

神奈川県後期高齢者医療広域連合
情報システム構築・運用関連業務委託等
要求仕様書

令和 7 年 12 月

神奈川県後期高齢者医療広域連合

余白

用語の定義

本仕様書で使用する用語の定義は、次のとおりとする。

神奈川県後期高齢者医療 広域連合電算処理システム (標準システム)	後期高齢者医療業務に係る資格管理、保険料の賦課、収納管理及び給付管理を行うための業務システム。インターネット接続なし。 令和6年度にオンプレミス環境からクラウド環境に移行した。
神奈川県後期高齢者医療 広域連合事務処理システム (庁内システム)	後期高齢者医療広域連合事務局内の文書管理、会計処理等を行うための情報システム。インターネット接続なし ^{※1} 。
広域連合	神奈川県後期高齢者医療広域連合を省略した表記。
広域連合情報システム	「後期高齢者医療制度」の運営を支えるシステムで、「標準セキュリティシステム」「庁内システム」「事務局 VDI システム」の総称。
標準セキュリティシステム	平成28年度に総務省が策定した「自治体情報システム強靭性向上モデル」のマイナンバー利用事務系のシステムのうち、標準システムにアクセスするための端末等の機器や、サーバー群を総称して、本書では「標準セキュリティシステム」と定義する。
庁内システム	平成28年度に総務省が策定した「自治体情報システム強靭性向上モデル」のLGWAN接続系のシステムのうち、広域連合事務局内で利用する端末等の機器や、サーバー群を総称して、本書では「庁内システム」と定義する。
事務局 VDI システム	広域連合事務局の職員が利用する仮想デスクトップ(以下、「VDI」という。)を構成する仮想化システム。標準セキュリティシステムを利用するためのVDI(標準VDI)と、庁内システムを利用するためのVDI(庁内VDI)がある。それぞれのVDIは機能的、セキュリティ的に独立している。
標準セキュリティシステム 仮想化基盤	標準セキュリティシステムのうち、主にサーバーのITインフラストラクチャを仮想化環境に統合したシステム基盤。
庁内システム仮想化基盤	庁内システムのうち、主にサーバーのITインフラストラクチャを仮想化環境に統合したシステム基盤。神奈川情報セキュリティクラウド(KSC)及び、総合行政ネットワーク(LGWAN)を利用するためのプラットフォーム機能を持つ。
標準 VDI	広域連合事務局で、標準セキュリティシステムを利用するためのVDI。インターネット接続しない。標準システムを利用するための独自の閉域網に接続し、二要素認証を行って端末を利用する。
庁内 VDI	庁内システムを利用するためのVDI。管理端末及び共用端末として利用する。二要素認証を行って端末を利用する。
VDI 利用端末	標準VDI及び庁内VDIを利用するため端末。手元端末。
標準物理端末	神奈川県下の各市区町村、広域連合事務局、国保連、国保連データセンターに配備した、標準システムを利用するための端末。インターネット接続しない。標準システムを利用するための独自の閉域網に接続し、二要素認証を行って端末を利用する。

一括転送端末	標準物理端末のうち、標準システムと医療保険者等向け中間サーバーとの情報連携を行う目的で利用する端末。標準端末と同一ネットワークに配置し、医療保険者等向け中間サーバーと通信を行うためのファイアウォールと専用のルータを必要とする。
統合専用端末	標準物理端末のうち、医療保険者等向け中間サーバーにアクセスするために設定した端末。インターネット接続なし。医療保険者等向け中間サーバーと通信を行うためのファイアウォールと専用のルータを必要とする。
庁内物理端末	庁内システムを利用するための物理端末。管理端末及び共用端末として利用する。二要素認証を行って端末を利用する。
神奈川県国民健康保険 団体連合会 (国保連)	国民健康保険法（昭和 33 年法律第 192 号）第 83 条 ^{※2} に基づき、会員である保険者（市町村及び国民健康保険組合）が共同でその目的を達成するため必要な事業を行うことを目的に設立された公法人。 神奈川県後期高齢者医療広域連合では、点検業務等を委託しているため、標準端末を国保連合会事務室に設置している。
神奈川情報セキュリティ クラウド (KSC)	神奈川県の自治体情報セキュリティクラウド。 自治体情報セキュリティクラウドは、近年のサイバー攻撃の複雑化・巧妙化を背景に、総務省が全国の自治体へ導入を推進しているもので、市町村が個別に実施しているセキュリティ対策を都道府県ごとに集約・強化するも。これにより市町村は高度なセキュリティ対策を独自に整備することなくサービスとして利用可能になる。
総合行政ネットワーク (LGWAN)	総合行政ネットワーク (LGWAN : Local Government Wide Area Network) は、地方公共団体を相互に接続する行政専用のネットワーク。

※1 インターネット接続は神奈川情報セキュリティクラウド(KSC)を経由し、仮想化環境で接続する。

※2 国民健康保険法第 83 条

(設立、人格及び名称)

第 83 条 保険者は、共同してその目的を達成するため、国民健康保険団体連合会（以下「連合会」という。）を設立することができる。

2. 連合会は、法人とする。

3. 連合会は、その名称中に「国民健康保険団体連合会」という文字を用いなければならない。

4. 連合会でない者は、「国民健康保険団体連合会」という名称又はこれに類する名称を用いてはならない。

目次

用語の定義	iii
目次	1
1 調達の概要	3
1.1 背景	3
1.2 目的	3
1.3 広域連合情報システムの全体概要図	4
1.4 システム機器要件	4
1.5 業務の範囲	4
1.6 契約件名及び履行期間	5
1.7 責任分界点	5
1.8 成果物	6
1.9 その他	6
2 標準セキュリティシステム機能要件	7
2.1 概要	7
2.2 サーバー要件	7
2.3 クライアント要件	9
2.4 ネットワーク要件	11
2.5 その他要件	11
3 庁内システム機能要件	12
3.1 概要	12
3.2 サーバー要件	12
3.3 クライアント要件	13
3.4 ネットワーク要件	14
3.5 LGWAN 接続要件	15
3.6 KSC 接続要件	15
3.7 その他要件	15
4 事務局 VDI システム機能要件	16
4.1 概要	16
4.2 サーバー要件	16
4.3 クライアント要件	17
4.4 ネットワーク要件	20
4.5 その他要件	21
5 構築要件	21
5.1 構築期間	21
5.2 業務体制	21
5.3 広域連合情報システム構築環境	21
5.4 機器の調達	22
5.5 システム構築	23
5.6 ネットワーク構築	24
5.7 VDI 構築	25
5.8 端末等のキッティング及び設置	25
5.9 データ移行	26
5.10 単体試験	26
5.11 結合試験	26
5.12 ユーザー試験	26
6 非機能要件	27
6.1 可用性	27
6.2 性能・拡張性	27
6.3 運用・保守性	27
6.4 移行性	27

6.5 セキュリティ	27
6.6 環境・エコロジー	28
7 運用・保守要件	28
7.1 窓口設置（共通）	28
7.2 監視（サーバー及びネットワーク）	29
7.3 障害の切り分け	30
7.4 システムの復旧	30
7.5 ハードウェア保守	30
7.6 運用支援	30
7.7 データバックアップ	32
7.8 実績報告	32
8 契約条件	32
8.1 契約条件	32

1 調達の概要

1.1 背景

神奈川県後期高齢者医療広域連合（以下、「広域連合」という。）は、75歳以上の高齢者等が加入する「後期高齢者医療制度」を運営しており、「後期高齢者医療制度」の運営を支えるシステム（以下、「広域連合情報システム」という。）を構築・運用している。当該システムは、神奈川県内のすべての市町村に配備され、恒久的に安全に安定して利用することが求められている。

広域連合情報システムは、平成28年度に総務省が策定した「自治体情報システム強靭性向上モデル」にならい、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の三層分離を実現した情報基盤であるが、令和9年3月末にシステムを構成する機器の賃貸借満了を迎えることから、機器の更改が必要となった。

1.2 目的

- (1) 標準システム等の業務システムの安定稼働を確保し、情報漏洩等のセキュリティ対策や運用面のさらなる向上を図る
- (2) 業務改善を含めた職員が安全に利用しやすい環境を構築する

次の項目に留意しながら、(1) (2) を実現するシステムを提案すること。

(ア) システムの安定稼働を確保し、セキュリティ対策や運用面のさらなる向上

広域連合情報システムではシステムを監視し安定稼働を維持すると共に、三層分離の実現、ウイルス対策や二要素認証等複数のセキュリティ対策を行ってきた。しかし、近年システムはますます複雑化し、システムが発報したアラートの原因を調査中にシステムの一部が利用できない事態が発生したことがあった。その反省から、さらなる安定稼働の確保に向けたシステムを構築すると共に、セキュリティ面や運用面の見直しを図る。

(イ) 職員が安全に利用しやすいシステムの構築

広域連合情報システムは定期的なプログラムの更新やウイルス対策ソフトのパターンファイルの更新を行い、システムの安定稼働を確保しながら、許可された機器以外の接続を遮断し、外部への不正持ち出し等の情報漏洩の予防を行っているが、日々巧妙化する攻撃に備え、職員が安全に利用しやすいシステムの提案を行うものとする。

また、広域連合及び拠点職員が安心してシステムを利用するため、利用拠点からの機器等に関する問い合わせに対して、広域連合職員でも即時解決できるような運用手順書等の充実を図る。

(ウ) 当該システムにおける、迅速な障害対応及び運用支援ができる仕組みの構築

現行システムでは保守受付窓口（24時間365日）を設置しているが、システム障害については発生条件の複雑さや、常に発生している障害ではない等、保守受付窓口への連絡から調査開始までに時間を要するといった様々な課題がある。本調達では、運用保守事業者と迅速に連携し、複雑化するシステム障害や障害と疑われる事象に対応できる支援や仕組みの構築を図る。

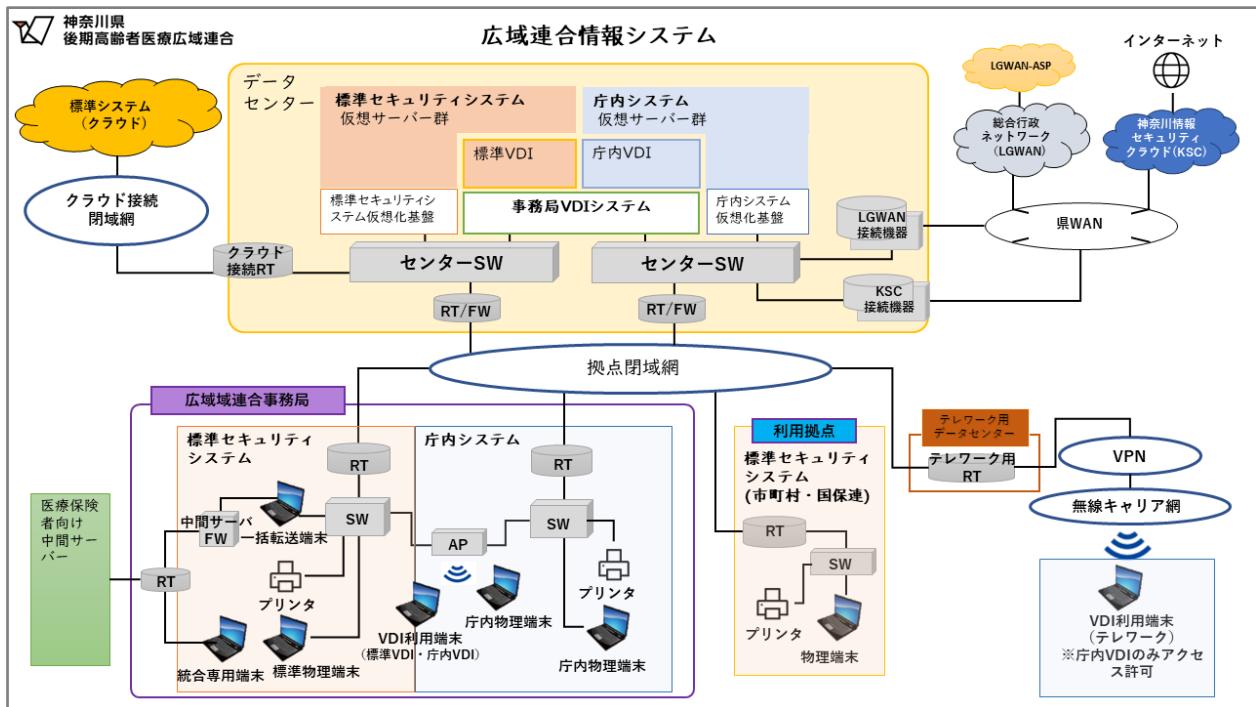
(エ) 業務に適した機器類の提案

現行システムの機器類は、サービス利用の要件を満たしているが、利用拠点より動作が重い等の申告が多く寄せられている。このような問題を解決すべく、本仕様書では、機器及びソフトウェアの利用方法を明記することで、業務により適した機器類の提案を行うものとする。

(オ) 現行システムと同等もしくは同等以上の製品の提案

標準セキュリティシステムは、神奈川県下の市町村の窓口等で日々利用されているため、端末やソフトウェアの起動等の待ち時間が極力短く、安全で安心して利用できる製品の提案を行うものとする。

1.3 広域連合情報システムの全体概要図



1.4 システム機器要件

構築対象機器は、次の別紙を参照すること。

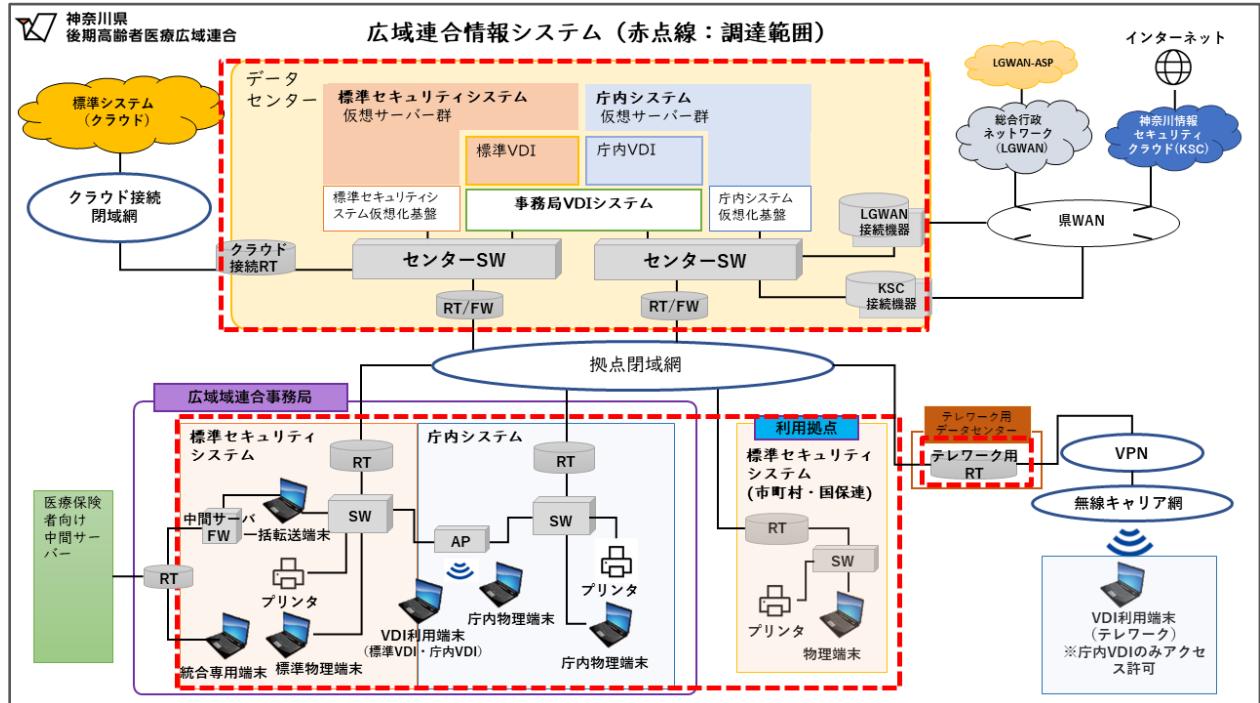
- (1)別紙1 現行システムクライアント端末仕様
- (2)別紙2 現行システムプリンタ、複合機、スキャナ仕様
- (3)別紙4 広域連合情報システムクライアント端末等台数一覧

