

神戸市サーバ仮想化基盤構築・運用業務
サーバ仮想化基盤 利用ガイドライン

令和6年3月15日
神戸市企画調整局デジタル戦略部
日本電気株式会社

—目次—

1. はじめに	1
2. サーバ仮想化基盤の概要	1
2.1. サーバ仮想化基盤の目的	1
2.2. サーバ仮想化基盤提供機能一覧	2
3. サーバ仮想化基盤の動作条件	3
3.1. システム全体構成	3
3.2. 仮想化サーバ共通用エリア	4
4. 仮想化サーバ共通システム構成	5
4.1. ハードウェア構成	5
4.2. ソフトウェア構成	6
4.3. ネットワーク構成	7
4.4. 共通利用サーバが提供する機能	8
4.5. 耐障害性・可用性	8
4.5.1. サーバ仮想化基盤の可用性	8
4.5.2. ネットワークの可用性	9
4.5.3. バックアップの信頼性	9
4.5.4. 冗長構成による信頼性	9
4.5.5. リソースの拡張性	10
5. サーバ仮想化基盤の提供サービス	11
5.1. 仮想マシン対象 OS	11
5.2. 提供可能なミドルウェア	12
5.2.1. 初期状態	13
5.2.2. 同一構成の仮想マシンに関する払い出しについて	14
5.3. 仮想ネットワーク機能	15
5.3.1. 仮想ネットワークの構成概要	15
5.3.2. 仮想ファイアウォール	16
5.3.3. 仮想ロードバランサ	17
5.3.4. サーバ仮想化基盤 FW_LB 設定ポータル	18
5.4. 時刻同期	18
5.5. バックアップ機能	19
5.5.1. 提供するバックアップ機能	19
5.5.2. 各バックアップで実施する処理について	20
5.5.3. 業務データバックアップの詳細	21
5.5.4. 1次バックアップの詳細	22
5.5.5. 2次バックアップの詳細	23
5.5.6. 遠隔地バックアップの詳細	24
5.5.7. バックアップ機能	25
5.6. クローン機能	27
5.7. 保守機能	28
5.7.1. 保守環境	28
5.7.2. 保守回線	28
5.7.3. 保守端末	30
5.8. パフォーマンス管理	31
5.8.1. vSphere DRS	31
5.8.2. vSphere DRS の自動化レベル	31
5.8.3. アフィニティルールの設定	32
5.9. ホストサーバの冗長化	33
5.9.1. vSphere HA	33
5.10. ライブマイグレーション機能	35

5.10.1. vMotion	35
5.11. 運用監視機能.....	36
5.11.1. サーバ仮想化基盤としての運用監視	36
5.11.1. 業務システムにおける運用監視	37
5.12. セキュリティ管理	38
5.12.1. セキュリティパッチ	38
5.12.2. ウイルス定義ファイルの更新	39
5.13. 障害時切り分け	40
5.13.1. 障害対応プロセス（開庁日業務時間内）	40
5.13.2. 障害対応プロセス（開庁日夜間及び休日）	41
5.13.3. 障害対応プロセス（障害検知元が監視システムの場合）	42
6. 責任分界点	43
6.1. 仮想マシン払い出しにおける責任分界点	43
6.1.1. 仮想マシン引き渡し時（業務システム導入前）	43
6.1.2. 仮想マシン引き渡し後.....	43
6.2. 運用時の責任分界点.....	44
7. サーバ仮想化基盤利用時の手続き.....	45
7.1. 役割分担	45
7.2. 支援内容	46
7.3. 時系列	47
7.4. サーバ仮想化基盤利用時に提供いただく情報.....	49
7.4.1. ヒアリングシート（利用申請）の作成、承認.....	49
8. サーバ仮想化基盤に関する問い合わせ	52
8.1. サーバ仮想化基盤に関する一般的な問合せ	52
8.2. 業務共通利用ソフトウェアに関する問合せ	52
9. 費用の考え方	53
9.1. 費用負担	53
9.2. 効果額算定	53

1. はじめに

本書は、業務所管課及び業務システム運用保守業者向けに、サーバ仮想化基盤を利用してシステム構築（移行）を実施する際に利用するものである。

2. サーバ仮想化基盤の概要

2.1. サーバ仮想化基盤の目的

本市庁内には、基幹系ネットワーク、情報系ネットワーク、専用ネットワーク、いずれのネットワークにも属さないスタンドアロンシステムなどの業務システムが存在する。これらの業務システムの高度化・複雑化に伴いサーバ数が増加しており、維持管理コストが増大するとともに設置スペースが枯渇している状況にある。

このような問題を解決するため、庁内情報システムの統合稼働環境として、サーバ仮想化基盤を導入・整備し、既存の業務システムを段階的に移行していくことにより、全体最適化を図り、TCOを削減していくことが目的である。

