

「宮崎県サーバ統合基盤提供業務」

サービス仕様書（利用者向け）



令和2年4月

第7版

目次

1 はじめに	4
1.1 本書の位置づけ.....	4
1.2 サーバ統合基盤の目的	4
2 サーバ統合基盤の概要	5
2.1 サーバ統合基盤の概要構成	5
2.2 サーバ統合基盤の提供サービス	6
2.3 システム担当課とサーバ統合基盤の役割分担	6
3 仮想マシンの仕様	7
3.1 仮想化技術（仮想化ソフトウェア）	7
3.2 仮想マシン	7
3.2.2 CPU	7
3.2.3 メモリ.....	7
3.2.4 NIC 及びネットワーク.....	7
3.2.5 ローカルディスク.....	7
3.3 OS	8
3.4 データベースソフトウェア.....	8
3.5 ファイルサーバ（NAS）	8
4 信頼性・可用性	9
4.1 vSphere High Availability(HA)の提供.....	9
4.2 業務システムのクラスタ構成への対応.....	9
4.3 構成機器の冗長化仕様.....	9
5 セキュリティ機能	10
5.1 セキュリティ概要	10
5.2 ウイルス対策機能.....	10
6 バックアップ機能の提供仕様	11
6.1 バックアップ概要図.....	11
6.2 バックアップ仕様.....	11
6.2.1 1次バックアップ.....	11
6.2.2 2次バックアップ.....	11
6.2.3 退避環境バックアップ.....	11
6.2.4 仮想マシンバックアップ仕様	12

6.2.5	ファイルサーバ（NAS）のバックアップ仕様.....	12
6.3	リストア仕様	13
6.3.1	仮想マシンのリストア	13
6.3.2	ファイルサーバ（NAS）のリストア.....	13
7	県庁 LAN 用ネットワーク機能	14
7.1	ネットワーク機能の提供仕様.....	14
7.2	機能の概要	14
7.2.1	負荷分散.....	14
8	運用保守及び監視について	15
8.1	運用保守	15
8.1.1	問合せ受付.....	15
8.2	サーバ統合基盤の監視	15
8.2.1	監視内容.....	15
8.2.2	障害申告受付	15
8.3	障害対応	15
8.3.1	障害対応.....	15
8.3.2	障害対象範囲	15
9	BCP 対策.....	16
9.1	退避環境による業務システム稼働機能の提供	16
9.2	退避環境による業務システム稼働優先順	16
9.3	ボリューム種別	16
9.4	退避環境への切り替え	16
10	制約事項	17

1 はじめに

1.1 本書の位置づけ

本仕様書は、「サーバ統合基盤」で提供されるサービス内容を記述した資料となります。

1.2 サーバ統合基盤の目的

サーバ統合基盤は、「eみやざき推進指針（宮崎県電子行政推進指針改定版）」に基づき、機器及び運用の統合によるコストの削減や、柔軟性の高い運用・監視・管理体制、仮想化の特性を活かした安定稼働を目的として提供しています。