1.5 業務の範囲

本件業務は、総務省が制定した「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」の内容について十分に把握した上で、広域連合情報システムの構築・運用・保守・管理を行うことを前提とし、業務の範囲（概要）は次のとおりとする。

- (1)広域連合情報システムの設計・構築（ネットワークの設計・構築を含む）
- (2)広域連合情報システムの機器の提案（機器の調達は別途入札を行う）
- (3)広域連合情報システムの各種ソフトウェア・ライセンスの提案（広域連合調達分を除く）
- (4)サーバー機器等のハウジング管理
- (5)市区町村等利用拠点用の機器設定及び配置等
- (6)サポート窓口の設置
- (7)サーバー及びネットワークの監視
- (8)障害対応・システム復旧対応
- (9)ハードウェア保守管理
- (10)広域連合情報システムの運用支援
- (11)データバックアップの管理
- (12)運用実績報告

調達範囲概要図



（※）LGWAN接続機器は広域連合が指定する種類の機器を調達すること。また、KSC接続機器、クラウド接続 RT（ルータ）は、広域連合が提供する。

1.6 契約件名及び履行期間

	契約件名	履行期間	備考
1	神奈川県後期高齢者医療広域連合情報システム構築業務委託	契約締結日～ 令和9年3月31日	—
2	神奈川県後期高齢者医療広域連合情報システム運用保守業務委託	令和9年4月1日～ 令和14年3月31日	—
3	神奈川県後期高齢者医療広域連合情報システム機器等賃貸借	令和9年4月1日～ 令和14年3月31日	別途入札を行う
4	神奈川県後期高齢者医療広域連合情報システムソフトウェア使用料	履行開始及び期間は別途 協議のこと	別途入札を行う

1.7 責任分界点

（1）現行システム事業者との責任分界点

現行システムの設定情報のうち、広域連合情報システムを構築するために必要な情報で、広域連合が提供した情報は、受託者に渡った時点から受託者の責任で管理し、当該業務の利用範囲に留めること。

広域連合情報システムの構築期間は現行システムが稼働中のため、現行システムへの影響を考慮し対応すること。特に新システムへの移行期間や現行システムと新システムとの切替時は、停止や性能劣化等を発生させない対策を講じ、万一、通信障害等の異常が発生した場合は、現行システムに切り戻しをしたうえで、速やかに原因究明を行うこと。

原因が新システムの構築に起因する場合は、対策を行った上で、是正及び予防措置を検討し、広域連合に報告し、了承を得ること。

(2) 標準システム関連事業者との責任分界点

標準セキュリティシステムの構築及び運用保守にあたり、標準システム環境、医療保険者向け中間サーバーのネットワーク、拠点閉域網に係る設定変更がある場合は、広域連合と関連事業者と協議した上で、受託者が対応すること。

(3) 庁内システム関連事業者との責任分界点

庁内システムの構築及び運用保守にあたり、LGWAN、KSC、テレワーク環境等に係る設定変更がある場合は、広域連合と関連事業者と協議した上で、受託者が対応すること。

また、庁内システムのネットワークに対する構成変更があった場合には、広域連合に対して必要な設定情報の提示を行い、了承を得ること。

1.8 成果物

(1) 構築時のプロジェクト進行に係る資料

契約締結日から移行完了までの全工程に渡り「5 構築要件」に記す構築に必要な資料（プロジェクト計画書、進捗報告書、会議記録、要件定義書等）を提出すること。提出方法は、原則として電子データとし、使用言語は日本語で、Microsoft Office の Word/Excel 等で作成した電子データを、メールやセキュリティで保護されたストレージを用いて提供する。

(2) 構築完了時の納入成果物（完成図書等）

次の内容を含む構築関連資料一式を、広域連合の承認を経た内容を電子媒体（DVD-ROM 等）で、広域連合が指示する場所に納入すること。完成図書等は構築後の保守を考慮し作成すること。使用言語は日本語と用紙サイズは A4 判縦型を原則とし、Microsoft Office の Word/Excel 等で作成すること。また、PDF 形式にした資料も提供すること。

（ア）物品一覧（調達明細及び数量）

（イ）構築時のプロジェクト進行に係る資料（プロジェクト計画書、進捗報告書、会議記録、要件定義書等）

（ウ）基本設計書（サーバー、ネットワーク）

（エ）詳細設計書（ネットワーク構成図、ラック搭載図、拠点レイアウト図、拠点ネットワーク構成図、ネットワーク機器詳細設定書、サーバー機器詳細設定書、IP アドレス一覧、各端末の設定情報一覧）

（オ）試験成績表（ネットワーク試験成績表、サーバー試験成績表、結合試験成績表）

（カ）保守手引書

（キ）運用管理手順書

（ク）機器等に設定したデータ

（ケ）管理アカウント一覧

（コ）各端末の復旧手順書及び復旧用資材

（サ）製品マニュアル

（シ）その他広域連合が求める資料

(3) 運用保守成果物

「7 運用・保守要件」に記す、月毎の定期報告書を提出すること。

1.9 その他

(1) 成果物の修正等

（ア）成果物に修正等がある場合、更新履歴と修正箇所等を示した上で修正後の全編を速やかに提出すること。

（イ）運用管理業務に関連する成果物については、広域連合と協議の上、必要に応じて記載内容を変更し、速やかに提出すること。

（ウ）別途契約において指示がある場合には、その指示に従うこと。

（エ）必要に応じて納入成果物の提出を求める場合があるため、作成資料は常に管理し、最新状態に保持すること。

(2) 検収

- (ア) 広域連合において、受託者立会いの上、広域連合が試験運用を実施後、次期広域連合情報システムに係る検収を実施する。なお、検収実施に際しては、可能な限り実運用を想定した必要十分な範囲の検証ができる方法を提案すること。
- (イ) 受託者は、前述「1.8 成果物」に則って納入成果物を提出すること。その際、広域連合の指示により、別途品質保証が確認できる資料を作成し、納入成果物と併せて提出すること。
- (ウ) 検収の結果、納入成果物の全部又は一部に不合格品が生じた場合には、受託者は直ちに引き取り、必要な修正を行った後、指定した日時までに修正が反映された全ての納入成果物を納入すること。
- (エ) 前述「1.8 成果物」以外にも、必要に応じて納入成果物としての提出を求める場合があるため、作成資料は常に管理し、最新状態に保持すること。

2 標準セキュリティシステム機能要件

2.1 概要

標準セキュリティシステムは、標準システムにアクセスする機器が強靭なセキュリティに守られ、安全に利用できるように構成したシステムである。標準セキュリティシステムはデータセンター内の仮想化基盤にサーバー群を構成し、専用回線で接続された神奈川県下 33 市町村、広域連合事務局、国保連、国保連のデータセンターのネットワーク上に端末を配置する。独立したネットワークを構成し、インターネットへの接続はしない。

2.2 サーバー要件

次に、サーバーの機能要件を記す。表の「次期製品」列に製品名が記載されている機能は、指定の製品を選定すること。「事業者にて選定」と記載されている機能は、履行期間内のサポート継続可能な製品を事業者にて提案すること。なお、参考として現行製品を記す。

要求機能	説明	次期製品	(参考) 現行製品	
			名称	利用状況
仮想化ソフトウェア	サーバーのリソースを仮想化し、仮想サーバーを効率的に稼働・管理するためのソフトウェアであること。	事業者にて選定	VMware vSphere Standard	※ 1
Active Directory	ユーザー管理、グループ管理、アクセス制限、名前解決、時刻同期等システムを管理することができること。	Windows Server	Windows Server	約 1,300 名
ユーザー認証 (二要素認証用)	生体認証やカード認証の認証機能を備えること。過去も含め認証記録を保持できること。	SmartOn ID 自治体専用強靭性向上特別パック	SmartOn ID 自治体専用強靭性向上特別パック	生体認証：約 1,300 名 カード認証：50 名

ファイル授受 (広域連合・拠点間)	<p>広域連合事務局と広域連合事務局以外の拠点がファイル授受を行うための機能を備えること。</p> <p>承認機能は不要。授受するファイルと伝言メモが残せると良い。(メール機能を使用せず、利用者閲覧権限を限定することができれば、ファイルを添付できる掲示板のようなものでも可。)</p> <p>現行システムでは、FileZen のプロジェクト機能を使って、広域連合と各拠点（市町村・国保連）のプロジェクトを作成し、職員にアクセス権を付与する。アクセス権を付与された職員等は、Web 画面からファイルとコメントのアップロードができるとともに、アクセス権が付与されたプロジェクトにアップロードされたファイルのダウンロードやコメントの閲覧ができる。</p> <p>(例) 広域連合と国保連でプロジェクト A を作成する。プロジェクト A のアクセス権を付与された広域連合と国保連の職員は、Web 画面にログインし、プロジェクト A にアップロードされたファイルのダウンロードやコメントの閲覧ができる。広域連合と国保連のアクセス権を付与されていない職員等はグループ A の情報にアクセスできない。</p>	事業者にて選定	FileZen	約 620 名
資産管理	<p>標準セキュリティシステム内のクライアント端末の資産管理を行い、外付けデバイス等の利用制限やソフトウェアを配布することができる。</p> <p>また、操作ログを取得することができる。</p>	事業者にて選定	SKYSEA Client View	約 360 台
バックアップ・リストア	<p>ファイルサーバーのデータや、各種サーバーの OS イメージのバックアップを行うこと。バックアップデータのリストアがされること。</p> <p>ファイル名やフォルダ名に漢字やカタカナや記号を含む場合も、文字化けすることなくバックアップ、リストアがされること。</p> <p>共有フォルダのデータは過去 7 日分のデータが復元可能のこと。それ以外は原則 4 世代管理とする。</p>	事業者にて選定	Arcserve UDP Appliance	12TB 使用率：約 86% ※ 2

ウイルス対策	次期システムでは Windows Defender を利用するため WSUS 中継サーバーを用意すること。Windows Defender の定義ファイルは、標準システム（クラウド）上にある WSUS サーバーから WSUS 中継サーバーを経由し、端末やサーバーに配信できること。それ以外の配布プログラムの制御ができること。	WSUS	Trend Micro Apex One	約 360 台
MAC アドレス認証	標準セキュリティシステムに接続する全ての機器について MAC アドレスで認証すること。登録されていない機器からのアクセスを防止すること。	事業者にて選定	NetAttest EPS	約 900 個登録可能な状態で運用
リモートアクセス	広域連合事務局の管理端末から、拠点の標準物理端末にリモートアクセスするため必要な機能を備えていること。	事業者にて選定	Soliton Secure Desktop	約 320 台
ストレージ	広域連合事務局や各拠点用のファイルサーバーとして利用できること。 拠点ごとにフォルダの利用を制限し、フォルダのサイズを拡張・縮小・新設する等、容易に変更できること。 必要に応じて、仮想マシンの構成ファイルや仮想ディスクファイル等のデータが格納できること。 また、標準セキュリティシステムの端末操作ログは 7 年間保管できること。	事業者にて選定	NetApp 本体 : FAS2750A-003-SC 拡張シェルフ : DS224C-10-1.2-12S-QS-N	ファイルサーバー領域 : 約 9.5TB 使用率 : 44% 増加量想定容量 : 約 500GB データストア領域 : ※ 1
ファイルサーバー	広域連合及び拠点から、ファイルサーバー（共有フォルダ）にアクセスできること。 広域連合及び拠点ごとに利用できるフォルダが存在し、アクセス制限できること。システムの管理者がフォルダのアクセス制限を付与することができるること。	事業者にて選定	NetApp 本体 : FAS2750A-003-SC 拡張シェルフ : DS224C-10-1.2-12S-QS-N	拠点毎のフォルダ数 : 83 各拠点フォルダの使用量を制限 ※ 3

(※ 1) プロポーザル参加表明書を提出した事業者のうち、「プロポーザル参加資格確認結果通知書」により参加資格を有すると認められた事業者は、広域連合事務室にて現行仕様書を閲覧可能とする。

(※ 2) 広域連合情報システム全体の利用状況。

(※ 3) Active Directory の OU (組織単位) やセキュリティグループでアクセス制限をかける。

2.3 クライアント要件

標準セキュリティシステムのクライアント端末は、標準物理端末（「統合専用端末」、「一括転送端末」を含む）と標準 VDI の 2 種類あるが、広域連合事務局で利用する標準 VDI は「事務局 VDI システム機能要件」に記載する。

標準物理端末の主な利用目的はブラウザを用いた標準システムへのアクセスである。

次に標準物理端末の機能要件を記す。表の「次期製品」列に製品名が記載されている機能は、指定の製品を選定すること。「事業者にて選定」と記載されている機能は製品を事業者にて提案すること。参考として現行製品を記す。

要求機能	説明	次期製品	(参考) 現行製品
Microsoft Windows	端末のオペレーティングシステム。	Windows 11 IoT Enterprise LTSC 2024	Windows 10 Enterprise LTSC 2019
ユーザー認証 (二要素認証用)	端末にログインする際、パスワード認証以外に生体認証やカード認証ができること。	SmartOn ID Client	SmartOn ID Client
Microsoft Office	Word 形式、Excel 形式等のデータ読み込み書き込が able こと。 一部の端末には、Microsoft Access が利用できる製品を適用すること。	Office LTSC Standard 2024	Office LTSC Standard 2019
	Office LTSC Professional Plus 2024	Office LTSC Professional Plus 2019	
Web ブラウザ	標準システムにアクセスする際に利用できること。一部の機能は Microsoft Edge の IE モードを利用してアクセスできること。	Microsoft Edge	Microsoft Edge
PDF 表示機能	pdf ファイルを正しく開くことができること。	Adobe Acrobat Reader	Adobe Acrobat Reader
ファイル授受 (広域連合・拠点間)	広域連合事務局と広域連合事務局以外の拠点間でファイル授受を行うことができること。 ショートカットからファイル授受システムにアクセスできること。	事業者にて選定	ショートカットで FileZen にアクセスする
認証プリント機能	端末からの印刷は、職員が所持する IC カード又はパスワードを用いて認証プリントを行うことができること。 IC カードは Mifare (マイフェア) 規格のものを使用する。	※	※
ウイルス対策	ウイルス対策ソフトは常に最新の状態に保たれ、安全な状態となっていること。	Windows Defender	Trend Micro Apex One
不正デバイス利用禁止	端末に接続するデバイスを制限できること。	事業者にて選定	SKYSEA Client View
外字の利用	広域連合が指定するソフトウェアを用いて外字を利用できること。	KAJ0_J 入力システム V7 後期高齢者医療広域連合電算処理システム対応版	KAJ0_J 入力システム V7 後期高齢者医療広域連合電算処理システム対応版
リモートアクセス	広域連合事務局の管理端末から、拠点の標準物理端末にリモートアクセス (Wake on LAN も利用可能) できること。	事業者にて選定	Soliton Secure Desktop
ファイルの圧縮・解凍	ファイルのパスワードによる暗号化・圧縮解凍を行うことができること。Zip や 7z 拡張子のファイルの圧縮解凍ができること。	7Zip	7Zip
バイナリ編集ソフト	バイナリデータを展開し編集できること。	Emeditor Pro	Emeditor Pro

