

別紙 A

機器等の要求仕様等

第三期サーバ仮想化統合基盤の賃貸借及び運用保守契約

令和7年4月

長崎県総務部スマート県庁推進課

【目次】

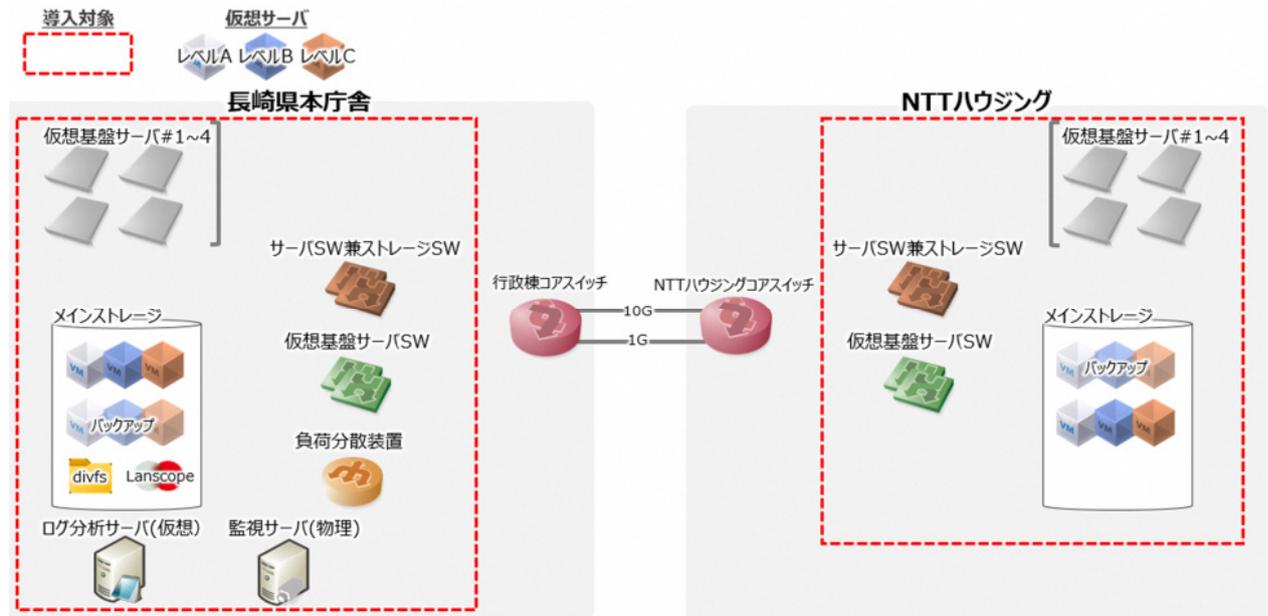
1. システム構成	3
1.1. システム構成図	3
2. ハードウェア構成	4
2.1. 共通要件	4
2.2. 庁舎側仮想化基盤サーバ	4
2.3. 庁舎側仮想化基盤ストレージ	4
2.4. 庁舎側監視サーバ	5
2.5. 庁舎側サーバスイッチ兼ストレージスイッチ	6
2.6. 庁舎側本庁コアスイッチ用機器	6
2.7. 庁舎側サーバスイッチ	6
2.8. データセンター側仮想化基盤サーバ	6
2.9. データセンター側仮想化基盤ストレージ	7
2.10. データセンター側サーバスイッチ兼ストレージスイッチ	8
2.11. データセンター側既存 L3 スwitch用機器	8
2.12. データセンター側サーバスイッチ	8
2.13. 庁舎側サーバ負荷分散装置	8
2.14. 庁舎側ファシリティ関連装置	9
2.15. データセンター側ファシリティ関連装置	9
3. ソフトウェア構成	9
3.1. 共通要件	9
3.2. 仮想化基盤ソフト	10
3.3. オペレーティングシステム等	10
3.3.1. オペレーティングシステム (Red Hat Linux)	10
3.3.2. オペレーティングシステム (Microsoft Server 2022 Datacenter)	10
3.3.3. ウイルス対策	10
3.4. 監視サーバ用ソフトウェア	11
3.5. ログ統合ソフトウェア	11
3.6. バックアップソフトウェア	12
4. システム構築要件	12
4.1. 構築に係る要件	12
4.1.1. 基本要件	12
4.1.2. サーバ共通	12
4.1.3. 仮想化基盤サーバ	13
4.1.4. ストレージ	13
4.1.5. ネットワーク	13
4.1.6. バックアップ	13
4.1.7. システム運用監視	13
4.1.8. ログ分析	14
4.2. プロジェクト管理の実施	14
4.3. 設計図書の作成	14
4.3.1. 基本設計書の作成	14
4.3.2. 運用設計書の作成	14
4.3.3. 詳細手順書の作成	15
4.3.4. 運用手順書の作成	15
4.4. テスト要件	15
4.4.1. テストの種類	15
4.4.2. テスト実施要件	16
4.4.3. テスト計画書の作成	16
4.4.4. テスト結果報告書の作成	16
4.5. 導入に係る要件	16

4.6. 教育に係る要件.....	17
4.6.1. 教育の種類.....	17
4.6.2. 教育実施方法.....	17
4.7. 機器設置に係る要件.....	17
4.7.1. 設置場所.....	17
4.7.2. LAN 配線.....	17
5. 運用保守要件.....	17
5.1. 運用保守要件.....	17
5.1.1. ハードウェア保守要件.....	17
5.1.2. ソフトウェア保守要件.....	18
5.1.3. 運用管理要件.....	18
5.1.4. 特記事項.....	19
5.2. 契約満了に伴う機器撤去.....	19
5.2.1. 基本要件.....	19
5.2.2. 作業方法.....	19
6. 作業の体制および方法.....	19
6.1. 作業体制.....	19
6.1.1. 受注者側の体制.....	19
6.1.2. 主要担当者.....	20
6.2. 作業方法.....	20
6.3. 導入.....	20
7. 特記事項.....	21
7.1. 全般.....	21
7.2. 情報セキュリティ対策.....	22
7.3. 受注者に関する条件.....	22
7.4. 担当者に関する条件.....	22

1. システム構成

1.1. システム構成図

第三期サーバ仮想化統合基盤のシステム構成図を以下に示す。



2. ハードウェア構成

2.1. 共通要件

調達対象となるハードウェアは以下のとおりとする。各機器のハードウェア要件を以下に示す。

・ 庁舎側仮想化基盤サーバ	4 台以上
・ 庁舎側仮想化基盤ストレージ	1 台以上
・ 庁舎側監視サーバ	1 台以上
・ 庁舎側サーバスイッチ兼ストレージスイッチ	必要数
・ 庁舎側本庁コアスイッチ用機器	必要数
・ 庁舎側サーバスイッチ	必要数
・ データセンター側仮想化基盤サーバ	4 台以上
・ データセンター側仮想化基盤ストレージ	1 台以上
・ データセンター側サーバスイッチ兼ストレージスイッチ	必要数
・ データセンター側既存 L3 コアスイッチ用機器	必要数
・ データセンター側サーバスイッチ	必要数
・ 庁舎側サーバ負荷分散装置	必要数
・ 庁舎側ファシリティ関連装置	1 式
・ データセンター側ファシリティ関連装置	1 式

2.2. 庁舎側仮想化基盤サーバ

- (1) サーバはラックマウントサーバとすること。
- (2) サーバの CPU は、基本動作周波数 (2.1GHz) コア数 (48 コア) プロセッサキャッシュメモリ (260MB) 相当以上の性能を有する CPU を 2 個搭載していること。
- (3) メモリは 768GB 以上搭載すること。
- (4) 内蔵記憶装置は、240GB 以上の Flash モジュールを 2 本ずつ搭載すること。
- (5) 電源ユニットおよびファンは冗長化されていること。加えて、活性交換が可能なこと。
- (6) エージェントソフトをインストールすることなく、仮想化基盤サーバのコンソールをリモートにて監視できること。
- (7) ラックマウントサーバの設定情報 (MAC アドレス、WWN、VLAN、UUID、BIOS、Boot Order) をプロファイルとして管理することで、保守交換を簡易化することが可能なこと。
- (8) 10GBase-SR ポートを 6 ポート以上、1GBase-T ポートを 4 ポート以上有すること。
- (9) 仮想環境下でのパフォーマンス劣化を防止する為に、仮想化サーバインフラと仮想化ソフトウェアが連携動作しネットワーク負荷をハードウェア側にオフロード出来る機能を有すること。また並行して仮想マシンがノード間を移動する機能をサポートすること。
- (10) Broadcom(旧: VMware)社が認定しているハードウェアであること。また、サーバメーカーも VMware vSphere 8.0 対応を認定していること。

