共通資料3

統合サーバの利用について

統合サーバを利用するにあたっては以下の資料を参照すること。

統合サーバにかかる概要	別紙１　統合サーバの概要
統合サーバの機器及び本システムが利用できるソフトウェア	別紙２　統合サーバを構成する機器類の詳細について
統合サーバへの移行方法	別紙３　移行方法の詳細について
構築や保守にかかる役割分担や注意事項	別紙４　統合サーバにかかる保守等の役割分担等について
バックアップ及びリストアにかかる詳細	別紙５　統合サーバにかかるバックアップ及びリストアの詳細について
監視にかかる詳細	別紙６　統合サーバにかかる監視の詳細について

【注意事項】

本資料において使用する用語の定義については、以下のとおり。

- 統合用サーバ：共通機能基盤統合用サーバ（DB 用統合用サーバを含む）のこと。
- 仮想マシン：共通機能基盤統合用サーバ上で構築する仮想的なハードウェアのこと。仮想マシンについては、通常のハードウェアと同様に利用が可能。
- 本システム：●●システムのこと。
- 本委託業務：●●システムの構築・運用保守の業務委託のこと

別紙１　統合サーバの概要

- 統合サーバは、それぞれ、「(IDC1) 統合用サーバ」「(IDC2) DB 用統合用サーバ (OCVS)」「IDC1 メインストレージ（メイン領域／/バックアップ領域)」「IDC2 メインストレージ（メイン領域／/バックアップ領域)」「vCenter サーバ」「稼働監視サーバ」「バックアップサーバ」「分散ファイアウォール」から構成される。
- 仮想化による統合を行うこととし、仮想化ソフトウェアとして統合用サーバ、及び、DB 用統合用サーバ共に「Broadcom 社製 VMWare vSphere 8.0 Update 3b」用いている。
- 統合用サーバ、及び、DB 用統合用サーバ上にシステム毎に仮想マシンを構築し、CPU やメモリ等の必要リソースを割り当てたうえで、仮想マシン上でシステムを構築する形となる。
- 統合用サーバ、及び、DB 用統合用サーバ上に構築したシステムにかかる全ての操作は、本県庁舎に設置した端末及びリモート保守環境から接続された端末から可能とする。
- 統合サーバ上における高可用性を確保したシステム構成（Oracle RAC 等）については、原則利用不可とする。

別紙2　統合サーバを構成する機器類の詳細について

統合サーバを構成する機器類及びソフトウェアの詳細仕様については、以下のとおり。

1　全体構成

- 統合サーバを構成するサーバ機器類の台数及び設置場所については以下のとおり。
- なお、これらサーバ機器類にかかる接続図については、「3　サーバ機器類にかかる概要図」を参照のこと。

環境	設置機器	台数	設置場所
オンプレミス環境	統合用サーバ	6台	IDC1
	メインストレージ	2台	
	vCenterサーバ(※1)	1台	
	稼働監視サーバ(※1)	1台	
	バックアップサーバ(※1)	1台	
	分散ファイアウォール(※1)	1台	
クラウド環境	DB用統合用サーバ	3台	IDC2
	メインストレージ	1台	
	オブジェクトストレージ	1台	
	vCenterサーバ(※1)	1台	
	バックアップサーバ(※1)	1台	
	分散ファイアウォール(※1)	1台	

※1 統合用サーバ上の仮想マシンとして動作する。

- システム構成に関連する役割・機能については次のとおり。
  - 統合用サーバ及びDB用統合用サーバにおいて、ライブマイグレーション機能を有する。
  - 統合用サーバ及びDB用統合用サーバにおいて、高可用性（HA）機能を有する。
  - IDC1およびIDC2のバックアップデータ対してランサムウェア対策を行う。
- それぞれのサーバ機器類及びソフトウェアの詳細は、「2　サーバ機器類及びソフトウェア」のとおり。

2　サーバ機器類及びソフトウェア（オンプレミス環境）

（1）統合用サーバ

ア　ハードウェア（1台当たりの基本スペック）

本体	台数	6台
	形状	ラックマウント型
	CPU	Intel Xeon Gold 6548N(2.8GHz 32Core)×2
	メインメモリ	1,024GB

※ VMwareをハイパーバイザーとする仮想マシンの実行環境として使用する。

イ　ソフトウェア

ソフトウェア	備考
VMware vSphere ESXi 8.0 Update 3g	

（2）IDC1メインストレージ（メイン領域、バックアップ領域）

ア　ハードウェア（1台当たりの基本スペック）

ストレージ本体	台数	2台
	形状	ラックマウント型
	ディスクドライブ	実容量240TB

※ ストレージにかかる接続構成については、「3　サーバ機器類にかかる概要図」を参照のこと。

※ 主に仮想マシンのディスク領域、オンプレミス環境の一次バックアップ領域及びクラウド環境の二次バックアップとして使用する。

（3）vCenterサーバ

ア　仮想ハードウェア

本体	台数	1台
	形状	統合用サーバ上の仮想マシンとして動作
	CPU	1P/4C
	メインメモリ	21GB
	ハードディスク	701.85GB
	DVD-ROM	統合用サーバのデバイスを利用

※ 主に統合用サーバにおける仮想マシンの管理を行う。

イ　ソフトウェア

ソフトウェア	備考
vCenter Server Appliance 8.0 Update 3g	vCenter アプライアンスパッケージ

（4）稼働監視サーバ

ア　仮想ハードウェア

本体	台数	1台
	形状	統合用サーバ上の仮想マシンとして動作
	CPU	1P/6C
	メインメモリ	8GB
	ハードディスク	2,000GB
	DVD-ROM	統合用サーバのデバイスを利用