業務システムの仮想化環境である「サーバ仮想化基盤」の構成は以下のとおりである。

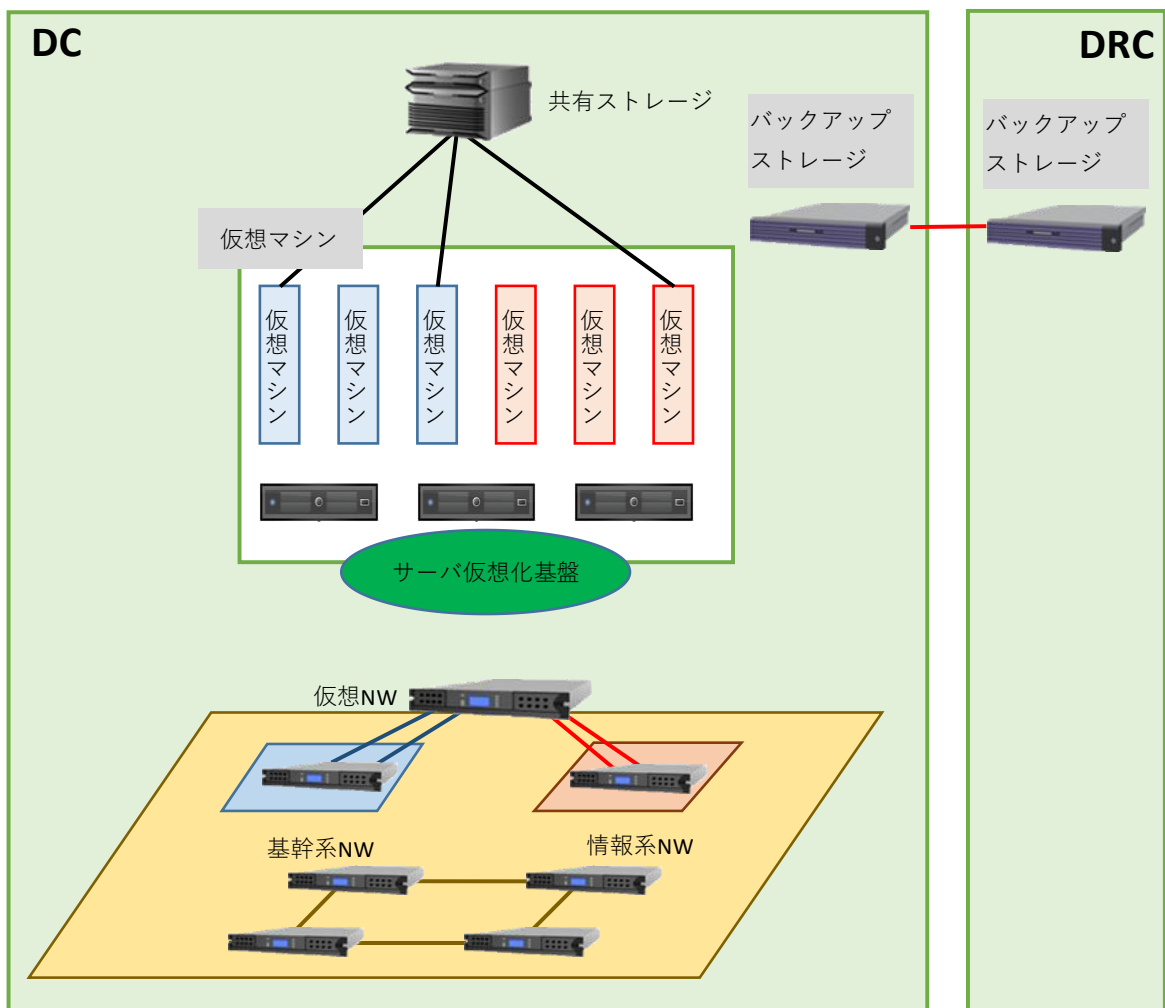


図2-1 サーバ仮想化基盤システム構成図（概要）

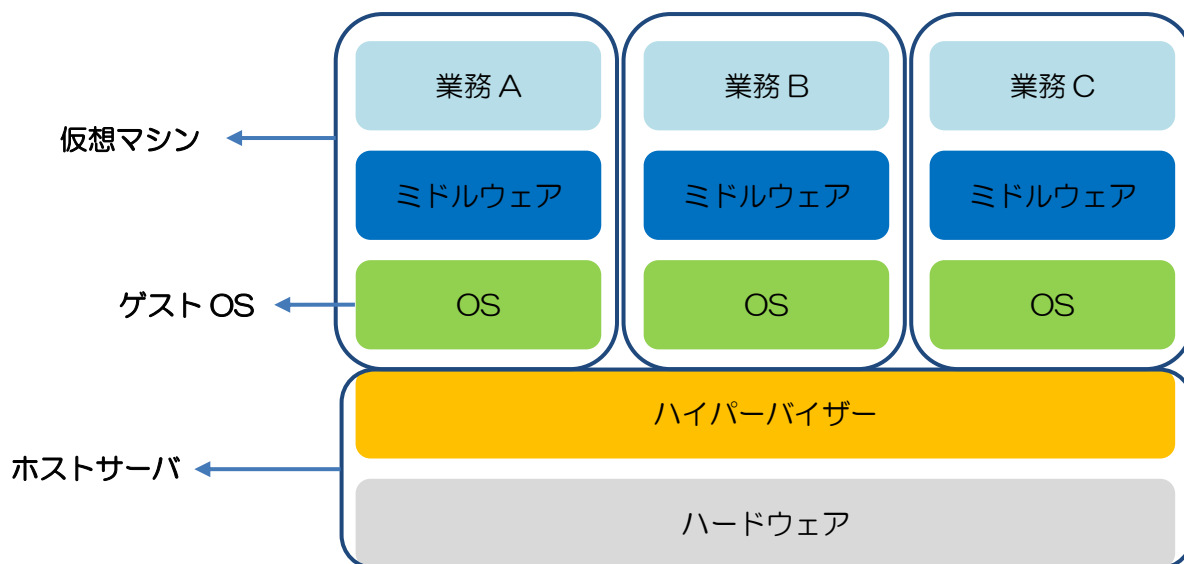


図 2-2 ホストサーバと仮想マシンの関係

2.2. サーバ仮想化基盤提供機能一覧

サーバ仮想化基盤で提供する機能は以下のとおりである。

表 2-1 提供機能一覧

	機能	説明
1	仮想マシン機能	サーバ仮想化基盤で提供する仮想マシン稼働環境の提供
2	仮想ネットワーク機能	サーバ仮想化基盤で提供する仮想ネットワークの機能 (仮想ロードバランサ、仮想ファイアウォール)
3	バックアップ機能	サーバ仮想化基盤で提供するバックアップの機能 (1 次、2 次、遠隔地バックアップ)
4	運用監視機能	サーバ仮想化基盤で提供する運用監視の機能
5	保守機能	サーバ仮想化機能で提供する保守の機能
6	冗長機能	サーバ仮想化基盤で提供する仮想化サーバの冗長機能

サーバ仮想化基盤システムのサービス提供時間は、24 時間 365 日とする。ただし、システムのメンテナンス等を除く。

3. サーバ仮想化基盤の動作条件

3.1. システム全体構成

サーバ仮想化基盤の機器は、火災対策やセキュリティが厳重で安全性の高いデータセンターに設置。また、激甚災害に対応するため、一部データを遠隔地保管するための機器は、ディザスタリカバリセンターに設置する。

