「宮崎県次期サーバ統合基盤提供業務」

サービス利用者向けサービス仕様書

きらきら、つながる。

QTnet

令和５年６月

第 1.2 版

株式会社 QTnet

承認			
宮崎県デジタル推進課		QTnet	

更新履歴

作成日	版	更新内容	作成者
2020/11/25	1.0	初版作成	麻生
2021/1/22	1.1	vSphere Web Client パスワードポリシー追記	〃
2023/6/26	1.2	使用可能な OS に RHEL9.x を追加	森

目次

1 はじめに

1.1 本書の目的

本書は、「宮崎県サーバ統合基盤」で提供されるサービス内容を記載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」に基づき、運用センターを中心とした柔軟性の高い運用・監視・管理体制・安定稼働を目的とし、利用者へ提供します。

2 サーバ統合基盤のシステム概要

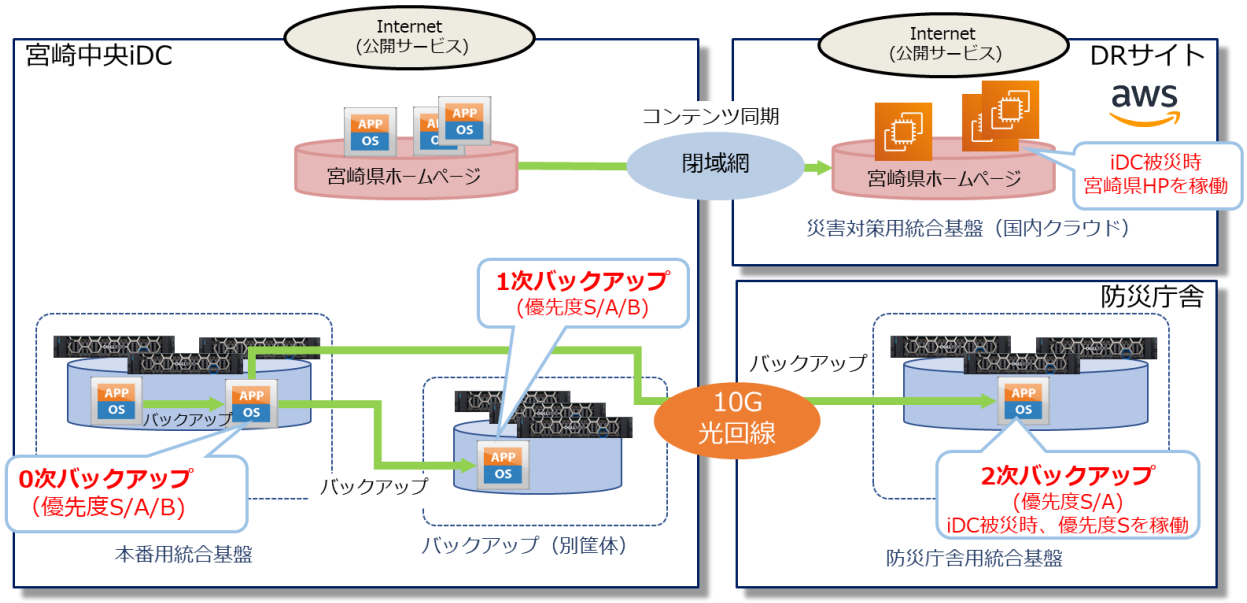
2.1 構成概要

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仮想化し再配分して「仮想マシン」を構成します。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。

令和 2 年度更改される新しいサーバ統合基盤では、性能を大幅に向上しています。

新たな特徴として、3 重のバックアップの取得や、宮崎県ホームページについてはクラウドサービスを利用した提供などがあります。

下図はサーバ統合基盤のイメージ概要となります。



2.2 サーバ統合基盤の提供サービス

利用可能なサービスは「インターネット公開システム」と「県庁 LAN 接続システム」で違いがあります。
※「インターネット公開システム」・・・公開 WEB のようにインターネット上へ公開しているシステム
※「県庁 LAN 接続システム」・・インターネット公開せず、宮崎県庁内部で利用されるシステム
それぞれ利用可能なサービスは下記となります。
各サービスの詳細については後述します。