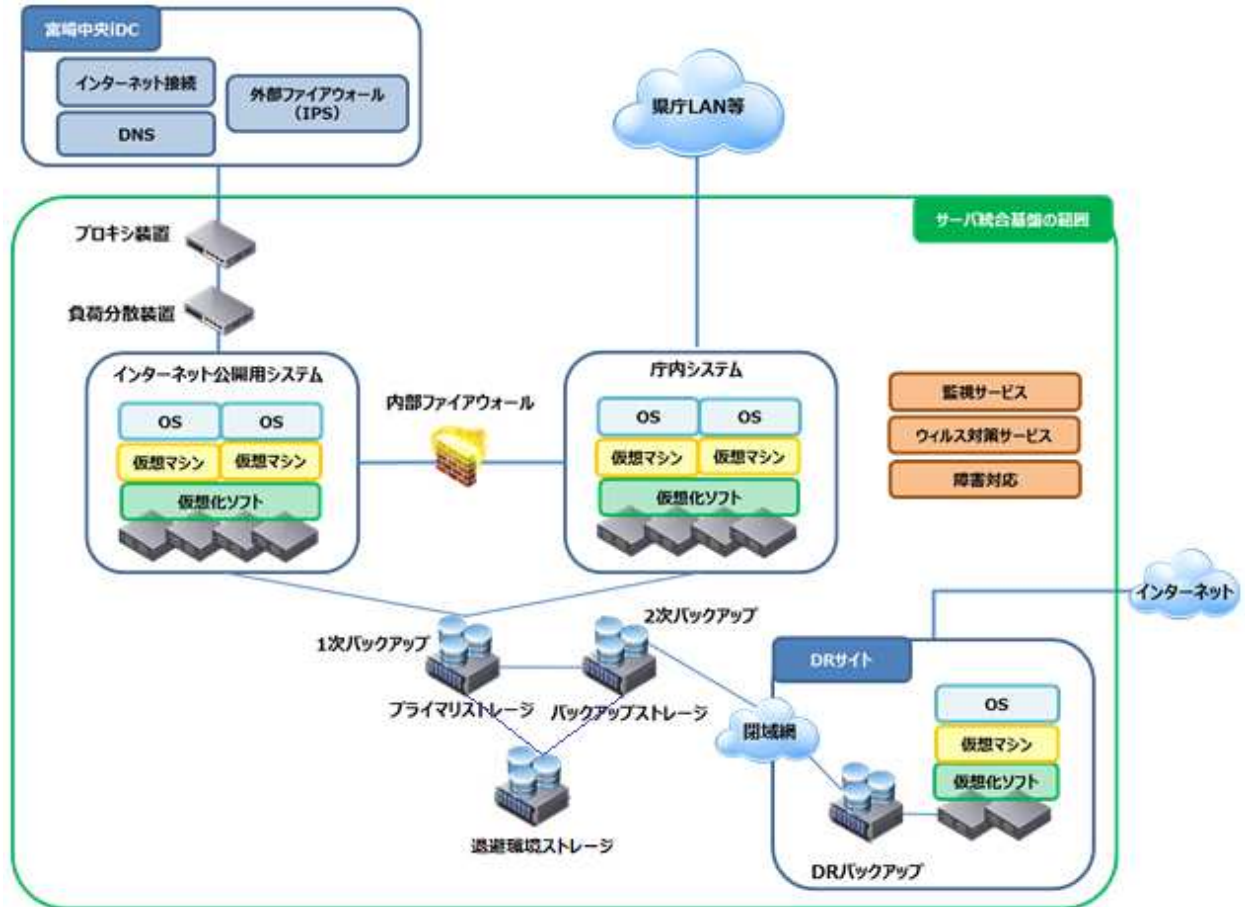
上記目的を踏まえ、サーバ統合基盤の積極的な利用をお願いします。

2 サーバ統合基盤の概要

2.1 サーバ統合基盤の概要構成

サーバ統合基盤全体の構成概要は、下図のとおりとなります。

サーバ統合基盤では、複数の物理サーバを仮想化技術により統合し、CPU やメモリ等のリソースを再配分して「仮想マシン」を構成しています。このため、仮想マシンのリソースに過不足が発生した場合も、容易に再配分ができ安定したシステムの運用、効率的な運用が可能となります。



2.2 サーバ統合基盤の提供サービス

それぞれ利用できるサービスは、下表のとおりとなります。

	インターネット 公開用システム	庁内システム	備考
仮想マシン	○	○	vCPU、メモリ、ディスク等のリソースを提供 (3.2 仮想マシンを参照)
OS	○	○	Windows、Linux 等を提供 (3.3 OS を参照)
データベース	△	△	Oracle を提供 (3.4 データベースソフトウェアを参照)
ファイルサーバ(NAS)	△	△	ファイルサーバ機能を提供 (3.5 ファイルサーバ(NAS)を参照)
ウイルス対策	○	○	統合的なウイルス対策を提供 (5.2 ウイルス対策を参照)
アクセス制御	○	○	IP/ポート番号で通信を制御
1次バックアップ	○	○	3世代のバックアップを提供 (6.2.1 1次バックアップを参照)
2次バックアップ	△	△	1世代のバックアップを提供 (6.2.2 2次バックアップを参照)
退避環境バックアップ	△	△	1世代のバックアップを提供 (6.2.3 退避環境バックアップを参照)
機器接続用スイッチ	△	△	通信事業者の回線、個別のネットワーク機器等を接続する場合に提供
iSCSI 接続ディスク	△	△	クラスタ構成を適用する際に提供
プロキシ装置	○	×	
負荷分散装置	○	△	
IPS	○	×	
外部ファイアウォール	○	×	
DNS	○	×	
リモートメンテナンス	△	△	リモートメンテナンス(SSL-VPN)を提供
監視	○	○	稼働監視等を提供