※例示品：(FTI 製 RX2530 M7 ラックベースユニット (Short Depth 筐体/2.5 インチ))

2.3. 庁舎側仮想化基盤ストレージ

- (1) NVMe 接続に対応したフラッシュのみを搭載したオールフラッシュストレージであること。
- (2) 372TB 以上の実効容量を提供すること。
- (3) ランサムウェア等のマルウェア対策として、ストレージ管理者の管理権限を用いても、ストレージのスナ

- アップショット機能で取得した LUN のスナップショットを設定された期間内は完全に消去することが不可能な機能を標準機能として有していること。また、追加のオプションライセンスなどが不要であること。
- (4) インラインでの重複排除機能を有し、可変長による重複判定が可能であること。
 - (5) Snapshot に含まれるデータも重複排除および圧縮の対象になること。
 - (6) オプションライセンスを必要とせずに、ストレージ本体の機能のみで、非同期および同期モードによる筐体外ストレージへのデータレプリケーション機能を有すること。
 - (7) 1 Lun のサイズは、1MB～最大 4PB まで作成できること。
 - (8) ストレージ筐体のコントローラは冗長構成で、片側のコントローラで障害が発生しても性能影響のないアクティブ-スタンバイ構成であること。一方がダウンした場合でも性能低下が無い構成であれば、アクティブ-アクティブ構成でもよい。
 - (9) コントローラ障害時にも Write 性能に影響が無いように、NVRAM (Write キャッシュ) は、ストレージコントローラ外に独立し、NVRAM、コントローラ共に 2 重化以上の可用性をもつこと。
 - (10) ストレージシステムの停止は、シャットダウンコマンドを入力しなくても、システムの停止方法は電源ケーブルを抜くことで対応可能であること。
 - (11) コントローラ、NVRAM、フラッシュデバイス、電源まで全てのコンポーネントをモジュール化し、性能影響なく障害時に交換できること。
 - (12) 暗号化済みドライブのデータは、当該筐体以外（別筐体に搭載）ではデータを読み出しできないこと。
 - (13) コントローラのメンテナンスや、コントローラ障害時の I/O 待機時間を低減させるために、NPIV をサポートしていること。
 - (14) メーカーのリモート保守サービスが標準機能で提供可能であること。
 - (15) ログは機器本体より 30 秒以上・1 分以内の間隔でメーカー提供のクラウドサポート基盤にログ転送し、13 ヶ月間保持できるサービスを、保守の範囲で提供可能であること。
 - (16) グローバルで稼働している機器から送信されるログを収集し、メーカーの提供するクラウドサポート基盤内にて、ログを解析・分析し、未然に障害を防ぐ対策、通知を通常の保守にて提供可能であること。
 - (17) ストレージ管理にあたり、GUI ベースの管理ツールを無償で提供すること。また、各種情報（容量、IOPS、遅延、スループット）がリアルタイムで可視化できること。

※例示品：(Pure Storage 社製 Pure Storage FlashArray C50R4-ETH)

2.4. 庁舎側監視サーバ

- (1) サーバはラックマウントサーバとすること。
- (2) サーバの CPU は、基本動作周波数 (2.6 GHz) コア数 (4 コア) プロセッサキャッシュメモリ (12MB) 相当以上の性能を有する CPU を搭載していること。
- (3) メモリは 32GB 以上搭載すること。
- (4) 内蔵記憶装置は、SAS 10,000 回転 600GB 以上の 2.5 インチ HDD を 3 本、パリティディスクを 1 本搭載し、また、スペアディスクを搭載すること。
- (5) 電源ユニットおよびファンは冗長化されていること。加えて、活性交換が可能なこと。
- (6) ラックマウントサーバの設定情報 (MAC アドレス、WWN、VLAN、UUID、BIOS、Boot Order) をプロファイルとして管理することで、保守交換を簡易化することが可能なこと。

※例示品：(FTI 製 PRIMERGY RX1330 M6 ラックベースユニット)

2.5. 庁舎側サーバスイッチ兼ストレージスイッチ

以下の仕様を満たす機器を2台構成とし、アクティブ-アクティブ構成とすること。

- (1) 10 Gbps Ethernet と 1Gbps Ethernet の切り替えが可能なポートを、1台あたり48ポート以上有すること。また、別途オプションを追加することにより、10 Gbps Ethernet を24ポート以上、もしくは400 Gbps Ethernet を6ポート以上搭載可能なこと。
- (2) 1台あたり、サーバとの接続を10Gbase-SR SFP+のモジュールを20個以上搭載すること。また、1000base-SR SFP+のモジュールを8個以上搭載すること。
- (3) 最大3.6Tbpsの帯域幅と1.2bpsのスループットを実装する1RUの製品であること。
- (4) 電源及びファンが冗長化されていること。加えて、活性交換が可能なこと。
- (5) VLAN ベース ACL (VACL) 、ポート ベース ACL (PACL) 、プライベート VLAN をサポートしていること。
- (6) 本装置2台を冗長化し構成し、両スイッチをまたいだリンクアグリゲーションが可能なこと。
- (7) L3スイッチとしての機能を有すること。

※例示品：(Cisco社製 Nexus 93180YC-FX)

2.6. 庁舎側本庁コアスイッチ用機器

庁舎側サーバスイッチ兼ストレージスイッチとの接続用に10Gbase-SR SFP+のモジュールを4個以上搭載すること。

※例示品：(Cisco社製 10GBase-SR SFP+ モジュール)

2.7. 庁舎側サーバスイッチ

以下の仕様を満たす機器を2台構成とし、アクティブ-アクティブ構成とすること。

- (1) 10BaseT/100BaseTX/1000BaseT ポートを24ポート以上、SFP スロットを4ポート以上有すること。
- (2) スwitching容量は108Gbps以上で、全ポートワイヤレートスループットであること。
- (3) 本装置2台を冗長化構成とし、両スイッチをまたいだリンクアグリゲーションが可能なこと。
- (4) スタック接続により、設定情報やルーティング情報などを全スイッチで共有が可能なこと。また、スタック帯域幅は80Gbps以上であること。

※例示品：(Catalyst 9200L-24T-4G 本体)

2.8. データセンター側仮想化基盤サーバ

- (1) サーバはラックマウントサーバとすること。
- (2) サーバのCPUは、基本動作周波数(2.1GHz)コア数(48コア)プロセッサキャッシュメモリ(12MB)相当以上の性能を有するCPUを2個搭載していること。
- (3) メモリは768GB以上搭載すること。
- (4) 内蔵記憶装置は、240GB以上のFlashモジュールを2本ずつ搭載すること。
- (5) 電源ユニットおよびファンは冗長化されていること。加えて、活性交換が可能なこと。
- (6) エージェントソフトをインストールすることなく、仮想化基盤サーバのコンソールをリモートにて監視できること。
- (7) ラックマウントサーバの設定情報(MACアドレス、WWN、VLAN、UUID、BIOS、Boot Order)をプロファイルとして管理することで、保守交換を簡易化することが可能なこと。
- (8) 10GBase-SRポートを6ポート以上、1GBase-Tポートを4ポート以上有すること。
- (9) 仮想環境下でのパフォーマンス劣化を防止する為に、仮想化サーバインフラと仮想化ソフトウェアが連携

動作しネットワーク負荷をハードウェア側にオフロード出来る機能を有すること。また並行して仮想マシンがノード間を移動する機能をサポートすること。

- (10) Broadcom(旧: VMware)社が認定しているハードウェアであること。また、サーバメーカーも VMware vSphere 8.0 対応を認定していること。

※例示品：(FTI 製 PRIMERGY RX2530 M7 ラックベースユニット)