※　主に統合用サーバ及び DB 用統合用サーバにおける機器、及び、仮想マシンの監視を行う。

イ　ソフトウェア

ソフトウェア	備考
RedHat Enterprise Linux 9	OS
Hinemos Manager 7.1.0	監視ソフトウェア
Hinemos Agent 7.1.0	監視エージェント

（5）バックアップサーバ

ア　仮想ハードウェア

本体	台数	1台
	形状	統合用サーバ上の仮想マシンとして動作
	CPU	1P/8C
	メインメモリ	16GB
	ハードディスク	135.5TB
	DVD-ROM	統合用サーバのデバイスを利用

※　主に統合用サーバにおける仮想マシンのバックアップを行う。

イ　ソフトウェア

ソフトウェア	備考
Windows Server 2022 Standard	OS
VMware Tools	仮想基盤連携
Veeam Backup & Replication 12.3	バックアップソフトウェア

3　サーバ機器類及びソフトウェア（クラウド環境）

（1）DB 用統合用サーバ

ア　ハードウェア（1 台当たりの基本スペック）

本体	台数	3 台
	形状	クラウドサービス
	CPU	Intel Xeon Platinum 8358(2.6GHｚ 16Core)×2
	メインメモリ	1024GB（1 台あたり）

※ VMware をハイパーバイザーとする仮想マシンの実行環境として使用する。

イ　ソフトウェア

ソフトウェア	備考
VMware vSphere ESXi 8.0 Update 3g	

（2）IDC2 メインストレージ（メイン領域、バックアップ領域）

ア　メイン領域（ブロック・ボリューム）

ストレージ	ブート・ボリューム	0.164TB
	メインボリューム	8.192TB
	管理用ボリューム	4.428TB

※ ストレージにかかる接続構成については、「3　サーバ機器類にかかる概要図」を参照のこと。

※ 主に仮想マシンのディスク領域として利用する。

イ　バックアップ領域（オブジェクトストレージ）

ストレージ	バックアップ・リポジトリ領域	129TB

※ ストレージにかかる接続構成については、「3　サーバ機器類にかかる概要図」を参照のこと。

※ クラウド環境の一次バックアップ領域、及び、オンプレミス環境の二次バックアップとして使用する。

（3）vCenter サーバ

ア　仮想ハードウェア

本体	台数	1 台
	形状	統合用サーバ上の仮想マシンとして動作
	CPU	1P/8C
	メインメモリ	30GB
	ハードディスク	915.85GB
	DVD-ROM	統合用サーバのデバイスを利用

※　主に統合用サーバにおける仮想マシンの管理を行う。

イ　ソフトウェア

ソフトウェア	備考
vCenter Server Appliance 8.0 Update 3g	vCenter アプライアンスパッケージ

（4）バックアップサーバ

ア　仮想ハードウェア

本体	台数	1 台
	形状	統合用サーバ上の仮想マシンとして動作
	CPU	1P/8C
	メインメモリ	16GB
	ハードディスク	520GB

※　DB 用統合用サーバにおける仮想マシンのバックアップを行う。

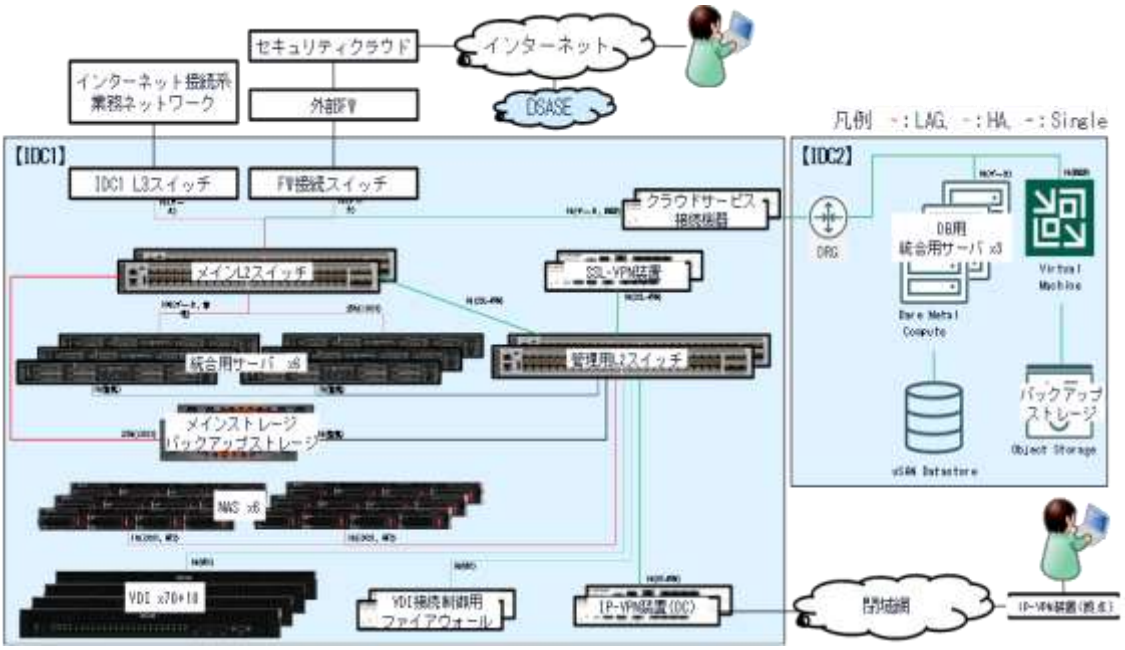
※　バックアップデータの保存は、IDC2 メインストレージ　バックアップ領域（オブジェクト・ストレージ）に行う。

