

福崎町情報セキュリティ強化サーバ環境構築業務
仕様書

令和4年5月

福崎町企画財政課

目次

1	業務概要	- 3 -
2	調達期間	- 3 -
3	現状構成	- 3 -
(1)	システム構成図.....	- 3 -
(2)	機器仕様	- 4 -
(3)	ライセンス数	- 4 -
(4)	利用者の環境	- 4 -
(5)	LGWAN 接続系とインターネット接続系のネットワークの分離	- 4 -
(6)	仮想デスクトップ環境	- 4 -
(7)	インターネットの閲覧	- 5 -
(8)	インターネット接続系における電子メールの利用	- 5 -
(9)	LGWAN 接続系とインターネット接続系のセグメント間の通信	- 5 -
4	要求仕様	- 6 -
(1)	更改範囲	- 6 -
(2)	共通仕様	- 6 -
(3)	個別仕様	- 6 -
①	仮想基盤システムの機能仕様	- 6 -
②	仮想デスクトップの機能仕様	- 7 -
③	セグメント間の通信	- 8 -
④	インターネットの閲覧	- 8 -
⑤	インターネット接続系における電子メールの利用	- 8 -
⑥	LGWAN 接続系とインターネット接続系のセグメント間の通信	- 8 -
⑦	管理用 PC の調達	- 9 -
⑧	兵庫県セキュリティクラウド用 UPS の調達	- 9 -
⑨	バックアップ環境の調達	- 10 -
⑩	その他	- 10 -
⑪	非機能要件	- 10 -
⑫	運用・保守	- 11 -
⑬	作業要件	- 11 -
⑭	プロジェクト管理	- 11 -
⑮	納品資料	- 11 -

1 業務概要

福崎町（以下「本町」という。）では、平成28年度より LGWAN 接続系とインターネット接続系との分離を行い、運用している。このたび、構築から5年を経過しサーバ機器等の保守サポートが終了することから、サーバ機器等の入替を行う必要がある。また、総務省では「自治体DX推進計画」の策定や「地方公共団体の情報セキュリティポリシーに関するガイドライン」等を参考にリプレースを実施し、端末の利用効率向上及び効果的運用を図ることができる環境の構築が求められている。本業務は、サーバ機器等の再構築を行い、本町が抱える課題への対応、個人情報保護等セキュリティの確保、行政運営の効率化および町民サービスの向上を目的として行うものである。

本業務の更新範囲及び基本要件については、以下のとおりである。なお、委託範囲の詳細は「4 要求仕様」に示す。

- ① LGWAN 接続系とインターネット接続系のネットワーク分離
- ② 仮想デスクトップ環境の構築
- ③ インターネットの閲覧
- ④ インターネット接続系における電子メールの利用
- ⑤ インターネット接続系と LGWAN 接続系のセグメント間通信