2.9. データセンター側仮想化基盤ストレージ

- (1) NVMe 接続に対応したフラッシュのみを搭載したオールフラッシュストレージであること。
- (2) 186TB 以上の実効容量を提供すること。
- (3) ランサムウェア等のマルウェア対策として、ストレージ管理者の管理権限を用いても、ストレージのスナップショット機能で取得した LUN のスナップショットを設定された期間内は完全に消去することが不可能な機能を標準機能として有していること。また、追加のオプションライセンスなどが不要であること。
- (4) インラインでの重複排除機能を有し、可変長による重複判定が可能であること。
- (5) Snapshot に含まれるデータも重複排除および圧縮の対象になること。
- (6) オプションライセンスを必要とせず、ストレージ本体の機能のみで、非同期および同期モードによる筐体外ストレージへのデータレプリケーション機能を有すること。
- (7) 1 Lun のサイズは、1MB~最大 4PB まで作成できること。
- (8) ストレージ筐体のコントローラは冗長構成で、片側のコントローラで障害が発生しても性能影響のないアクティブ-スタンバイ構成であること。一方がダウンした場合でも性能低下が無い構成であれば、アクティブ-アクティブ構成でもよい。
- (9) コントローラ障害時にも Write 性能に影響が無いように、NVRAM (Write キャッシュ) は、ストレージコントローラ外に独立し、NVRAM、コントローラ共に 2 重化以上の可用性をもつこと。
- (10) ストレージシステムの停止は、シャットダウンコマンドを入力しなくても、システムの停止方法は電源ケーブルを抜くことで対応可能であること。
- (11) コントローラ、NVRAM、フラッシュデバイス、電源まで全てのコンポーネントをモジュール化し、性能影響なく障害時に交換できること。
- (12) 暗号化済みドライブのデータは、当該筐体以外（別筐体に搭載）ではデータを読み出しできないこと。
- (13) コントローラのメンテナンスや、コントローラ障害時の I/O 待機時間を低減させるために、NPIV をサポートしていること。
- (14) メーカーのリモート保守サービスが標準機能で提供可能であること。
- (15) ログは機器本体より 30 秒以上・1 分以内の間隔でメーカー提供のクラウドサポート基盤にログ転送し、13 ヶ月間保持できるサービスを、保守の範囲で提供可能であること。
- (16) グローバルで稼働している機器から送信されるログを収集し、メーカーの提供するクラウドサポート基盤内にて、ログを解析・分析し、未然に障害を防ぐ対策、通知を通常の保守にて提供可能であること。
- (17) ストレージ管理にあたり、GUI ベースの管理ツールを無償で提供すること。また、各種情報（容量、IOPS、遅延、スループット）がリアルタイムで可視化できること。
- (18) 電源は、200V の環境がないため、100V で稼働できる構成にて導入すること。

※例示品：(Pure Storage 社製 Pure Storage FlashArray C50R4-ETH)

2.10. データセンター側サーバスイッチ兼ストレージスイッチ

以下の仕様を満たす機器を2台構成とし、アクティブ-アクティブ構成とすること。

- (1) 10 Gbps Ethernet と 1Gbps Ethernet の切り替えが可能なポートを、1台あたり48ポート以上有すること。また、別途オプションを追加することにより、10 Gbps Ethernet を24ポート以上、もしくは400 Gbps Ethernet を6ポート以上搭載可能なこと。
- (2) 1台あたり、サーバとの接続を10Gbase-SR SFP+のモジュールを30個以上搭載すること。また、1000base-SR SFP+のモジュールを8個以上搭載すること。
- (3) 最大3.6Tbpsの帯域幅と1.2bpsのスループットを実装する1RUの製品であること。
- (4) 電源及びファンが冗長化されていること。加えて、活性交換が可能なこと。
- (5) VLAN ベース ACL (VACL) 、ポート ベース ACL (PACL) 、プライベート VLAN をサポートしていること。
- (6) 本装置2台を冗長化し構成し、両スイッチをまたいだリンクアグリゲーションが可能なこと。
- (7) L3スイッチとしての機能を有すること。

※例示品：(Cisco社製 Nexus 93180YC-FX)

2.11. データセンター側既存 L3 スイッチ用機器

庁舎側既存 L3 スイッチ用機器と同構成とする。

※例示品：(Cisco社製 10GBase-SR SFP+ モジュール)

2.12. データセンター側サーバスイッチ

以下の仕様を満たす機器を2台構成とし、アクティブ-アクティブ構成とすること。

- (1) 10BaseT/100BaseTX/1000BaseT ポートを48ポート以上、SFP スロットを4ポート以上有すること。
- (2) スイッチング容量は108Gbps以上で、全ポートワイヤレートスループットであること。
- (3) 本装置2台を冗長化構成とし、両スイッチをまたいだリンクアグリゲーションが可能なこと。
- (4) スタック接続により、設定情報やルーティング情報などを全スイッチで共有が可能なこと。また、スタック帯域幅は80Gbps以上であること。

※例示品：(Cisco社製 C9200L-24T-4G)

2.13. 庁舎側サーバ負荷分散装置

以下の仕様を満たす機器を2台構成とし、アクティブ-スタンバイ構成とすること。

- (1) IPv4 ルータ機能として Static、RIPv1/v2、OSPF v2、BGP v4 をサポートしていること。
- (2) IPv6 ルータ機能として Static、RIPng をサポートしていること。
- (3) VLAN(PortVLAN、TagVLAN、MACVLAN)をサポートしていること。
- (4) NAT (アドレス変換) /NAPT(IP マスカレード)をサポートしていること。
- (5) SNMPv1、SNMPv2c、SNMPv3 プロトコルにて、MIB II および拡張 MIB の監視に対応していること。
- (6) 全てのログに関してマニュアル (日本語) にて記載があること。
- (7) 日本語 WebUI と CLI の両方での設定が可能で、CLI は telnet と S S H をサポートしていること。
- (8) 故障監視方式として、以下の方式をサポートし、故障時、サーバを負荷分散対象サーバから外すことができること。(バック LAN 監視、装置監視、サービス監視、アプリケーション監視、負荷計測エージェントによる監視、任意の装置監視)
- (9) 消費電力が82W以下であること。
- (10) MARK スイッチがあり、保守作業が容易なこと。

※例示品：(FTI 製 IPCOM EX2-1100)

2.14. 庁舎側ファシリティ関連装置

- (1) 今回導入する機器を操作するためのコンソールを準備すること。なお、コンソールは県側で提供する EIA 規格準拠のラックに搭載可能なこと。
- (2) コンソールは 19 インチ幅のラック搭載型とし、サイズは 1U/台以内とし、スライドして収納可能であること。
- (3) キーボードは OADG 準拠の日本語 109A 配列であること。
- (4) モニターの画面サイズは 17 インチ以上とし、解像度は SXGA 以上、液晶は TFT 方式であること。
- (5) モニターの切替をキーボードで操作でき、ホットキー切替機能を有すること。
- (6) KVM スイッチは 8 ポート以上であること。

※例示品：(富士通製 17 インチ ラック・コンソール(RC25)、アナログ KVM スイッチ(8 ポート))

2.15. データセンター側ファシリティ関連装置

- (1) 今回導入する機器を操作するためのコンソールを準備すること。なお、コンソールは県側で提供する EIA 規格準拠のラックに搭載可能なこと。
- (2) コンソールは 19 インチ幅のラック搭載型とし、サイズは 1U/台以内とし、スライドして収納可能であること。
- (3) キーボードは OADG 準拠の日本語 109A 配列であること。
- (4) モニターの画面サイズは 17 インチ以上とし、解像度は SXGA 以上、液晶は TFT 方式であること。
- (5) モニターの切替をキーボードで操作でき、ホットキー切替機能を有すること。
- (6) KVM スイッチは 8 ポート以上であること。
- (7) 移行期間中に必要となった場合、機器に応じて必要となるラックを受託者にて手配すること。
(EIA-310-D に準拠した 19 インチラックで 42U, 幅 695 mm×奥行 11,00 mm (外形寸法), 前後鍵付き扉を備えること。)

※例示品：(富士通製 17 インチ ラック・コンソール(RC25)、アナログ KVM スイッチ(8 ポート))

3. ソフトウェア構成

3.1. 共通要件

- (1) 全てのソフトウェアは高い信頼性を有するものであり、メーカー・ベンダ等の保証又は動作確認済のものであること。
- (2) 豊富な利用実績を有するとともに、十分な稼働期間を背景とし安定した動作を客観的に証明可能な市販パッケージ製品の標準機能を利用して構築すること。ただし、オープンソースソフトウェアを利用する場合、市販アプリケーションと同等の信頼性が認められ、継続的な保守対応が望めるものに限り認めるものとし、利用にあたっては受注者にて保証すること。
- (3) ISO、JIS、ANSI 等の公的な規格に定めのある製品については、当該規格に準拠したものであること。
- (4) 更新機器等を構成するソフトウェアは、同種の機器毎にバージョン等を統一すること。
- (5) サービスパックまたはパッチ類に関しては発注者（以下、県という）と協議のうえ、最新のものを適用すること。