イ　ソフトウェア

ソフトウェア	備考
Windows Server 2022 Standard	OS
VMware Tools	仮想基盤連携
Veeam Backup & Replication 12.3	バックアップソフトウェア

3　サーバ機器類にかかる概要図

統合サーバにかかる機器類の概要図を以下に示す。



別紙３　移行方法の詳細について

統合サーバへの移行方法は、通常の機器更新と同様に、仮想マシン上における環境構築とデータ移行を行う（以下、『再構築による移行』という）。

１　移行作業及び役割分担

・ 仮想環境上で稼働しているシステム及び物理環境上で稼働しているシステムを統合サーバ上で稼働するシステムとして移行するための作業の流れ・概要及び役割分担は以下のとおり。
・ なお、移行にあたっては、仮想マシンの台数及びスペック、バックアップ及び監視等について統合計画書を作成して、本県及び統合サーバにかかる構築業者と調整の上で実施する。

工程名	作業概要	県	統	受
計画・設計	既存システムの調査を実施する。	△	△	○
	仮想マシンに係るリソース等に関する統合計画書を作成する。	×	×	○
	統合計画書を基に移行スケジュール及び統合サーバの仮想マシンに関するリソース等について調整・決定する。	○	△	○
移行	既存システムのデータを取得する。	×	×	○
	統合サーバ上で稼働するシステムは、仮想マシンの移行を行う。 物理環境上で稼働しているシステムは、統合計画書に基づき、統合サーバに仮想マシンを作成し、OSをインストールする。	×	○	×
	仮想化支援機能、バックアップ及び監視等の設定を行う。	×	○	×
	統合サーバの仮想マシン上で環境構築を行い、既存システムのデータを移行する。	×	×	○
	統合サーバの環境に合わせてシステムの調整を行う。	×	×	○
確認	システムの動作確認を実施する。	×	△	○

※　県：本県、統：統合サーバにかかる構築業者、受：受託業者
※　○：主体的に実施、△：サポートを実施、×：作業なし

・ 原則として、移行にかかる全ての作業は受託業者が実施することとなるが、本県及び統合サーバにかかる構築業者の承認の元、一部の作業を統合サーバにかかる構築業者に依頼することができる。なお、このとき必要となる費用や資料等については、受託業者が負担することとなるので注意すること。
・ 仮想マシンは、統合計画書で指定されたネットワークに繋がった状態で作成される。

別紙４　統合サーバにかかる保守等の役割分担等について

統合サーバを利用する際における保守等の考え方及び役割分担の詳細については、以下のとおり。

１　統合サーバを利用するために必要となる調整及び設計項目等

本システムが統合サーバを利用する際に必要となる調整及び設計項目等については、以下のとおり。

これらの調整等を本県及び統合サーバにかかる構築業者との間で実施し、本県及び統合サーバにかかる構築業者と合意したうえで、統合サーバを利用することができる。

なお、保守等の役割分担の詳細については、「２　統合サーバを利用する際の役割分担」を参照のこと。

（1）保守設計

【条件】

- 本システムの保守にかかる設計を行うこと。
- 受託業者から統合サーバにかかる構築業者へ依頼が可能な業務にかかる詳細については、後述の「２　統合サーバを利用する際の役割分担」を参照すること。

【要件】

- 本システムを安定的に稼働させるために必要となる定期的な再起動や日常点検等の詳細について、もれなく設計を行ったうえで、統合サーバにかかる構築業者と調整が必要となる保守等について整理を行うこと。
- バックアップ及びリストアについて必要となる設計を行うこと。なお、バックアップは統合サーバにかかる構築業者で提供される全体バックアップをベースとすることとし、その詳細については、統合サーバにかかる構築業者から説明やサポートを受けること。（バックアップ及びリストアの詳細は「別紙５　統合サーバにかかるバックアップ及びリストアの詳細について」を参照のこと。）
- 本システムにおいて必要とする可用性・保守性についての設計を行うこと。なお、統合サーバに実装する vSphere vMotion、vSphere HA を利用することも可能であるが、これらの機能を利用するために必要なライセンス等は本委託業務において用意すること。
- 障害時の検知方法や対応について、設計を行うこと。なお、障害監視には、統合サーバが提供する統合監視機能を利用することができるが、設計は受託業者が実施すること。
- 統合監視機能を利用するにあたって、受託期間中においては、統合監視機能が配信する通知メールを常に受信できるようにすること。
- 本県からの連絡または統合監視機能等からの通知メールにより、障害発生を確認した場合は、統合サーバにかかる構築業者と協力のうえ、障害の原因切り分けやシステムの再起動等の障害対応を行い、正常稼働状態に復帰させること。
- 統合サーバにかかる保守業務については、統合サーバにかかる構築業者が実施するが、本システムの保守業務との役割分担や障害対応時の原因切り分け方法等についても調整を行ったうえで、設計に盛り込むこと。
- 作成した各種設計については、本県にレビューを行い、承認を受けたうえで次のステップに進むこと。

（2）必要機器等のサイジング

【条件】

- 本システムに必要となる統合サーバ上の仮想ハードウェア、スペック及びソフトウェア等について統合計画書を基に検討を行い、必要となる仮想ハードウェア、スペック及びソフトウェア等についてサイジングを行うこと。