サービス	インターネット公開システム	県庁 LAN 接続システム	備考
仮想マシン	○	○	仮想 CPU、メモリ、ディスク等のリソースを提供
OS	○	○	Windows、Linux を提供
データベース	○	○	Oracle データベースを提供 ※ MS-SQL はシステム担当課で調達が必要
ファイルサーバ(NAS)	○	○	ファイルサーバ機能を提供
ウイルス対策	○	○	基盤側でウイルス対策を提供 ※OS が Linux の場合は、システムにウイルス対策エージェントのインストールが必要
通信制御	○	○	IP アドレス/ポート番号で通信を制御
0 次バックアップ	○	○	スナップショットによる仮想マシンバックアップを提供
1 次バックアップ	○	○	別筐体への仮想マシンバックアップを提供
2 次バックアップ	△	△	遠隔地（防災庁舎）への仮想マシンバックアップを提供 ※優先度 S/A の仮想マシン
外部機器接続用スイッチ	○	○	物理機器の接続ポートを提供
iSCSI 共有ディスク	○	○	クラスタリングシステムへ iSCSI 共有ディスク領域を提供
リバースプロキシ	○	×	公開システムへリバースプロキシを提供
プロキシ	○	○	インターネット接続用のプロキシを提供 ※宮崎中央 iDC 側の提供機能となります ※メンテナンス目的での利用に限ります
負荷分散	○	○	仮想マシンへのアクセス負荷分散機能を提供
IPS/IDS	○	×	IPS/IDS（侵入検知）機能を提供 ※宮崎中央 iDC 側の提供機能となります
外部ファイアウォール	○	×	外部からのアクセス制御 IP アドレス/ポート番号で制御
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 ※主にシステム保守事業者へ提供
監視	○	○	仮想マシンの監視を提供 監視ポータル画面を提供

凡例　○：提供　　△：一部提供　　×：未提供

※その他「MAIN（旧 MJH21）接続システム」、「独自 LAN 接続システム」、「マイナンバー接続システム」が存在しますが、記載は除外します。

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業務の役割分担は下記となります。

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	○	-	○	-	○	-	Apache 等
データベース	○ (※)	○ (※)	○	-	○	-	Oracle はサーバ統合基盤で提供 ※ MS-SQL はシステム担当課で調達が必要
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。 ※引き渡し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 Linux OS はエージェント導入が必要
仮想マシン	-	○	-	○	-	○	

3 サービスの仕様

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 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

3.2.1 基本事項

(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同等の機能を有し提供します。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、デジタル推進課と協議のうえ、追加することが可能です。

(4) 仮想マシン名は、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) CPU は仮想コア単位で 1 コアから提供します。処理能力は Intel Xeon Gold 6230 相当です。

3.2.3 メモリ

(1) 1GB 単位で仮想メモリを提供します。

3.2.4 ネットワーク

インターネット公開／県庁 LAN 等のシステムの系統 および接続するネットワークにより仮想 NIC を提供します。

(1) インターネット公開システム

種類	用途	備考
サービス用 LAN	インターネット公開用、稼働監視用	標準で提供
ファイルサーバ用 LAN	ファイルサーバ（CIFS/NFS）接続用	必要に応じ提供
管理用 LAN	リモートメンテナンス用	標準で提供

(2) 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、稼働監視用	標準で提供
ファイルサーバ用 LAN	ファイルサーバ（CIFS/NFS）接続用	必要に応じ提供
管理用 LAN	リモートメンテナンス用	標準で提供
連携用 LAN	インターネット公開システムとの連携用	必要に応じ提供

(3) MAIN（旧 MJH21）接続システム

種類	用途	備考
サービス用 LAN	MAIN 接続用	標準で提供
ファイルサーバ用 LAN	ファイルサーバ（CIFS/NFS）接続用	必要に応じ提供
管理用 LAN	稼働監視用、リモートメンテナンス用	標準で提供

(4) 独自 LAN 接続システム

種類	用途	備考
サービス用 LAN	独自 LAN 接続用	標準で提供
ファイルサーバ用 LAN	ファイルサーバ（CIFS/NFS）接続用	必要に応じ提供
管理用 LAN	稼働監視用、リモートメンテナンス用	標準で提供