2 調達期間

① 構築期間

契約締結日から納品検査日（令和4年10月31日）まで

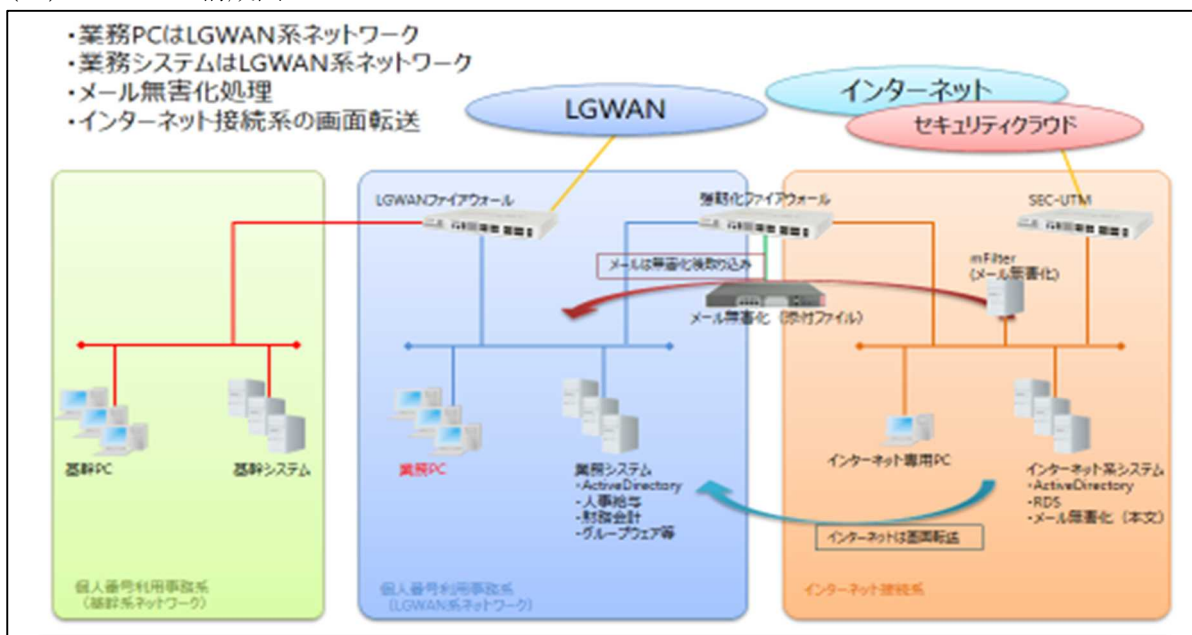
② 運用保守期間

システム運用開始日（令和4年11月1日）から令和9年10月31日までの60ヶ月

3 現状構成

本町の現行システムの構成は、以下のとおりである。

(1) システム構成図



(2) 機器仕様

種別	メーカー	型番	台数
リモート接続用機器	富士通	SR-S324TL2/Si-R G100	2台
	アライドテレシス	CentreCOM FS705TX V2	2台
仮想基盤用 AD サーバ	富士通	PRIMERGY RX2520 M1	1台
ホスト用サーバ	富士通	PRIMERGY RX2520 M1	3台
AD サーバ	富士通	PRIMERGY RX1330 M2	1台
ファイル無害化用機器	Asgent	SandBlast	1台
ファイアウォール	Asgent	CPAP-TE100X4VM	1台
仮想サーバ用 UPS	富士通	Smart-UPS SMT 1500RMJ	1台
AD サーバ用 UPS	富士通	Smart-UPS SMT 1500RMJ	1台
兵庫県セキュリティクラウド用 UPS	富士通	Smart-UPS SMT 1500RMJ	1台
管理用 PC	富士通	FMVK06008	2台

(3) ライセンス数

種別	メーカー	型番	ライセンス数
OS	Microsoft	Windows Server 2012 R2 Standard	5
CAL	Microsoft	WinSrvcsCAL 2016 Gov DvcCAL	250
	Microsoft	WinRmtDsktpSrvcsCAL 2016 OLP NL Gov UsrCAL	150
Proxy	デジタルアーツ	i-FILTER Ver.9 Standard Edition	250
メール無害化	デジタルアーツ	m-FILTER MailFilter & Archive	250
ウイルス対策	トレンドマイクロ	ウイルスバスター コーポレート エディション Plus	250

(4) 利用者の環境

- ① 物理端末の合計台数は 250 台で、OS は Windows10 Pro(64bit)である。
- ② Windows10 Pro のバージョンは 1903 である。

(5) LGWAN 接続系とインターネット接続系のネットワークの分離

- ① LGWAN 接続系とインターネット接続系の境界にファイアウォールを設置し、ネットワークを分離している。
- ② 設置しているファイアウォールは、FortiGate である。

(6) 仮想デスクトップ環境

- ① インターネット接続系に仮想サーバを構築し、LGWAN 接続系の物理端末から SBC 方式により、インターネット接続系の仮想端末を利用している。
- ② 仮想端末へのログインは、インターネット接続系に設置された AD により、ユーザ ID 及びパスワードで認証している。インターネット接続系の AD は、LGWAN 接続系の AD と同期をとっている。

③ 仮想端末で利用しているアプリケーションは以下のとおり。

種別	メーカー	アプリケーション名
ブラウザ	Google	Google Chrome
	Microsoft	Internet Explorer
ビューワー	Microsoft	Word Viewer
	Microsoft	Excel Viewer
圧縮・解凍	Schezo	LhaPlus

