別が容易になるようにすること（例：システム画面の外枠を色線で囲む、背景色を変更できる等）
3-3-4	セキュアコンテナ内で、Officeを起動することができること。 ただし、LGWAN側のOfficeを利用する等とし、1ライセンスでLGWAN側もセキュアコンテナ内のOfficeも利用できるものであること。 ※ただし、上記からOffice内の同一アプリケーションをLGWAN側とセキュアコンテナ内で同時起動できなくても良い。
3-3-5	インターネット側のファイルをセキュアコンテナ内に一時保存することができること。
3-3-6	セキュアコンテナ内のファイルについて、ファイル無害化システムにファイルを送る際は、手動でファイル無害化システムにログインすることなく、右クリックなどの簡易な操作でファイル無害化システムに送り、ファイル無害化システムにて無害化処理を実施することが出来ること。 無害化されたファイルは、LGWAN端末側から取り出すことができること。
3-3-7	システムがインストールされた端末上に安全にファイルを閲覧、編集するための保護領域を作成すること
3-3-8	保護領域内で実行されたアプリケーションと、OSや保護領域外で実行された他のアプリケーション間とのデータ通信を禁止できること
3-3-9	一時保存したファイル、および操作履歴やキャッシュは、LGWAN端末側の他のアプリケーションに参照されないこと
3-3-10	一時保存したファイル、および操作履歴やキャッシュはセキュアコンテナの利用終了時、またはシステムからログアウトするタイミングで消去することができること
3-3-11	ユーザ側ではセキュアコンテナに関する設定やソフトウェアの追加等が実行できないよう制御できること
3-3-12	PDFファイルやWord、Excel、PowerPoint等のMicrosoft Officeファイルを別のアプリケーションに引き渡すことなくセキュアコンテナ内で表示が行えること

（4）ファイル無害化システムに求める機能

項番	内容
3-4-1	LGWAN接続系とインターネット接続系の両環境間のファイル通信について、ファイル無害化システムを介して可能であること。 LGWAN接続系からインターネット接続系へのファイル転送については、無害化しない。 インターネット接続系からLGWAN接続系へのファイル転送については、無害化を実施する。
3-4-2	別紙「ファイル一覧」のファイルを無害化対象として取り扱うことができ、ファイル拡張子単位で管理者による無害化可否を選択できること。
3-4-3	特定の管理端末（IN専用）から複数のウイルス（マルウェア）対策エンジンを利用し無害化対象外ファイルのスキャンができること。（マルチスキャン機能）
3-4-4	拡張子での判断だけではなく、ファイルの内容を見て判断できること。
3-4-5	無害化によりOfficeファイルのマクロが削除されること。
3-4-6	別紙ファイル一覧のファイル形式を維持したまま無害化してダウンロードする機能を有すること
3-4-7	ファイルを開かずに無害化処理を実施すること。
3-4-8	対象ファイルが圧縮ファイルである場合、圧縮ファイルを展開した後に各ファイルに対して無害化を行うこと。
3-4-9	対象ファイルが圧縮ファイルである場合、無害化が終了した後に再圧縮されること。
3-4-10	圧縮ファイルに圧縮ファイルが含まれる場合は、再帰的に展開、無害化及び圧縮が行われること。
3-4-11	パスワード付き圧縮ファイルについては、一階層の圧縮ファイルのみ無害化の対象とし、二階層以上の圧縮ファイルの場合は無害化処理を行わず、取り込みを禁止すること。圧縮ファイルの形式はZIP・RAR・7zが可能であること。
3-4-12	パスワード付きのMicrosoft Officeファイル及びパスワード付きのPDFファイルも無害化の対象とすること。
3-4-13	パスワード付きファイル等については無害化システム取込時にユーザがパスワードを入力することで無害化できること。
3-4-14	インターネット接続環境のファイル等をLGWAN接続環境への取りこむ際は、インターネット接続環境から本調達の無害化システムのフォルダ等を介して登録し、LGWAN接続環境からフォルダ等を介して無害化ファイルの取り込みを行うこと。
3-4-15	LGWAN接続環境で生成したファイル等をインターネット接続環境へ持ち出す際には、LGWAN接続環境のフォルダ等を介して登録し、インターネット接続環境のフォルダ等を介してファイルの持ち出しを行うこと。
3-4-16	システムに登録したファイルが無害化のサポート対象ファイルではなかった場合、エラーが表示されること。
3-4-17	無害化済みのファイルの保存期間を定義できること。保存期間を超過したファイルは自動的に削除可能であること。
3-4-18	無害化済みのファイルを削除する期間は、システムに登録したファイルに対して設定できること。
3-4-19	ファイルの持ち出し時に第三者承認を要求できること。
3-4-20	第三者承認機能の適用は、システムに登録したファイルに対して設定できること。また、インターネット接続環境からLGWAN接続環境への取り込み、LGWAN接続環境からインターネット接続環境への持ち出しの各々に対しても設定できること。
3-4-21	LGWAN環境で持出フォルダ等にアップロードしたファイルは第三者承認後、自動的にインターネット環境の持ち出しフォルダ等から持ち出せること。
3-4-22	システム全体の設定に加えて、任意のグループに対する設定が行えること。
3-4-23	任意のグループに対する設定には、ユーザ管理、第三者承認の有無、自己承認の可否等を含むこと。
3-4-24	第三者承認機能を使用する際に、承認者の不在時等に一時的に承認者を変更できること。または、複数の承認者をあらかじめ設定できること。
3-4-25	承認者の設定は役職等で一括設定できること。
3-4-26	人事異動の際、アカウントと役職情報等の紐づけが容易にできCSV登録できること。 容易にできない場合や機能がない場合、ＳＥ対応でも可能とするが、年2回の人事異動対応を保守費用に含めること。
3-4-27	無害化の履歴を記録し、管理者又は利用者が確認できること。
3-4-28	無害化の履歴には、利用者ID、ファイル名、無害化日時、承認者ID、承認日時を含むこと。
3-4-29	利用者の操作はWebブラウザ経由とし、利用者認証を行うこと。グループウェアと連動してシングルサインオンできる機能があれば望ましい。