(5) マイナンバー接続システム

種類	用途	備考
サービス用 LAN	マイナンバー接続用 ファイルサーバ（CIFS/NFS）接続用 （マイナンバー専用） 稼働監視用	標準で提供

(6) その他

記載用途以外に NIC を追加する場合は、別途協議とします。

OS 初期設定時に、サーバ統合基盤側で必要なルーティングを設定します。

3.2.5 ローカルディスク

(1) 容量 10GB 単位で提供されます。

(2) 「バックアップ」の項に記載内容に基づいてバックアップされます。

3.3 OS の仕様

3.3.1 使用可能な 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 2019	Standard	
Windows Server 2016	Standard	
Windows Server 2012	Standard	
Windows Server 2008※	Standard	※2008R2 のみサポート ※Microsoft サポート終了
Red Hat Enterprise Linux	–	9.x, 8.x, 7.x, 6.x
CentOS	–	8.x, 7.x, 6.x
SUSE Linux Enterprise Server	–	15, 15 SP1, 15 SP2, 12 SP5, 12 SP4, 12 SP3, 12 SP2, 11 SP4
Debian	–	10.x, 9.x
Ubuntu	–	20.04, 18.04, 16.04

(2) 上記以外の OS の利用については別途デジタル推進課、運用センターと協議とします。
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) Windows Server 2012 以前の OS を新規インストールする場合など、供給が終了した OS で仮想マシン構築する場合は、OS のメディア、アクティベートライセンスキーはシステム担当課で用意ください。

3.4 データベースの仕様

3.4.1 ソフトウェアバージョン

(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。

データベースソフトウェア名	エディション	備考
Oracle Database	Standard Edition 2	

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。
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) 10GB 単位で提供します。
(2) 接続方式として CIFS または NFS を選択可能です。
(3) 「バックアップ」の項に記載内容に基づいてバックアップされます。

3.6 ウイルス対策

(1) トレンドマイクロ社の Deep Security 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 の仮想マシンに対しては、エージェントレス型を提供します。
(3) Linux の仮想マシンに対しては、エージェント型（インストールが必要）を提供します。
(4) ウイルス対策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) ウイルス対策機能で駆除もしくは隔離できない場合は、システム担当課へ対処を要請します。
デジタル推進課と協議し、ネットワークを強制的に切断することがあります。
切断後はシステムの利用ができなくなります。

3.7 通信制御

3.7.1 アクセス制御機能

(1) インターネット公開システムと県庁 LAN 接続システム間など、系統が異なるシステム間の通信を IP アドレス＋ポート番号で制御します。
(2) 同一系統内のネットワークセグメントを超える通信は、IP アドレスを条件にアクセスリストで制御します。
(3) その他、システム間で特別な連携などが必要な場合は、連携用 LAN を提供します。

3.8 バックアップ

3.8.1　0 次バックアップ

(1) サーバ統合基盤の筐体内に仮想マシンのバックアップを取得します。
(2) システムの論理障害などの際に 0 次バックアップを利用して仮想マシンを復旧します。
(3) システム優先度 S/A/B のシステムが対象となります。

3.8.2　1 次バックアップ

(1) 稼働中のサーバ統合基盤とは別の機器に仮想マシンのバックアップを取得します。
(2) 稼働中の統合基盤全体が障害となった場合に 1 次バックアップを利用して仮想マシンを復旧します。
(3) システム優先度 S/A/B のシステムが対象となります。

3.8.3　2 次バックアップ

(1) 遠隔地（防災庁舎）に仮想マシンのバックアップを取得します。
(2) 宮崎中央 iDC でサーバ統合基盤サービスが提供不可となった場合に利用します。
(3) 優先度 S/A のシステムが対象となります。
(4) 優先度 S のシステムは防災庁舎側で仮想マシンとして起動しサービスを再開することが可能です。
(5) 優先度 A のシステムは防災拠点側でデータの保管が可能です。

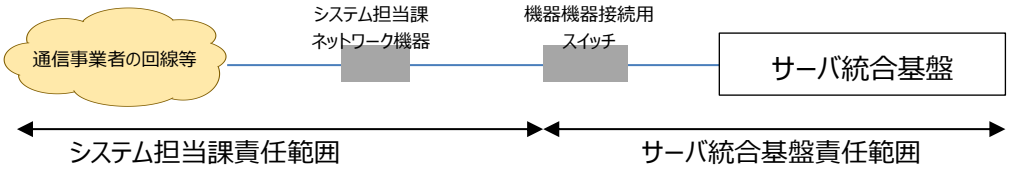
3.9 外部機器接続用スイッチ

(1) 通信事業者の回線や個別の物理機器を利用するシステム向けに、サーバ統合基盤に接続するためのスイッチを提供します。
(2) 接続する物理機器・回線は宮崎中央 iDC に設置し、システム仮想サーバとの通信を可能とします。
(3) 接続条件及び構成概要は以下のとおりとなります。