凡例 ○：標準提供サービス △：オプション提供 ×提供なし（別途協議）

2.3 システム担当課とサーバ統合基盤の役割分担

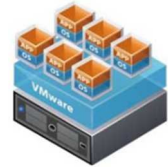
システム担当課とサーバ統合基盤の業務の役割は下記のとおりとなります。

区分	調達/提供区分		構築区分		運用/障害対応区分		備考
	システム 担当課	サーバ 統合基盤	システム 担当課	サーバ 統合基盤	システム 担当課	サーバ 統合基盤	
アプリケーション	○	-	○	-	○	-	
ミドルウェア	○	-	○	-	○	-	
データベース	-	○ (※)	○	-	○	-	Oracle はサーバ統合基盤で提供 ※ MS-SQL は 2020 年 3 月 31 日をもって新規の提供を終了
OS	-	○	○ (※)	○	○	-	個別に OS の調達は不要 構築時は、最新のパッチを適用した 状態で OS を提供。 ※ 運用開始後のパッチ適用等は、 各課で実施
ウイルス対策	-	○	-	○	-	○	サーバ統合基盤で統合的にセキュリティ 対策を提供
仮想マシン	-	○	-	○	-	○	サーバ統合基盤より、既存の物理サ ーバリソース(CPU、メモリ、ディスク)の 実使用量相当の仮想マシンを提供
ファシリティ	-	-	-	-	-	-	市内データセンターのファシリティを利用 するため UPS 等個別調達は不要

3 仮想マシンの仕様

3.1 仮想化技術（仮想化ソフトウェア）

- (1) サーバ統合基盤は VMware vSphere 6.5 により構成されています。ご利用(予定)のアプリケーションが VMware vSphere で動作可能か事前にご確認ください。



3.2 仮想マシン

- (1) サーバ統合基盤に作成される仮想マシンは、一般的なハードウェアで提供されるサーバとほぼ同等の機能を有します。仮想化技術によってハードウェアに依存する部位は仮想化され、サーバ統合基盤上で管理されます。この為、システム担当課はハードウェアの管理（設計、構築、運用、監視）は不要となります。
- (2) 仮想マシンへのリソース割当については、現状のシステムのリソース使用状況等を考慮して、最適なリソースをご提供します。
- (3) 仮想マシンのサーバリソースが不足した場合は、情報政策課と協議の上、追加することが可能です。
- (4) 仮想マシンのサーバ名は、サーバ統合基盤の命名規約に沿って決定されます。

3.2.2 CPU

- (1) 1vCPU(= 1 コア相当)単位で提供されます。処理能力は Intel® Xeon® Processor E5-2630 相当です。

3.2.3 メモリ

- (1) 1GB 単位で提供されます。

3.2.4 NIC 及びネットワーク

県庁 LAN 接続システム

種類	用途	備考
サービス用 LAN	県庁 LAN 接続用、業務システム監視用	必須
ファイルサーバ用 LAN	ファイルサーバ (CIFS/NFS) 接続用	オプション
管理用(1)LAN	ウイルス対策監視、リモートメンテナンス用	必須
システム連携用 LAN	他のシステム(ネットワーク)との連携用	オプション

3.2.5 ローカルディスク

- (1) 10GB 単位で提供されます。
- (2)「6 バックアップ機能の提供仕様」に基づいてバックアップされます。

3.3 OS

(1) 仮想マシンで利用可能な OS は下記のとおりです。

OS 名	エディション	備考
Windows Server 2016	Standard	提供可能なリソース上限あり
Windows Server 2012 R2	Standard	
Windows Server 2012	Standard	
Windows Server 2008 R2	Standard/Enterprise	メーカーサポート期限：2020/1/14
Windows Server 2008	Standard/Enterprise	メーカーサポート期限：2020/1/14
Windows Server 2008 x64	Standard/Enterprise	メーカーサポート期限：2020/1/14
Windows Server 2003 R2	Standard/Enterprise	サポート終了
Windows Server 2003	Standard/Enterprise	サポート終了
Red Hat Linux	Enterprise	5.6 以上/6.1 以上
CentOS	-	4.9 以上/5.6 以上/6.1 以上
SuSE Linux	Enterprise Server	9/10/11
Debian	-	6.0/7.x