3.2. 仮想化基盤ソフト

本ソフトウェアにおいては、極力業務システム移行時のリスクを最小限化するために「VMware Cloud Foundation バージョン 8」以上を使用すること。ライセンス数は、仮想化サーバ構成に基づき必要分用意すること。また仮想化管理ソフトウェアとして「VMware vCenter Server バージョン 8」以上を用意すること。

- (1) 仮想化ハイパーバイザを用いてハードウェアと OS を分離したサーバ（以下仮想サーバ）を稼働可能な環境（以下仮想基盤）を構成すること。なお、仮想化ハイパーバイザのみで構成され、セキュリティや運用上の観点から管理用 OS など的一切含まないこと。
- (2) 仮想サーバ及び仮想サーバを構成するファイルは、仮想サーバを停止することなく基盤を構成するハードウェア間を任意に移動できること。
- (3) 仮想化ハイパーバイザは物理メモリの実容量よりも多くのメモリを仮想サーバに割当可能な機能として、ページ共有機能、バルーニング機能、メモリ圧縮機能を有すること。その際、専用ドライバのインストール等が不要なこと。
- (4) 仮想サーバを停止することなく、仮想 CPU や仮想ディスク、仮想 NIC の割当量を拡張可能なこと。
- (5) 仮想基盤の負荷の偏りを軽減し、全体のリソースを効率よく利用するために、仮想マシンを再配置することで物理ホストの負荷を自動的にロードバランシングする機能をハイパーバイザが有すること。仮想マシンの再配置の決定にあたっては、仮想マシンの CPU、メモリ、ネットワーク負荷のほか、ホスト間移行による影響を加味した計算が行われること。
- (6) 仮想環境における仮想サーバのネットワークのプロビジョニング、管理、および制御を一元化できる分散スイッチ機能を有すること。
- (7) 分散スイッチ上で流れる通信に対してファイアウォール制御を行い、ラテラルムーブメント対策として、同一セグメント内の仮想マシン間の通信制御が可能であること。なお、収集した情報に基づき、推奨するファイアウォールのルールが提示可能な機能も有すること。
- (8) ファイアウォールにてブロックした通信について、ログを残しておくことができること。なお、一定期間内で大量のブロックログが発生した際は指定の宛先へ通知が可能なこと。
- (9) 仮想基盤内の健全状況やリソース消費状況の状況を簡単に把握することを目的に、管理画面のカスタマイズやレポート作成が可能なこと。
- (10) 1つの管理ツールにて仮想環境の運用管理を実装できること。

3.3. オペレーティングシステム等

3.3.1. オペレーティングシステム (Red Hat Linux)

- (1) オペレーティングシステムのライセンスとしてレッドハット社製 Red Hat Enterprise Linux 日本語版相当以上のライセンスを仮想化サーバ台数分用意すること。
- (2) 仮想化管理サーバのオペレーティングシステムのライセンスも必要数用意すること。

3.3.2. オペレーティングシステム (Microsoft Server 2022 Datacenter)

- (1) オペレーティングシステムのライセンスとして Microsoft 社製 Windows Server 2022 Datacenter 日本語版相当以上のライセンスを仮想化サーバ台数分用意すること。
- (2) 仮想化管理サーバのオペレーティングシステムのライセンスも必要数用意すること。
- (3) MS Windows Server 2022 Device CAL ライセンス&ソフトウェアアシュアランスを 6000 ライセンス分用意すること。

3.3.3. ウィルス対策

- (1) バックアップサーバにおいては、トレンドマイクロ社ウイルスバスター コーポレートエディションのクライアントとしてサーバの保護をおこなうこと。なお、必要なライセンスは県が別途調達したものをを使用すること。

3.4. 監視サーバ用ソフトウェア

本ソフトウェアにおいては、統合システム用仮想化サーバ台数に基づき必要分用意すること。

- (1) 物理サーバと仮想サーバの関係を自動的に取得し、シャーシ、サーバなどのハードウェアと、サーバ上で動作している OS(物理 OS、VM ホスト、VM ゲスト)の関係をツリー構造で表示可能であること。
- (2) サーバのハードウェアリソースの稼動状態を監視し、状態に応じたアイコンで表示可能であること。
- (3) 物理サーバ、物理スイッチ、仮想サーバ、仮想スイッチのリソース間の結線状態および VLAN 設定を表示可能であること。
- (4) テンプレートの作成、登録、公開までを WebGUI で行うことが可能であること。
- (5) レポート機能として、VM ホストのリソース (CPU/メモリ等) 使用状況一覧、VM ホスト毎の仮想マシンのリソース使用量積み上げ、仮想マシンのリソース使用状況一覧を表示可能であること。
- (6) リソース使用量の閾値監視およびメールでの通知が可能であること。
- (7) OS のハングアップを監視し、応答が無いサーバを再起動、又はサーバ切替処理を行う事により、ハードウェア障害だけでなく、OS レベルの障害にも対応し、事業継続性を向上することが可能であること。

3.5. ログ統合ソフトウェア

本ソフトウェアにおいては、ログ収集機器に基づき 5 デバイス分用意すること。

- (1) syslog(UDP/TCP/TLS)にてログを収集する機能を有すること。
- (2) REST API にてクラウドサービスより取得できる JSON データを収集する機能を有すること。
- (3) SCP、FTP、HTTP(S)といったプロトコルを利用してサーバよりファイルを収集する機能を有すること。
- (4) ローカルホストよりログファイルを取得もしくはコピーする機能を有すること。
- (5) ログを圧縮して保存できること。
- (6) ログのローテーション機能(指定した期間を超えたログを削除する)を有すること。
- (7) 収集したログをダウンロード出来る機能を有すること。
- (8) 収集したログを検索出来る機能を有すること。
- (9) ライセンスによるログ収集対象の制限がないこと。
- (10) ライセンスによるログのデータ保管期間に制限がないこと。
- (11) 収集したログデータに対して設定した文字列を条件としてアラート通知できる機能を有すること。
- (12) 監視によって得られたデータに対してしきい値を設定しメールでのアラート通知をする機能を有すること。
- (13) 監視によって得られたデータを時系列ベースのグラフにて描画する機能を有すること。
- (14) 監視における閾値をカスタマイズする機能を有すること。
- (15) Web ベースのインターフェイスを介し、ユーザ定義の条件により検索・集計・レポートが実行できること。
- (16) Palo、A10、シスコを含む異なる種類のログを統一的に扱う仕組みを有すること。
- (17) 独自形式のログデータを解析する機能を有すること。
- (18) ログ収集にて取得したデータを元に日次・週次・月次にてレポートを生成する機能を有すること。
- (19) レポート結果を PDF に変換する機能を有すること。
- (20) 生成したレポートをメールにて配信する機能を有すること。
- (21) ログ収集にて取得した複数のデータを基にしたメールでのアラート機能を有すること。
- (22) ログまたは監視データの分析状況が視覚的に確認可能なダッシュボード機能を有すること。
- (23) 収集したデータから AI による将来予測ができること。
- (24) レポート画面から任意の項目でドリルダウン (クローズアップ分析) して対象のログを絞り込めること。
- (25) 製品ライセンスの制限により、上限を超えたログが欠落するライセンス体系ではないこと。
- (26) ログデータは常に圧縮された状態で保管・管理できること。
- (27) 国産ソフトウェアであること。

3.6. バックアップソフトウェア

本ソフトウェアにおいては、統合システム用仮想化サーバ台数に基づき必要分用意すること。

- (1) Broadcom(旧:VMware)社が提供している vStorage API (VDDK:Virtual Disk Development Kit) と連携し、仮想環境上の仮想マシンは VM 単位のバックアップが可能なこと。また、リストアはファイル単位でも可能なこと。
- (2) 仮想マシン全体のバックアップ・リストアが可能なこと。
- (3) 物理マシンと同様な運用イメージでリモートバックアップ・リストアが可能なこと。
- (4) マルチプラットフォーム (Windows/Linux) に対応していること。
- (5) 仮想マシンの増減に関わらず追加ライセンス等が発生しない製品であること。
- (6) Windows/Linux とともにファイル・フォルダ単位のリストアが可能なこと。
- (7) 管理コンソール GUI が日本語化されていること。
- (8) Windows/Linux とともに管理コンソール GUI からバックアップ・リストアが可能なこと。
- (9) Windows/Linux とともに初回のみフルバックアップを取得し、以降の継続的なバックアップは差分バックアップのみで運用可能であること。
- (10) バックアップ方式として D2D 運用が可能であること。