(※) 職員各自が、利用端末のプリンタのプロパティを設定する。

2.4 ネットワーク要件

- (1) 標準セキュリティシステムのネットワークの範囲は次のとおり。
 - (ア) 現行データセンター内のクラウド接続ルータと、次期データセンター内のルータ間
 - (イ) 次期データセンター内
 - (ウ) 次期データセンター内ルータと、各拠点のルータ間
 - (エ) 各利用拠点（市区町村、広域連合、国保連、国保連データセンター）内
- (2) 標準セキュリティシステムのネットワークは閉域網である。
- (3) (1) (ア)、(ウ) のネットワークは、現在契約中の閉域網を利用するため、同様の閉域網を用いてセキュアなネットワークを構築すること。
- (4) 利用拠点及び、データセンター内の機器については有線ケーブルを用いて配置すること。
- (5) 中間サーバー用ルータと統合専用端末との間は LAN ケーブルを用いて配置すること。
- (6) 統合専用端末は標準セキュリティシステムの認証情報を利用するため、標準セキュリティシステムとも接続できるように配線を行うこと。
- (7) 端末が増える拠点については LAN ケーブルを敷設すること。
- (8) また、全拠点において端末設置時に既存 LAN ケーブルが問題なく利用できることを確認し、破損等が生じている場合は、再敷設をすること。キッティング、ネットワーク敷設等、業務履行に当たり発生した廃材、梱包材等は、関連法令に従い、適切に処分することとし、その費用を含むものとする。
- (9) 運用終了後、設置した機器について、広域連合の指示により適切な方法で処分すること。
- (10) 各拠点のネットワーク敷設について
 - (ア) エンハンスドカテゴリ 5e 以上の LAN ケーブルを使用すること。
 - (イ) LAN ケーブルの色は、オレンジ色を使用すること。
 - (ウ) 後日のレイアウト細部変更を考慮し、広域連合が指示する余長をとること。
 - (エ) 終端部には、行き先タグ（タイラップ型）を付けること。タグの表記は別途指示する。
 - (オ) 既存の物品（モール等）を流用できる場合には使用して良いこととする。ただし、不要となつた物品は、特別に指示する場合を除き、撤去すること。
 - (カ) LAN ケーブルを敷設し、成端した後、測定器等により検査を行うこと。
 - (キ) 不具合が検出された場合は、直ちに是正措置をとること。

2.5 その他要件

- (1) プリンタ
プリント解像度 600dpi × 600dpi 以上のレーザープリンタとし、給紙トレイと手差しトレイがあり、認証プリントが実現可能な機種とすること。
なお、現行システムで導入しているプリンタは別紙 2 のとおりとし、プリント速度と給紙トレイはマイナス 20 パーセントを下回らないことを目安として選定を行うこと。
現行システムはプリンタサーバーを設置していないが、必要に応じて提案することも可能とする。
- (2) 中間サーバー用ファイアウォール
中間サーバー用ファイアウォール（以下、「中間サーバー用 FW」という。）は、広域連合事務局の一括転送端末が、医療保険者等向け中間サーバーと通信を行うために設置するものである。
中間サーバーに接続するための設定値（パラメータ）は、現行品と同じ内容を設定する。設定値（パラメータ）については、事業者が決定後、決定した事業者に連絡する。
- (3) 管理端末
標準物理端末のうち、1 台は管理端末とする。管理端末は IC カード認証ができること。管理端末は拠点端末及び標準 VDI、標準 VDI を利用するための管理画面、標準システムのサーバーにリモートアクセスできること。また、管理端末はクローニングツールを用いて、状態を復元できるようにすること。

3 庁内システム機能要件

3.1 概要

庁内システムは、広域連合事務局の業務で利用する機器が強靭なセキュリティに守られ、安全に利用できるように構成したシステムである。データセンター内の仮想化基盤にサーバー群を構成し、データセンター、広域連合事務局、テレワーク用ルータを設置するデータセンター間を専用回線で接続する。

庁内システムは独立したネットワークを構成し、LGWAN や KSC と接続することができる。インターネットへの直接接続は行わない。

3.2 サーバー要件

次に、サーバーの機能要件を記す。表の「次期製品」列に製品名が記載されている機能は、指定の製品を選定すること。「事業者にて選定」と記載されている機能は履行期間内のサポート継続可能な製品を事業者にて提案すること。なお、参考として現行製品を記す。

要求機能	説明	次期製品	現行（参考）	
			製品名	利用状況
仮想化ソフトウェア	サーバーのリソースを仮想化し、仮想サーバーを効率的に稼働・管理するためのソフトウェアであること。	事業者にて選定	VMware vSphere Standard	※ 1
Active Directory	ユーザー管理、グループ管理、アクセス制限、名前解決、時刻同期等システムを管理することができるこ	Windows Server	Windows Server	64 名
ユーザー認証（二要素認証用）	生体認証やカード認証の認証機能を備えること。過去を含めた認証記録を保持できること。	SmartOn ID 自治体専用 強靭性向上 特別パック	SmartOn ID 自治体専用 強靭性向上特別パック	生体認証：64名 カード認証：3名
資産管理	庁内システム内のクライアント端末の資産管理を行い、外付けデバイス等の利用を制限や、ソフトウェアを配布することができること。 また、操作ログを取得できること。	事業者にて選定	SKYSEA Client View	約 130 台
バックアップ・リストア	ファイルサーバーのデータや、各種サーバーの OS イメージのバックアップを行うこと。バックアップデータのリストアができること。 ファイル名やフォルダ名に漢字やカタカナや記号を含む場合も、文字化けすることなくバックアップ、リストアができること。 共有フォルダのデータは過去 7 日分のデータが復元可能のこと。それ以外は原則 4 世代管理とする。	事業者にて選定	Arcserve UDP Appliance	12TB 使用率：約 86% ※ 2

ウイルス対策	次期システムでは Windows Defender を利用するため WSUS 中継サーバーを用意すること。Windows Defender の定義ファイルは、LGWAN サービス又は KSC の特定通信を用いて WSUS サーバーから WSUS 中継サーバーを経由し、端末やサーバーに配信できること。それ以外の配布プログラムの制御がされること。	WSUS	Trend Micro Apex One	約 70 台
MAC アドレス認証	庁内システムに接続する全ての機器について MAC アドレスで認証すること。登録されていない機器からのアクセスを防止すること。	事業者にて選定	NetAttest EPS	約 900 個登録可能な状態で運用
メールサーバー	LGWAN 上で他の自治体とのメールの送受信を行うための送信サーバーと受信サーバーの機能を備えること。現行のデータが確実に見れること。	Exchange Server	Exchange Server	ユーザー：アカウント：64 名 業務アカウント：20 個 容量：800GB 使用率：14%
ストレージ	広域連合事務局内のファイルサーバーとして利用できること。 必要に応じて、仮想マシンの構成ファイルや仮想ディスクファイル等のデータを格納すること。 庁内システムの操作ログを、1 年間分保管できること。	事業者にて選定	NetApp 本体：FAS2750A-003-SC 拡張シェルフ：DS224C-10-1.2-12S-QS-N	ファイルサーバー領域：約 1 TB 使用率：67% 年間増加量（見込）：約 150GB データストア領域：※ 1
ファイルサーバー	庁内ファイルサーバー（共有フォルダ）にアクセスすることができる。システムの管理者がフォルダのアクセス制限を付与することができる。	事業者にて選定	NetApp 本体：FAS2750A-003-SC 拡張シェルフ：DS224C-10-1.2-12S-QS-N	※ 3

（※ 1）プロポーザル参加表明書を提出した事業者のうち、「プロポーザル参加資格確認結果通知書」により参加資格を有すると認められた事業者は、広域連合事務室にて現行仕様書を閲覧可能とする。

（※ 2）広域連合情報システム全体の利用状況。

（※ 3）Active Directory の OU（組織単位）やセキュリティグループでアクセス制限をかける。

3.3 クライアント要件

庁内システムのクライアント端末は、庁内物理端末と庁内 VDI の 2 種類あるが、庁内 VDI は「事務局 VDI システム機能要件」に記載する。

庁内物理端末の用途は、庁内システム管理用（管理端末）と、Web 会議用（共用端末）である。

次に庁内物理端末の機能要件を記す。表の「次期製品」列に製品名が記載されている機能は、指定の製品を選定すること。「事業者にて選定」と記載されている機能は製品を事業者にて提案すること。要求機能の「KSC ソフトウェア」は、本調達案件を契約した事業者に広域連合から別途提供する。参考として現行製品を記す。

要求機能	説明	次期製品	(参考) 現行製品
Microsoft Windows	端末のオペレーティングシステム。	Windows 11 IoT Enterprise LTSC 2024	Windows 10 Enterprise LTSC 2019
ユーザー認証 (二要素認証用)	端末にログインする際、パスワード認証以外に生体認証やカード認証を行うことができるようになること。	SmartOn ID Client	SmartOn ID Client
Microsoft Office	Word 形式、Excel 形式等のデータ読み込み書き込めるようになること。	Office LTSC Standard 2024 又は Microsoft 365 Apps for business	Office LTSC Standard 2019
Web ブラウザ	LGWAN-ASP サービスで提供されるグループウェアや財務会計システム等を利用できること。	Microsoft Edge	Microsoft Edge
PDF 表示機能	pdf ファイルを開くことができるようになること。	Adobe Acrobat Reader	Adobe Acrobat Reader
認証プリント機能	端末からの印刷は、職員が所持する IC カードを用いて認証プリントを行うことができるようになること。 IC カードは Mifare (マイフェア) 規格のものを使用する。	※ 1	※ 1
ウイルス対策	ウイルス対策ソフトは常に最新の状態に保たれ、安全な状態となっていること。	Windows Defender	Trend Micro Apex One
不正デバイス利用禁止	情報資産を管理し、許可されたデバイスのみ利用できる。	事業者にて選定	SKYSEA Client View
ファイルの圧縮・解凍	ファイルのパスワードによる暗号化・圧縮解凍を行うことができる。Zip や 7z 拡張子のファイルの圧縮解凍ができるようになること。	7Zip	7Zip
オフィス向け文書管理ソフトウェア	広域連合の保有する DocuWorks データが使用できること。	DocuWorks	DocuWorks
KSC ソフトウェア	KSC サービスを利用するためのソフトウェアが利用できること。	KSC 提供ソフトウェア ※ 2	KSC 提供ソフトウェア ※ 2

(※ 1) 職員各自が、利用端末のプリンタのプロパティを設定する。

(※ 2) 広域連合から受託者に提供する。

3.4 ネットワーク要件

- (1) 庁内システムのネットワークの範囲は次のとおりである。
 - (ア) 次期データセンター内
 - (イ) 次期データセンター内ルータと、広域連合事務局のルータ間
 - (ウ) 広域連合事務局内
 - (エ) 次期データセンター内ルータと、テレワーク用データセンターのルータ間
 - (2) 庁内システムのネットワークは閉域網である。
 - (3) (1) (イ) (エ) のネットワークは、現在契約中の閉域網を利用するため、VPN を用いてセキュアなネットワークを構築すること。
 - (4) データセンター内の機器については有線ケーブルを用いて配置すること。

- (5) 広域連合事務局内の端末については、有線 LAN と無線 LAN の両方が利用可能なこと。
- (6) 端末設置時に既存 LAN ケーブルが問題なく利用できることを確認し、破損等が生じている場合は、再敷設をする。キッティング、ネットワーク敷設等、業務履行に当たり発生した廃材、梱包材等は、関連法令に従い、適切に処分することとし、その費用を含むものとする。
- (7) 運用終了後、設置した機器について、広域連合の指示により適切な方法で処分すること。
- (8) 無線 LAN のアクセスポイントはステルス機能を搭載し、ステルスマードを有効にし、安全に接続できること。
- (9) ネットワーク敷設について
 - (ア) エンハンスドカテゴリ 5e 以上の LAN ケーブルを使用すること。
 - (イ) LAN ケーブルの色は、白色を使用すること。
 - (ウ) 後日のレイアウト細部変更を考慮し、広域連合が指示する余長をとること。
 - (エ) 終端部には、行き先タグ（タイラップ型）を付けること。タグの表記は別途指示する。
 - (オ) 既存の物品（LAN ケーブル等）を流用できる場合には使用して良いこととする。ただし、不要となつた物品は、特別に指示する場合を除き、撤去すること。
 - (カ) LAN ケーブルを敷設し、成端した後、測定器等により検査を行うこと。
 - (キ) 不具合が検出された場合は、直ちに是正措置をとること。

3.5 LGWAN 接続要件

府内システムから LGWAN への接続は、LGWAN 接続ルータ提供事業者から提供されたルータ（以下、LGWAN ルータという。）と、本調達範囲である LGWAN 用ファイアウォールと L2SW を用いて接続すること。広域連合は現在、第四次 LGWAN の機器を利用し、シングル構成としている。

本調達では第五次 LGWAN の機器に変更し、現行のシングル構成から二重構成（ホットスタンバイ）として、ネットワーク帯域幅を 50Mbps に増速予定であるため、事業者選定の機器についてはオーバースペックにならないように選定すること。

また、本調達で事業者が選定する機器は、LGWAN ルータと LGWAN ファイアウォールとの間で、LGWAN ルータ以外の機器が送出した BPDU が LGWAN ルータに流入しない設定ができること。また、LGWAN ルータとの通信制御に使用しない不要な制御プロトコル（DTP/CDP/LLDP 等）パケットを LGWAN ルータに流入しない設定ができること。

なお、LGWAN 用ファイアウォールと L2SW の代わりに、ファイアウォール機能を持ち、VLAN 設定や通信制御等の機能を保持する機器を選定することは不可とする。

LGWAN への接続は、県ノードを経由で接続するため、広域連合と接続日程を調整し実施すること。

LGWAN サービス提供者から示される必要な情報は、広域連合から受託者に別途提供する。

LGWAN 機器を接続する時は、府内システムと LGWAN の間の機器との通信の正常性確認を実施すること。

3.6 KSC 接続要件

府内システムから KSC への接続は、既に接続している KSC 接続機器を利用するため、次期システムに移行する際は、府内システムと KSC の間の機器との通信の正常性確認を実施すること。