(2) Windows Server 2003 系、Windows Server 2008 系、Windows Server 2012 系に関しては情報政策課が管理している CAL (Client Access License) を使用できます。

但し、Windows Server 2016 に関しては、別途 CAL (Client Access License) の購入が必要となります。

また、Windows Server 2016 を利用するにあたり提供可能なリソースに上限があるため別途協議とします。

(3) 上記以外の VMware vSphere で動作がサポートされている OS の利用については別途協議とします。

(4) VMware vSphere で動作がサポートされない OS については提供できません。

3.4 データベースソフトウェア

(1) サーバ統合基盤では以下のデータベースソフトウェアを提供します。

ミドルウェア名	エディション	備考
Oracle Database 12c	Standard	

※上記より古いバージョンのデータベースソフトウェアもご利用になれます。

※Microsoft SQL Server の新規提供は 2020 年 3 月 31 日をもって終了しました。

(2) 上記以外のデータベースソフトウェアを導入する場合は、各システム担当課で調達をお願いします。

3.5 ファイルサーバ (NAS)

(1) サーバ統合基盤では、ファイルサーバ (NAS) を提供することが可能です。

(2) 10GB 単位で提供されます。

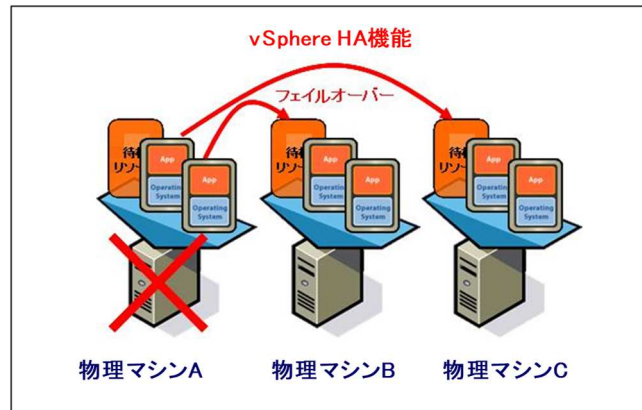
(3) 接続方式として CIFS または NFS が選択可能です。

(4) 「6 バックアップ機能の提供仕様」に基づいてバックアップされます。

4 信頼性・可用性

4.1 vSphere High Availability(HA)の提供

- (1) サーバ統合基盤で提供する仮想マシンは、高信頼性機能（vSphere HA）が提供されます。
- (2) vSphere HA は、仮想マシンを監視し、ハードウェアとゲスト OS の障害を検出します。
- (3) OS の障害を検出すると、仮想マシンを自動的に再起動します。また、仮想マシンの障害を検出すると、クラスタ内の他の vSphere ホスト上で仮想マシンを再起動します。



4.2 業務システムのクラスタ構成への対応

- (1) vSphere HA 機能で信頼性、可用性が満たせない場合に、iSCSI によるストレージ接続を提供いたします。
- (2) iSCSI により、システム担当課で準備するクラスタソフトウェア（MSCS、CLUSTERPRO 等）を使用したシステムを構築できます。