【要件】

- 本システムは、別途本県が調達する統合サーバ上での構築を予定しているが、統合サーバ上では、CPU のコア数、メモリ及びディスクを仮想ハードウェアとして各システムに割り当てる形となるため、本システムの運用に必要となる仮想ハードウェアのスペックについてサイジングを行い、本県に統合計画書として提示すること。
- なお、運用開始後も CPU、メモリ及びディスクについては追加割り当てが可能のため、サイジングに当たっては過大なスペックにならないように十分留意すること。
- なお、サイジングの結果、必要となるソフトウェアライセンス数に変化があったとしても、その費用は本委託業務の範囲内となるので注意すること。
- 本県が別途調達する統合サーバについては、「別紙２　統合サーバ環境を構成する機器類の詳細について」を参照のこと。

【想定】

- 本システムに必要な機器やスペックは、現行のシステムが安定して稼働しているサーバと同程度のスペック（CPU：●コア、メモリ：●GB、HDD：●GB 等）であれば、安定した運用が可能であると想定している。

（3）環境構築

【条件】

- 統合サーバ上にシステムの構築または移行を行うこと。
- なお、本システムの構築に必要となるソフトウェアの内、本県が用意するソフトウェア以外に必要となるライセンスについても納入を行うこと。

【要件】

- 統合サーバ上における仮想マシンの作成等については、統合サーバにかかる構築業者が対応を行うが、本システムの構築にかかる作業については、全て実施すること。
- 本システムの移行にあたっては、できるだけ本システムの停止時間が短くなるように留意すること。
- ソフトウェアに関するライセンスは、「別紙２　統合サーバ環境を構成する機器類の詳細について」を参考に必要なソフトウェアのライセンスを納入すること。
- Microsoft 社製の製品を新規で購入する場合は、調達数量や購入条件に応じて ESA、SCE、Select Plus for Government、SPLA、CSP 等を利用することができる。
- オンプレミス環境で利用する Microsoft 社製 Windows（サーバ OS 、Windows Server 2016 以降、Windows Server 2022 まで）については、本県があらかじめソフトウェアライセンスを用意するため、受託業者による購入は不要である。ただし、Windows Server 2025 については、本県が CAL を別途調達予定であるため、調達後利用可能となるので利用可否については本県に確認すること。

・ クラウド環境で利用する Microsoft 社製 Windows（サーバ OS 、Windows Server 2016 以降、Windows Server 2025 まで）については、本県があらかじめソフトウェアライセンスを用意するため、受託業者による購入は不要である。
・ サーバ OS として Microsoft 社製 Windows を利用する場合、Service Pack 等は最新版を適用する。
・ DB 用統合用サーバ環境で「Oracle Database Standard Edition 2」を利用する場合、本県がソフトウェアライセンスを用意するため、受託業者による購入は不要である。

2　統合サーバを利用する際の役割分担

上記「（1）保守設計」で記述した受託業者と統合サーバにかかる構築業者における、保守及びサポートにかかる役割分担の詳細については以下のとおり。

※下記の記述の内、【想定】となっていないものについては全て【要件】として対応すること。

（1）役割分担

・ 本システムの保守及びサポートにかかる役割分担は以下のとおり。

作業内容	統合サーバにかかる構築業者等	受託業者
システム及びデータバックアップ、リストア	ア	ア
スナップショットの作成、削除	イ	イ
稼働監視	ウ	ウ
性能・構成管理		オ
ログ管理		カ
セキュリティ管理		キ
日常運用業務に対する支援、提案		ク
パッチによる影響等の情報提供		ケ
パッチインストール		コ
停電対応	エ	
障害一次切り分け	オ	
障害対応（システム障害の対応）		サ
障害対応（ハード障害の対応）	カ	
障害後是正措置・予防措置（システム障害時）		シ
障害後是正措置・予防措置（ハード障害時）	キ	
運用マニュアルの改訂		ス
既存システムにかかる従前からの保守業務	㊟	㊟

※ 表中のア～ク、ア～スは以下の「（2）共通機能基盤（統合サーバ）にかかる構築業者が行うもの」及び「（3）受託業者が行うもの」を参照のこと。

※ 表中の※㊟は以下の「（4）役割分担を行ったうえで実施するもの」を参照のこと。

（2）統合サーバにかかる構築業者が行うもの

以下の業務について受託業者は、統合サーバにかかる構築業者に対し、作業の実施について依頼できるものとする。

ア．システム及びデータバックアップ、リストア

- 統合サーバにおける全体バックアップを利用したバックアップ及びリストアを行う。

イ　スナップショットの作成、削除

- vCenter サーバより、仮想マシンのスナップショットの作成、削除の環境を提供する。

ウ　稼働監視

- 統合監視機能により、死活監視（ping 監視）、プロセス・ポート／サービス監視、Web アプリケーション監視、リソース監視（CPU 使用率、メモリ使用率、ディスク使用率）の環境を提供する。

エ　停電対応

- 統合サーバ設置場所において、電気設備点検等で停電が発生する場合は、統合サーバの停止・起動を行う。

オ　障害一次切り分け

- 障害が発生した場合、障害の一次切り分けを行う。

カ　障害対応（ハード障害の対応）

- ハードウェアに起因する障害の場合は、ハードの修理または交換を行う。

キ　障害後是正措置・予防措置（ハード障害時）

- ハードウェア障害に関する情報を収集したうえで、原因を分析し、同様の障害が発生しないように是正措置・予防措置を講じる。

（3）受託業者が行うもの

- 以下の業務については、受託業者にて行うこと。

ア　システム及びデータバックアップ、リストア

- 統合サーバにおける全体バックアップを利用したバックアップ及びリストアを行う場合は、統合サーバにかかる構築業者が作業を実施するため、保守の実施に必要な作業指示書等の作成を行う。なお、一部のバックアップデータ（ファイル/フォルダ単位）のリストアについて、仮想マシンのコンソール上での作業は、統合サーバにかかる構築業者の指示により受託業者が実施する。