3-4-30	ファイル無害化、ファイルダウンロード・アップロード操作を記録し、ログとして参照可能であること
3-4-31	無害化を行う場合、仮想環境が実行されるユーザ毎のセキュアな領域で無害化処理が実行可能であること。また、IN系専用端末からもブラウザで実行可能であること。
3-4-32	ユーザー数は1500ライセンス以上とする。
3-4-33	必要なログおよび設定のバックアップが自動でできること。
3-4-34	パスワードが無いメール添付のファイルはファイル無害化後、無害化メールに添付して送信すること。なお、現在使用のメールシステムを利用しない場合や既存メールシステム及びメールサーバに設定変更が必要な場合は別途その設定、機器費、構築費、保守費を計上すること。
3-4-35	無害化できない添付ファイルはメールにその旨記載され送付されること。
3-4-36	無害化システムへ取込際にパスワードを入力できること。
3-4-37	特定のフォルダ等にデータを移動すると自動で無害化できること。パスワードが必要な場合は入力画面が表示されること。
3-4-38	一度の処理で無害化できるファイル容量等の制限ができること。
3-4-39	別紙「無害化構成」の仕組みを構築すること。

（5）ADに求める機能

項番	内容
3-5-1	ドメインの管理ができること
3-5-2	DNSの機能を有すること
3-5-3	NTPの機能を有すること

No.	ファイル形式	拡張子
1	Microsoft Word	doc、docx、docm
2	Microsoft Excel	xls、xlsx、xlsm
3	Microsoft PowerPoint	ppt、pptx
4	Open Document テキスト	odt
5	Open Document スプレッドシート	ods
6	Open Document プレゼンテーション	odp
7	一太郎	jtd、jtdc
8	PDF	pdf
9	DocuWorks	xdw
10	テキストファイル	txt
11	CAD	DWG、DXF、JWW、SFC、P21
13	画像ファイル	png 、 gif 、 bmp 、 jpg(jpeg) 、 tif(tiff)、WDP
14	音声ファイル	mp3
15	動画ファイル	mp4
16	パスワード付きの Microsoft Word(オプション)	doc、docx、docm
17	パスワード付きの Microsoft Excel(オプション)	xls、xlsx、xlsm
18	パスワード付きの Microsoft PowerPoint(オプション)	ppt、pptx
19	Microsoft Rights Managent で暗号化した Microsoft Word	doc、docx、docm
20	Microsoft Rights Managent で暗号化した Microsoft Excel	xls、xlsx、xlsm
21	Microsoft Rights Managent で暗号化した Microsoft PowerPoint	ppt、pptx
22	Rich Text Format	Rtf
23	CSVファイル	csv
24	圧縮ファイル	zip,tar,rar,7z,gz
26	Adobe Illustrator	ai
28	QuickTime	mov