4.3 構成機器の冗長化仕様

- (1) サーバ統合基盤を構成する機器及びネットワーク経路は、原則としてすべて冗長化されています。

5 セキュリティ機能

5.1 セキュリティ概要

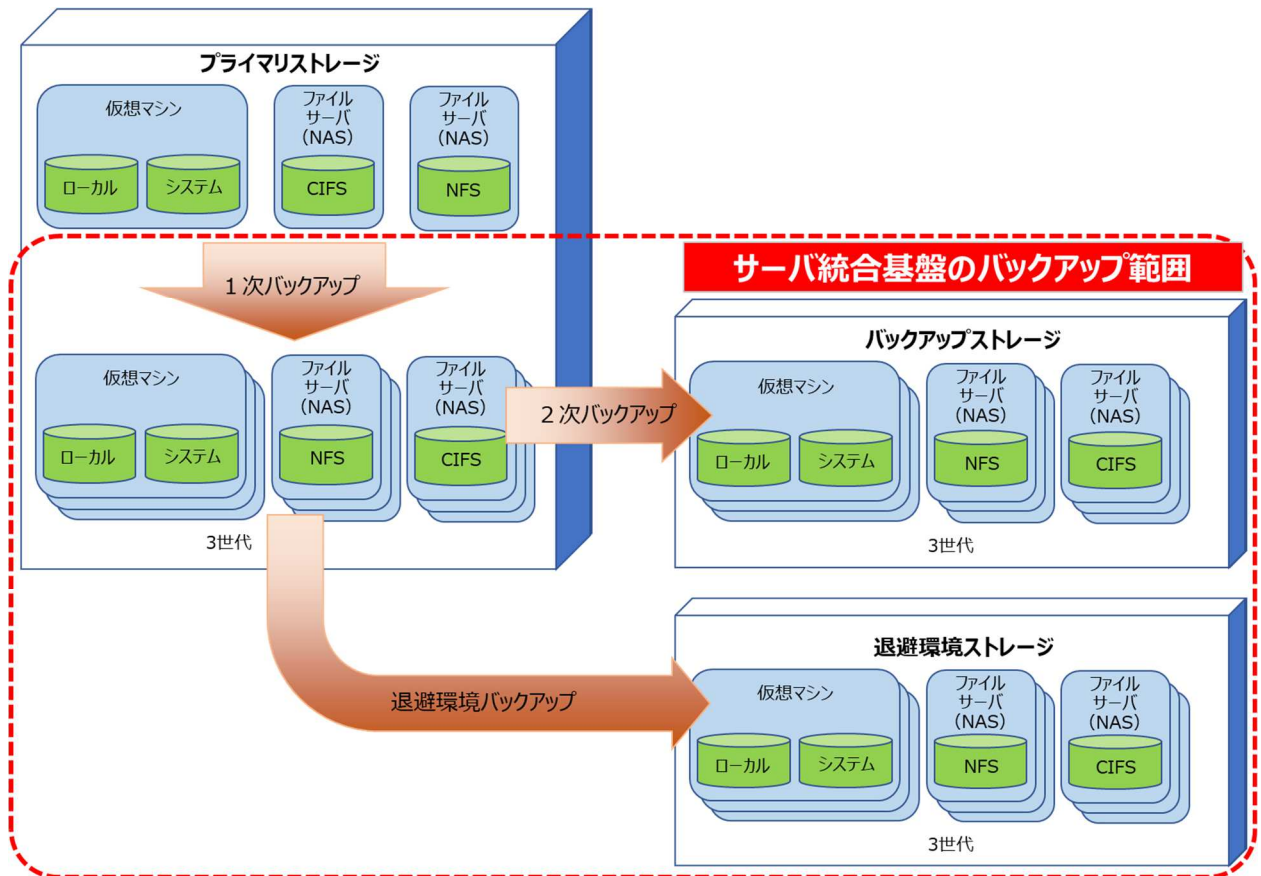
- (1) サーバ統合基盤では、「ウイルス対策機能」と「アクセス制御機能」の2つのセキュリティ機能を提供しております。各システムは、これらの機能を利用することで基本的なセキュリティ対策を実装できます。
- (2) インターネット公開システムについては、市内データセンターが提供するセキュリティ機能を利用することができます。
- (3) ウイルス対策及びアクセス制御以外に、個別システムのセキュリティ対応が必要な場合は、セキュリティ対策の実装を考慮願います。
- (4) 各システムにおける Windows Update については、宮崎県情報政策課所管の WSUS サーバを利用することができます。利用を希望される場合は情報政策課と別途協議することとします。

5.2 ウイルス対策機能

- (1) DeepSecurity（トレンドマイクロ社）相当のウイルス対策機能を、仮想マシン単位に提供します。
- (2) Windows 系の仮想サーバに対しては、エージェントレス型を提供します。
- (3) Linux 系の仮想サーバに対しては、エージェント型（仮想サーバにインストール）を提供します。
- (4) ウイルスのパターンファイルは、サーバ統合基盤運用センターで最新版を自動適用します。
- (5) ウイルスを検知し、ウイルス対策機能で駆除若しくは隔離ができなかった場合は、サーバ統合基盤運用センターで提供している NIC を強制的に切断いたします。切断後、業務システムのご利用ができなくなります。

6 バックアップ機能の提供仕様

6.1 バックアップ概要図



6.2 バックアップ仕様

6.2.1 1次バックアップ

- (1) 1次バックアップは全システムに提供します。
- (2) 毎日午前 1:00 から順次、自動的に実行されます。
- (3) 最大 3 世代 (3 日間) のデータが保持され、古いデータから破棄されます。