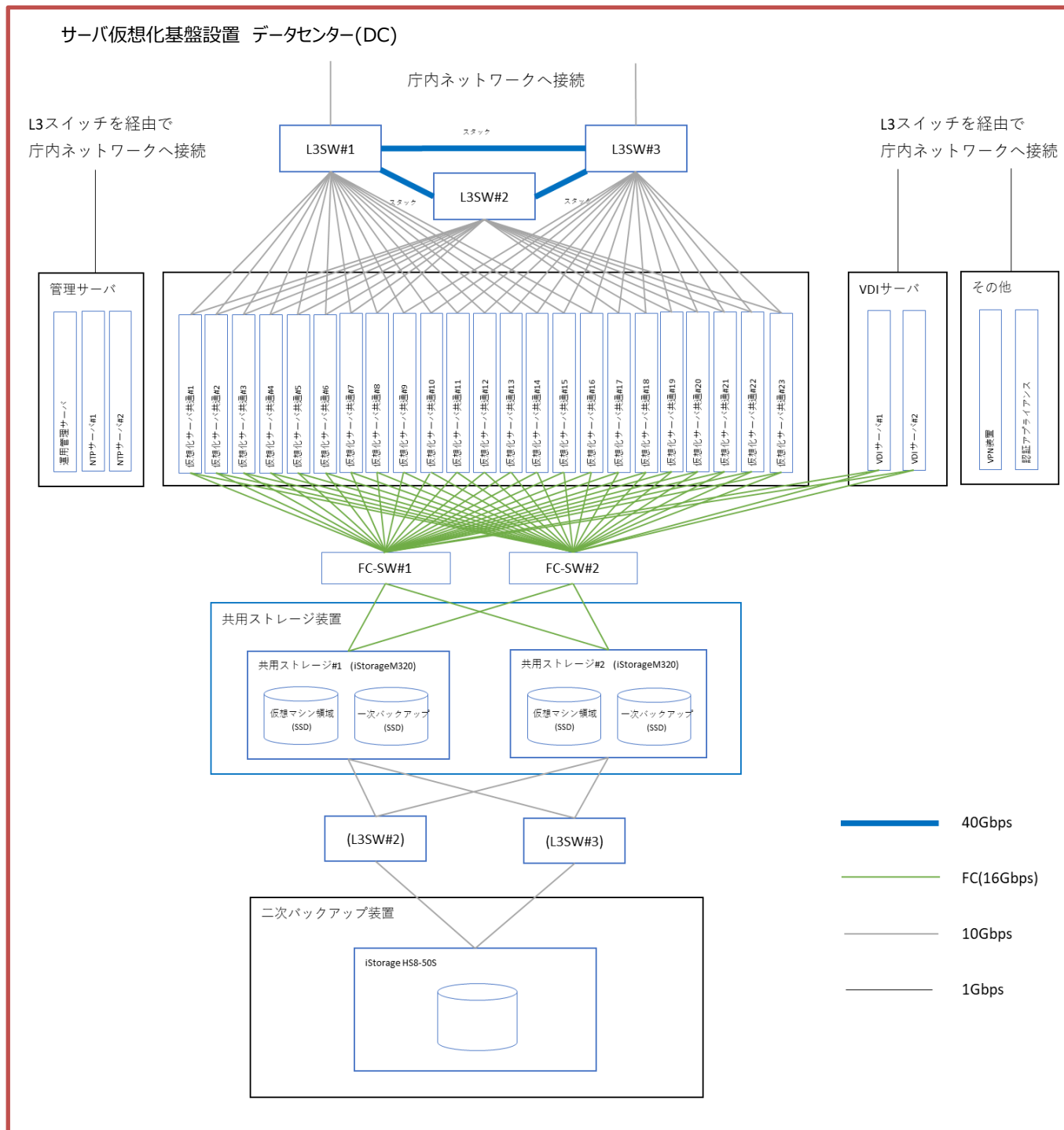


図3-1 DC 構成

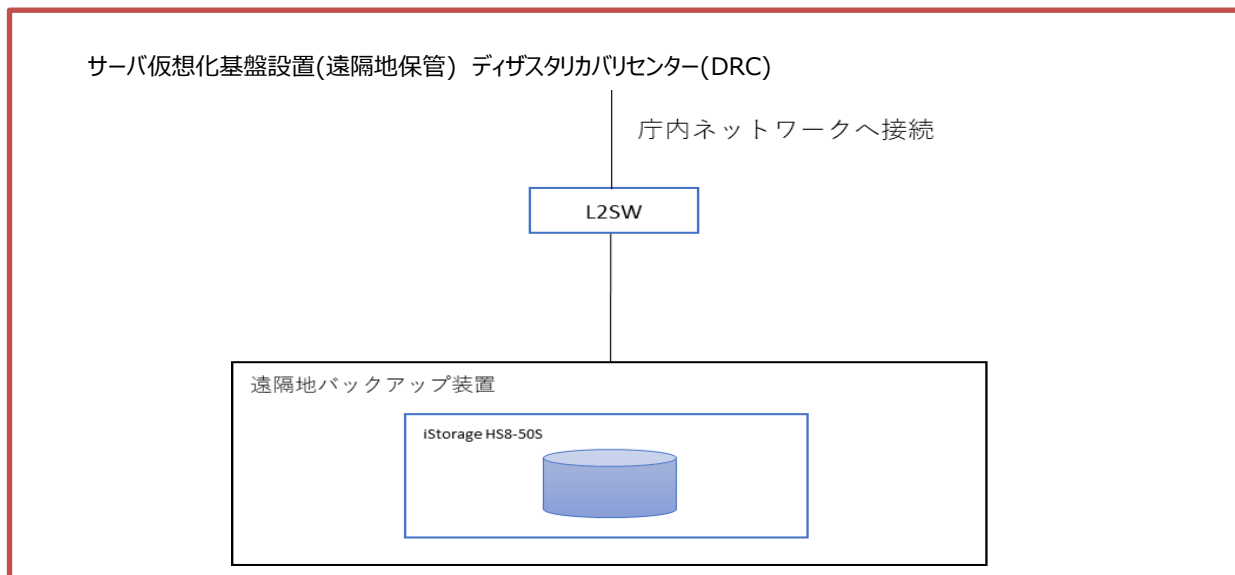


図3-2 DRC 構成

3.2. 仮想化サーバ共通用エリア

仮想マシンが稼働する仮想化サーバ共通用エリアは、23 台の仮想化サーバで構成している。うち、業務システムが稼働する仮想化サーバ共通は 20 台、サーバ仮想化基盤用管理サーバが稼働する仮想化サーバ(管理用) 1 台、予備サーバ 2 台とし、システムの負荷分散、冗長化、耐障害性を図っている。

- 仮想化サーバ 共通#1～#20 上で業務用システムが稼働
- 仮想化サーバ 共通#23 上でサーバ仮想化基盤用管理サーバが稼働
- 仮想化サーバ 共通#21、#22 は予備サーバ