【接続条件】

項目	内容
接続インターフェイス	RJ-45
インターフェイス速度	10/100/1000Mbps
Speed 設定	Auto
Duplex 設定	Auto
機器冗長化	二重化
Link Aggregation	対応可能

【構成概要】



3.10 iSCSI 共有ディスク

(1) サーバ統合基盤の HA 機能では信頼性、可用性要件が満たせないシステムに対し、iSCSI 接続による共有ディスクを提供いたします。
(2) 提供する iSCSI 共有ディスクにより、クラスタリング（MSFC など）を使用したシステムを構築可能とします。
(3) クラスタリングの設定はシステム担当課で実施ください。

3.11 リバースプロキシ

(1) インターネット公開システムに対しリバースプロキシの機能を提供します。
(2) リバースプロキシの利用可能プロトコルは、HTTP(80)、HTTPS(443)となります。
(3) システムへ WEB 通信の代理応答および Web コンテンツキャッシング機能が利用できます。

3.12 プロキシ

(1) OS やアプリケーションのアップデート用に Web プロキシ(port 80/443)を提供します。
(2) 「インターネット公開システム」、「県庁 LAN 接続システム」ではサービス用 LAN で提供します。
(3) 「MAIN（旧 MJH21）接続システム」、「独自 LAN 接続システム」では管理用 LAN で提供します。
(4) マイナンバー接続システムでは利用できません。

3.13 負荷分散

(1) システムに対して負荷分散の機能を提供します。
(2) インターネットから公開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、Round Robin 方式、Least Connection 方式が利用できます。

方式	内容
Round Robin	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
Least Connection	コネクション数が少ないサーバへ振り分け

(4) セッション維持方式は、Source IP 方式、Cookie 方式を利用できます。

方式	内容
Source IP	クライアントの IP アドレスを条件にセッションを維持
Cookie	初回アクセス時に Cookie を挿入し、その Cookie 情報を元にセッションを維持

(5) SSL アクセラレーション機能等も利用できます。サーバ証明書については、「*.pref.miyazaki.lg.jp」を提供可能です。その他ドメインのサーバ証明書はシステム担当課にてご準備願います。

3.14 IPS/IDS

(1) インターネット公開のシステムに対し宮崎中央 iDC が提供する IPS/IDS 機能で不正侵入対策を提供することが可能です。

3.15 外部ファイアウォール

(1) インターネットからの「インターネット公開システム」への不正アクセス対策として、外部ファイアウォールを提供します。
(2) システム毎に IP アドレス＋ポート番号での通信制御が可能です。

3.16 リモートメンテナンス

(1) リモートからのサーバメンテナンス用として、SSL-VPN 機能を提供します。
　　利用可能期限の設定されたログインアカウントを発行します。

(2) システム担当課および運用センターの担当者に限定し機能を提供します。

3.17 監視

(1) システムの監視を 24 時間 365 日実施します。障害検知した場合は、指定のメールアドレスにアラートメールを送信します。
(2) サーバ統合基盤設備の監視を 24 時間 365 日実施します。障害検知した場合は、運用センターの保守対応で切り分け及び修理・交換対応を行います。
(3)以下の項目の監視が可能です。

監視項目		内容
稼働監視	死活監視	PING による死活監視
	ポート監視	指定ポート番号の疎通可否を監視
	Web 監視	指定 URL への応答有無、応答時間などを監視
性能監視	CPU 監視	CPU 使用率の最大値や平均値を監視
	メモリ監視	メモリやスワップの使用率の最大値や平均値を監視
	ネットワーク監視	ネットワークインタフェースを通して送受信されるトラフィック量を監視
	ファイルシステム監視	ディスク使用率を監視
	プロセス監視	Windows サービスや、Linux/Unix プロセスの稼動を監視
状態監視	Windows イベントログ監視	Windows イベントログを監視
イベント監視	Linux OS ログ監視	Linux サーバの OS ログを監視
	アプリケーションログ監視	Windows 及び Linux サーバ上のアプリケーションログを監視します。 （例）Oracle、Apache、Java などのログ