データセンターを移設する場合は、KSC 接続機器を移設する必要があるため、広域連合と接続日程を調整し実施すること。

広域連合が指定した製品や事業者が選定した製品を利用するにあたり、やむを得ず特定通信を行う場合は、必要な情報を全て提供し、広域連合の許可を得ること。

3.7 その他要件

(1) プリンタ

プリント解像度 600dpi × 600dpi 以上のレーザープリンタとし、給紙トレイと手差しトレイがあり、認証プリントが実現可能な機種とすること。

なお、現行システムで導入しているプリンタは別紙 2 のとおりとし、プリント速度と給紙トレイはマイナス 20 パーセントを下回らないことを目安として選定を行うこと。

現行システムはプリンタサーバーを設置していないが、必要に応じて提案することも可能とする。

(2) 入退室システム

広域連合事務局では入退室システムを設置しており、庁内物理端末又は庁内 VDI から入退室システムにアクセスする。

入退室システムには広域連合事務局の庁内システムのネットワークの IP アドレスを設定しており、IP アドレスは今後も変更する予定はないため、広域連合事務局内の庁内システムのネットワークアドレスは現行のとおりとする。なお、やむを得ず変更する場合は、広域連合と協議すること。

広域連合事務局内に設置する庁内システムのセンタースイッチ (L2SW) の 1 ポート及び予備用として 2 ポートを入退室システム用に確保すること。

(3) テレワーク用ルータ

広域連合では、VDI 利用端末に契約中の USB ドングル (USB 型通信デバイス) を接続し、現在契約中のテレワーク用データセンターを経由して、広域連合情報システムのデータセンター内の事務局 VDI システムにアクセスすることでテレワークを実現している。

テレワーク用ルータは、テレワーク用データセンターに設置する。(移設はしない。)

VDI 利用端末に USB ドングルを接続して利用できる VDI は、庁内 VDI のみとする。(標準 VDI には接続しないこと。)

テレワーク用ルータとテレワーク用データセンター内の接続インターフェースは 1000BASE-LX とし、テレワーク用データセンターに設置されている光ファイバケーブル (SMF) を用いて接続すること。参考に現行のテレワーク用ルータ及びセキュリティライセンス、光モジュールを記載する。

表 1. (参考) 現行のテレワーク用ルータ

種類	品名	数量
ルータ	ISR 1100 8 Ports Dual GE WAN Ethernet Router	1 台
セキュリティライセンス	Security License for Cisco ISR 1100 8P Series	1 式
光モジュール	1000BASE-LX/LH SFP transceiver module MMF/SMF 1310nm DOM	1 個

テレワーク用ルータの設定値と設置場所は、事業者が決定後、決定した事業者に連絡する。

(4) 庁内物理端末

庁内物理端末 4 台は IC カード認証ができること。

(5) 管理端末

庁内物理端末のうち、1 台は管理端末とする。管理端末は IC カード認証ができること。管理端末は庁内 VDI 及び庁内 VDI を利用するための管理画面、庁内システムのサーバーにリモートアクセスできること。また、管理端末はクローニングツールを用いて、状態を復元できるようにすること。

4 事務局 VDI システム機能要件

4.1 概要

広域連合事務局は、標準 VDI と庁内 VDI を利用して業務を行う。職員に一人 1 台の VDI 利用端末を配布し、各職員に割り当てた標準 VDI と庁内 VDI に接続する。事務局 VDI システムは、データセンター内に構築した事務局 VDI システム仮想化基盤上に標準 VDI と庁内 VDI を配備する。庁内 VDI は広域連合事務局の職員が利用する。標準 VDI は広域連合事務局の職員のうち標準システムを利用する職員が利用する。

4.2 サーバー要件

次に、サーバー要件を記す。表の「次期製品」列に製品名が記載されている機能は、指定の製品を選定すること。「事業者にて選定」と記載されている機能は履行期間内のサポート継続可能な製品を事業者にて提案すること。なお、参考として現行製品を記す。

要求機能	説明	次期製品	現行（参考）	
			製品名	利用状況
仮想化ソフトウェア	サーバーのリソースを仮想化し、仮想サーバーを効率的に稼働・管理するためのソフトウェアであること。システムを管理する職員が操作しやすい製品が望ましい。	事業者にて選定	VMware vSphere Standard	※
仮想デスクトップ	広域連合事務局で利用する標準VDIと庁内VDIを構成・管理するソフトウェアであること。システムを管理する職員が操作しやすい製品が望ましい。	事業者にて選定	VMware Horizon	※
バックアップ・リストア	サーバーのOSイメージのバックアップを行う。バックアップデータのリストアもできること。現行は4世代管理としている。	事業者にて選定	Arcserve UDP Appliance	標準セキュリティ及び庁内で共用 ※
ストレージ	必要に応じて、仮想マシンの構成ファイルや仮想ディスクファイル等のデータを格納すること。	事業者にて選定	NetApp 本体：FAS2750A-003-SC 拡張シェルフ：DS224C-10-1.2-12S-QS-N	標準セキュリティ及び庁内システムで共用 ※
ファイル授受 (標準VDI・庁内VDI間)	標準VDIと庁内VDIでのファイル授受を安全に行う機能があること。職員がファイル授受を行う際に、上長による承認ができる機能を持つこと。また、ファイルの無害化できること。	事業者にて選定	FileZen S	42名

(※) プロポーザル参加表明書を提出した事業者のうち、「プロポーザル参加資格確認結果通知書」により参加資格を有すると認められた事業者は、広域連合事務室にて現行仕様書を閲覧可能とする。

4.3 クライアント要件

次に、標準VDI、庁内VDI、VDI利用端末のクライアント要件を記す。表の「次期製品」列に製品名が記載されている機能は、指定の製品を選定すること。「事業者にて選定」と記載されている機能は製品を事業者にて提案すること。要求機能の「KSC ソフトウェア」は、本調達案件を契約した事業者に広域連合から別途提供する。参考として現行製品を記す。

(1) 標準 VDI

要求機能	説明	次期製品	(参考) 現行製品
Microsoft Windows	端末のオペレーティングシステム。	Windows 11 IoT Enterprise LTSC 2024	Windows 10 Enterprise LTSC 2019
ユーザー認証 (二要素認証用)	端末にログインする際、パスワード認証以外に生体認証やカード認証を行うことができる。	SmartOn ID Client	SmartOn ID Client
Microsoft Office	Word 形式、Excel 形式等のデータ読み込み書き込が能够すること。	Office LTSC Standard 2024	Office LTSC Standard 2019
Web ブラウザ	標準システムにアクセスする際に利用する。一部の機能は Microsoft Edge の IE モードを利用してアクセスすることができる。	Microsoft Edge	Microsoft Edge
PDF 表示機能	pdf ファイルを開くことができる。	Adobe Acrobat Reader	Adobe Acrobat Reader
ファイル授受 (広域連合・拠点間)	広域連合事務局と広域連合事務局以外の拠点間でファイル授受を行うことができる。 ショートカットからファイル授受システムにアクセスできること。	事業者にて選定	ショートカットで FileZen にアクセスする
ファイル授受 (標準 VDI・庁内 VDI 間)	標準 VDI と庁内 VDI でのファイル授受を安全に行うことができる。 ショートカットからファイル授受システムにアクセスできること。	事業者にて選定	ショートカットで FileZen S にアクセスする
認証プリント機能	端末からの印刷は、職員が所持する IC カードを用いて認証プリントを行う。IC カードは Mifare (マイフェア) 規格のものを使用する。	※	※
ウイルス対策	ウイルス対策ソフトは常に最新の状態に保たれ、安全な状態となっていること。	Windows Defender	Trend Micro Apex One
不正デバイス利用禁止	情報資産を管理し、許可されたデバイスのみ利用できること。	事業者にて選定	SKYSEA Client View
外字の利用	広域連合が指定するソフトウェアを用いて外字を利用することができる。	KAJ0_J 入力システム V7 後期高齢者医療広域連合電算処理システム対応版	KAJ0_J 入力システム V7 後期高齢者医療広域連合電算処理システム対応版
ファイルの圧縮・解凍	ファイルのパスワードによる暗号化・圧縮解凍を行うことができる。Zip や 7z 拡張子のファイルの圧縮解凍ができる。	7Zip	7Zip
バイナリ編集ソフト	バイナリデータを展開し編集できること。	Emeditor Pro	Emeditor Pro

(※) 職員各自が、利用端末のプリンタのプロパティを設定する。

(2) 庁内 VDI

要求機能	説明	次期製品	(参考) 現行製品
Microsoft Windows	端末のオペレーティングシステム。	Windows 11 IoT Enterprise LTSC 2024	Windows 10 Enterprise LTSC 2019
ユーザー認証 (二要素認証用)	端末にログインする際、パスワード認証以外に生体認証やカード認証を行うことができる。なお、現行システムは、VDI 利用端末と庁内 VDI のシングルサインオンを行っている。	事業者にて選定	SmartOn ID Client
Microsoft Office	Word 形式、Excel 形式等のデータ読込及び書込が可能。また、Microsoft Access が利用できる製品を適用すること。	Office LTSC Professional Plus 2024 又は Microsoft 365 Apps for business	Office LTSC 2019 Standard
Web ブラウザ	LGWAN-ASP サービスで提供されるグループウェアや財務会計システム等を利用する。インターネットへの接続はできない。	Microsoft Edge	Microsoft Edge
PDF 編集機能	pdf ファイルを編集することができる。広域連合が指定した庁内 VDI にインストールする。	機能制限ライセンス付き Acrobat Standard DC (デスクトップ専用)	機能制限ライセンス付き Acrobat Standard DC (デスクトップ専用)
PDF 表示機能	pdf ファイルを閲覧ためのソフトウェア。PDF 編集機能がインストールされた庁内 VDI 以外の庁内 VDI にインストールする。	Adobe Acrobat Reader	Adobe Acrobat Reader
ファイル授受 (標準 VDI・庁内 VDI 間)	標準 VDI と庁内 VDI でのファイル授受を安全に行うことができる。ショートカットからファイル授受システムにアクセスすること。	事業者にて選定	ショートカットで FileZen S にアクセスする
認証プリント機能	端末からの印刷は、職員が所持する IC カードを用いて認証プリントを行うことができる。IC カードは Mifare (マイフェア) 規格のものを使用する。	※ 1	※ 1
ウイルス対策	ウイルス対策ソフトは、常に最新の状態に保たれ、安全な状態となっていること。	WSUS	Trend Micro Apex One
不正デバイス利用禁止	情報資産を管理し、許可されたデバイスのみ利用すること。	事業者にて選定	SKYSEA Client View

ファイルの圧縮・解凍	ファイルのパスワードによる暗号化・圧縮解凍を行うことができる。Zip や 7z 拡張子のファイルの圧縮解凍ができる。	7Zip	7Zip
オフィス向け文書管理ソフトウェア	広域連合の保有する DocuWorks データが使用できること。	DocuWorks	DocuWorks
KSC ソフトウェア	KSC サービスを利用するためのソフトウェアが利用できること。	KSC 提供ソフトウェア ※2	KSC 提供ソフトウェア ※2

(※1) 職員各自が、利用端末のプリンタのプロパティを設定する。

(※2) 広域連合から受託者に提供する。

(3) VDI 利用端末

要求機能	説明	次期製品	(参考) 現行製品
Microsoft Windows	端末のオペレーティングシステム。	Windows 11 IoT Enterprise LTSC 2024	Windows 10 Enterprise LTSC 2019
ユーザー認証 (二要素認証用)	端末にログインする際、パスワード認証以外に生体認証やカード認証を行うことができること。	事業者にて選定	SmartOn ID Client
Web ブラウザ	OS 標準のブラウザがインストールされていること。 インターネットへの接続はできない。	Microsoft Edge	Microsoft Edge
不正デバイス利用禁止	情報資産を管理し、許可されたデバイスのみ利用できること。	事業者にて選定	SKYSEA Client View
VDI クライアント	標準 VDI 及び庁内 VDI に接続するためのソフトウェアが利用できること。	事業者にて選定	Horizon Client

4.4 ネットワーク要件

- (1) 事務局 VDI システムに構築された標準 VDI と庁内 VDI は論理的に分離されたネットワークに配置すること。
- (2) 標準 VDI は標準セキュリティシステムのリソースのみアクセスでき、庁内システムのリソースにはアクセスできないこと。
- (3) 庁内 VDI は庁内システムのリソースのみアクセスでき、標準セキュリティシステムのリソースにはアクセスできないこと。
- (4) ネットワークは閉域網である。
- (5) データセンターのルータと広域連合事務局のルータ間は、閉域網を利用するため、VPN を用いてセキュアなネットワークを構築すること。
- (6) データセンター内の機器については有線ケーブルを用いて配置すること。
- (7) 広域連合事務局内の VDI 利用端末は、有線 LAN と無線 LAN の両方が利用可能のこと。ただし、通常は無線 LAN 接続を行うため、無線 LAN が利用できない時の予備として有線 LAN が利用可能な状態にしておくこと。
- (8) 無線 LAN のアクセスポイントはステルス機能を搭載し、ステルスマードを有効にすること。
- (9) 端末設置時に既存 LAN ケーブルが問題なく利用できることを確認し、破損等が生じている場合は、再敷設をする。キッティング、ネットワーク敷設等、業務履行に当たり発生した廃材、梱包材等は、関連法令に従い、適切に処分することとし、その費用を含むものとする。
- (10) 運用終了後、設置した機器について、広域連合の指示により適切な方法で処分すること。

4.5 その他要件

(1) プリンタ

プリント解像度 600dpi×600dpi 以上のレーザープリンタとし、給紙トレイと手差しトレイがあり、認証プリントが実現可能な機種とすること。

なお、現行システムで導入しているプリンタは別紙2のとおりとし、プリント速度と給紙トレイはマイナス 20 パーセントを下回らないことを目安として選定を行うこと。

現行システムはプリンタサーバーを設置していないが、必要に応じて提案することも可能とする。

5 構築要件

5.1 構築期間

契約締結日から令和9年3月31日まで

機器の納入：令和8年10月1日（予定）

リース開始日：令和9年4月1日

5.2 業務体制

本件業務を実施するに当たっては、次の事項に沿って業務体制を整え、適切にプロジェクト管理を行うこと。

- (1) 円滑な業務遂行が実現可能な体制を作り、その進捗管理や品質管理等プロジェクト運営管理の手法についても明確にすること。
- (2) 本業務に係るプロジェクトマネージャーを配置するとともに、連絡窓口を明確にすること。
- (3) 契約締結後、10営業日以内に全体スケジュール、プロジェクトマネージャー及び業務体制等を記載したプロジェクト計画書を作成し、提出すること。
- (4) 定期的に進捗報告を行い、会議開催日から5営業日以内に会議記録を広域連合に提出すること。
- (5) 基本設計の工程に移行する前に、要件定義書を作成し、広域連合に提出すること。
- (6) 突発的な問題については適宜報告・必要に応じて会議を行い、早期解決に努めること。
- (7) 本件業務にかかる意思決定は、原則として書面で行うものとする。

5.3 広域連合情報システム構築環境

「2 標準セキュリティシステム機能要件」「3 庁内システム機能要件」「4 事務局 VDI システム機能要件」に基づき設計したシステムを構成する機器（回線等外部サービスを利用するもの及び各拠点に設置するものを除く。）を次の要件を満たすデータセンターに設置する。