④ 仮想端末から物理端末の USB デバイス等の使用を禁止（制限）している。

⑤ 仮想端末からの印刷は、LGWAN 接続系に設置されたプリンタに出力している。

(7) インターネットの閲覧

① Proxy サーバとして、兵庫県に設定されている i-Filter を利用している。

② i-Filter のライセンスは、本町で保有している。

(8) インターネット接続系における電子メールの利用

① インターネットを利用した電子メールの送受信には、LGWAN 接続系と同じドメイン (@town.fukusaki.lg.jp) を使用している。

② インターネットからの受信メールは、以下の処置を行ったうえで、LGWAN 接続系の物理端末のグループウェアで閲覧している。

- ・ 添付ファイルの無害化後、再添付
- ・ リンク先の無効化
- ・ 本文のテキスト化

③ 添付ファイルが暗号化されており、無害化／再添付ができない場合、庁内の m-Filter Archive に保存されたメールを取得し、無害化したうえで LGWAN 接続系端末へ持ち込んでいる。

④ m-Filter のライセンスは、本町で保有している。

(9) LGWAN 接続系とインターネット接続系のセグメント間の通信

① LGWAN 接続系とインターネット接続系の間は、以下の特定通信のみ許可している。

通信元	通信先	特定通信の内容
LGWAN 接続系	インターネット接続系	RDP
インターネット接続系	LGWAN 接続系	AD 関連

② 許可された特定通信以外は、通信経路（IP アドレス）に加え、アプリケーションプロトコル（ポート番号）レベルで制限している。

③ インターネット接続系から LGWAN 接続系へのデータの受け渡しは、SandBlast を経由して無害化している

4 要求仕様

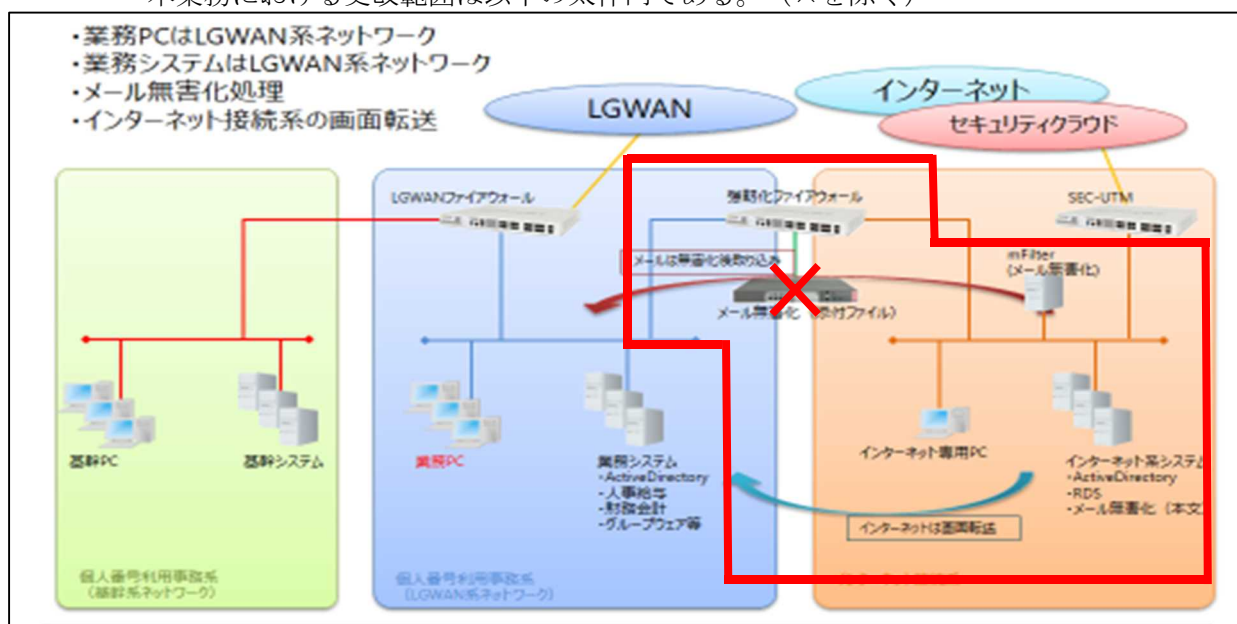
本仕様書の基本要件を実現するために必要な一連の作業すべてを含めること。

また、本仕様書を満たす機器、ライセンス等一式の調達を含むこと。

※機器の台数や構成についてはあくまで参考として提示しているものであり、構成が異なる場合でも同等以上の環境を構築できる場合は本町と協議の上変更できることとする。また、サーバOS等の各ライセンスについては最新のものを使用することが望ましいが、最新でないものを使用する場合には本町と協議の上決定すること。