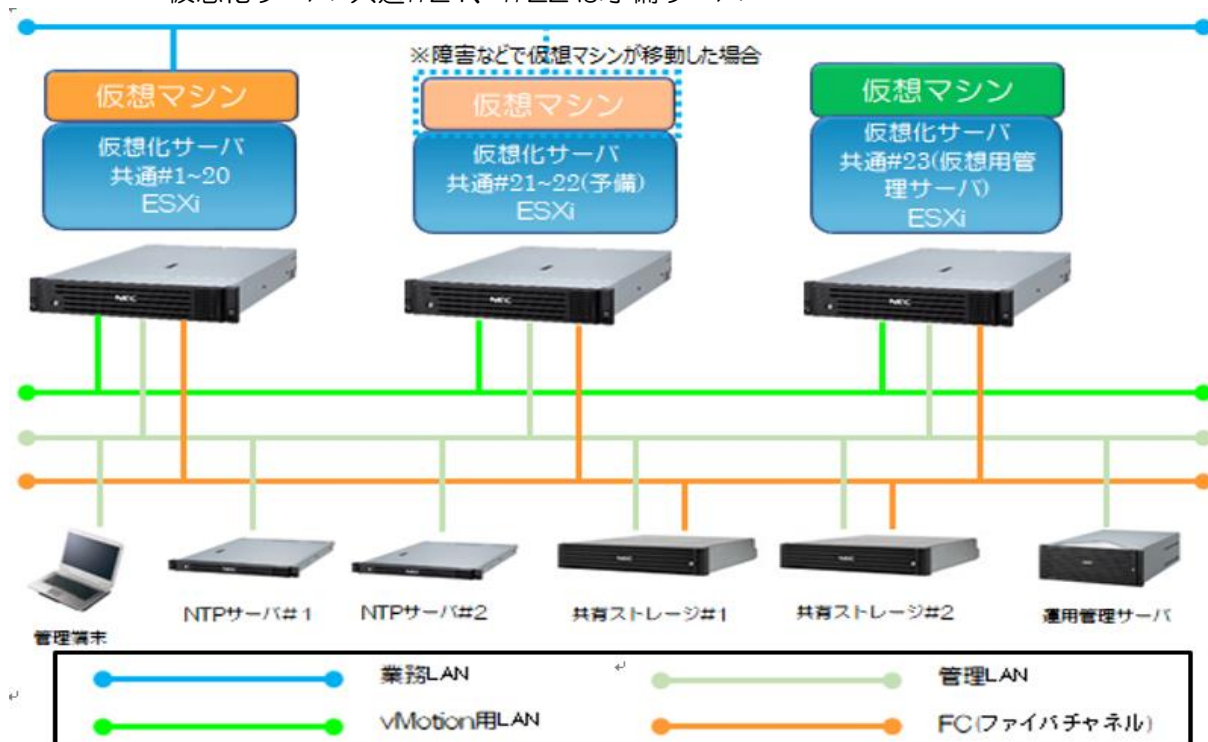


図3-3 仮想化サーバ共通用エリア

4. 仮想化サーバ共通システム構成

4.1. ハードウェア構成

仮想化サーバ共通システムを構成するホストサーバ、共有ストレージ、バックアップサーバのスペックは以下のとおりである。

表4-1 スペック一覧

	機器		スペック
1	ホストサーバ (23 台)	CPU	Xeon Gold 6258R (2.7 GHz)
2		メモリ	DDR4-2933 Registered DIMM
3	共有ストレージ (2 台)	仮想マシン領域	SAS SSD (2.5 型) RAID-6/60
4		業務データバックアップ領域	SAS SSD (2.5 型) RAID-6/60
5		1 次バックアップ領域	SAS SSD (2.5 型) RAID-6/60
6	バックアップ サーバ	2 次バックアップ	SATA ディスク (3.5 型 7.2krpm) 独自構成
7		遠隔地バックアップ	SATA ディスク (3.5 型 7.2krpm) 独自構成

※ ホストサーバ と 共有ストレージ間は FC 接続 (16GB)

4.2. ソフトウェア構成

サーバ仮想化基盤に使用するソフトウェアは以下のとおりである。

表4-2 サーバ仮想化基盤で使用するソフトウェア

ソフトウェア名	バージョン	用途	説明
VMware ESXi	7.0 (仮想化サーバ 共通#1～#23)	仮想化 OS	ハイパーバイザー型の仮想化ソフトウェア
VMware vCenter Server	7.0	運用管理	サーバ仮想化基盤を管理するソフトウェア 複数のホストサーバを統合管理する また、仮想マシンに対する操作ログを管理する
VMware vRealize Operations Manager	8.6		性能分析、キャパシティ管理、レポート機能 などを備えた、仮想環境のリソース管理ソフトウェア
VMware NSX-T	3.1	ネットワーク 仮想化	ネットワーク仮想化のプラットフォームソフトウェア ファイアウォール、ロードバランサなどのネットワーク機器をソフトウェア上で構成する
Windows Defender	Windows update で配信される最新バージョン	ウイルス対策	Windows OS で使用するウイルス対策ソフトウェア リアルタイム保護 スキャン保護 改ざん防止機能 アプリケーション監視機能 SmartScreen の機能を備える
Symantec Endpoint Protection	14.3	ウイルス対策	Linux OS で使用するウイルス対策ソフトウェア ウイルスとスパイウェアの対策 ブラウザ侵入防止 (ブラウザ攻撃を自動的に検出して遮断) LiveUpdate (ウイルス定義ファイルの更新) の機能を備える ※Windows OS で使用する場合は、業務所 管課で別途ライセンスを調達する必要がある
SKYSEA	16	セキュリティ 監視	IT 資産の統合運用管理ソフトウェア 保守端末の操作ログの管理 の機能を備える