4. システム構築要件

4.1. 構築に係る要件

4.1.1. 基本要件

構築に際して、各種ハードウェア及びソフトウェアに設定すべき事項は、以下のとおりである。各項目について、機器構成や設定内容を選定した理由や判断基準を基本設計書又は運用設計書に記載すること。

- (1) 第三期サーバ仮想化統合基盤は 24 時間 365 日の稼働を求められることから、厳重な稼働監視により障害の早期発見及び迅速な復旧を行い、信頼性可用性の向上を図ること。
- (2) 本調達に含まれるサーバ、ストレージ等については、仮想化技術ソフトウェア、基本ソフトウェア、アプリケーションソフトウェア等をインストールし、別途指示するところにより、IP アドレス、ドメイン名 (FQDN) 及びセキュリティの確保に必要な設定を行った状態で納入すること。
- (3) 今後の調達の公平性を鑑み、データ保持の必要性があるなど継続性の高いと考えられる機器及びソフトウェアについては、製造元の企業と資本関係のない企業によって、導入実績の多数ある製品を採用すること。また、ソフトウェアについては、ソフトウェアの製造元等の特定の製造元製機器のみでなく、他社製品等の機器においても稼働保証がされている製品を採用すること。
- (4) 十分な実績、品質及び信頼性を有するものを採用すること。

4.1.2. サーバ共通

- (1) 導入する OS 及びソフトウェアについて、通常状態で稼働するものの、使用しない機能については、セキュリティの観点からプロセスの停止及びサービスの停止を行う必要があるため、これらを特定し停止すること。
- (2) 「3.3.3. ウイルス対策」に従い必要な設定作業を行い、サーバ保護を確実に実施すること。
- (3) 基準となる時刻に、システム機器の時刻を同期するため、NTP による同期を行うこと。また、調達機器への伝播方法について設計すること。なお、NTP は庁内の NTP サーバを参照することとする。
- (4) 内蔵ハードディスクの冗長化について、主系から副系に切り替わる方法・条件を明確にすること。
- (5) ネットワークインタフェースの冗長化について、稼働率を勘案して、適切な冗長化方式を決定すること。
- (6) サーバの冗長化・負荷分散について、サーバの冗長化・負荷分散を行う場合には、適切な冗長化・分散方法を選定し、設定すること。また、冗長化を行う場合には、障害発生時にフェイルオーバーする場合の条件を明確にすること。負荷分散を行う場合には、障害発生時に当該サーバへの分散を停止する条件を明確にすること。
- (7) 災害時の復旧作業を迅速に行うために必要なバックアップ、復旧方式を選定し、設定すること。なお、保存期間やタイミングについては、県と協議すること。
- (8) サーバで実行される定期・不定期処理を明確にすること。

4.1.3. 仮想化基盤サーバ

- (1) データセンター及び長崎県庁舎にそれぞれ、仮想化基盤サーバを4台ずつ配置すること。また、データセンター及び長崎県庁舎で構成する仮想化基盤サーバは別クラス構成とすること。
- (2) 導入するOS及びソフトウェアについて、通常状態で稼働するものの、使用しない機能については、セキュリティの観点からプロセスの停止及びサービスの停止を行う必要があるため、これらを特定し停止すること。
- (3) 「移行対象サーバ一覧」については契約後に受注者に開示する。
- (4) 仮想化基盤サーバの負荷に応じて仮想マシンが自動的に他の仮想化基盤サーバに移動するよう構成すること。
- (5) 既存のActive Directoryと連携し、各仮想マシンに適切なアクセス権限が割当てられるよう構成すること。
- (6) 全ての仮想マシンを日次でバックアップできるように構成すること。
- (7) オペレーティングシステム等のソフトウェアのライセンスおよび仮想インスタンス数を考慮した構成とすること。
- (8) 複数の仮想化基盤サーバで跨いだ仮想スイッチ構成するなどハイパーバイザの運用性が容易になるように、ライセンスに提供されている機能を用いた構成とすること。
- (9) 下記OSの仮想環境でのOSテンプレートを作成すること。
 - (ア) RHEL 9.5
 - (イ) Windows Server 2022 Standard
 - (ウ) Acronis バックアップアプライアンス

4.1.4. ストレージ

- (1) パフォーマンス及び仮想化環境に適切な構成の観点から、仮想サーバが問題なく利用できるようにディスクやLUNなどのストレージの構成を行うこと。
- (2) バックアップストレージと連携してバックアップ及びリストアが行えるように構成すること。
- (3) パフォーマンス及び仮想化環境に適切な構成の観点から、仮想サーバが問題なく利用できるようにディスクやLUNなどのストレージの構成を行うこと。
- (4) バックアップストレージと連携してバックアップ及びリストアが行えるように構成すること。
- (5) 長崎県庁舎については既存各所属ファイルサーバとの統合が行えるよう構成をすること。各所属ファイルサーバに関する要件については別添の「各所属ファイルサーバの要求仕様」を参照。

4.1.5. ネットワーク

- (1) 第三期サーバ仮想化基盤システムのサーバ群及びストレージなど本システムを収容するL3スイッチ/L2スイッチとして構成すること。
- (2) サーバ等の各機器がスイッチを跨いだリンクアグリゲーションとなるように構成を行うこと。
- (3) 既設ネットワークとの接続においては、県と協議し業務に支障が無いように接続設計及びスケジュールの調整を行い実施すること。

4.1.6. バックアップ

- (1) 各仮想サーバについて専用のバックアップ装置に対して、スケジュールによるバックアップを行うこと。
- (2) 仮想マシン単位でバックアップ、リストアを行えるように構成すること。
- (3) 統合ストレージ障害時においてもデータ保護が行われるように構成すること。
- (4) バックアップ時には、トラフィック等が既存システムに影響のないよう、スケジュールを設定すること。
- (5) 業務サーバのアプリケーションバックアップ及び、遠隔地への保管方法についても実施方法の提示を行うこと。
- (6) バックアップを実施したデータについては、別途ランサムウェア対策として暗号化された領域を含む構成とすること。

4.1.7. システム運用監視

- (1) 仮想化基盤システムの物理サーバと仮想サーバについて、シャーシ、サーバなどのハードウェアと、サーバ上で動作しているOS(物理OS、VMホスト、VMゲスト)の状態を監視可能なように構成すること。
- (2) 仮想サーバのマイグレーション(物理サーバ間移動)操作が可能ないように構成すること。

- (3) ハードウェア等の障害発生時にも、システム停止時間を短縮できるように構成すること。
- (4) 運用管理者の操作性を考慮したシステムとすること。

4.1.8. ログ分析

- (1) 県と協議の上定めたサーバ・ネットワーク機器のログ分析・レポート作成を行うこと。
- (2) ログ分析対象システムに影響のないよう、エージェントレスで利用できるよう構成を行うこと。
- (3) ログ分析のスケジュールについては別途県と協議の上定める。

4.2. プロジェクト管理の実施

構築業務期間中に以下の文書を作成し、設計・構築実施計画書の記載に基づき各種管理を行い、プロジェクト管理を実施すること。また、プロジェクト管理については、受注者の品質マネジメントシステムを活用して品質の向上を図ること。

- (1) 構築業務着手時に、設計・構築実施計画書を作成すること。
- (2) 設計・構築実施計画書に記載すべき事項は以下のとおりである。
 - (ア) 用語定義
 - (イ) 適用範囲
 - (ウ) プロジェクト実施体制
 - (エ) 会議体
 - (オ) スケジュール
 - (カ) 成果物
 - (キ) 制約条件及び前提条件
 - (ク) レビュー実施方針
 - (ケ) 文書管理要領
 - (コ) 情報セキュリティ対策要領
 - (サ) 進捗管理要領
 - (シ) 課題・問題管理要領
 - (ス) 変更管理要領
 - (セ) 品質管理要領
 - (ソ) コミュニケーション要領
 - (タ) リスク管理要領
 - (フ) 設計・構築実施計画書の改訂手順
- (3) 必要に応じて、進捗報告書を作成すること。なお、本調達においては、EVMによる進捗管理は実施しない。