(1) 更改範囲

本業務における更改範囲は以下の太枠内である。(×を除く)



(2) 共通仕様

- ① 「新たな自治体情報セキュリティ対策の抜本的強化について」(平成27年12月25日)及び「自治体情報セキュリティ対策の見直しについて」(令和2年5月22日)の指針をすべて満たすこと。
- ② 「3 現状構成」の記載事項及び下記「(3) 個別仕様」をすべて満たすこと。なお、重複する項目は、「(3) 個別仕様」を優先する。
- ③ 職員の利便性向上につながる提案を行うこと。
- ④ システム管理者の負担軽減につながる提案を行うこと。
- ⑤ 更改するシステムは24時間365日稼働することを基本とし、必要な冗長構成、バックアップを提案すること。
- ⑥ 利用対象とするユーザ数は250名とし、最大150名の同時接続ができる構成及び必要ライセンスを調達に含めること。

(3) 個別仕様

- ① 仮想基盤システムの機能仕様

- (ア) 仮想化基盤サーバはHCI 構成または3Tier 構成のいずれでも構わないこととするが、本契約で導入するシステムが稼働するにあたり問題ないリソースを確保した構成とすること。
- (イ) x86 ベースのサーバハードウェアプラットフォームを採用していること。
- (ウ) 10GbE に対応したネットワークインターフェースを2ポート以上搭載すること。
- (エ) ディスク、電源ユニットは、できる限り電源を停止せずにオンラインで交換・増設が可能であること。
- (オ) CPU、メモリ、ハードディスク、電源、ファン、電圧、温度の障害検知機能があること。また、検知した場合に管理者およびメーカーサポートに通知する機能を有すること。
- (カ) LED の点灯等により障害発生箇所が容易に判別できる機能を有すること。
- (キ) ハードウェア及びソフトウェア障害・修理等の受付対応時間は、平日8時30分から17時15分(土・日・祝日除く)とするが、それ以外の時間帯でも可能な限り柔軟な対応ができること。障害時の対応については、現地派遣・現地修復を基本とし、本町からの障害連絡後、翌営業日以降に技術員を派遣し訪問修理に対応すること。パーツ配送と交換サービスが5年間付帯していること。
- (ク) ディスク交換後の故障ディスクについては、データの廃棄証明書を提出すること。
- (ケ) ストレージ領域は、オールフラッシュ構成もしくはSSDとHDDを組み合わせたハイブリッド構成のいずれかとする。ただしハイブリッド構成の場合は、性能面を重視し頻繁にアクセスするデータを自動的にSSD階層に配置しSSDの性能を担保できる仕組みであること。
- (コ) ストレージのファームウェアの不具合などによる障害を配慮し、ストレージ装置は複数筐体構成または冗長構成で構築すること。

② 仮想デスクトップの機能仕様

- (ア) シンクライアントシステムの管理用画面は日本語のUIが提供されること。
- (イ) 画面転送方式はVDI方式、SBC方式、Linuxサーバ上のコンテナにブラウザを用意する仮想ブラウザ方式のいずれかをサポートしていること。
- (ウ) 仮想デスクトップで利用するアプリケーションを以下に示す。利用にあたって個別設定が必要なアプリケーションや記載のないアプリケーションがある場合は、本町と協議の上検討すること。

- ・ Adobe Acrobat Reader DC (PDFファイルの閲覧ができること)
- ・ Google Chrome
- ・ Microsoft Edge
- ・ Microsoft Office Viewer (Word、Excel、PowerPoint)
- ・ 一太郎ビューア (最新版)

※仮想デスクトップ上で使用する既存業務システムが正常に動作するように設定を行うこと。指定するアプリケーションの詳細な設定は、別途打合せのうえ決定する。

- (エ) どの仮想化サーバに接続してもユーザ特定の情報を読み込むためのユーザプロファイル機能を有すること。
- (オ) その他の方式での導入の場合、本仕様書に記載の要件を満たすことを明示すること。