- (1) 所在地が広域連合事務局から公共交通機関を利用して概ね1時間圏内の場所であること。
- (2) 本件業務に関する立ち入り検査（年1回以上）が行えること。
- (3) 耐震及び防火設備を備えていること。
- (4) 災害時に無停止で電源供給がなされること。
- (5) 空調設備が完備されていること。
- (6) キャリアフリーで回線が敷設可能のこと。
- (7) 入退室管理システムを備えていること。
- (8) サーバー等設置場所の監視が24時間体制で行われていること。
- (9) 熱源機器・空調機器が冗長化されていること。
- (10) 建物内ネットワーク経路が冗長化されていること。
- (11) 建物内通信機器（ルータ／スイッチ）が冗長化されていること。
- (12) 地震時に被害や施設の機能停止が発生した場合に早期に復旧できるための体制・準備（緊急対応マニュアル、防災マニュアル、BCP等）が整備されていること。

データセンターは、現行データセンターの利用又は他のデータセンターの利用のどちらも可能とする。ただし、現行データセンターに設置してある標準システム（クラウド）に接続するルータについては、原則移設しないこととする。なお、当該機器をシステムの構成上やむを得ず移設する場合は、標準システムの業務影響を伴わず標準システム（クラウド）への正常接続が担保されることを条件とし、移設に係る費用について構築の見積額に含めること。

5.4 機器の調達

「2 標準セキュリティシステム機能要件」「3 庁内システム機能要件」「4 事務局 VDI システム機能要件」に基づき設計したシステムを構成するサーバー及びネットワーク機器、端末等の機器を事業者選定後に広域連合が調達する。

機器の選定に当たっては、構築後の運用面も含めた総合的な費用対効果を考慮すること。数量については、次期システムに設置する端末台数と、現行システムの構成に基づき「別紙4 広域連合情報システム クライアント端末等台数一覧」にまとめたので参考にすること。ただし、受託者により設計思想が異なるため、仕様を満たすという条件のもと、公告した上限額を超えない金額で、別紙4に記載したネットワーク機器とは異なるスペックの機器を選定しても良いこととする。

原則として、機器と併せてメーカーの保守サービスを購入することとし、調達費用に含めること。

調達した機器は、原則として広域連合が排他的使用権を持つものとすること。

調達する機器の明細（定価及び調達想定価格を含み）を機器一覧表に記載し、提案時に提出すること。

(1) 全般

(ア) 機器の配送

配送は機器リース事業者が行い、費用は機器リース事業者が負担する。

(イ) システム機器の取り外し

取り外しは機器リース事業者が行い、費用は機器リース事業者が負担する。

(ウ) データ消去

機器のデータ消去は、機器リース事業者が機器設置場所ごとのデータ消去を行うこととする。

消去方法はHDD 及び SSD は物理破壊することとする。なお、データ消去実施後、機器リース事業者はデータ消去証明書を提出することとする。

(エ) 機器撤去及び集積

撤去及び集積は機器リース事業者が行い、費用は機器リース事業者が負担する。

(オ) 別紙4のクライアント端末は、セキュリティスロット付きの端末を選定すること。

(カ) 別紙4のセキュリティワイヤーはシリンドー錠を選定すること。

(キ) データセンター内の機器は19インチラックに配置するため、必要に応じてラックマウントするための資材を本調達に含めること。

(2) 標準セキュリティシステム機器調達要件

(ア) 標準セキュリティシステム仮想化基盤の構築に必要な機器一式。

(イ) 少なくとも5年間（次々期機器更改まで）は拡張せずに使用できるスペックを備えていること。

(ウ) 標準セキュリティシステム機能要件のクライアント要件を満たすクライアント端末、ソフトウェア（広域連合が提供するものを除く）、プリンタ、スキャナ及びこれら機器の構築・運用に必要な物品。

(エ) 各機器の現行仕様は別紙1、別紙2で定める。

(オ) クライアント端末にインストールするソフトウェアは別紙3で定める。

(カ) 端末のUSBポートType-Aは3ポート以上が望ましいが、ノートブック端末に限り2ポートあれば良いものとする。なお、端末のUSBポートにUSBポートHUBを接続し、ポート数を確保することは不可とする。

(キ) ローカルディスクのドライブ構成は、「5.8 端末等のキッティング及び設置」を参照すること。

(ク) 端末は内蔵DVDドライブ搭載モデルが望ましいが、ノートブック端末に限り内蔵のDVDドライブ未搭載モデルの選定も可能とする。

(ケ) 「後期高齢者医療広域連合電算処理システム仕様書（構成編）第2.7版（令和7年4月24日）」（※）の広域連合端末仕様は次のとおりである。

表2. 広域連合端末仕様

No.	区分	仕様
1	CPU	3.1GHz 以上のプロセッサー。
2	メインメモリ	4GB 以上 (8GB 以上推奨)。
3	内蔵ディスク	250GB 以上。
4	OS	バージョン情報「標準システムクライアント端末のサポート対象 OS 等」に記載。
5	ディスプレイ	解像度 1280×768 以上。
6	USB ポート	マウスや外部記憶媒体等、利用する周辺機器に応じて選択。

(※) 標準システム集約機関提供資料。当該事業の委託契約を締結後、受託者には必要最低限の情報を提供するものとする。

(3) 庁内システム機器調達要件

- (ア) 庁内システム仮想化基盤の構築に必要な機器一式。
- (イ) 少なくとも 5 年間 (次々期機器更改まで) は拡張せずに使用できるスペックを備えていること。
- (ウ) 庁内システム機能要件のクライアント要件を満たすクライアント端末、ソフトウェア (広域連合が提供するものを除く)、プリンタ、複合機及びこれら機器の構築・運用に必要な物品。
- (エ) 庁内物理端末は、広域連合が支給する。プリンタの現行仕様は別紙 2 で定める。
- (オ) クライアント端末にインストールするソフトウェアは別紙 3 で定める。

Microsoft Office については、Office LTSC 2024 又は Microsoft 365 を 5 年間利用することを提案するものとする。Office LTSC 2024 の場合は、運用期間中にサポート期限を迎えるため、期限経過後も Office を継続して利用するための調達費用を Office LTSC 2024 の価格を用いて算出し、本調達の見積額に含めること。Microsoft 365 の場合は、LGWAN が提供するサービスであるマイクロソフト社のサーバーに中継するための仕組みを利用し、Microsoft Entra 認証を行い、クライアント端末と利用者を制限できる方法での提案をすること。そのため、Microsoft 365 や Microsoft Entra ID、Microsoft Intune 等の必要なライセンスを本調達の見積額に含めること。

- (カ) 無線 LAN アクセスポイントについては、必要に応じて電源供給するための機器を調達すること。
また、調達した機器は保守の対象とすること。

(4) 事務局 VDI システム機器調達要件

- (ア) 事務局 VDI システム仮想化基盤の構築に必要な機器一式。
- (イ) 少なくとも 5 年間 (次々期機器更改まで) は拡張せずに使用できるスペックを備えていること。
- (ウ) 事務局 VDI システム機能要件のクライアント要件を満たす VDI 及び端末、ソフトウェア (広域連合が提供するものを除く) 及びこれら機器の構築・運用に必要な物品。
- (エ) 各機器の現行仕様は別紙 1、別紙 2 で定める。
- (オ) クライアント端末にインストールするソフトウェアは別紙 3 で定める。

府内 VDI にインストールするソフトウェアのうち、Microsoft Office については、Office LTSC 2024 又は Microsoft 365 を 5 年間利用することを提案するものとする。Office LTSC 2024 の場合は、運用期間中にサポート期限を迎えるため、期限経過後も Office を継続して利用するための調達費用を Office LTSC 2024 の価格を用いて算出し、本調達の見積額に含めること。Microsoft 365 の場合は、LGWAN が提供するサービスであるマイクロソフト社のサーバーに中継するための仕組みを利用し、Microsoft Entra 認証を行い、クライアント端末と利用者を制限できる方法での提案をすること。そのため、Microsoft 365 や Microsoft Entra ID、Microsoft Intune 等の必要なライセンスを本調達の見積額に含めること。

- (カ) 無線 LAN アクセスポイントについては、必要に応じて電源供給するための機器を調達すること。
また、調達した機器は保守の対象とすること。

5.5 システム構築

- (1) サーバーはデータセンター内に設置すること。
- (2) サーバーは仮想化基盤上に構築すること。

- (3) 仮想化基盤は、2台以上の物理サーバーで可用性を重視した構成とすること。
- (4) 物理サーバーを仮想化する基本ソフトウェアはハイパーバイザ型とすること。
- (5) 冗長化構成とし、障害が発生した場合でも業務が停止しない構成であること。
- (6) 物理的な故障によるデータ消失を防止する構成にすること。
- (7) システム障害時でも、仮想サーバーの無停止移動等により、サービスを継続する高可用性を実現すること。
- (8) 物理サーバー群、仮想サーバー群は、定期・不定期に必要なセキュリティパッチを適用する等、適切なセキュリティ対策を講じること。なお、適用を行う必要がある場合は、必ず検証作業を行った上で実施すること。
- (9) 5年間は利用可能のこと。
- (10) 必要に応じて、利用期間の延長が可能のこと。
- (11) 事業者が設計・構築する仮想化基盤と仮想化サーバー群は、三層分離が実現できれば、運用や保守の観点から機能を共通化することも可能とする。

5.6 ネットワーク構築

(1) 基本要件

広域連合情報システムが、安全に安心して利用できるようにネットワークを設計し、設計したネットワークを全拠点に構築する。定められた日程の中で、疎通確認を含めた全ての工程が完了するよう工事及び作業を行うこと。なお、市区町村担当者との日程調整も業務に含むものとする。

構築に際しては、事前検証等のため、データセンターと広域連合事務局間、データセンターと新国保連事務室間の疎通開始を優先して行うこと。なお、標準セキュリティシステムのクラウド接続ルータが現行拠点に設置されており、現行データセンターと次期データセンターと異なる場合は、次期データセンターと現行データセンター（別紙5 広域連合情報システム接続拠点一覧「データセンター2」「データセンター3」）間の疎通開始も優先して行うこと。

配線作業については既設配線環境を流用することも可能であるが、ネットワーク設計の結果、再敷設が必要な範囲が生じた場合（レイアウト変更含む）は新規敷設すること。なお、新設箇所については既設配線がないため新規敷設すること。

(2) データセンター内

- (ア) 障害に備えて冗長化構成にすること。
- (イ) ループ検出機能を有すること。
- (ウ) ネットワーク機器等のステータス監視ができること。
- (エ) VLAN等のネットワーク設計を行い、セキュリティを考慮した設定を行うこと。
- (オ) ネットワーク機器障害時には、自動的に利用可能な経路に瞬時に切り替えできること。
- (カ) 使用しないポートについては、不正接続等を防止する対策を講じること。
- (キ) クラウド接続ルータを現行のデータセンターから移設しない場合は、本調達でシステムを構築するデータセンターとの通信用のネットワーク環境を構築すること。
- (ク) クラウド接続ルータを、本調達でシステムを構築するデータセンターに移設する場合は、標準システム（クラウド）への接続及び拠点から標準システム（クラウド）へアクセスできることを確認すること。
- (ケ) テレワーク用ルータの交換作業では、接続の正常性を確認すること。

(3) 標準セキュリティシステム接続拠点

- (ア) 接続拠点は、「別紙5 広域連合情報システム接続拠点一覧」を参照すること。
- (イ) 一部拠点を除いて、現行システムの機器等の入れ替え作業となるため、他のシステムの機器を含めた周辺の機器等を破損することのなきよう十分に注意して作業すること。受託者の責において発生した場合には、修復に伴う費用を受託者が負担すること。
- (ウ) 安全性を考慮し作業量と作業時間を最小限にできるネットワーク設計を行うこと。
- (エ) 広域連合からネットワーク設定変更の依頼があった場合、迅速に対応ができる体制を取っておくこと。
- (オ) 登録した機器以外の接続による不正アクセスを防止する機能を導入すること。

(カ) 抱点間の通信は、データセンターと各抱点間、広域連合事務局と各抱点間のみ可能とし、市区町村抱点間の通信は不可とすること。

(4) 広域連合事務局

- (ア) 広域連合事務局の所在地は「別紙5 広域連合情報システム接続抱点一覧」を参照すること。
- (イ) 現行システムの機器等の入れ替え作業となるため、他のシステムの機器を含めた周辺の機器等を破損することのなきよう十分に注意して作業すること。受託者の責において発生した場合には、修復に伴う費用を受託者が負担すること。
- (ウ) 庁内物理端末及びVDI利用端末の接続のための有線LANと無線LAN設備を整備すること。
- (エ) 標準物理端末の接続のための有線LAN設備を整備すること。
- (オ) 有線LAN、無線LAN共に、不正アクセス、盗聴、なりすまし等の脅威から守られた設定を行うこと。有線LAN、無線LANそれぞれに接続する機器は、広域連合から指示を行う。
- (カ) 無線LANは安定した通信品質及びセキュリティを確保するための工夫を施し、事務局内に適切なアクセスポイントを配置すること。(事務局床面積は9階：514.97m²、11階：220.23m²。同時接続台数は約70台。) なお、無線LANアクセスポイントへの電源供給方法は事業者の提案次第とするが、前述「(3)庁内システム機器調達要件」「(4)事務局VDIシステム機器調達要件」のとおり、電源供給のために調達した機器も5年間の保守の対象とすること。
- (キ) 無線LANはIEEE標準規格として、IEEE802.11a/b/g/n/ac/axに対応しており、十分な帯域と安定した接続環境を確保すること。通信の暗号化はWPA2以上とし、IEEE802.11iに準拠したAES-CCMPによる暗号化方式を使用すること。
- (ク) 統合専用端末は、標準セキュリティシステムの有線LANの他に、既設のマイナンバーネットワークに有線LAN接続を行うものとすること。

5.7 VDI構築

VDIは次の内容を考慮し構築すること。初期構築時のVDIの数量は、「別紙4 広域連合情報システムクライアント端末等台数一覧」の標準VDI及び庁内VDIを参照すること。

- (1) 画面転送プロトコルには信頼性が高く狭帯域に最適な画面転送プロトコルを採用すること。
- (2) 最大接続台数の規模でサイジングを行い、CPU、メモリ及びストレージについてはサイジングの根拠を示す資料を提示すること。なお、VDI 1台に割り当てるリソースの最低基準値は次のとおりとする。

CPU：4vCPU、メモリ：8GB、ディスク：200GB
- (3) 管理が容易に行えること。各端末に対して、一括でソフトウェアの導入・削除・変更ができること。
- (4) VDI利用端末とVDI間のデータ授受ができないこと。
- (5) ファイル授受(標準VDI・庁内VDI間)用ソフトウェアを除き、標準VDIと庁内VDIの間のデータ授受ができないこと。(クリップボードリダイレクトをOFFにすること)
- (6) ログオンストーム対策、ブートストーム対策ができること。