4.3. 設計図書の作成

4.3.1. 基本設計書の作成

基本設計書は、第三期サーバ仮想化統合基盤システムの基本構成、設計方針、設計内容を決定した理由を説明した資料である。基本設計書の作成にあたっては、県担当者の指示に従って、必要に応じて現行システム運用事業者との打合せを行いながら作成すること。

なお、基本設計書に記載する事項は以下を想定しており、設計レビューの中で県担当者と合意を図りながら決定することとする。

- (1) 管理規則
- (2) 適用範囲
- (3) システム概要
- (4) サーバ設計
- (5) ストレージ設計
- (6) ネットワーク設計
- (7) 設備設計

4.3.2. 運用設計書の作成

運用設計書は、業務実施体制、種々の管理手法、システムの運用に必要な事項及び運用手順書の作成に必要な

前提条件、作成方針を記載する。

なお、運用設計書に記載する事項は以下を想定しており、設計レビューの中で県担当者と合意を図りながら決定することとする。

- (1) システム監視
- (2) 障害対応
- (3) セキュリティ対策
- (4) データ管理要件
- (5) 月次報告
- (6) 定期点検作業
- (7) 保守管理に使用する様式

4.3.3. 詳細手順書の作成

詳細設計書は、基本設計書及び運用設計書に基づいて作成されるもので、各機器に設定される設定情報や諸元を記載する。

なお、詳細設計書に記載される事項は、以下を想定しており、設計レビューの中で県担当者と合意を図りながら決定することとする。

- (1) ハードウェア情報
- (2) ソフトウェア情報
 - (ア) OS 名称及びバージョン情報
 - (イ) パーティション情報
 - (ウ) ネットワーク設定情報
 - (エ) サービス設定情報
 - (オ) インストールソフトウェア情報
 - (カ) パラメータ設定情報
 - (キ) 適用パッチ情報

4.3.4. 運用手順書の作成

運用手順書は運用設計書のうち、個別の運用業務の具体的な手順を示したものである。

なお、運用手順書に記載される事項は、以下を想定しており、設計レビューの中で県担当者と合意を図りながら決定することとする。

- (1) 定型作業実施手順
- (2) 定型外作業実施手順

4.4. テスト要件

機器の初期不良の検出及び「4.3 設計図書の作成」において作成した各種設計図書の妥当性を確認するため、テストを実施すること。

4.4.1. テストの種類

- (1) 単体テスト
機器の初期不良の検出及び機器単体レベルでの設計内容の妥当性を検出するテストを実施すること。
- (2) 結合テスト
今回の調達範囲内における機器相互間の稼働が適切であることを確認すること。
- (3) セキュリティテスト
設計書と同等の設定を施した状況において、導入するシステムにセキュリティ上の脆弱性がないか確認すること。
- (4) 障害テスト
障害発生時に障害を適切に検出し、ログへの書き出しが適切に行われるか、アラートが適切に通知されるか及び冗長構成の切り替わりが適切に行われるかを確認すること。
- (5) 運用テスト
システム運用及び運用業務が適切に実施できるか、運用設計書及び運用手順書の妥当性を検証すること。
- (6) 総合テスト(移行リハーサル)

ネットワーク機器を中心として、第三期サーバ仮想化統合基盤の接続リハーサルを実施し、今回の調達対象と他のシステムとの接続性を確認し、システム全体が問題なく稼働することを確認すること。なお詳細（日時、手順、範囲等）については県担当者と協議し業務に支障が無いように実施すること。

4.4.2. テスト実施要件

- (1) テスト開始時において、システムの適切な稼働が確認できる最新のバージョンのパッチが適用されていること。
- (2) 単体テスト、結合テストは受注者側の設備にて行うこと。なお、セキュリティテスト、障害テスト及び運用テストは、本番環境にて既存機器と並行稼働した状況で実施すること。
- (3) 総合テスト以外のテストの実施に当たっては、現行システムを停止せずに実施すること。

4.4.3. テスト計画書の作成

テスト計画書は、テストの実施方針やテスト項目を記載するものである。

テスト計画書に記載する事項は以下を想定しており、設計レビューの中で県担当者と合意を図りながら決定すること。

- (1) テスト実施体制
- (2) テストスケジュール
- (3) テスト実施環境
- (4) 合否判定基準
- (5) テスト実施項目一覧

4.4.4. テスト結果報告書の作成

テスト結果報告書は、テスト計画書において用意したテスト項目の実施結果とテストにおいて合否判定が否となったものの対応状況及びテストの結果を受けた品質見解を記載するものである。

4.5. 導入に係る要件

第三期サーバ仮想化統合基盤で導入するハードウェア、OS 及びミドルウェアにあわせた作業を実施すること。なお、現行サーバの仮想環境への移行については、今回の調達範囲内とする。

- (1) 導入に関する作業内容
導入に関する作業内容については、設計レビューの中で県担当者と合意を図りながら決定すること。
- (2) 導入作業の実施時間帯
平日昼間帯の作業とする。ただし、庁内 LAN との接続等既存環境に影響を与える可能性がある作業については、閉庁日の夜間とすること。
- (3) 導入に関する文書の作成
導入に関する大枠について、受発注者間の認識の合意を図るために作成すること。導入計画書へ記載する事項は以下のとおりとする。
 - (ア) マスタスケジュール
 - (イ) 導入時の作業手順概要
- (4) 導入手順書の作成
導入計画書の趣旨に従って、導入作業の手順を示した導入手順書を作成すること。なお、導入手順書には以下の事項を記載すること。
 - (ア) 作業項目番号
 - (イ) 作業内容
 - (ウ) 想定作業所要時間
 - (エ) 作業完了確認方法
 - (オ) 切り戻しの判断方法
- (5) 導入結果報告書の作成
導入手順書の作業完了確認方法の合否結果を記した上で、導入作業全体を総括した導入結果報告書を作成すること。
- (6) 本調達において庁舎内のネットワークに多大な影響をあたえることから既存ネットワーク導入ベンダと入念な打ち合わせを行いベンダの承認ならびに本県の承認を得ること。なお、当該費用は、本調達に含ま

れるものとする。

- (7) 業務に影響を与えないよう現状の仮想化基盤の調査を行い、その結果を報告書として報告すること。なお、当該費用は、本調達に含まれるものとする。

4.6. 教育に係る要件

4.6.1. 教育の種類

- (1) 受注者は、運用管理者に対し調達設備等に係る運用等（機器の操作等の訓練を含む）に関する研修を行うこと。なお、当該費用は、本調達に含まれるものとする。

4.6.2. 教育実施方法

第三期サーバ仮想化統合基盤の操作等について、運用管理者に対して教育・訓練を実施すること。なお、運用管理者研修は、以下のとおり実施すること。

- (1) 対象者
県スマート県庁推進課システム運用管理者等（10名程度）
- (2) 研修内容
 - (ア) 第三期サーバ仮想化統合基盤システムの概要
 - (イ) 第三期サーバ仮想化統合基盤システム運用における対応事項
 - (ウ) 各機能の運用操作手順
- (3) 教材
教育訓練方法において使用する運用管理者用テキストを事前に作成し、県の確認を得ること。あわせて、第三期サーバ仮想化統合基盤システムにて導入する全ての機器及びソフトウェアの製品マニュアルを必要部数準備すること。

4.7. 機器設置に係る要件

4.7.1. 設置場所

設置場所となる長崎県ネットワーク基盤設置場所については、次の要件に従うこと。

- (1) 利用可能な空間には制限があるため、ラックを新設する必要が生じて設置計画～作業を行う際は、県担当者だけではなく、場所の管理者とも協議・調整し、必要な申請等をおこなうこと。
- (2) スラブ面の床荷重は 1000kg/m²であるため、耐荷重に支障がないようにすること。
- (3) ラックに供給される電源容量は、100V が 1 系統あたり 20A を 4 系統、200V が 50A を 1 系統となるため、導入する機器の負荷容量を算出し、範囲内で機器を配置すること。
- (4) 今回導入する機器については、要件の範囲内で、新設ラック側を中心に設置すること。
- (5) 機器搬入に際し発生した部材（段ボール・クッション材等）は、受注者の負担で廃棄すること。

4.7.2. LAN 配線

- (1) ラックに收容された各機器の接続に必要な LAN 配線については、受注者の負担で行うこと。
- (2) ラック間の各機器の接続および室内の LAN 配線との接続は受注者の負担で行うこと。
- (3) ケーブルを敷設する際に既設の防火措置材等を撤去した場合は、現状に合わせて復旧させること。
- (4) ケーブルにはラベル等により適切な表示を行い、容易に識別できるようにすること。