③ セグメント間の通信

- (ア) インターネット接続系より LGWAN 利用端末へファイル持ち込みの際は、無害化が自動で実行された状況で取り込むことができること。なお、上長承認等の機能を有し、選択可能な仕組みとすること。
- (イ) ファイル無害化、ファイル転送操作を記録しログとして参照可能であること。また、ログは最低1年間保管できること。
- (ウ) 以下のソフト等で作成されたファイルについて、無害化処理を実行できること。なお、対応拡張子を明記すること。
(Microsoft Word、Microsoft Excel、Microsoft PowerPoint、Just Systems 一太郎、PDF、画像形式、CAD)
- (エ) インターネット経由でファイルを LGWAN 接続系端末へ取り込む場合、スクリプトやマクロについてファイルから除去（サニタイズ）できること。
- (オ) 最低限 2GB のファイルに対して無害化できること。
- (カ) LGWAN 接続系からインターネット接続系へファイル転送が必要な場合は、無害化が自動で実行された状況で取り込むことができること。なお、上長承認等の機能を有し、選択可能な仕組みとすること。
- (キ) 仮想環境から印刷する際、接続元の端末で登録されているプリンタを仮想側で自動的に認識し、接続元ネットワークと仮想側ネットワークが分離された状態で、プリンタ設定を行わずに利用できること。
- (ク) 接続元の情報系端末に接続した USB メモリ等の外部記憶装置を、仮想環境で使用できないように制御すること。

④ インターネットの閲覧

- (ア) LGWAN 接続系の物理端末から WEB 会議が利用できること。
- (イ) 兵庫県整備の i-Filter250 ライセンスを含めて構築し、Web フィルタリングを行うこと。

⑤ インターネット接続系における電子メールの利用

- (ア) 兵庫県整備の m-Filter を利用して、インターネットから受信したメールの原本を最低1ヶ月保存し、保存期間を経過したメールは自動削除する設定を行うこと。
- (イ) メールを送受信ログを最低1年間保存する設定を行うこと。

⑥ LGWAN 接続系とインターネット接続系のセグメント間の通信

- (ア) LGWAN 接続系とインターネット接続系間のデータ受け渡しに関するログを最低

1年間保存できること。

- (イ) LGWAN 接続系とインターネット接続系の間で最低 2GB 以上のデータの受け渡しができること。

⑦ 管理用 PC の調達

調達に伴う事項は次の通りとする。また、納入に付随する設定等の作業及び 5 年間の保守パックを含むこと。

(ア) 購入物品等の名称及び数量

- ・ ノート型パーソナルコンピュータ：1 台
- ・ ソフトウェア、ライセンス等：1 式

(イ) ノート型パーソナルコンピュータ仕様

名称	仕様
OS	Windows10 Pro 64bit 版 ※Windows11 インストールモデルの場合は、Windows10 へダウングレードを行うこと。
CPU	インテル® Core™i3 プロセッサ 第 9 世代 同等以上
メモリ	8GB 以上(メーカー純正品に限る)
HDD	SSD(256GB 以上)
ネットワーク	1000Base-T/100Base-TX/10Base-T と同等以上でイーサネットポートを本体に内蔵。 ・ LAN カード (PC カード) 不可 ・ 無線 LAN 機能を無効化 (無線 LAN 無) して納入すること
各種ポート	USB ポート：3 ポート以上実装 (うち 2 ポート以上は USB3.0 以上)。 (シリアルポートは非搭載でも可)
キーボード	テンキー付きキーボード (JIS 標準配列)
その他	フラットポイント内蔵、USB レーザーマウス 1 個添付 電源:内蔵バッテリー及び AC アダプタ添付、標準で 100V に対応すること

(ウ) ソフトウェア仕様

種別	メーカー	アプリケーション名
ブラウザ	Google	Google Chrome
	Microsoft	Microsoft Edge
Office ソフト	Microsoft	Office Professional 2019
PDF	Adobe	Adobe Acrobat Reader DC

⑧ 兵庫県セキュリティクラウド用 UPS の調達

- (ア) 兵庫県セキュリティクラウド用の UPS (5 年間の保守費用を含む) を調達し、交換すること。

指定機種：APC 社 Smart-UPS SMT 1500RMJ 台数：1 台

- (イ) 交換後は、兵庫県セキュリティクラウド用のサーバ及び UTM の正常性を確認すること。

⑨ バックアップ環境の調達

- (ア) バックアップ方式はイメージバックアップとすること。
- (イ) 復元はサーバ単位、ファイル単位に対応していること。
- (ウ) バックアップソフトの管理用画面は日本語の UI が提供されること。
- (エ) バックアップスケジュールとして、日次、週次、月次に対応していること。
- (オ) フルバックアップは初回のみとし、日々のバックアップは増分にて行えること。