5.8 端末等のキッティング及び設置

- (1) 設置する端末等の機器類は「別紙4 広域連合情報システムクライアント端末等台数一覧」に従うこと。ただし、データセンター内の機器構成については、受託者により設計思想が異なるため、仕様を満たすという条件のもと必要な機器を選定すること。
- (2) 端末にインストールするソフトウェアは「別紙3 次期システムクライアント端末ソフトウェア」を参照すること。
- (3) キッティング手順及び項目表を作成し、確認しながら作業を進めること。また、作業の履歴を残すこと。
- (4) 標準物理端末2台(統合専用端末用、一括転送端末用)の納入は、広域連合事務局のネットワーク構築の少なくとも2週間前とし、キッティング完了後すぐに納入すること。
- (5) 庁内物理端末は、リース機器ではなく、広域連合資産を利用する。
- (6) VDI利用端末は、テレワーク時のUSBドングルが利用できるように設定を行うこと。

- (7) 統合専用端末及び一括転送端末の独自の設定は原則として広域連合で実施するが、ネットワークの設定や接続テストについて、必要に応じて技術的な支援を行うこと。
- (8) 抱点の所在地は、「別紙5 広域連合情報システム接続抱点一覧」を参照すること。なお、別紙5の「所在地」に「詳細は非公開」と記載されている抱点については、受託者に通知する。
- (9) 「別紙5 広域連合情報システム接続抱点一覧」のうち、広域連合事務局と、新国保連合会事務室はユーザー試験を行うため、先行導入抱点とすること。
- (10) 先行導入抱点でユーザー試験を行い、システムが正常に動作することが確認された後、残りの抱点の設置作業を行うこと。
- (11) 標準物理端末のローカルディスクのドライブ構成は次のとおりとし、フォーマット形式はNTFS とすること。また、ブラウザ等の設定については、別途受託者に通知する設定を反映すること。
 - C ドライブ：250GB 以上
 - D ドライブ：150GB 以上
- (12) 端末等の機器の設置場所は、広域連合から受託者に提供する抱点レイアウト図に従い設置すること。ただし、機器を設置時に、抱点職員から設置位置の変更の要望があった場合、LANケーブルの余長の範囲内で、机1台程度の距離の変更は許容するものとする。
- (13) 抱点に端末を設置する際、セキュリティワイヤーを取り付けること。
- (14) 抱点にて取り外した旧システムの機器は、抱点職員が指示する場所に保管すること。

5.9 データ移行

既存運用の維持を目的として、現行システムより次のデータを移行すること。データ移行対象はADサーバー情報、認証情報（SmartOn登録ユーザー情報）、ファイルサーバー内データ、Exchangeサーバーの4点とする。データ移行の際は、データ移行した全てのデータが正しく移行されていることを確認すること。なお、ファイルサーバーのフォルダ名に特殊文字が使われている等で、データ移行が失敗する場合は、広域連合に連絡の上、対応方法を協議すること。

5.10 単体試験

受託者は、システム構築、ネットワーク構築の単体試験項目を作成し、広域連合の承認を得たうえで実施すること。実施結果は構築完了時の納入成果物に含めること。

5.11 結合試験

受託者は結合試験の項目を作成し、広域連合の承認を得たうえで実施すること。結合試験は、データセンター内に設置する管理端末を用いて「2 標準セキュリティシステム機能要件」「3 庁内システム機能要件」「4 事務局VDIシステム機能要件」の動作を確認すること。実施結果は構築完了時の納入成果物に含めること。

5.12 ユーザー試験

先行導入する広域連合事務局と新国保連合会事務室でユーザー試験を行う。試験内容は当該要求仕様書のクライアント要件に基づき受託者が作成し、広域連合と協議のうえ確定する。試験結果に不適合が検出された場合、受託者は、速やかに原因を調査し、対策を講じること。

6 非機能要件

6.1 可用性

広域連合情報システムは原則的に24時間365日継続的に利用できることとする。特に、神奈川県下市町村役場の開庁時間と、標準システム開庁時間（平日及び、指定の土日祝日の午前8時30分～午後6時）は、職員が利用中のシステムが停止しないシステムを構築すること。

なお、オペレーションシステムやファームウェアのバージョンアップ等の保守等の理由でシステムを停止する必要がある場合は、広域連合と調整の上、原則開庁時間外でシステムを停止することとする。ただし、冗長構成等により、システム利用を保持したまま作業が可能の場合を除く。

万一、故障等が発生し、機器を含むシステム又はシステムの一部が停止した場合は、即時に別系統への切替が行われるような設計を行うこと。

業務停止を伴う障害が発生した場合は、即時復旧に努めるとともに、障害発生直前のトランザクションを確認し、発生前の状態までデータを復旧させること。

6.2 性能・拡張性

標準セキュリティシステム機能要件、庁内システム機能要件、事務局VDIシステム機能要件と別紙を参考し、利用者数、利用端末数、回線帯域を考慮し、適切なスペックの機器類を選定すること。

広域連合情報システムの各システムは仮想化基盤上に構築するため、CPU、メモリ、ディスク容量等の拡張が容易であるが、利用状況による割当見直し等、必要に応じてリソースを拡張できるように設計すること。

6.3 運用・保守性

「7 運用・保守要件」を参照すること。

6.4 移行性

旧システムから新システムへの移行は、広域連合との協議の上、移行期間、移行体制、移行リハーサルを含む移行計画を作成すること。

移行の具体的な方法や手順をまとめ、広域連合に提出すること。提出した内容は、広域連合の了解を得た上で移行を行うこと。また、広域連合からの指摘があれば反映すること。特に市区町村の拠点にネットワーク機器や端末を設置する場合、概ね利用中の契約回線を利用するため、業務影響の無い時間帯で、効率よくかつ正確に移行作業を実施すること。

移行対象設備は、予め移行対象や作業場所を確認した上で、正しく設置すること。

ファイルサーバーやメールサーバー等の旧システムからの移行データは、データ量が大きいため、予め新システムへデータを移行した上で完全移行時に差分を移行する等の作業方法を検討し、データの移行漏れを防ぐこと。

なお、ファイルサーバーについては、階層上位の一部のフォルダについてフォルダ名の変更を検討しているため、広域連合と協議の上作業を行うこと。

移行時のトラブル発生時の連絡体制と復旧方法をまとめ、広域連合に提出すること。

6.5 セキュリティ

標準システム（マイナンバー利用事務系）を利用する、標準セキュリティシステムについては、特定個人情報を扱うため、セキュリティを十分に考慮したシステムを設計するとともに、アクセス記録を7年間保管・参照できるシステムを構築すること。

広域連合情報システムは「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」に従い、少なくとも1年間分のアクセス記録を保持・参照できるシステムを構築すること。

広域連合情報システムは、自治体情報システムの三層分離で構成されているため通常のインターネット接続環境に比べ不正アクセスのリスクが低いと考えられるが、ソフトウェア更新等のためのローカルブレークアウト利用が必要になる場合や人為的な操作等によるシステムの脅威を洗い出し、影響の分析を実

施した上で、システムを設計・構築すること。特に、キッティング等の複数の作業者が複数の端末に対して作業する場合は、機器を導入する前にセキュリティ診断を行うことを考慮すること。また、機器導入前後に係わらず、セキュリティリスクを発見した場合は、速やかに広域連合に連絡し、対策を協議し講じること。

広域連合情報システムは、広域連合が認めた職員だけが利用できるように、認証機能や、利用制限を可能とすること。構築・保守・運用にあたっては、事業者によるシステムの利用制限を必要最低限とするここと。

広域連合情報システムのデータは、伝送時や蓄積時に暗号化する等の措置をとることで、秘匿性を高めること。なお、暗号化できないものや、閉域網等のほぼリスクのない経路での伝送や蓄積に対しては、暗号化しないことも認めるものとする。

システムの不正監視を行い、不正監視アラートが検出された場合は、速やかに広域連合に報告し、原因を究明すること。また、トレースログを取得可能のこと。また、データが改ざんされない仕組みを検討すること。

セキュリティインシデントが発生した時に、早期発見し、被害の最小化、復旧の支援等をするための体制作りを行うこと。

6.6 環境・エコロジー

導入する製品は、製品安全規格に適合し、可能な限り環境負荷に配慮した製品を選定すること。

キッティング等を行う際は、決められた区画の中で、漏洩のリスクなきよう、入退室記録、機器の数量確認、作業時に利用する記録表、工具、ソフトウェインストール用の記録媒体等必要な物品を管理すること。

7 運用・保守要件

7.1 窓口設置（共通）

(1) システム障害、ソフトウェア操作方法、標準セキュリティシステム及び府内システム、事務局 VDI システムに関する疑義等について、広域連合（各拠点を含む）システム担当からの問い合わせを受け付ける体制を整えること。

○サポート対応時間

(ア) 月曜日から金曜日（土曜日、日曜日、祝日、年末年始を除く）

午前 8 時 30 分から午後 6 時

(イ) 時間延長（～午後 8 時）

年間 16 回以内

(ウ) 休日臨時対応

年間 5 日以内

※障害発生時や運用上の都合により、上記時間外に対応が必要な場合は別途協議の上、対応を実施すること。

（参考）令和 6 年度窓口問合せ件数

年間件数：33 件

現地対応件数：9 件（オンライン保守にて端末交換）

表3. 令和6年度窓口問合せ件数

期間	機器種別件数			月間問合せ件数
	端末	プリンタ	ネットワーク	
4月	2	0	0	2
5月	3	2	0	5
6月	4	1	0	5
7月	2	0	0	2
8月	0	4	0	4
9月	0	1	0	1
10月	1	1	1	3
11月	1	2	0	3
12月	2	0	0	2
1月	1	1	0	2
2月	1	2	0	3
3月	1	0	0	1
令和6年度合計	18	14	1	33

7.2 監視（サーバー及びネットワーク）

(1) 標準セキュリティシステム及び庁内システム（広域連合側 LGWAN ネットワーク機器を含む）、事務局 VDI システム、本調達で設置したテレワーク及び中間サーバーネットワーク機器の稼働状況を 24 時間 365 日監視し、障害発生時には速やかに報告及び必要な処置につなげること。監視項目は次の項目とするが、運用保守開始に向けて監視項目については協議を行った上で確定とすること。

表4. 監視項目（参考例）

種別	メーカー	対象機器	監視項目			
			Ping	SNMP	OS ※1	ログ
サーバー(物理)	Dell	管理基盤サーバー	✓	✓	✓	✓
ストレージ	NetApp	管理基盤用兼 ファイルサーバ用ストレージ	✓	✓		
バックアップ	Arcserve	バックアップサーバ	✓	✓		
スイッチ	Cisco	DC3サーバ収容スイッチ	✓	✓	✓	✓
ファイアウォール	Cisco	LGWAN接続ファイアウォール	✓	✓	✓	✓

※1:リソース/ポート/プロセス等への監視

- (2) リソース（メモリ、ディスク）使用率が設定した上限値を超えないか監視すること。
- (3) 監視センターまでの通信は VPN サービスを利用したクローズドネットワークとし、回線費用も本業務内に含めること。なお、監視システムを提案により別途構築する場合は、すべての費用を計上し、本業務内に含めること。
- (4) 標準セキュリティシステム及び、庁内システム、事務局 VDI システムの監視ができるここと。
- (5) 監視については、Ping 監視を広域連合が定めるスケジュールに従い、24 時間 365 日対応で行うこと。

7.3 障害の切り分け

- (1) 窓口への報告又は監視により障害を検知した場合には、広域連合及び必要に応じてハードウェア保守事業者又は広域連合が指定する標準システム運用業者への連絡調整、指示受け等、協議のうえ基準を定め、一次対応を行うこと。一次対応は24時間365日対応で行い、速やかに復旧のための対応をとること。
- (2) 過去の障害情報を検索し、対応できる事象がある場合は、回答又は解決方法を実施する。ただし、システムへの侵入、ウイルス感染等、セキュリティに関するインシデントである可能性がある場合は、速やかに広域連合に報告し、広域連合の指示に基づいて対応すること。
- (3) 過去の障害情報を検索し、対応できる事象がない場合、緊急度、優先順位、影響範囲等を考慮して、適切な問題処理を行うこと。
- (4) 発生した障害、その対応内容及び対応結果について記録を作成し、一元的に保管及び管理し、緊急度合に応じて広域連合に報告すること。

7.4 システムの復旧

- (1) 標準セキュリティシステム及び庁内システム、事務局VDIシステム構成機器に係る障害復旧時間は、広域連合に責めのない原因の障害については、原則として受付から6時間以内とすることとするが、完了できない場合は、原因の確認から対応方針の確定までは必ず行うこと。
- (2) 根本的に解決できない場合は、広域連合の了承を得た上で、一時的な対応を実施すること。かつ、恒久的な解決策を策定又は関連事業者に依頼すること。
- (3) 障害発生時に、迅速にシステムを再稼働し、運用停止時間が極力短くなるよう、復旧手順や体制を整備しておくこと。
- (4) 復旧に際して、広域連合への第一報を迅速に行い、復旧完了まで、時系列に随時報告を行い、情報の共有を図ること。

7.5 ハードウェア保守

- (1) 機器リースにより令和14年3月末までのハードウェア保守サービスが提供されることから、障害発生時には保守事業者との連絡調整を行い、6時間以内に対応を完了すること。
- (2) 年1回、対象機器について定期点検を行うこと。
- (3) 定期点検において異常が発見された場合は、速やかに広域連合及び保守事業者との連絡調整を実施すること。
- (4) ハードディスク等の記録媒体を使用する場合は、事前に報告した上で、使用後のハードディスク等の全てのデータを消去すること。消去は不可逆的であるものとし、故障等により消去が不可能な場合は、物理的に破壊すること。

7.6 運用支援

- (1) 保守作業に伴う機器の設定変更については、運用業務に含めること。ただし、大規模な設計変更が必要な事項については、別途協議する。
- (2) 本業務の保守対象機器の故障の予兆を検知したときは、広域連合に確認のうえ、保守事業者との連絡調整を実施すること。
- (3) 標準セキュリティシステム及び庁内システム、事務局VDIシステムの稼働状況を分析・調査し、改善が必要な場合は提案を行うこと。
- (4) 導入したハードウェア及びソフトウェアに脆弱性が発見された場合は、広域連合に報告のうえ、速やかに対策を行うこと。
- (5) 保守作業等に伴い設定等に変更が生じた場合は、隨時、関連ドキュメント(保守手引書、パラメータシート、運用手順書等)を修正し、広域連合に提出すること。なお、ドキュメントのバージョン及び更新履歴を明記すること。