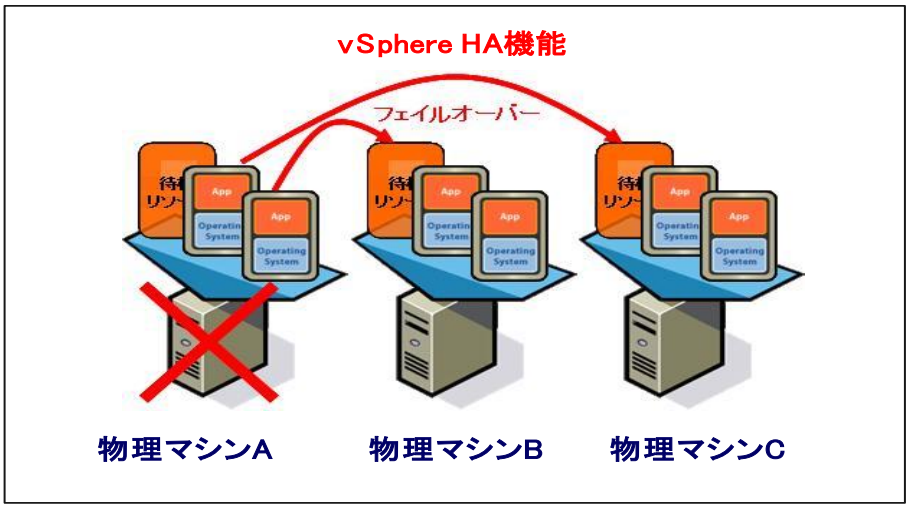
(4) 監視は、「サービス用 LAN」を介して監視します。なお、MAIN（旧 MJH21）接続システムは、「管理用 LAN」を介して監視します。

(5) 各システムの監視状況を確認可能な「監視ポータル」画面をシステム担当課に提供します。

4 信頼性・可用性

4.1 高可用性の提供

(1) サーバ統合基盤で提供する仮想マシンは、高可用性（HA）機能を提供します。
(2) システムが稼働しているホストサーバに障害が発生した場合も、システムは自動的に再起動します。



(3) ホストサーバの負荷状況に応じて自動的に仮想マシンを再配置し、負荷を平準化します。
(4) 複数の仮想化マシンで構成されたシステム（多重化された Active Directory サーバなど）について同一ホストサーバ上に配置されないように制御し、ホストサーバの障害による影響を抑えることが可能です。

4.2 構成機器の冗長化仕様

(1) サーバ統合基盤を構成するサーバおよびネットワーク機器は、原則としてすべて冗長化し、単一機器障害でのサービス影響が無い構成としています。

5 セキュリティ

5.1 基本事項

(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) サーバ統合基盤で提供する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。

(3) 各システムにおける Windows Update については、宮崎県デジタル推進課所管の WSUS サーバを利用する方針とし、利用を希望する場合はデジタル推進課と別途協議ください。