4.3. ネットワーク構成

サーバ仮想化基盤で利用する主なネットワーク構成は以下のとおりである。

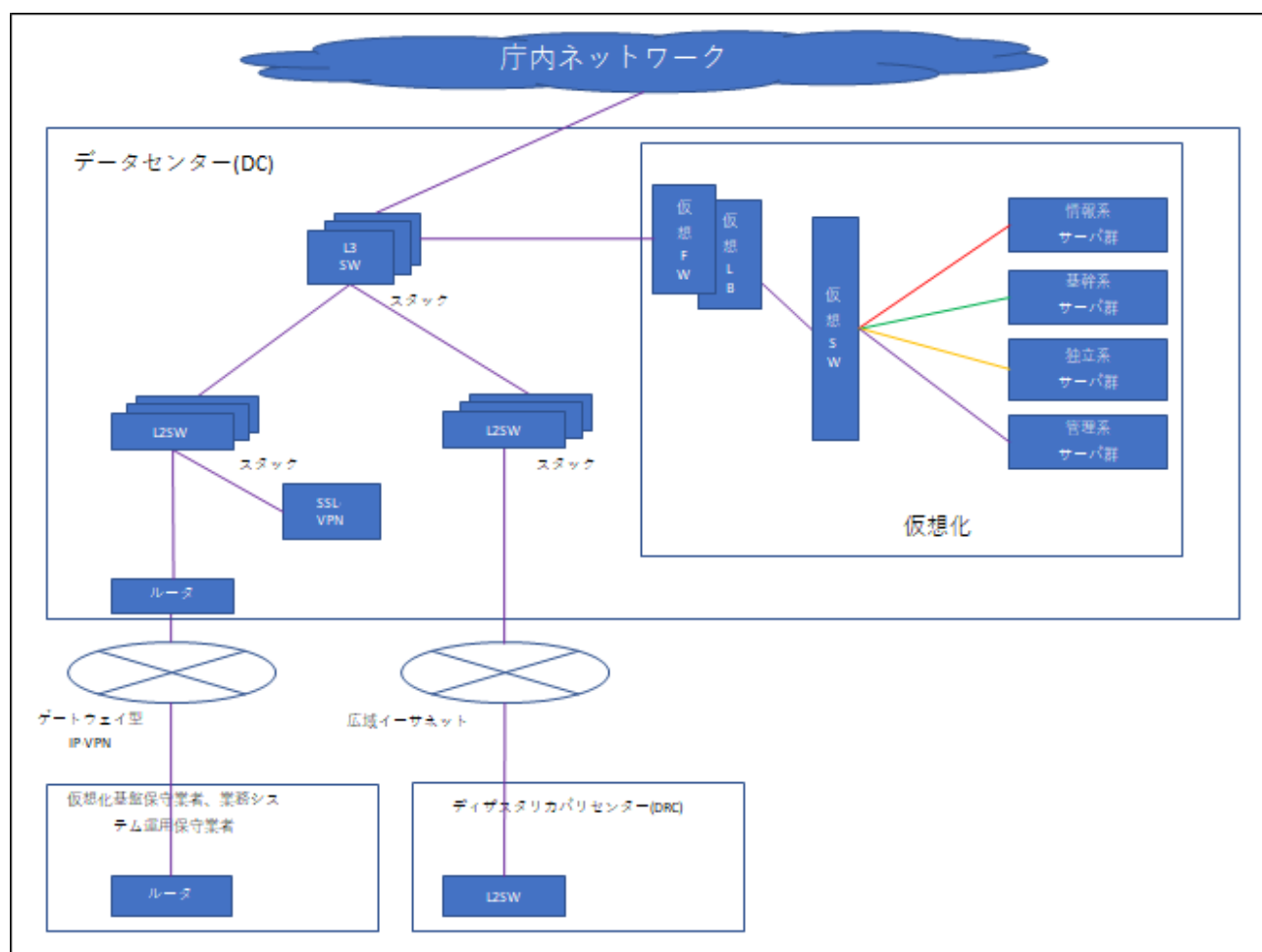


図4-1 ネットワーク構成図

4.4. 共通利用サーバが提供する機能

サーバ仮想化基盤を利用する業務システムは、次の各共通利用サーバが提供する機能を利用できる。

下表の機能を使用する場合は、仮想マシンに対して業務システム運用保守業者にて必要な設定をおこなう。

表 4-3 共通利用サーバが提供する機能

機能	基幹系	情報系	独立系
SEP (ウイルス定義ファイル配信)	基幹系ネットワークが 機能を提供	情報系ネットワークが 機能を提供	サーバ仮想化基盤が 機能を提供
WSUS (Windows OS 系 ウイルス定義ファイル配信 WindowsOS 系 セキュリティパッチ配信)			
NTP (時刻同期用)			
DNS (ドメイン、IP アドレス関連付 け用)			機能提供なし
SMTP (運用監視のアラート通報用 メールサーバ)			