- (6) 標準セキュリティシステム及び庁内システム、事務局 VDI システムが円滑に運用できるよう、広域連合のシステム担当に対し、運用期間中 1 回は操作研修を行うこと。研修資料は、研修実施日の 7 日前までに電子データで広域連合へ提出すること。また、広域連合システム担当が広域連合職員に操作研修を行うことができるよう支援すること。
- a. 研修場所 広域連合事務局（横浜市神奈川区栄町 8 番地 1）
 - b. 研修日時 運用開始後に指定
- (7) 業務完了後、使用した機器等について、広域連合の指示により適切な方法で処分すること。その際、機器等に記録された全データを、不可逆的に消去し、消去した旨を証明する書類を提出すること。
- (8) 今後のシステム変更や運用に関する技術的支援や問合せ対応を行うこと。
- (9) 運用終了後に、次のシステムに係る受託事業者が本件の受託者と異なる場合は、移行等に係る技術的な協力及び試験等について誠実に協力すること。
- (10) 次の作業について、支援業務を行うこと。
- (ア) 年度切り替え、人事異動等に伴う庁内システム及びの設定作業に協力すること。
 - (イ) 広域連合担当職員への運用等に関する研修（必要に応じて 1 回程度）を行うこと。
 - (ウ) クライアント端末に対する Microsoft Windows Update 適用作業（年 3 回程度）を行うこと。
 - (エ) クライアント端末への外字ファイルの配信・適用を行うこと（年 1 回程度）その他、リモート保守業務への支援を行うこと。
 - (オ) クライアント端末等の障害時には、再キッティング等を行い他のクライアント端末と同様の状態に戻すこと。
- (11) ウィルス対策、データ管理・保護対策及びネットワーク環境等について、安定的かつ確実なシステム運用が継続できるよう、適宜提案を行うこと。
- (12) ソフトウェア更新等標準セキュリティシステム及び庁内システム、事務局 VDI システムに導入されているソフトウェアについて、ソフトウェアベンダからのパッチ（不具合修正を目的とするパッチ、脆弱性対策を目的とするセキュリティパッチの両方を含む。）の提供情報及び脆弱性に関する情報を継続的に収集し、必要に応じて報告すること。
- (13) OS・ミドルウェアの不具合修正資源の適用（各システム 1-2 回/年）
保守関連事業者から提供される修正版の OS・ミドルウェアの不具合修正資源を、システムに適用する計画を作成し、広域連合の承認の上で適用を実施すること。
- (14) ウィルスパターンファイルの適用（適宜）
- (15) 広域連合情報システムに関する技術的問題点、機器のバグ、パッチ及びバージョンアップ等に関する情報を速やかに提供すること。また、OS・ミドルウェアや仮想化ソフト等についてはソフトウェアベンダがアナウンスする保守期間内で定期リリースされるバージョンアップ用のファイルやシステム・セキュリティに多大な影響を及ぼす緊急性の高いパッチファイルは、バージョンアップの対象とする。ただし、メーカーサポート終了によるバージョンアップや後継製品等への移行要否判断及び費用については別途協議を行うこととする。パッチ、バージョンアップ等の適用を実施する場合は、スケジュールを提示して広域連合の承認を受けた上で、実施すること。なお、必要に応じて、事前検証等を実施し、影響範囲を特定すること。
- (16) 物理サーバー群、仮想サーバー群は、定期・不定期に必要なセキュリティパッチを適用する等、適切なセキュリティ対策を講じること。併せて、メーカーのサポートが確実に得られるよう環境を保持すること。適用を行う場合は、当該パッチ適用による影響を十分調査し、実施手順を確立して行うこと。なお、不測の事態に備え、切り戻し等の手順を確立すること。
- (17) 構築した環境にサーバー証明書を適用した場合は、証明書の有効期限が切れる前に証明書の更新を行うこと。
- (18) 定期メンテナンスは庁内システム及び標準セキュリティシステム運用時間外に行うものとし、必ず事前に実施日を広域連合と調整すること。

7.7 データバックアップの管理

- (1) バックアップスケジュールに基づき、データのバックアップ結果確認を行うこと。
- (2) バックアップスケジュールはファイルサーバーにおいては日次差分バックアップで7世代保存、その他のシステムサーバーにおいては週次での差分バックアップを設定し4世代の保管を最低基準とすること。
- (3) 障害発生時等にバックアップの必要性が求められる場合、広域連合の指示に従い、障害発生前に取得したバックアップデータからファイルの復元を行うこと。
- (4) 標準セキュリティシステムの認証関係のバックアップは、当該年度を除く7年分を保持できるよう対応すること。

7.8 実績報告

- (1) 次の項目を含む月毎の実績報告書を、広域連合事務局へ、紙媒体及び電子ファイルで各正副1部、原則として翌月10日までに提出すること。なお、使用言語は日本語とし、用紙サイズはA4判横型を原則とする。電子ファイルについては、Microsoft OfficeのWord/Excel等で作成すること。また、PDF形式にした資料も提供すること。
 - (ア) 標準セキュリティシステム及び庁内システム、事務局VDIシステム稼働状況
 - (イ) 標準セキュリティシステム及び庁内システム、事務局VDIシステムに係る障害発生状況
 - (ウ) 標準セキュリティシステム及び庁内システム、事務局VDIシステム障害発生連絡等の受付・処理状況
 - (エ) インシデント発生、受付及び処理状況
 - (オ) その他広域連合が報告を求める事項
- (2) 実績報告に伴い広域連合が口頭での説明又は調整を必要とする場合は、適宜、会議を開催すること。また、障害・インシデントが発生した場合は、隨時、発生状況、原因及び影響範囲、対応状況等について書面で報告すること。

8 契約条件

8.1 契約条件

(1) 知的財産権の帰属等

本件業務において作成した成果物に対する権利は、本業務にかかる費用の支払いが完了したときに、受託者から広域連合に移転するものとする。ただし、権利の移転前であっても、広域連合が必要な範囲において、成果物を利用することができる。

受託者は、成果物に係る著作者人格権を行使しないものとする。

本件業務の遂行に関し、第三者との間で著作権に係る権利侵害の紛争等が生じた場合は、当該紛争の原因が専ら広域連合の責めに帰す場合を除き、受託者は自らの負担と責任においてその紛争等の一切を処理するものとする。

(2) 契約不適合責任

引き渡された目的物が種類、品質又は数量に関して契約の内容に適合しないものである場合（受託者が広域連合に移転した権利が契約の内容に適合しないものである場合を含む。）は、広域連合は、受託者に対し、履行の追完の請求、代金の減額の請求（不適合が広域連合の責めに帰すべき事由によるものであるときを除く。）、損害賠償の請求及び契約の解除をすることができる。

受託者が種類又は品質に関して契約の内容に適合しない目的物を広域連合に引き渡した場合において、広域連合がその不適合を知った時から1年以内にその旨を受託者に通知しないときは、広域連合は、その不適合を理由として、履行の追完の請求、代金の減額の請求、損害賠償の請求及び契約の解除をすることができない。ただし、受託者が引渡しの時にその不適合を知り、又は重大な過失によって知らなかつたときは、この限りでない。

(3) 守秘義務及び個人情報保護

受託者は、本件業務により知り得た情報について、個人情報であるか否かを問わず、業務の実施に必要な範囲内においてのみ利用するものとし、いかなる場合も第三者に漏らしてはならない。また、所定の場所以外に持ち出してはならない。これは、契約終了又は契約が解除された後においても同様とする。

受託者は、本件業務の履行に関して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を遵守し、個人情報の適切な管理のために必要な措置を講じなければならない。

(4) 再委託の制限

受託者は、本件業務の全部もしくは重要な部分を、一括して第三者に再委託してはならないものとする。

受託者は、本件業務の一部を第三者に再委託する際は、次の項目を記載した書面を事前に広域連合に通知し、承認を得なければならない。

- (ア) 再委託を行う理由
- (イ) 再委託する業務の内容
- (ウ) 再委託先に対する業務管理方法
- (エ) 再委託する業務に含まれる情報の種類
- (オ) 再委託先の情報セキュリティ管理体制
- (カ) 再委託先が本仕様書を遵守する旨の誓約書

(5) 善管注意義務

機器等の配達、設置、保守等の業務に従事するものは、善良な管理者の注意をもって本件業務の実施に当たるとともに、情報セキュリティ対策について細心の注意を払うものとする。

(6) その他

本仕様書に定めのない事項及び疑義が生じた場合は、必要に応じて広域連合と受託者が協議して書面にて合意するものとする。

受託者は当該契約による作業を実施するため個人情報を取り扱う場合には、個人情報保護のため、約款特記事項（個人情報の保護）及び情報セキュリティポリシーを遵守しなければならない。なお、委託者から依頼があった場合には監査の実施及び報告をすること。

別紙1 現行システムクライアント端末仕様

1 ハードウェア

(1) 標準物理端末 (デスクトップ端末)

分類	品名・規格・機種等	性能等	メーカー	備考
PC	HP ProDesk 600 G6 SFF/CT	Intel(R) Core(TM) i5-10500(6C/3.1GHz/12M) 8GB (8GBx1) DDR4 DIMM 2666MT/s 500GB HDD 7200rpm (SATA3) TPM2.0準拠 (暗号機能) DVD-ROMドライブ USBポート Type-C x 1、 Type-A 3.2 Gen2 x 2 Type-A 3.2 Gen1 x 5 Type-A 2.0 x 2 LAN 1000BASE-T / 100BASE-TX / 10BASE-T	HP	リース対象
ディスプレイ	HP 23.8インチワイドIPSモニター P24v	解像度 1,920×1,080	HP	リース対象
キーボード	HP USB 320 キーボード (日本語)	OADG準拠日本語109Aキー ¹ ボード サイズ：426.2 × 110.9 × 16.7 mm 質量：413g ケーブル長：180cm	HP	リース対象
マウス	HP USB 320 マウス	ホイール付き2ボタンレーザーマウス USB接続 サイズ：103.8 × 63.4 × 35.5 mm 質量：75.8g ケーブル長：180cm	HP	リース対象

(2) 標準物理端末 (ノートブック端末)

分類	品名・規格・機種等	性能等	メーカー	備考
PC	HP 250 G7/CT	インテル(R) Core(TM) i5-1035G1 (1.0-3.6GHz) /15.6インチワイドFHD (1920×1080) ディスプレイ 8GB (8GB×1) DDR4-2400 DVD-RWドライブ 500GB HDD 5400rpm (SATA) TPM2.0準拠 (暗号機能) USB3.2(Gen 1)ポート×3 LAN 1000BASE-T / 100BASE-TX / 10BASE-T	HP	リース対象
マウス	HP USB 320 マウス	ホイール付き2ボタンレーザーマウス USB接続 サイズ：103.8 × 63.4 × 35.5 mm 質量：75.8g ケーブル長：180cm	HP	リース対象

(3) VDI利用端末 (ノートブック端末)

分類	品名・規格・機種等	性能等	メーカー	備考
PC	HP ProBook 450 G8/CT Notebook PC	インテル(R) Core(TM) i5-1235U /15.6インチワイドFHD (1920×1080) ディスプレイ 8GB (8GB×1) DDR4-3200 128 GB M.2 SSD(PCIe NVMe) TPM2.0準拠 (暗号機能) USB3.2(Gen 1)ポート×3 LAN 1000BASE-T / 100BASE-TX / 10BASE-T	HP	リース対象
マウス	HP USB 320 マウス	ホイール付き2ボタンレーザーマウス USB接続 サイズ：103.8 × 63.4 × 35.5 mm 質量：75.8g ケーブル長：180cm	HP	リース対象

別紙2 現行システムプリンタ、複合機、スキャナ仕様

1 プリンタ

(1) A4モノクロレーザープリンタ

分類	品名・規格・機種等	性能等	メーカー	備考
A4モノクロプリンタ (1系統ネットワーク)	ApeosPort VII P4022	【プリント速度】片面A4：48枚/分 【プリント解像度】1,200dpi×1,200dpi 【給紙容量】給紙トレイ：550枚 手差しトレイ：150枚 【排紙容量】250枚 【両面印刷】可能 【オプション】 ・ICカードリーダー（広域連合事務局内のみ）	富士フィルムビジネス イノベーション	市町村、広域連合事務局 (標準セキュリティシステム・庁 内システム両システムで利 用)

(2) A3カラー高速プリンタ

分類	品名・規格・機種等	性能等	メーカー	備考
A3カラー高速プリンタ (2系統ネットワーク)	ApeosPort Print C5570	【プリント速度】片面A3：27枚/分 A4：55枚/分 【プリント解像度】1,200dpi×2,400dpi 【給紙容量】給紙トレイ：560枚×2段 手差しトレイ：100枚 【排紙容量】400枚以上 【両面印刷】可能 【オプション】 ・増設ネットワークボード： ・2トレイモジュール：560枚×2段 ・大容量給紙トレイ（1段）：2300枚 ・フィニッシャーB3 【オプション】 ・ICカードリーダー（広域連合事務局内のみ）	富士フィルムビジネス イノベーション	広域連合事務局内のみ (標準セキュリティシステム・庁 内システム両システムで利 用)

(3) A3カラープリンタ

分類	品名・規格・機種等	性能等	メーカー	備考
A3カラープリンタ (2系統ネットワーク)	ApeosPort Print C4570	【プリント速度】片面A3：22枚/分 A4：45枚/分 【プリント解像度】1,200dpi×2,400dpi 【給紙容量】給紙トレイ：560枚×2段 手差しトレイ：100枚 【排紙容量】400枚以上 【両面印刷】可能 【オプション】 ・増設ネットワークボード（広域連合事務局内のみ） ・ICカードリーダー（広域連合事務局内のみ）	富士フィルムビジネス イノベーション	・広域連合事務局内 (標準セキュリティシステム・庁 内システム両システムで利 用) ・国保連事務室内

(4) A3モノクロ複合機

分類	品名・規格・機種等	性能等	メーカー	備考
A3モノクロ複合機 (1系統ネットワーク)	ApeosPort 4570PFS	【プリント速度】片面A4：45枚/分 【プリント解像度】1,200dpi×2,400dpi 【給紙容量】給紙トレイ：560枚×4段 手差しトレイ：100枚 【排紙容量】400枚以上 【両面印刷】可能 【オプション】 ・増設ネットワークボード ・ICカードリーダー	富士フィルムビジネス イノベーション	広域連合事務局内のみ (庁内システムで利用)

2 ドキュメントスキャナ

分類	品名・規格・機種等	性能等	メーカー	備考
ドキュメントスキャナ	imageFORMULA DR-C240	【読み取り速度】片面A4 24bitカラー：20枚/分以 上、モノクロ：45枚/分以上 【読み取り解像度】300dpi	キヤノン	国保連事務室内

別紙3 次期システムクライアント端末ソフトウェア

要求機能	製品	調達方法	インストール台数					備考
			標準セキュリティシステム	庁内システム	事務局VDIシステム			
標準物理端末	庁内物理端末	標準VDI	庁内VDI	VDI利用端末				
Microsoft Windows	Windows 11 IoT Enterprise LTSC 2024	事業者	350	4	47	67	69	–
ユーザー認証	SmartOn ID 自治体専用強靭性向上特別パック	事業者	350	4	47	67	69	カード認証は指定の標準物理端末と 庁内物理端末に設定すること。 生体認証はカード認証以外の端末 に設定すること。
Microsoft Office	Office LTSC Standard 2024	事業者	340	–	47	–	–	指定の端末にインストールすること。
	Office LTSC Professional Plus 2024	事業者	10	–	–	–	–	指定の端末にインストールすること。
	Office LTSC Standard 2024 又は Microsoft 365 Apps for business	事業者	–	4	–	–	–	提案した製品をインストールすること。
	Office LTSC Professional Plus 2024 又は Microsoft 365 Apps for business	事業者	–	–	–	67	–	提案した製品をインストールすること。
Webブラウザ	Microsoft Edge	OS標準	350	4	47	67	69	–
PDF編集機能	機能制限ライセンス付き Acrobat Standard DC (デスクトップ専用)	事業者	–	–	–	15	–	指定の端末にインストールすること。
PDF表示機能	Adobe Acrobat Reader	広域連合より提供	350	4	47	52	–	指定の端末にインストールすること。
ウイルス対策	Windows Defender	OS標準	350	4	47	67	69	–
不正デバイス利用禁止	事業者にて選定	事業者	350	4	47	67	69	–
ファイルの圧縮・解凍	7Zip	広域連合より提供	350	4	47	67	–	–
オフィス向け文書管理ソフトウェア	DocuWorks	事業者	–	4	–	67	–	–
ファイル授受 (広域連合・拠点間)	事業者にて選定	事業者	350	–	47	–	–	–
ファイル授受 (標準VDI・庁内VDI間)	事業者にて選定	事業者	–	–	47	67	–	–
外字の利用	KAJO_J入力システムV7後期高齢者医療広域連合 電算処理システム対応版	広域連合より提供	350	–	47	–	–	–
リモートアクセス	事業者にて選定	事業者	350	–	–	–	–	–
バイナリ編集ソフト	EmeditorPro	広域連合より提供	350	–	47	–	–	–
KSCソフトウェア	KSC提供ソフトウェア	広域連合より提供	–	4	–	67	–	–
VDIクライアント	事業者にて選定	事業者	–	–	–	–	69	–
クローニングツール	事業者にて選定	事業者	1	1	–	–	–	指定の時期に、管理端末のイメージ を取得すること。