6.2.2 2次バックアップ

- (1) 情報政策課と協議の上、必要と判断される一部重要システムをバックアップします。
- (2) 2次バックアップを実施するシステムは、毎日午前 4 時に 1次バックアップも同時に実施します。
- (3) 1次バックアップのデータが別筐体のバックアップストレージにコピーされます。

6.2.3 退避環境バックアップ

- (1) 情報政策課と協議の上、必要と判断されるシステムをバックアップします。
- (2) 毎日午前 1:00 から順次、自動的に実行されます。
- (3) 1次バックアップのデータが別筐体の退避環境ストレージにコピーされます。

6.2.4 仮想マシンバックアップ仕様

- (1) OS のインストール領域、ローカルディスク領域を対象としたバックアップです。
- (2) バックアップ直前、自動的に仮想マシンの停止が行われます。
- (3) バックアップ完了後、自動的に仮想マシンが起動されます。
- (4) 仮想マシンの停止が難しい場合は、起動したままバックアップを行います。

注意点

バックアップのタイミングで、仮想マシンが停止できない場合は、データの整合性が保てない場合があります。

6.2.5 ファイルサーバ (NAS) のバックアップ仕様

- (1) ファイルサーバ (NAS) の CIFS 領域及び NFS 領域を対象としたバックアップです。
- (2) ファイルサーバ (NAS) は起動したままバックアップを行います。

注意点

バックアップのタイミングで、ファイルサーバ (NAS) のファイルに更新処理などが発生していた場合は、ファイルの整合性が保てない場合があります。ファイルサーバ (NAS) を使用しているサーバや端末を停止するなどの対応が必要です。

6.3 リストア仕様

6.3.1 仮想マシンのリストア

- (1) 仮想マシンのリストアは、サーバ統合基盤運用センターで実施します。リストアが必要となった場合は、運用センターへ連絡ください。

6.3.2 ファイルサーバ (NAS) のリストア

- (1) ファイルサーバ (NAS) のリストアは、ファイル/フォルダ単位で復元することが可能です。
- (2) ファイル/フォルダのアクセス権限は、リストア前の権限が引き継がれます。
- (3) ファイルサーバ (NAS) のリストアは、利用者が自ら実施可能です。

7 県庁 LAN 用ネットワーク機能

7.1 ネットワーク機能の提供仕様

- (1) サーバ統合基盤から、負荷分散機能が提供されます。

7.2 機能の概要

7.2.1 負荷分散

- (1) 県庁 LAN に接続している任意のサーバに対して負荷分散装置の機能を提供します。
- (2) 県庁 LAN から業務サーバの通信に対してのサーバ負荷分散に利用できます。
- (3) 負荷分散方式は、RoundRobin 方式、LeastConnection 方式が利用できます。

方式	内容
RoundRobin	クライアントからのアクセスを順番に対象サーバへ振り分けを実施
LeastConnection	対象のサーバが保持しているコネクション数を基に負荷分散を実施

8 運用保守及び監視について

8.1 運用保守

8.1.1 問合せ受付

運用センターは、サーバ統合基盤に関する問合せを平日 8:30～17:30 の時間帯で受け付けます。

8.2 サーバ統合基盤の監視

8.2.1 監視内容

監視センターは、サーバ統合基盤設備の監視を 24 時間 365 日実施します。障害を検知した場合は、利用申込書で指定されたメールアドレスにアラートメールを送信します。

8.2.2 障害申告受付

(1) 障害申告は、24 時間 365 日受け付けます。

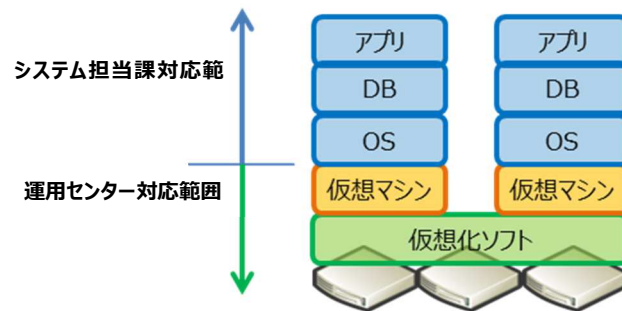
8.3 障害対応

8.3.1 障害対応

(1) サーバ統合基盤設備の障害については、24 時間 365 日で対応します。

8.3.2 障害対象範囲

(1) サーバ統合基盤運用センターの障害対応範囲は、仮想マシン以下及びご提供するネットワークとなります。OS やデータベース (DB)、アプリケーションについては、システム担当課にて障害対応をお願い致します。なお、サーバ統合基盤(運用センター)は問題解決のための支援を行います。