5.2 インターネット公開システムのセキュリティ

5.2.1 不正アクセス対策

(1) インターネットから「インターネット公開システム」への不正アクセス対策として、ファイアウォール機能を提供し接続可能なプロトコル、ポート番号を制御します。

(2) 「インターネット公開システム」と「県庁 LAN 接続システム」の間の通信に関しては、IP アドレス＋ポート番号での通信制御を実施します。

5.2.2 不正侵入対策

(1) 宮崎中央 iDC が提供する IPS/IDS 機能での不正侵入対策を可能とします。

5.3 マイナンバー系のセキュリティ

(1) 「マイナンバー系システム」は原則閉じたネットワークとし外部との接続を不可とします。

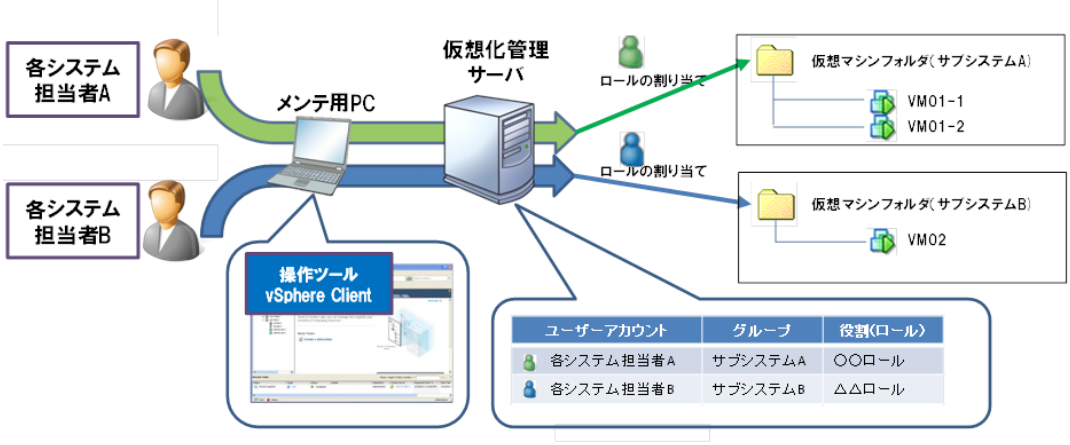
5.4 アカウント管理

(1) 仮想化管理サーバはログインユーザにてアクセス管理を行います。
ログインユーザの種別として、「管理者」と「閲覧者」の 2 タイプのユーザ権限を用意します。
各ユーザの操作権限は以下のとおりです。

操作		管理者権限	閲覧者権限
仮想マシンの操作	新規作成	×	×
	削除	×	×
	電源起動	○	×
	電源停止	○	×
	コンソール画面操作	○	○

	CD/DVD のマウント	○	×
	USB のマウント	○	×
CPU、メモリリソースの変更		×	×
サーバ統合基盤のログ閲覧		○	○

(2) システム担当者が操作できる仮想マシンを限定することで、不必要なサーバへのアクセスを抑止します。



(3) vSphere Web Client は許可された庁内のユーザから接続を可能とします。
パスワードポリシーは以下のとおりです。

方式
・パスワードの長さは 8 文字以上とする
・パスワードには英字の大文字を 1 文字以上含める
・パスワードには英字の小文字を 1 文字以上含める
・パスワードには数字を 1 文字以上含める
・パスワードには特殊文字(記号)を 1 文字以上含める

5.5 仮想マシン操作環境の提供

(1) システムの移行作業やメンテナンスを行うため、宮崎中央 iDC 内の運用センターに作業専用端末（Windows クライアント）を設置しています。
(2) VMware vSphere Web Client (Web Client)を利用し、仮想マシンの制御が行えます。
(3) 作業専用端末では以下のソフトウェアが利用できます。

ソフトウェア	用途
Web Client	仮想マシンのメンテナンス用（Web ベース） システムコンソール画面の操作

※システム側のセキュリティポリシーにより、上記ソフトウェアの通信が制限されている場合があります。

5.6 作業端末の持ち込み

作業端末の持ち込みについては、デジタル推進課と事前に協議ください。
運用センター内での持ち込み PC 接続では、VMware vSphere Web Client での操作ができませんので、以下のようなツールにて、各仮想マシンへアクセスしてください。

ソフトウェア・サービス・ツール	用途
SSH/Telnet/RDP/VNC 等	仮想マシンの OS の操作
FTP/ファイル共有/SCP 等	仮想マシンとのデータの送受信

6 バックアップ

6.1 バックアップ概要

サーバ統合基盤では障害に備え、仮想マシンのバックアップを取得します。

バックアップは以下の 3 種類を提供します。

分類	バックアップ場所
0 次バックアップ	稼働中のサーバ統合基盤の機器筐体内に取得
1 次バックアップ	稼働中のサーバ統合基盤と別の機器に取得
2 次バックアップ	防災庁舎に取得