5. 運用保守要件

5.1. 運用保守要件

5.1.1. ハードウェア保守要件

- (1) 機器故障時の修理
機器に故障が発生した場合の対応は、24 時間 365 日とし、原則 2 時間以内に復旧するように、オンサイト保守対応を行うこと。

(2) ドライバ等の提供

提供するハードウェアは、稼働期間全体にわたって、BIOS、ドライバ及び OS の最新データ及びパッチが継続的に提供されること。

5.1.2. ソフトウェア保守要件

(1) 修正ソフトウェアの提供

(ア) 提供するソフトウェアは、稼働期間全体にわたって、セキュリティホール等に対する情報及びプログラムの修正モジュールが継続的に提供されること。

(イ) 構築及び運用期間を通じて、当該情報を無償にて速やかに提供する体制を構築すること。

(2) 障害発生時の問い合わせ対応

(ア) 運用期間を通じて、ソフトウェア保守サポートが実施可能であること。

(イ) ソフトウェアに関連する障害が発生した場合、ログの解析等、詳細の切り分けに関する対応窓口を用意し、支援すること。なお、受付時間帯は、24 時間 365 日対応とする。

5.1.3. 運用管理要件

(1) 事業者資格

(ア) 今回導入する第三期サーバ仮想化統合基盤と同程度の運用支援業務を請け負った実績があること。

なお、「3. ソフトウェア構成」に記載しているソフトウェアに記載している機能を有するソフトウェアの知識・技能を有する技術者を派遣すること。

(イ) 個人情報の取り扱いを適切・適正に行っている事業者としてプライバシーマークを有していること。

(ウ) 情報セキュリティ管理体制の構築・運用に取り組み、国際規格である ISMS 適合性評価制度 ISO9001 及び 27001 の認定を有している組織/部門が責任を持って実施すること。

(エ) IT サービスマネジメントの国際規格である ISO20000 規格を取得していること。

(2) 運用管理体制

(ア) 受注者は、本作業を履行できる体制を設けるとともに、作業に先立ち以下の事項について報告し、県の了承を得ること。

- ・受注者側の体制
- ・受注者側の統括責任者
- ・連絡体制（受注者側の対応窓口）

なお、担当者は、官公庁における共通基盤の構築・保守実績を有すること。

(イ) 技術者は 1 名以上とする。

(ウ) 技術者は、ハードウェア、ソフトウェア、ネットワーク等に関する十分な知識と豊富な経験を有するシステム・エンジニアとし後記する支援業務内容を迅速かつ適切に遂行する能力を有する者とする。

(エ) 技術者は運用業務を来庁して行い、利用環境の助言や改善策など提案すること。

(オ) 来庁時以外の場合でも要請受付後 1 時間以内で到着できる場所に所在し対応出来ること。

(カ) 仮想化基盤運用時間は 24 時間 365 日とし、24 時間 365 日の監視を行うこと。

(3) 支援業務内容

(ア) 別添の「第三期サーバ仮想化統合基盤運用基準書」に沿った運用対応を行うこと。

業務実施に際して「4.3.2 運用設計書の作成」に沿った運用設計書を作成、県担当者の承認を得た上で作業を実施すること。

(イ) 技術サポート体制として導入作業中及び運用開始後最低 3 ヶ月は VCP、CCNP 技術者及びネットワークスペシャリスト（経済産業省認定）以上の技術を有する者をプロジェクトに参加させ且つ、九州内に仮想化環境の構築経験を有する者を配置し、トラブル発生時に迅速に対応できる体制をとること。

(ウ) 障害対応状況を迅速に共有できる仕組み・体制を提供すること。

※業務実施に際し、リモートメンテナンス環境整備も可とするが下記条件を満たし、かつ県の承認を得た上で許可する。

(1) リモートサービス提供拠点を、2 か所（それぞれ異なる都道府県）以上有していること。

(2) リモートサービス提供拠点において、入室の際に必ず二要素認証（ID 入力と生体認証）を行っていること。
また、物理的セキュリティ対策（入退室の管理、監視カメラによる監視・記録、鍵保管管理）が施されている

こと。

- (3) 接続端末の対策（パソコン操作の記録・抑止、可搬記録媒体の利用制限）を施すこと。
- (4) 接続時に、県担当者の許可操作等によって初めてリモートメンテナンスが可能となる仕組みを整備すること。
- (5) 震災や疫病など大規模災害が発生した際に、単一拠点もしくは複数拠点が閉鎖となった場合でも、代替拠点にてリモートサービスを提供できること。
- (6) リモートサービス提供拠点において、法定点検等で停電が発生した場合でも継続してサービス提供できるよう、複数の変電所から電力の供給を受けていること。

5.1.4. 特記事項

- (1) 保守の実施について、賃貸借契約期間中は追加費用が発生することなく契約金額内で対応すること。
- (2) 通常使用の状況で障害が発生した場合についても、機器費用・作業費用・出張費用などの追加費用が発生することなく受注金額内で対応すること。

5.2. 契約満了に伴う機器撤去

5.2.1. 基本要件

- (1) 本調達により納入した機器等を契約期間満了に伴い撤去すること。
- (2) 撤去する際には、県の指示に従い、情報漏えいを防ぐために機器のデータ（ハードディスクだけでなく、不揮発性メモリに保存されている設定情報を含む）の確実な消去を行うこと。

5.2.2. 作業方法

- (1) 撤去機器のハードディスクについては完全消去を行うため、固定パターンデータによる塗り潰し、ランダムパターンデータによる塗り潰し、及びこれらを併用した塗り潰しを2回以上行い、データの再生・読み出しが出来ないようにすること。
- (2) データの消去が完了したことを、県に対し書面で報告すること。

6. 作業の体制および方法

6.1. 作業体制

6.1.1. 受注者側の体制

想定している構築時の受注者側の担当者及び役割分担は下表のとおりである。

なお、ここでは県側で想定している体制を記載しているが、プロジェクト進行に支障のない範囲で、県の承認があれば、兼務を認めることとする。

受注者側の担当者及び役割分担表

担当者名	役割
プロジェクト管理者 (必要に応じて補佐を配置することを認める。)	<ul style="list-style-type: none"> ・ 構築及び移行プロジェクト全体を統括する。 ・ 設計・構築実施計画書を作成する。 ・ 進捗報告書を作成する。 ・ 定例会議の議事を運営する。 ・ 各種設計図書の作成作業の管理を行う。 ・ 移行期間中の運用の月次報告を行う。 ・ 各グループの進捗状況の確認を行い、工程に変更を要する場合は、影響度合い等のリスク分析を行い、変更計画を立案する。 ・ 課題管理表の管理を行い、各グループに課題の解決を促す調整。
技術統括管理者	<ul style="list-style-type: none"> ・ 各設計グループの設計内容の整合性を図る。 ・ 複数のグループに関連する課題を解決する。
サーバ設計管理者	<ul style="list-style-type: none"> ・ サーバに関する基本設計書、詳細設計書等の作成に関する業務を管理する。

	<ul style="list-style-type: none"> 設計書レビューのレビューイとして、関係者へのレビューを行う。
サーバ設計グループ	<ul style="list-style-type: none"> サーバ設計管理者の指示に従い、基本設計書、詳細設計書等の作成を行う。
ネットワーク設計管理者	<ul style="list-style-type: none"> ネットワークに関する基本設計書、詳細設計書等の作成に関する業務を管理する。 設計書レビューのレビューイとして、関係者へのレビューを行う。
ネットワーク設計グループ	<ul style="list-style-type: none"> ネットワーク設計管理者の指示に従い、基本設計書、詳細設計書等の作成を行う。
運用設計管理者	<ul style="list-style-type: none"> 運用設計に関する業務を担い、運用設計書や運用手順書等の作成に関する業務を管理する 設計書レビューのレビューイとして、関係者へのレビューを行う。
運用設計グループ	<ul style="list-style-type: none"> 運用設計管理者の指示に従い、運用設計書や運用手順書等の作成を行う。
プロジェクト責任者	<ul style="list-style-type: none"> プロジェクト管理者が実施するプロジェクトを監理する。 プロジェクト管理者の所属する部門の部門長を想定している。 社内における決裁・承認権限を有している。
品質管理者	<ul style="list-style-type: none"> 受注者の社内品質マネジメントシステムに基づいて、品質を管理する。 プロジェクト管理者に対する改善指導ができる立場であり、品質管理部門の本調達に関する担当者を想定している。