イ　スナップショットの作成、削除

- vCenter サーバより、本システムのスナップショットの作成、削除を行う。なお、スナップショットについては、統合サーバへの影響を考慮し、不要となり次第速やかに削除する運用とすること。（スナップショットの利用は推奨となる 3 日間までとする。3 日を超える保持を確認した場合は、統合サーバにかかる構築業者にて削除を実施する。長期保持が必要である場合、バックアップデータとして保持とする。その旨統合サーバにかかる構築業者に作業依頼すること。）

ウ　稼働監視

- 統合監視機能により、本システムの死活監視、プロセス・ポート／サービス監視、Web アプリケーション監視、リソース監視（CPU 使用率、メモリ使用率、ディスク使用率を行う。ただし、Web アプリケーション監視については、統合サーバにかかる構築業者へ監視用 Web アプリケーション資材の提供が必須となり、実装にあたって受託事業者は、統合サーバかかる構築業者等に協力すること。

オ. 性能・構成管理

- サーバのリソースについて、不足がないか定期的にチェックを行う。
- また、本システムにかかるハードウェア構成、ネットワーク構成、ソフトウェア構成等について、管理を行う。

カ. ログ管理

- 各種ログ（エラーログ、メール送信ログ等）について異常がないかチェックし、定期的に報告する。

キ. セキュリティ管理

- 不正アクセスの有無や、ウィルス検出件数等をチェックし、定期的に報告する。

ク　日常運用業務に対する支援、提案

- 統合サーバにかかる構築業者は本システムの運用業務全般を実施するために必要となる技術支援を行うこと。
- 必要に応じて性能を改善するための計画策定・対策を立案し、本県と協議のうえ対策方法の提案を行うこと。
- 統合サーバにかかる構築業者は各種報告を行うための支援を行うこと。
- 統合サーバのバージョンアップや環境変化による動作確認等を行うこと。
- 統合サーバのメンテナンスに伴う本システムの停止、起動を行うこと。

ケ　パッチによる影響等の情報提供

- 本システムで使用するソフトウェア製品に関するバグフィックス、セキュリティ対応等のパッチがリリースされた場合、速やかにその内容の調査を行い、適用の可否を本県に報告すること。また、適用できない場合は、適用するためのシステム改修の内容を本県に報告すること。なお、パッチリリースから情報の提供までの期間はMicrosoft 社のパッチは●日以内、その他の製品のパッチは●日以内とする。
- なお、本システムで影響を及ぼす恐れのあるパッチの提供がある場合、受託業者がパッチ適用を実施したうえで、本システムへの影響の有無を確認すること。

コ. パッチインストール

- 受託業者により本システムへの影響がないと判断されたパッチのインストールを行う。
- パッチ適用による障害が発生した場合は、受託業者にて障害対応を行うこと。

サ. 障害対応（システム障害の対応）

- 統合サーバにかかる構築業者にて障害の発生原因の切り分けが困難である場合は、統合サーバにかかる構築業者からの連絡に基づき、障害の切り分け支援を行うこと。
- システムに起因する障害の場合は、システムの改修または設定変更等を行う。
- 障害によりソフトウェアやデータが破損した場合、バックアップデータ等より速やかに復旧を行うこと。また、必要に応じて、システムの再セットアップを行うこと。
- なお、統合サーバの全体バックアップによるバックアップを実施している場合は、統合サーバにかかる構築業者がリストア等の作業を行うため、復旧のために必要となる動作確認や各種作業を行うこと。

シ. 障害後是正措置・予防措置（システム障害時）

- システム障害に関する情報を収集したうえで、原因を分析し、同様の障害が発生しないように是正措置・予防措置を講じること。また、直ちに障害原因が判明しない場合は、本県の了承を得たうえで、継続して調査を行い、障害原因の特定に努めること。

- 障害情報、是正措置・予防措置の内容は障害記録として体系的に記録し、常に活用できるように保存すること。

ス. 運用マニュアルの改訂

- 保守作業により、ドキュメント等の修正が発生した場合には履歴管理を行ったうえで速やかに各種ドキュメントを修正すること。尚、ドキュメントの修正にあたっては本県へ説明を行ったうえで、承認を受けること。

（4）役割分担を行ったうえで実施するもの

- 本システムにおいて従前から実施していた保守業務の内、「（2）統合サーバにかかる構築業者が行うもの」及び「（3）受託業者が行うもの」の範囲に含まれない業務について、原則として、受託業者が実施すること。
- ただし、統合サーバにかかる構築業者との調整により、一部の作業について依頼することも可とする。
- なお、その際に発生する費用等についても、本委託業務の範囲内となるので、注意すること。

別紙５　統合サーバにかかるバックアップ及びリストアの詳細について

統合サーバ上で利用できるバックアップ及びリストア等の詳細については、以下のとおり。

１　バックアップ及びリストアの方式

（1）バックアップ方法

バックアップ方法については、以下のとおり。

バックアップ単位	リストア単位	実施ソフトウェア
全体バックアップ	仮想マシン単位 (Windows、Linux) ファイル/フォルダ単位	Veeam Backup & Replication（以下、「Veeam B&R」とする。）