上記の仮想マシンバックアップとは別に、サービス利用者が独自のポリシーで OS 上のファイルなどをファイルサーバへバックアップすることを可能とします。

6.2 バックアップ対象

以下にバックアップ対象とそのバックアップ内容について記載する。

対象	バックアップ分類	バックアップ主導者	説明
仮想マシン OS 上のデータ (DB・アプリケーションデータなど)	0 次バックアップ	システム担当課	・システム担当課が手法を選択し、提供されるファイルサーバ領域にバックアップを行ってください。（手法例：export や dump 等の手法を利用してバックアップデータを作成する等）
仮想マシン	0 次バックアップ	サーバ統合基盤管理者	・システムに不整合が発生した場合などに、迅速に復旧するための仮想マシンのバックアップ。 ・iSCSI 接続で利用しているディスクについてもバックアップ対象に含まれます。
	1 次バックアップ		・稼働中の統合基盤全体が障害となった場合に復旧するための仮想マシンのバックアップ。
	2 次バックアップ		・宮崎中央 iDC でサーバ統合基盤サービスが提供不可となった場合に復旧するための仮想マシンのバックアップ。 ・優先度 S/A の仮想マシンが対象です。
ファイルサーバ（NAS）	0 次バックアップ		・誤操作などで誤って削除・変更したファイルのバックアップ。 ・利用者自身でファイル復旧が可能です。
	2 次バックアップ		・宮崎中央 iDC がサービス提供不可となった場合に、遠隔地でファイルサーバのファイル復旧を行うためのバックアップ。

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。
　　仮想マシンの障害で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。

(2)リストアが必要となる想定ケースとリストア方法

想定ケース	リストア対象	リストア方法	RPO	RTO
仮想マシンが破損した場合 仮想マシンの論理障害	仮想マシン単位	【優先度 S/A/B のシステム】 0 次バックアップから仮想マシン単位のリストア	24 時間 (*1)	2 時間
宮崎中央 iDC サーバ統合基盤が稼働不可となる障害	仮想マシンすべて	【優先度 S/A/B のシステム】 1 次バックアップからすべての仮想マシンをリストア	24 時間 (*1)	1 週間 (*2)
宮崎中央 iDC が利用不可の場合	優先度 S の仮想マシン	【優先度 S のシステム】 2 次バックアップを元に S のみ防災拠点庁舎環境で仮想マシンリストア後、起動 優先度 A のシステムはデータ保管のみ可能	24 時間 (*1)	2 日

(*1) 優先度 A/B のシステムのリカバリについて、宮崎中央 iDC の本番用クラスタの復旧後に 1 次バックアップを利用して復旧します。
　　RPO24 時間は障害発生時点から 24 時間以内を意味します。
(*2) 優先度 S のシステムは防災庁舎を利用することで RTO が 2 日になります。

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、利用者で実施可能です。

(4)リストアが必要となる想定ケースとリストア方法

想定ケース	リストア対象	リストア方法	RPO	RTO
ファイルを誤って削除した場合、 ファイルが破損した場合	ファイル単位	【優先度 S/A/B(すべて)のシステム】 0 次バックアップからファイル単位のリストア（NAS）	24 時間	2 時間

7 定期メンテナンス

(1) サーバ統合基盤運用センターは、サーバ統合基盤の設備メンテナンスを月 1 回行います。
(2) メンテナンスは原則として無停止で行います。
(3) メンテナンスにより業務システムを停止する必要がある場合は、1 か月前までにサーバ統合基盤ポータルなどで通知します。

8 運用保守について

8.1 運用保守

8.1.1 問合せ受付

(1) 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。
お問い合わせは、電話またはメールでの受付となります。

電話番号
0985-88-1785

メールアドレス	問合せ内容
support@mpis.jp	運用開始後の問い合わせ

(2) リモートメンテナンスの利用申請等が可能な「運用ポータル」画面を提供します。

8.1.2 障害申告受付

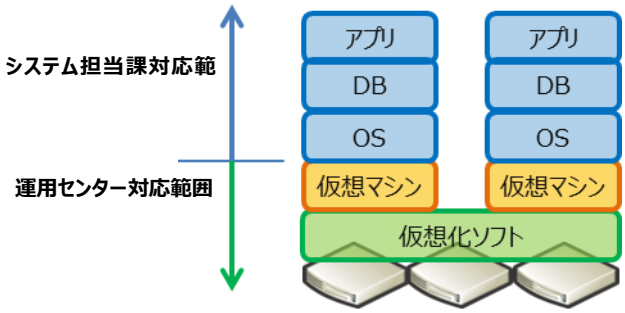
(1) 障害申告は、24 時間 365 日受け付けます。
(2) 障害申告は、電話での受付となります。
電話番号：0985-88-1785
※時間帯により自動的に以下の受付箇所に転送されます。
[平日 8:30～17:30 の時間帯]
受付箇所：運用センター（デンサン）
[休日・夜間（平日 8:30～17:30 以外）の時間帯]
受付箇所：監視センター（QTnet SOC）