4.5. 耐障害性・可用性

サーバ仮想化基盤で使用するサーバ、共有ストレージ、ネットワーク機器などについては、以下のような耐障害性、可用性を備えている。

4.5.1. サーバ仮想化基盤の可用性

サーバ仮想化基盤では、VMware vSphere HA を使用することで、ホストサーバに障害が発生した場合、その上で稼働していた仮想マシンを自動的に他のホストサーバ上で再起動させ、業務のダウンタイムを最小限に抑える構成としている。

※vSphere HA の詳細については、「5.9.1 vSphere HA」を参照

また、VMware vSphere DRS を使用することで、ホストサーバに負荷が集中した場合、その上で稼働する仮想マシンを別のホストサーバ上に再配置し負荷分散を図る構成としている。

※vSphere DRS の詳細については、「5.8.1 vSphere DRS」を参照

さらに、オーバーコミット機能により、ホストサーバに搭載された CPU 以上に、各仮想マシンに対して CPU を割り当て、最適なりソースコントロールをおこなうことができる。

4.5.2. ネットワークの可用性

サーバ仮想化基盤では、VMware NSX-T のネットワーク仮想化機能を使用することで、業務要件に合わせた柔軟なネットワークサービスを提供する。

分散仮想スイッチ機能では、タグ VLAN に対応したセグメント分割が可能となり、異なるホストサーバで動作する仮想マシンが同一のスイッチに接続したように相互通信ができる。

セグメント分割に考え方として、

- ① 情報系、基幹系、独立系ネットワークセグメント
- ② 各業務単位のネットワークセグメント

単位で分散仮想スイッチを構築することで、ネットワークの負荷分散を図っている。

仮想ファイアウォール機能では、業務システム用ネットワークと上位ネットワーク間の North-South(南北)トラフィックの制御をおこなっている。

仮想ロードバランサ機能では、複数のサーバ間でネットワークトラフィックの負荷分散をおこなっている。

4.5.3. バックアップの信頼性

サーバ仮想化のバックアップは、共有ストレージ内の筐体内複製による「1次バックアップ」、別筐体のバックアップサーバへの「2次バックアップ」および激甚災害等発生の際に対応するためのデータを複製する「遠隔地バックアップ」を備えることにより、障害発生時の復旧をおこなうことができる。

サーバ仮想化基盤のバックアップ機能に関する詳細は、「5.5. バックアップ機能」を参照のこと。

4.5.4. 冗長構成による信頼性

サーバ仮想化基盤で導入しているサーバについて、障害が発生しやすい「HDD」、「電源モジュール」「ファン」については二重化かつ活性保守が可能な構成を採用している。また、障害によるサーバ停止が発生した場合、その上で稼働していた仮想マシンを自動的に他のホストサーバ上で再起動させ業務継続することができる、サーバの冗長構成としている。

共有ストレージについては、デュアルコントローラで構成され、主要部品についても完全二重化しており、部品故障時も業務継続可能な構成としている。

ネットワーク機器は、3 台の機器によるスタック構成としており、1 台で障害が発生しても縮退動作で継続することが可能な構成としている。

障害発生時にも障害の影響を受けることなく障害メッセージを通知できるように運用管理サーバは、無停止型 FT サーバを用いることで物理的に二重化している。

サーバ — 共有ストレージ間の接続経路は冗長化されており、片系障害時には自動的にパス切替がおこなわれる。

表4-4 耐障害性・可用性

装置	耐障害性・可用性
運用管理サーバ	FT（フォルトトレランス）サーバを導入することによる、ハードウェアの部品の二重化
ホストサーバ	ハードディスクのRAID 構成 電源・ファンの二重化 LAN の冗長化 仮想化サーバの冗長構成（稼働 21 台 + 予備 2 台） VMware の vMotion、HA 機能
共有ストレージ	ハードディスクのRAID 構成 電源・ファン・コントローラ・FC（ファイバチャネル）装置の二重化
FC スイッチ	電源・ファンの二重化 FC スイッチ機器の冗長化
ネットワーク機器	電源・ファンの二重化 ネットワーク機器の冗長化
ファシリティ	データセンターの利用