（2）仮想マシンバックアップ方式の考え方

仮想マシンのバックアップ方式についての考え方は以下のとおり。

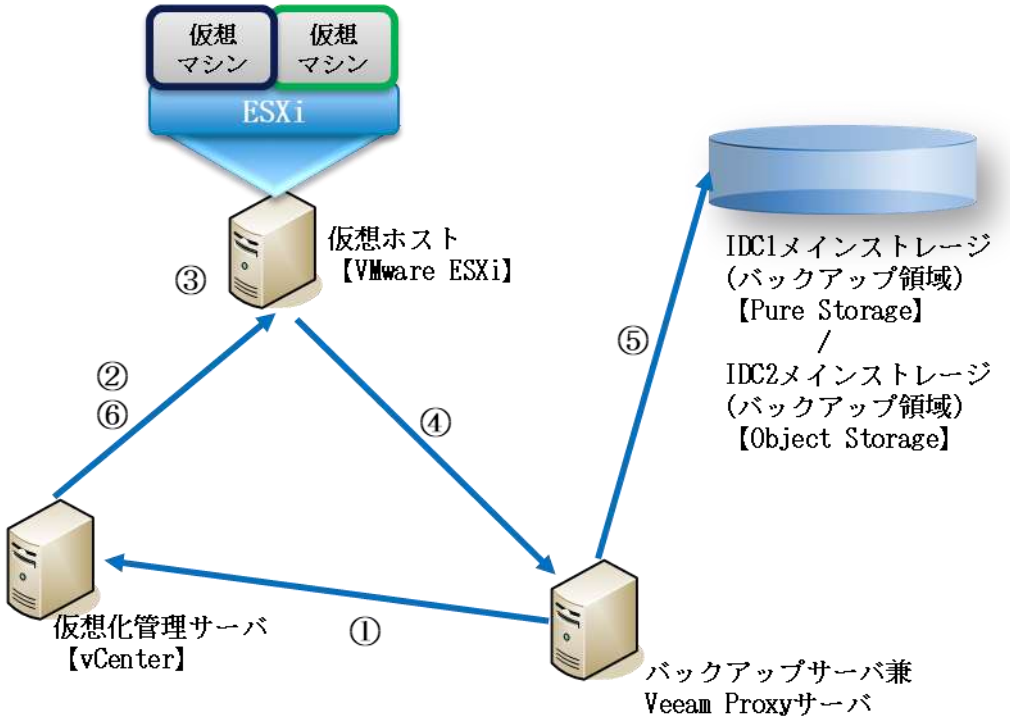
項目			方針
バックアップ	通常バックアップ	全体バックアップ	➢ Veeam B&R にて全体バックアップを取得する。 ➢ バックアップは、日次でバックアップ（増分）を行う。 ➢ 情報システム（業務サービス）への影響を極力減らすために、18:00 から翌 6:00 を目処に、運用を考慮して統合サーバにかかる構築業者と協議の上バックアップを実施する。 また、保管世代数は 5 世代とする。 なお、臨時のバックアップも世代数に含まれるため注意すること。 ➢ バックアップの開始時間はシステム単位とする。
	二次バックアップ		➢ オンプレミス環境にて全体バックアップで取得したデータを二次バックアップとして、クラウド環境のメインストレージへ退避する。 ➢ クラウド環境にて全体バックアップで取得したデータを二次バックアップとして、オンプレミス環境のメインストレージへ退避する。
	リストア		➢ 仮想マシンのリストアは、「仮想マシン単位」、「ファイル/フォルダ単位」の 2 種類より必要に応じて手動にて実施する。 ➢ 二次バックアップにより取得したデータからのリストアも可能。

（3）全体バックアップ

Veeam B&R により取得される。以下に本方式の詳細を示す。

設計項目	方式
処理概要	➢ 仮想マシン全体のバックアップを取得し、リストアは、仮想マシン単位、ファイル/フォルダ単位で実施する。
留意事項	➢ 仮想マシン上で DB を利用している場合には、必要に応じて、Veeam B&R によるバックアップ実施前に本システムにてオンラインバックアップ等を実施し、DB の一貫性を確保したバックアップを実施すること。 ※「３　制限事項とバックアップデータの整合性について」参照