6.1.2. 主要担当者

(1) プロジェクト管理者

(ア) プロジェクトマネジメントに関する以下のいずれかの資格又はこれに準ずる公的な資格を有すること。

プロジェクトマネージャ、技術士(情報工学部門)、技術士(総合技術監理部門(情報工学を選択科目とする者))、PMP(Project Management Professional)

(イ) 同様のシステム規模の更改に関して、プロジェクト管理者の実績を有すること。

(ウ) 今回実施する作業内容と同様の作業経験を5年以上有すること。

(2) プロジェクト管理者補佐(必要に応じて配置)

(ア) 今回実施する作業内容と同様の作業経験を3年以上有すること。

(3) 構築作業従事者

構築作業従事者のうち、1名以上が以下の項目に関する資格を有し、関係する設計作業に従事していること。

(ア) Broadcom社(旧VMWare)の技術資格VCP-DCV2023以上

(イ) Cisco社のCCNPもしくは同等のネットワークに関する資格

(ウ) 経済産業省認定ネットワークスペシャリスト、もしくはテクニカルエンジニア(ネットワーク)

6.2. 作業方法

(1) 設計図書の作成作業においては、受注者側設備において実施すること。

(2) 今回新規に調達する機器以外のテストに必要な機器については、受注者にて手配すること。

(3) 単体テスト、結合テストを実施する場所は、受注者側の設備にて行うこと。なお、セキュリティテスト、障害テスト及び運用テストは、本番環境にて既存機器と並行稼働した状況で実施すること。

(4) 受注者側でテストを実施する場所は、県に機密保持に関する誓約書を提出した者以外が入室できない環境で行うこと。これによらない場合は、県で使用するホスト名、IPアドレス等を機器の設定情報に登録せずに、テスト内容が担保できる設定情報にて検証を行うこと。

6.3. 導入

(1) 破損等に関する対応

受注者の責において機器の搬入・設置に関して起きた一切の事故・障害及び諸設備の破損等は、県担当者が指定する者の指示に従い、受注者が無償にて当該設備の復旧又は交換を速やかに行うこと。

- (2) 機器の搬入及び搬出
 - (ア) 機器の搬入及び搬出に当たっては、県担当者と搬入ルート及び入構車両に関する調整を行うこと。
 - (イ) 庁舎内の搬入ルートにおいて、県から指示のあった箇所については、養生を行うこと。
- (3) 作業届の作成

作業を実施する場合は、作業実施日の 5 業務日前までに、県担当者へ作業届を提出し、承認を得ること。
- (4) 作業場所

県の定めた場所において、作業を行なうこと。

なお、以下の事由が生じた場合については別途協議を行うこととする。
- (5) 受注者の責任で制御できない事由
 - (ア) 電力供給の障害
 - (イ) 通信回線の障害
 - (ウ) 調達範囲外の機器の障害
 - (エ) 自然災害の不可抗力
- (6) 発注者の責任に帰する事由
 - (ア) 発注者の作為または不作為
 - (イ) 本契約に定める発注者の義務不履行
 - (ウ) 発注者の誤った作業依頼
- (7) 発注者と受注者との間での合意事由
 - (ア) 定期保守のための停止
 - (イ) 機器の導入やシステムの構成変更作業
 - (ウ) その他発注者の要求に基づく業務上必要な停止等
- (8) その他、受注者の責めに帰さない事由
 - (ア) 受注者が保証したシステム環境以外での使用
 - (イ) 他システムに起因する事象
 - (ウ) 悪意ある第三者による不正行為

7. 特記事項

7.1. 全般

- (1) 本調達仕様書は、受注者に業務遂行を求める最低限の基準を示したものである。したがって、本調達仕様書に記述していない事項であっても、本業務に必要と認められる事項は、県と協議の上、これを行うこと。
- (2) 受注者は、県の指示に従い、本調達仕様書の内容について業務を行うこと。また、本調達仕様書の内容等に疑義が生じた場合は、県と協議の上、決定するものとする。
- (3) 受注者は、常に作業場所を整理・整頓し、安全に留意して事故の防止に努めるとともに、労働基準法、労働安全衛生法を遵守して安全の徹底を図り、作業を行うこと。
- (4) 機器の搬入・設置に関して起きた一切の事故・障害及び諸設備の破損等は、県及び県が指定する者の指示に従い、受注者が当該設備を無償にて速やかに復旧又は交換すること。
- (5) 受注者が行う提案や報告及び相談等はすべて書面をもって実施し、内容について県の承認を得ること。
- (6) 受注者は、本調達に基づく業務を第三者に委託してはならない。ただし、本業務全体に大きな影響を及ぼさない補助的業務について、事前に県から承認を得た場合はこの限りではない。この場合、再委託の内容、そこに含まれる情報、再委託先、その他再委託先に対する管理方法等を書面により提出すること。
- (7) 現地調査、移行作業等、各拠点に入室を要する際には、受注者の監理下において実施すること。

7.2. 情報セキュリティ対策

- (1) 長崎県の情報セキュリティポリシーに基づき、セキュリティ対策を実施することとする。
- (2) 受注者は、本業務の実施時において知り得た情報の取り扱いに十分留意し、他に漏えい等が行われないようにすること。
- (3) 本業務に従事する全員と個別に守秘義務契約を締結していること。
- (4) 会社全体としてセキュリティポリシーの策定・運用・教育を行い、適切な文書管理・情報管理が行われていること。
- (5) 注者側設備においては、十分な情報セキュリティを確保していることを設計・構築実施計画書及び運用設計書の情報セキュリティ対策要領の中で明記すること。
- (6) 次の事項を必ず定め、設計・構築実施計画書及び運用設計書に記載すること。
 - (ア) 県から貸し出された資料又は支給を受けた物品等については、善良なる管理者の注意をもって保管及び管理するものとし、紛失又は破損の場合は直ちに県に報告し、県の指示に従って措置を講ずること。
 - (イ) 責任者及び監督者を定めること。
 - (ウ) 業務体制及び従事者を明確にすること。
 - (エ) 従事者の担当範囲を明確にすること。
 - (オ) 作業場所等に関して、情報の漏えい等の防止及び情報システムのセキュリティ確保のための措置を講ずること。

7.3. 受注者に関する条件

- (1) 構築業務の実施部門が、品質マネジメントシステムである ISO 9001:2008 認証を取得していること。または、ISO 9001:2015 に準拠した品質マネジメントシステムを運用していること。
- (2) 委託を行う場合においては、受注者の品質、情報セキュリティ及び IT サービスの各マネジメントシステムに従って、再委託先についても受注者と同等の取り組みを実施させること。
- (3) 本件と同等の利用者数規模のシステムの更改に関する案件の実施経験を有すること。

7.4. 担当者に関する条件

- (1) 本業務を遂行させるために必要な知識及び経験を有するものを担当させること。
- (2) 十分な体制を確保した上、責任体制を明確にし、全社的対応を図ること。なお、体制について具体的な資料を提出すること。
- (3) 体制を変更する必要がある場合には、1 か月前までに設計・構築実施計画書の改訂案を提示し、事前に県の承認を得ること。なお、担当者の異動が発生する場合には、後任の担当者に対して、本業務に支障をきたさないように十分な訓練を実施した後に業務の引継ぎを行い、県に引継ぎ結果を報告すること。
- (4) 担当者の病気により欠務が生じる場合は、その旨及び代行する担当者を速やかに県に報告し、承認を得ること。なお、代行する担当者は当日の業務に支障をきたさないようにすることができる者を担当させること。
- (5) 県は、以下の場合においてプロジェクト管理者の交代を求めることができる。
 - (ア) 作業計画に2週間以上の遅れが生じ、その遅れを1か月以上解消できない時。
 - (イ) 同一の問題が、1か月以上継続した時。
 - (ウ) 作業計画の遅れや問題の原因として、作業実施者が必要な技能を習得していないと認められ、その状況が1か月以上解消できない時。
- (6) 県は、以下の場合においてプロジェクト管理者補佐、ネットワーク設計責任者、運用設計責任者の交代を求めることができる。
 - (ア) 十分なコミュニケーション能力がない時。
 - (イ) 業務品質が低く、問題を指摘したにもかかわらず改善が見られない時。