⑩ その他

- (ア) 導入するサーバ用の UPS を調達し、電源障害時には UPS 管理ソフトウェア等と連携して導入したサーバ、ストレージ等を安全に自動シャットダウンできるように設定すること。
- (イ) アナログ KVM スイッチ (8 ポート) を 1 台調達し、使用するために必要な備品も併せて調達すること。
- (ウ) ラックコンソールを 1 台調達し、使用するために必要な備品も併せて調達すること。
- (エ) サーバ群の適切な構成上、ネットワーク機器 (L2 スイッチ等) が必要な場合は、受託者にて必要な性能及び数量のネットワーク機器を用意すること。なお、この場合の当該ネットワーク機器の設置及び設定にかかる費用も本調達の中を含めること。
- (オ) 各サーバについては、本庁舎 1F 情報管理室に設置するサーバラックに設置すること。

⑪ 非機能要件

- (ア) 受託者は、導入作業を開始するにあたり、本町における既存環境 (サーバ、ネットワーク及び住民システム等) を調査し、それを基にシステム導入計画、構成計画、設定提案書を作成し、本町と協議の上承認を得ること。
- (イ) すべての機器において、それぞれの機能を正常かつ安全に必要なできるように、必要な機器の搬入、設置配線接続工事を行うこと。
- (ウ) システム導入計画策定時に定義したスケジュールに基づく進捗管理を実施すること。
- (エ) 受託者は、納入作業における打合せ記録、各種報告書等を本町の指示に従い提出すること。
- (オ) 本調達の作業については、スケジュールリングと事前評価を十分に行い、本町の日常業務に支障が無いように配慮すること。
- (カ) 本町の業務に影響がある場合、協議を実施し、本町の許可を得た後に実施すること。
- (キ) 設定作業に必要な情報については、優先交渉権を獲得した提案者に開示する。

⑫ 運用・保守

- (ア) 更改したシステムに対し、5年間（60ヶ月）の運用・保守を行うこと。
- (イ) 少なくとも開庁日の8時30分から17時15分の間は運用・保守対応が可能な体制をとること。
- (ウ) 一元的な受付体制をとること。
- (エ) 障害の切り分けから復旧まで対応可能な体制をとること。なお、リモートでの運用保守に必要な回線及びネットワーク機器等は受託者が用意すること。
- (オ) ハードウェアは5年間のオンサイトまたはリモートにて保守を行うこと。
- (カ) 可能な限り短時間で駆け付け可能な体制をとること。
- (キ) ソフトウェアは、必要なバージョンアップ（パッチの適用を含む）を5年間行うこと。

⑬ 作業要件

- (ア) 本町と受託者の他、既存業者、兵庫県セキュリティクラウドの関係者等を含む役割分担を明確にすること。
- (イ) 庁舎への入館、搬入、作業等に必要手続きは本町の指示に従うこと。
- (ウ) 移行、切り替え等、システム停止を伴う作業は、夜間、休日に行うこと。
- (エ) サーバ室内の空きラック及び空き電源は使用可能であるが、不足する場合は、必要な物品、作業等を調達に含めること。なお、一次側の電源が不足する場合は、事前に本町の担当者と協議を行うこと。

⑭ プロジェクト管理

- (ア) 必要な計画書、手順書等を作成し、都度、本町と協議を行うこと。
- (イ) 作業の進捗及び発生した不具合等は、都度、本町に報告すること。

⑮ 納品資料

- (ア) 本番稼働に必要な品質検証及び準備が完了していることを本町とともに評価したのち、それぞれの提出時期に必要な資料を提出すること。なお、以下の表に必要な書類の例を示す。
- (イ) 運用開始前には、それまでに提出する必要がある資料をすべて取りまとめた完成図書を提出すること。

種別	資料の例	納品形態	提出時期
プロジェクト管理資料	・プロジェクト計画書 ・工程表 ・体制表	紙及び電子媒体	着手前
調達機器関連資料	・ハードウェア一覧 ・ソフトウェア一覧 ・製品カタログ ・取扱説明書 ・保証書	紙及び電子媒体	納品前