拠点名	分類 システム名	クライアント端末										ネットワーク機器(※2)						プリント				その他		備考		
		標準セキュリティシステム			事務局VDIシステム				ネットワーク機器(※2)						プリント				その他							
		標準物理端 末 ノートPC	標準物理端 末 デスクトップPC 及び ディスプレイ	標準物理端 末 ノートPC (※1)	庁内物理端末 ノートPC (ノート PC)	VDI 利用端末 (ノート PC)	標準VDI	庁内VDI	ルータ	L3SW (48ポート)	L2SW (24ポート)	L2SW (16ポート)	L2SW (12ポート)	L2SW (8ポート)	FireWall	無線AP	A4モノクロ レーザー ¹ プリンタ	A3カラーハイ 速プリンタ	A3カラーブ リント	複合機	ドキュメント スキャナ	セキュリティ USBメモリ (32MB)	セキュリティ ワイヤー (※3)			
1 神奈川県後期高齢者医療広域連合	横浜市神奈川区栄町8-1 ヨコハマポートサイドタワー	57		4	69	47	67	2		2	1	7	6		5	2	1	1	1		10		標準セキュリティシステム 庁内システム 事務局VDIシステム			
2 横浜市・開発センター	横浜市戸塚区(詳細は非公開)	1						1															1			
3 横浜市・データセンター	横浜市都筑区(詳細は非公開)	1						1															1			
4 横浜市役所・本庁	横浜市中区本町6-50-10	4						1					1									3	4			
5 横浜市・鶴見区役所	横浜市鶴見区鶴見中央3-20-1	4						1															4			
6 横浜市・神奈川区役所	横浜市神奈川区広谷1丁目3-8	4						1															4			
7 横浜市・西区役所	横浜市西区中央1-5-10	2						1															2			
8 横浜市・中区役所	横浜市中区日本大通35	3						1															3			
9 横浜市・南区役所	横浜市南区蒲舟町2-33	4						1															4			
10 横浜市・保土ヶ谷区役所	横浜市保土ヶ谷区川辺町2-9	4						1															4			
11 横浜市・磯子区役所	横浜市磯子区磯子3-5-1	4						1															4			
12 横浜市・金沢区役所	横浜市金沢区泥亀2-9-1	5						1															5			
13 横浜市・港北区役所	横浜市港北区大豆戸町26-1	5						1															5			
14 横浜市・戸塚区役所	横浜市戸塚区戸塚町16-17	6						1															6			
15 横浜市・港南区役所	横浜市港南区港南4-2-10	5						1															5			
16 横浜市・旭区役所	横浜市旭区鶴ヶ崎1-4-12	5						1															5			
17 横浜市・緑区役所	横浜市緑区寺山町118	4						1															4			
18 横浜市・瀬谷区役所	横浜市瀬谷区二ツ橋町190	3						1															3			
19 横浜市・栄区役所	横浜市栄区桂町303-19	3						1															3			
20 横浜市・泉区役所	横浜市泉区と泉中央5-1-1	4						1															4			
21 横浜市・青葉区役所	横浜市青葉区市ヶ尾31-4	5						1															5			
22 横浜市・都筑区役所	横浜市都筑区茅ヶ崎中央32-1	3						1															3			
23 川崎市役所・本庁	川崎市川崎区宮本町1 川崎市役所第三庁舎	3						1					1									1	3			
24 川崎市役所・事務センター	川崎市川崎区(詳細は非公開)	4																					4			
25 川崎市・川崎区役所	川崎市川崎区東田町8	3						1															3			
26 川崎市・幸区役所	川崎市幸区戸手本町1-11-1	3						1															3			
27 川崎市・中原区役所	川崎市中原区小杉町3-245	3						1															3			
28 川崎市・高津区役所	川崎市高津区下作延2-8-1	3						1															3			
29 川崎市・多摩区役所	川崎市多摩区登戸1775-1	3						1															3			
30 川崎市・宮前区役所	川崎市宮前区宮前平2-20-5	3						1															3			
31 川崎市・麻生区役所	川崎市麻生区万福寺1-5-1	3						1															3			
32 相模原市役所・本庁	相模原市中央区中央2-11-15	9						1					1									1	9			
33 相模原市役所・コールセンター	相模原市中央区中央2-11-15	4																					4			
34 相模原市役所・高齢・障害支援課	相模原市中央区富士見6-1-1 ウェルネスさがみはらA館	1						1															1			
35 相模原市・緑区役所	相模原市緑区西橋本5-3-21 (緑区合同庁舎内)	1						1															1			
36 相模原市・南区役所	相模原市南区相模大野5-31-1 (南区合同庁舎内)	1						1															1			
37 相模原市・津久井保健福祉課	相模原市緑区中野613-2	1						1															1			
38 相模原市・相模湖保健福祉課	相模原市緑区と瀬896	1						1															1			
39 相模原市・城山保健福祉課	相模原市緑区久保沢1-3-1	1						1															1			
40 相模原市・藤野保健福祉課	相模原市緑区小瀬2000	1						1															1			
41 横須賀市役所	横須賀市小川町11番地 横須賀市役所本庁舎	9						1					1										1	9		
42 横須賀市役所・追浜行政センター	横須賀市夏島町9							1																		
43 横須賀市役所・田浦行政センター	横須賀市船越町6-77							1																		
44 横須賀市役所・逸見行政センター	横須賀市東逸見町2-29																									

別紙5 広域連合情報システム接続拠点一覧

令和7年12月現在

	拠点名	所在地	帯域	備考
1	神奈川県後期高齢者医療広域連合	横浜市神奈川区栄町8-1 ヨコハマポートサイドビル9階	50M	2回線 標準セキュリティシステム 庁内システム
2	横浜市・開発センター	横浜市戸塚区（詳細は非公開）	10M	
3	横浜市・データセンター	横浜市都筑区（詳細は非公開）	100Mx2	冗長化
4	横浜市役所・本庁	横浜市中区本町6-50-10	20M	
5	横浜市・鶴見区役所	横浜市鶴見区鶴見中央3-20-1	10M	
6	横浜市・神奈川区役所	横浜市神奈川区広台太田町3-8	10M	
7	横浜市・西区役所	横浜市西区中央1-5-10	10M	
8	横浜市・中区役所	横浜市中区日本大通35	10M	
9	横浜市・南区役所	横浜市南区浦舟町2-33	10M	
10	横浜市・保土ヶ谷区役所	横浜市保土ヶ谷区川辺町2-9	10M	
11	横浜市・磯子区役所	横浜市磯子区磯子3-5-1	10M	
12	横浜市・金沢区役所	横浜市金沢区泥亀2-9-1	10M	
13	横浜市・港北区役所	横浜市港北区大豆戸町26-1	10M	
14	横浜市・戸塚区役所	横浜市戸塚区戸塚町16-17	10M	
15	横浜市・港南区役所	横浜市港南区港南4-2-10	10M	
16	横浜市・旭区役所	横浜市旭区鶴ヶ峰1-4-12	10M	
17	横浜市・緑区役所	横浜市緑区寺山町118	10M	
18	横浜市・瀬谷区役所	横浜市瀬谷区二ツ橋町190	10M	
19	横浜市・栄区役所	横浜市栄区桂町303-19	10M	
20	横浜市・泉区役所	横浜市泉区和泉中央北5-1-1	10M	
21	横浜市・青葉区役所	横浜市青葉区市ヶ尾31-4	10M	
22	横浜市・都筑区役所	横浜市都筑区茅ヶ崎中央32-1	10M	
23	川崎市役所・本庁	川崎市川崎区宮本町1 川崎市役所第三庁舎	100M	
24	川崎市役所・事務センター	川崎市川崎区（詳細は非公開）	-	
25	川崎市・川崎区役所	川崎市川崎区東田町8	10M	
26	川崎市・幸区役所	川崎市幸区戸手本町1-11-1	10M	
27	川崎市・中原区役所	川崎市中原区小杉町3-245	10M	

	拠点名	所在地	帯域	備考
28	川崎市・高津区役所	川崎市高津区下作延2-8-1	10M	
29	川崎市・多摩区役所	川崎市多摩区登戸1775-1	10M	
30	川崎市・宮前区役所	川崎市宮前区宮前平2-20-5	10M	
31	川崎市・麻生区役所	川崎市麻生区万福寺1-5-1	10M	
32	相模原市役所・本庁	相模原市中央区中央2-11-15 相模原市役所本庁舎	100M	
33	相模原市役所・コールセンター	相模原市中央区中央2-11-15 相模原市役所本庁舎	-	
34	相模原市役所・高齢・障害支援課	相模原市中央区富士見6-1-1 ウェルネスさがみはらA館	10M	
35	相模原市・緑区役所	相模原市緑区西橋本5-3-21 (緑区合同庁舎内)	10M	
36	相模原市・南区役所	相模原市南区相模大野5-31-1 (南区合同庁舎内)	10M	
37	相模原市・津久井保健福祉課	相模原市緑区中野613-2	10M	
38	相模原市・相模湖保健福祉課	相模原市緑区与瀬896	10M	
39	相模原市・城山保健福祉課	相模原市緑区久保沢1-3-1	10M	
40	相模原市・藤野保健福祉課	相模原市緑区小渕2000	10M	
41	横須賀市役所	横須賀市小川町11番地 横須賀市役所本庁舎	80M	
42	横須賀市役所・追浜行政センター	横須賀市夏島町9	10M	プリンタのみ設置
43	横須賀市役所・田浦行政センター	横須賀市船越町6-77	10M	プリンタのみ設置
44	横須賀市役所・逸見行政センター	横須賀市東逸見町2-29	10M	プリンタのみ設置
45	横須賀市役所・衣笠行政センター	横須賀市公郷町2-11	10M	プリンタのみ設置
46	横須賀市役所・西行政センター	横須賀市長坂1-2-2	10M	プリンタのみ設置
47	横須賀市役所・大津行政センター	横須賀市大津町3-34-40	10M	プリンタのみ設置
48	横須賀市役所・浦賀行政センター	横須賀市浦賀5-1-2	10M	プリンタのみ設置
49	横須賀市役所・久里浜行政センター	横須賀市久里浜6-14-2	10M	プリンタのみ設置
50	横須賀市役所・北下浦行政センター	横須賀市長沢2-7-7	10M	プリンタのみ設置
51	平塚市役所	平塚市浅間町9-1 平塚市役所本庁舎	10M	
52	鎌倉市役所	鎌倉市御成町18-10 鎌倉市役所	10M	
53	藤沢市役所	藤沢市朝日町1-1 藤沢市役所本庁舎1階	10M	
54	小田原市役所	小田原市荻窪300 小田原市役所	10M	
55	茅ヶ崎市役所・本庁	茅ヶ崎市茅ヶ崎1-1-1 茅ヶ崎市役所	10M	

	拠点名	所在地	帯域	備考
56	茅ヶ崎市役所・小出支所	茅ヶ崎市芹沢888	10M	プリントのみ設置
57	逗子市役所	逗子市逗子5-2-16 逗子市役所	10M	
58	三浦市役所	三浦市城山町1-1 三浦市役所本庁舎	10M	
59	秦野市役所	秦野市桜町1-3-2 秦野市役所本庁舎	10M	
60	厚木市役所	厚木市中町3-17-17 厚木市役所本庁舎	10M	
61	大和市役所・本庁	大和市下鶴間1-1-1 大和市役所本庁舎	10M	
62	大和市役所・渋谷分室	大和市福田2021-2 高座渋谷駅前複合ビル	10M	
63	伊勢原市役所	伊勢原市田中348 伊勢原市役所本庁舎	10M	
64	海老名市役所	海老名市勝瀬175-1 海老名市役所本庁舎	10M	
65	座間市役所	座間市緑ヶ丘1-1-1 座間市役所	10M	
66	南足柄市役所	南足柄市関本440 南足柄市役所本庁舎	10M	
67	綾瀬市役所	綾瀬市早川550 綾瀬市役所	10M	
68	葉山町役場	三浦郡葉山町堀内2135 葉山町役場本庁舎	10M	
69	寒川町役場	高座郡寒川町宮山165 寒川町役場本庁舎	10M	
70	大磯町役場	中郡大磯町東小磯183 大磯町役場本庁舎	10M	
71	二宮町役場	中郡二宮町二宮961 二宮町役場	10M	
72	中井町役場	足柄上郡中井町比奈窪56 中井町役場	10M	
73	大井町役場	足柄上郡大井町金子1995 大井町役場	10M	
74	松田町役場	足柄上郡松田町松田惣領2037 松田町役場	10M	
75	山北町役場	足柄上郡山北町山北1301-4 山北町役場本庁舎	10M	
76	開成町役場	足柄上郡開成町延沢773 開成町役場	10M	
77	箱根町役場	足柄下郡箱根町湯本256 箱根町役場本庁舎	10M	
78	真鶴町役場	足柄下郡真鶴町岩244-1 真鶴町役場	10M	
79	湯河原町役場	足柄下郡湯河原町中央2-2-1 湯河原町役場第一庁舎	10M	
80	愛川町役場	愛甲郡愛川町角田251-1 愛川町役場新庁舎	10M	
81	清川村役場	愛甲郡清川村煤ヶ谷2216 清川村役場	10M	
82	国保連合会事務室	横浜市西区楠町27-1 神奈川県国保会館	50M	
83	新国保連合会事務室	横浜市神奈川区鶴屋町3-29-4	50M	

	拠点名	所在地	帯域	備考
84	令和9年新拠点	神奈川県北部エリア	10M（予定）	新規
85	データセンター1	東京都中央区（詳細は非公開）	30M	
86	データセンター2	(提案による)	100M（予定）	新規
87	データセンター3	横浜市泉区（詳細は非公開）	100M	現行データセンター
88	テレワークデータセンター	横浜市都筑区（詳細は非公開）	30M	

別紙6 スケジュール概略

	令和8年 4月	5月	6月	7月	8月	9月	10月	11月	12月	令和9年 1月	2月	3月	4月以降
プロジェクト計画書・要件定義書提出	▲												
システム設計		■											
データセンター契約					▲								
機器調達・設置							■						
ネットワーク構築								■	■	■			
システム構築・テスト							■						
端末等設置								■	■	■			
操作研修等										■	■	■	
運用・保守											■		■