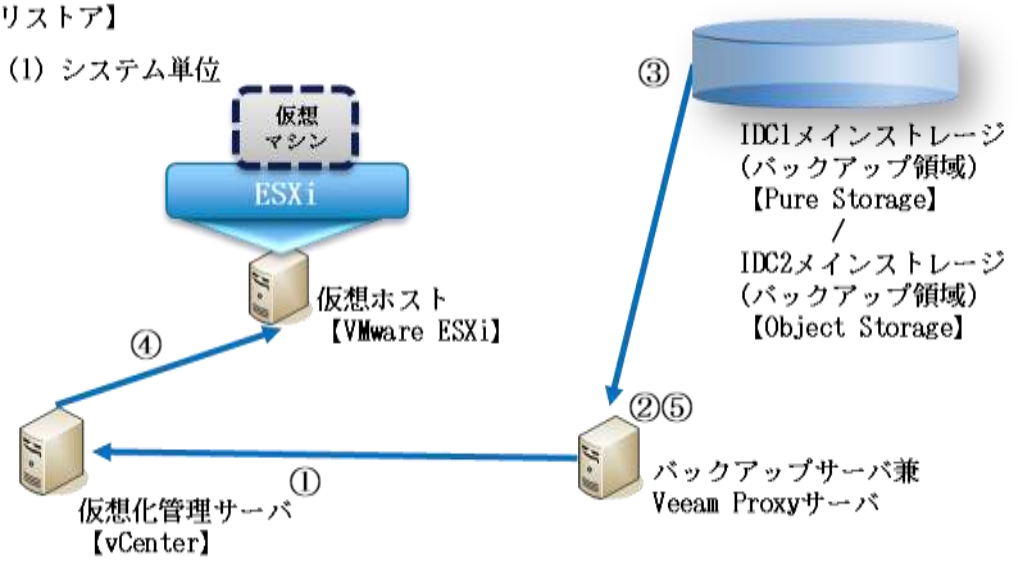
【バックアップ(システム単位）】



番号	処理内容
①	バックアップの開始
②	対象仮想マシンのスナップショットの作成
③	CBT により前回バックアップ以降に変更されたブロックを判別
④	バックアップデータをプロキシが読み取り
⑤	バックアップデータの保存
⑥	スナップショットの削除

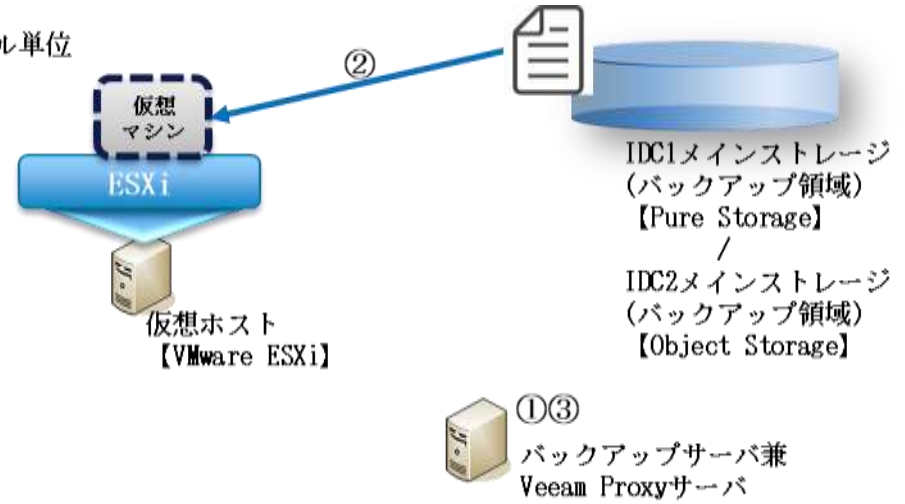
【リストア】

(1) システム単位



番号	処理内容
①	リストア対象の仮想マシンの名前の変更もしくは、仮想マシンの削除
②	リストア開始
③	バックアップデータを対象のデータストアに転送
④	vCenter へ仮想マシンの登録
⑤	リストア完了

(2) ファイル単位



番号	処理内容
①	リストア開始
②	リストア先の仮想マシンの特定フォルダに対象ファイルを復元
③	リストア完了

2　バックアップ及びリストアにかかる設計等

（1）バックアップ及びリストアにかかる詳細設計

- 本システムにおける障害対応にかかる考え方等を勘案したうえで決定することとなる。
- 統合サーバが提供するバックアップ以外に独自のバックアップが必要な場合は本県に提案を行い、承認を得ること。なお、独自のバックアップを構築する場合、テストの実施や設定変更等の作業及び保守期間における各種作業等について、受託業者がすべて実施することとなるので注意すること。
- バックアップにかかる全ての詳細設計を実施すること。また、障害時におけるリストア等についても設計を行うこと。
- なお、バックアップにかかる詳細設計については、統合サーバにかかる構築業者からのサポートが受けられるため、活用すること。

（2）バックアップ及びリストアのテスト

- バックアップにかかる詳細設計後、本システムにおけるバックアップ及びリストアについて各種テストを実施すること。
- テストは、受託業者が主体的に実施することとなるが、統合サーバにかかる構築業者からのサポートが受けられるため、活用すること。

（3）本システムの障害時対応

- 本システムの障害時における対応については、詳細設計に応じて実施すること。

3　制限事項とバックアップデータの整合性について

（1）バックアップおよびリストアにかかる制限事項

本システムのバックアップ・リストアを行ううえでの制限事項を以下に示す。

制限内容	理由	制限該当方式
バックアップデータの一貫性が保証できない場合がある。	サービスの継続性を優先し、仮想マシンの OS 停止あるいはサービスの停止を行わないため	全体バックアップ方式
オープンファイルについて、更新前のデータのバックアップは可能だが、更新中のデータはバックアップできない。	製品の仕様による	全体バックアップ方式

（2）バックアップデータの整合性

本システムのバックアップにて担保するデータの整合性を以下に示す。

DB については、通常起動中に一貫性のとれたバックアップの取得ができないため、必要に応じて、全体バックアップ実施時刻前に、オンラインバックアップまたはダンプ処理等一貫性を確保したバックアップを行うのが望ましい。

バックアップ対象	仮想マシン状態	全体バックアップ
一般データ	OS 停止	○
	通常起動	○
オープンファイル	通常起動	○※1
DB	OS 停止	○
	サービス停止	○
	通常起動	×