9 BCP 対策

9.1 退避環境による業務システム稼働機能の提供

(1) 退避環境の付帯機能として、以下①または②の条件に該当する場合、一部重要業務システムデータ（システム領域・データ領域）をプライマリストレージまたはバックアップストレージから退避環境ストレージに切替えて、業務システムを継続稼働させる機能を提供します。

- ①プライマリストレージまたはバックアップストレージが障害停止し、復旧に 24 時間以上掛かる見込みの場合
- ②業務システムの停止が伴うプライマリストレージまたはバックアップストレージの計画メンテナンス時に業務システムの業務停止が困難な場合

9.2 退避環境による業務システム稼働優先順

(1) 県が定める業務システムの BCP 復旧優先順と目標復旧時間(RTO) を踏まえ、下表のとおり退避環境における業務システムの稼働優先度の高い順に「S」「A」「B」の 3 つのボリューム種別に分類し、ボリューム種別ごとに退避環境利用条件を定義します。

ボリューム種別		優先度	概要	データ保全	退避環境利用 ^{※1}	データ更新 ^{※2}	逆同期 ^{※3}
S	個別重要システム	高	・退避環境利用時にデータ更新あり ・更新データの反映(逆同期)が必須なシステムを配置 ・業務システム毎に個別のボリュームを割当	○	○	○	○
A	重要システム	中	・退避環境利用時にデータ更新可能 ・更新データの反映(逆同期)が不要なシステムを配置 ・同一ボリューム上に複数の業務システムを配置	○	○	○	×
B	その他システム	低	・退避環境利用不可（データ保全のみ） ・同一ボリューム上に複数の業務システムを配置	○	×	-	-

※1 プライマリストレージまたはバックアップストレージの停止時に退避環境に切り替えて業務システムを稼働する。○：可能 ×：不可

※2 退避環境で稼働する業務システムによるデータ更新の可否。○：可能 ×：不可 -：対象外

※3 退避環境で稼働する業務システムが更新したデータをプライマリストレージまたはバックアップストレージの復旧後に反映する。

○：反映する ×：反映しない -：対象外

9.3 ボリューム種別

(1) R1 年度時点の各業務システムのボリューム種別は「別紙 1 業務システム・ボリューム種別一覧」のとおりとします。

9.4 退避環境への切り替え

- (1) 業務システムを退避環境に切り替えて運用するためには、事前に情報政策課と協議が必要です。
- (2) 災害が発生し、プライマリストレージまたはバックアップストレージが停止した場合、情報政策課からの指示のもと、業務システムを退避環境に切り替えて運用を開始します。
- (3) 計画メンテナンス時にも、災害発生時と同様、情報政策課からの指示のもと、業務システムを退避環境に切り替えて運用を開始します。
- (4) 災害等発生時に退避環境に切り替えて運用する業務システムは、県が定める BCP 復旧対象のシステムを優先します。

※業務システムのボリューム種別が「S」または「A」であっても、BCP 復旧優先システムの対象でない場合、退避環境の負荷状況によっては業務システムを稼働させることができないことがあります。

10 制約事項

- (1) サーバ統合基盤では、テープ、DLT、CD-ROM、DVD-ROM、USB メモリ等の媒体には対応していません。本サービスへのデータ移行やデータ取り出しについてはネットワーク経由のみになります。業務上、上記媒体を扱う必要がある場合は、事前に情報政策課と協議が必要です。
- (2) CPU ライセンスが適用されるソフトウェア等をサーバ統合基盤に移行する場合は、ライセンスを十分確認する必要があります。事前に情報政策課へお問合せください。
- (3) サーバ統合基盤（VMware vSphere）に対応していないクラスタ製品は利用できません。
- (4) サーバ統合基盤（VMware vSphere）に対応していないソフトウェアは利用できません。
- (5) VMware HA によるクラスタ切り替えでは、仮想サーバの再起動が行われます。仮想サーバ起動時に必要な業務プロセスが自動起動するよう対策を講じてください。