8.1.3 障害対応

サーバ統合基盤設備の障害については、24 時間 365 日対応します。

8.1.4 障害対象範囲

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原因調査をお願いします。
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。



8.2 サービスレベル（SLA）

(1) サービス統合基盤のサービスレベルは下記とします。

項目	概要	SLA
サービス時間	サービス提供時間	24 時間 365 日
監視・通報時間	障害発生時に利用者に通知する時間帯	24 時間 365 日
サーバ稼働率	サービスが稼働している割合 (計画停止、保守時間、片系の故障時間を除く)	99.99%
一次報告※1	障害発生時、利用者に通知する時間	30 分
報告※2	障害発生後、原因及び復旧状況に要する時間	60 分

*1：1 次報告はシステム担当課へのメール配信または運用ポータルへの掲載とします。
*2：報告はデジタル推進課への電話またはメールでの報告とします。

9 BCP

9.1 防災庁舎による業務システム稼働機能の提供

(1) 宮崎中央 iDC でサーバ統合基盤サービスを提供不可となる状況となった場合に、防災庁舎でシステムの稼働を可能とします。

(2) 優先度 S の仮想マシンが対象となります。
(3) 優先度 S のインターネット公開システムは、外部 DNS に記載されたレコード書き換えることによりユーザのアクセスを防災庁舎に切り替えます。
(4) 宮崎中央 iDC のサーバ統合基盤が復旧した場合、防災庁舎から優先度 S の仮想マシンデータを逆コピーし宮崎中央 iDC で優先度 S の仮想マシンを稼働します。
(5) 優先度 A のシステムは防災庁舎でのデータ保管を行います。
宮崎中央 iDC のサーバ統合基盤が復旧した場合、防災庁舎に保管された優先度 A の仮想マシンデータを元に宮崎中央 iDC へ優先度 A の仮想マシンを復旧させます。
(6) 優先度 B の仮想マシンは防災庁舎での稼働・データ保管の対象外となります。

(7) 下表のとおり防災庁舎環境の利用条件を定義します。

種別		優先度	概　　要	データ保全	システム稼働	逆コピー
S	個別重要システム	高	・防災庁舎で稼働可能 ・更新データの反映(逆コピー)が必要	○	○	○
A	重要システム	中	・防災庁舎でデータ保管可能	○	－	－
B	その他システム	低	・防災庁舎での稼働、データ保管不可	－	－	－

9.2 DR（ディザスタリカバリ）

(1) 重要システムのサービス停止時に稼働可能な DR サイトを提供します。
(2) DR サイトはパブリッククラウドサービスを利用し国内拠点で稼働します。
(2) 現在の DR 対象システムは県庁ホームページシステムです。
(3) 切替の際は、コンテンツ管理（CMS）担当者によるコンテンツの最新化が必要です。
(4) 外部 DNS に記載された WWW レコードを書き換えることによりユーザのアクセスを DR サイトに切り替えます。

(5) DR サイトへの切替が想定されるケースと切替方法

想定ケース	対象	切替方法	RPO	RTO
県庁ホームページ システムの障害によるサービス停止	WEB サーバ	・DR サイトでの HP サーバのコンテンツ最新化 ・外部 DNS サーバのレコード変更 ・HP サーバの公開設定	1 時間	1 時間

10 制約事項

(1) サーバ統合基盤では、磁気テープ等の外部デバイスへのバックアップには対応していません。
(2) 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になります。
(3) CD-ROM、DVD-ROM、USB メモリ等の外部デバイスについては運用センター設置の作業専用端末（Windows クライアント）から利用可能です。
(4) 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。事前にデジタル推進課へお問合せください。
(5) サーバ統合基盤（VMware vSphere）に対応していないクラスタリング機能は利用できません。
(6) 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。
(7) ホストサーバの障害時は、各システムの仮想サーバは再起動されます。システム起動時に必要な業務プロセスが自動起動するよう設定ください。