【○ ： 整合性のとれたバックアップが可能 / × ： 整合性のとれたバックアップ不可】

※1 ： VMware Snapshot により取得可能。保存前のデータは取得不可。

別紙６　統合サーバにかかる監視の詳細について

統合サーバ上で利用できる監視の詳細については、以下のとおり。
これらの機能について、統合サーバにかかる構築業者と調整のうえ、利用することができる。

１　監視方式

（1）機能一覧

以下の監視機能を使用して統合監視を実施する。

監視項目	説明
死活監視	監視対象仮想マシン等に対して ping コマンドを発行し、応答可否により障害判定する。
リソース監視	監視対象のリソース（CPU、メモリ、ディスク使用率）を取得し、閾値に対する評価で障害判定する。
プロセス・ポート／サービス監視	監視対象のプロセス・ポート／サービス（Windows プロセスおよびサービス、Linux プロセス、各種ポート）の稼働有無により障害判定する。
Web アプリケーション監視	監視対象サイトにアクセスし、レスポンス内容により障害判定する。

（2）死活監視

死活監視の方式は以下のとおり

- 監視サーバから本システムのハードウェア機器及び仮想マシンに対して１分毎に１回監視を行う。
- 初回の無応答時以降、２回連続して応答がない場合は障害が発生していると判断し、メール通知を実施する。
- ICMP 返答の許可が必要となる。

（3）リソース監視

リソース監視の方式は以下のとおり

- 監視サーバから本システムに対して５分間隔にて CPU、メモリ、及び、ディスクの監視を行う。
- リソース監視を行う場合には、監視対象となる仮想マシンに監視エージェントの導入及び SNMP サービスの有効化が必要となる。
- 閾値を超えた場合にシステム障害が発生していると判断し、メール通知を実施する。
- リソースの使用率が収集間隔内で閾値を超えた場合、閾値に対する評価で障害判定する。
- 閾値は原則、以下の通りとする。

監視対象	閾値警告	閾値危険
CPU 使用率	75%以上	90%以上
メモリ使用率	90%以上	95%以上
ディスク使用率	75%以上	85%以上

- SNMP 監視を利用する監視（プロセス監視、リソース監視）については、下記設定に準拠すること。

設定項目	設定値
コミュニティ名	MieKiban
ポート番号	161
バージョン	2c

（4）プロセス・ポート／サービス監視

プロセス・ポート／サービス監視の方式は以下のとおり

- 監視サーバから本システムのプロセス、ポート、及び、Windows サービスに対して 5 分毎に 1 回監視を行う。
- サービス監視について、指定したサービスが起動していない場合、障害が発生していると判断し、メール通知を実施する。
- プロセス監視について、指定したプロセスが指定された数量存在していない場合、障害が発生していると判断し、メール通知を実施する。
- プロセス監視を行う場合には、監視対象となる仮想マシンにて SNMP サービスを有効化が必要となり、情報システム（業務システム）より監視対象のプロセスに該当するプロセス名(名称)と引数(記号、文言及び数値)の提示が必要となる。(サンプル値提供)
- ポート監視について、初回の無応答時以降、2 回連続して応答がない場合は障害が発生していると判断する。
- ポート監視を行う場合には、監視対象のポート番号を提示する必要がある。(サンプル値提供)
- Windows サービス監視について、指定した Windows サービスが「実行中」の状態以外場合は障害が発生していると判断する。
- Windows サービス監視を行う場合には、仮想マシンに以下の設定が必要となる。
  - リモートコンピュータ管理の許可
  - Basic 認証の許可
  - Windows サービス監視で HTTP を利用する場合は、非暗号通信の許可
  - Windows サービス監視で HTTPS を利用する場合は、証明書の登録、Hinemos マネージャの Keystore への証明書の登録
  - リモートアクセス用 OS ユーザ（Administrators グループに所属させる。）
  - 管理対象の Windows サーバに Windows Remote Management（以降、WinRM）の設定を行う。
  - WinRM のユーザ名、パスワード、ポート番号、プロトコル、タイムアウト、試行回数の設定

（5）Web アプリケーション監視

Web アプリケーション監視の方式は以下のとおり

- 監視サーバから本システムに対して 1 分毎に 1 回「HTTP」による監視を行う。
- 指定された URL に対する HTTP リクエストに対して 5 秒以内に応答がない、または HTTP レスポンスボディ(200)の応答でない場合は障害が発生していると判断し、メール通知を実施する。
- Web アプリケーション監視を行う場合には、監視対象 URL または動作確認スクリプト及び判定ページの提示、成否判断の判定方法の提示が必要となる。(HTTP レスポンスボディの提示等)
- 判定結果から条件分岐によるリレー処理は行えない。
- 個人番号関係事務系のネットワーク（10.254.12.0/22）に対しては監視は行えない。

2　監視エージェントについて

（1）監視エージェントの要否

監視方式によっては、仮想マシン上に監視エージェントをインストールする必要がある。監視エージェントの要否を以下に示す。

機能	Linux	Windows
死活監視	◎	◎
プロセス・ポート／サービス監視	◎	◎
Web アプリケーション監視	◎	◎
リソース監視	○	○

◎エージェントレスで利用可能

○監視エージェントのインストールにより一部実現

（2）監視エージェントの対応 OS

監視エージェントの対応 OS を以下に示す。

OS 種別	対応 OS	32bit	64bit
Windows	Windows Server 2012	－	○
	Windows Server 2012 R2	－	○
	Windows Server 2016	－	○
	Windows Server 2019	－	○
	Windows Server 2022	－	○
	Windows Server 2025	－	○
Linux	Red Hat Enterprise Linux 7	－	○
	Red Hat Enterprise Linux 8	－	○
	Red Hat Enterprise Linux 9	－	○
	Red Hat Enterprise Linux 10	－	○