	<ul style="list-style-type: none"> ・ライセンス証書 ・インストール媒体 		
設計資料	<ul style="list-style-type: none"> ・設計計画書 ・基本設計書 ・詳細設計書 ・システム構成図 ・ネットワーク構成図 ・ラック搭載図 ・機器構成図 ・作業計画書 ・試験計画書 ・作業手順書 ・試験手順書 	紙及び電子媒体	構築着手前
構築資料	<ul style="list-style-type: none"> ・試験成績書 ・操作マニュアル 	紙及び電子媒体	構築完了後
運用保守資料	<ul style="list-style-type: none"> ・運用保守マニュアル ・各種手順書 ・運用保守体制図 	紙及び電子媒体	運用開始前
完成図書	<ul style="list-style-type: none"> ・上記を取りまとめたもの 	製本 2 部 電子記録媒体 1 枚	運用開始前
運用保守資料	<ul style="list-style-type: none"> ・運用保守の報告書 	紙及び電子媒体	都度

[別紙]

福崎町個人情報取扱特記事項

(条例等の遵守)

第1 受注者は、業務を遂行するにあたり、取り扱う個人情報については、別に定める「福崎町個人情報保護条例」及び「個人情報保護法」、「福崎町情報セキュリティ対策基準」を遵守し、個人の権利利益を侵害することのないよう、セキュリティに対する基本方針を持つなど、個人情報の取扱いを適切に行わなければならない。

(収集の制限)

第2 受注者は、この契約による業務を遂行するために、個人情報を収集する必要があるときは、業務の目的を達成するために必要な範囲内で、適法かつ公正な手段により行わなければならない。

(目的外利用・第三者への提供の禁止)

第3 受注者は、この契約による業務を遂行するにあたり、直接又は間接に知り得た個人情報を発注者の承諾なしに契約の目的以外の目的に利用し、又は発注者の承諾なしに第三者に提供してはならない。

(漏えい、滅失及びき損の防止)

第4 受注者は、この契約による業務を遂行するにあたり、直接又は間接に知り得た個人情報について、個人情報の漏えい、滅失及びき損の防止その他個人情報の適正な管理のために必要な措置を講ずるよう努めなければならない。

(廃棄又は消去)

第5 受注者は、この契約による業務を遂行するにあたり、直接又は間接に知り得た個人情報について、保有する必要がなくなったときは、確実かつ速やかに廃棄し、又は消去するとともに、発注者にその旨を報告しなければならない。

(秘密の保持)

第6 受注者は、この契約による業務を遂行するにあたり、直接又は間接に知り得た個人情報をみだりに他人に知らせてはならない。この契約が終了し、又は解除された後においても同様とする。

(複写又は複製の禁止)

第7 受注者は、この契約による業務を遂行するために、発注者から引き渡された個人情報が記録された資料等を発注者の承諾なしに複写又は複製してはならない。

(業務従事者への周知)

第8 受注者は、この契約による業務に従事している者に対して、在職中及び退職後においても、この契約による業務に関して、直接又は間接に知り得た個人情報をみだりに他人に知らせ、又は不当な目的に使用してはならないことなど、個人情報の保護に必要な事項を周知させるものとする。

(再委託の禁止)

第9 受注者は、発注者が承諾した場合を除き、この契約による業務については、自ら行い、第三者にその取扱いを委託してはならない。

(資料等の返還等)

第10 受注者は、この契約による業務を遂行するために、発注者から提供を受け、又は受注者自らが収集し、若しくは作成した個人情報が記録された資料等は、この契約完了後直ちに発注者に返還し、又は引き渡すものとする。

ただし、発注者が別に指示したときは当該方法によるものとする。

(立入調査)

第11 発注者は、受注者が契約による業務を遂行するにあたり、取り扱っている個人情報の状況について、随時調査することができる。

(事故発生時における報告)

第12 受注者は、この契約に違反する事態が生じ、又は生じるおそれのあることを知ったときは、速やかに発注者に報告し、発注者の指示に従うものとする。

(権利義務の譲渡等の禁止)

第13 受注者は、この契約によって生じる権利又は義務を第三者に譲渡し、もしくは継承させ、又は権利を担保に供することはできない。

ただし、書面により発注者の承諾を得たときはこの限りではない。

(契約解除と損害賠償)

第14 発注者は、受注者が前各条のいずれかに違反したときは、本契約を解除できるものとする。また、これによって生じた損害に対して受注者は賠償をしなければならない。その賠償額は、発注者受注者協議のうえ定めるものとする。

以上