4.5.5. リソースの拡張性

サーバ仮想化基盤で導入しているサーバについて、増設の可能性が高いメモリを拡張可能な構成としている。

共有ストレージについて、拡張筐体であるエンクロージャを追加することで、ディスクを増設可能な構成としている。

5. サーバ仮想化基盤の提供サービス

5.1. 仮想マシン対象 OS

サーバ仮想化基盤のゲスト OS として、下記 OS を提供可能である。

表5-1 対象 OS

Microsoft Windows	Microsoft Windows Server 2022
	Microsoft Windows Server 2019
	Microsoft Windows Server 2016
	Microsoft Windows 11
	Microsoft Windows 10
Linux	Red Hat Enterprise Linux 9
	Red Hat Enterprise Linux 8
	Red Hat Enterprise Linux 7
	CentOS 7

- ※ 今後リリースされる Microsoft Windows、Linux の最新 OS は、サーバ仮想化基盤の提供対象 OS とする。(提供時期は別途調整とする。)
- ※ サーバ仮想化基盤のサポートポリシーとして、サポート期限が終了した OS については提供対象外とし、原則として利用を許可しない。
ただし、サポート期限後まもなくシステムの再構築を控えている等の場合は、デジタル戦略部に相談すること。
- ※ 神戸市職員はマイクロソフト社製品のライセンスについて Microsoft 365 E3 のライセンスを契約、保有しているため Microsoft Windows Server の CAL は調達不要である。(事業者の職員分は必要分を準備すること。)
- ※ 事業者が保守端末で Microsoft Windows 10 もしくは Windows 11 を利用する場合は、事業者にてライセンスを準備する必要がある。また、保守端末より仮想環境に払い出す検証用端末へアクセスする場合は Windows E3 または VDA ライセンスを利用用途により準備する必要がある。

提供する Windows 系ゲスト OS のバージョンについて

OS:

- ・各 OS のセキュリティパッチ未適用状態のバージョン
- ・各 OS の最新セキュリティパッチ適用状態のバージョン

の 2 種類を提供可能

5.2. 提供可能なミドルウェア

サーバ仮想化基盤として提供可能なミドルウェアは下記のとおりである。

表5-2 提供可能なミドルウェア

データベース	Oracle Database Standard Edition 2
	Microsoft SQL Server Standard Edition

表5-3 提供可能なバージョン

製品名	バージョン
Oracle Database 19c Standard Edition	19.3.0
Microsoft SQL Server 2022	
Microsoft SQL Server 2019	
Microsoft SQL Server 2016	

- ※ サーバ仮想化基盤のサポートポリシーとして、サポート期限が終了したミドルウェアについては提供対象外とし、原則として利用を許可しない。
- ※ Microsoft SQL Server の CAL は、サーバ仮想化基盤で用意したプロセッサライセンスを使用するため、調達は不要である。
- ※ 提供可能なバージョンについては定期的に変更となるため、デジタル戦略部に個別に問合せをおこなうこと。

5.2.1. 初期状態

サーバ仮想化基盤で提供する仮想マシンの初期状態は、下記のとおりである。

表5-4 サーバ仮想化基盤で提供する仮想マシンの初期状態

	Windows	linux
コンピュータ名 (ホスト名)	コンピュータ名（ホスト名）については、ヒアリングシートの回答を元に設定。	
ネットワーク設定	NIC1：情報系ネットワーク/基幹系ネットワークの IP アドレス設定 ※IP アドレスは、サーバ仮想化基盤が業務システムに払い出すネットワークから任意に付与 ※IPv6 は無効 ※Windows のファイアウォールは無効 ※linux の iptables による通信制限は無し	
管理者アカウント	ローカル管理者アカウント (Administrator) を引き渡し。	root ユーザ root 権限を持ったユーザを作成 (wheel グループ) sudo を使用し管理者コマンドを実行可能とする
参加ドメイン	ドメインへ未参加の状態引き渡し	無し
停止するサービス	-	<ul style="list-style-type: none"> • smartd サービス • avahi-daemon • blue-tooth • cups サービス • NetworkManager サービス (IP アドレス設定に必要な時は停止しない)
仮想マシンのリソース割り当て	ヒアリングシートで確認した内容を元に、仮想マシンに対してリソースの割り当てを実施する。 (CPU、メモリ、ハードディスク容量、ネットワークインタフェース) Windows は定期的に調査をおこない、リソース過剰と判断できる場合は最適なリソースの再割り当てを実施する。	
パーティション構成	ヒアリングシートで記載された容量、ドライブを割り当て	ゲスト OS の引き渡し時は、下記パーティション構成で提供する。 ただし、「/ (ルート)」の容量については、ヒアリングシートの値で設定 ※「表 5-5 パーティション構成」参照
OS インストール	<ul style="list-style-type: none"> • インストールオプション GUI 使用サーバ (GUI ツールによる管理を可能にするため) 	<ul style="list-style-type: none"> • インストールパッケージ Red Hat Enterprise Linux インストール時に選択できるパッケージグループの内の、[サーバ]パッケージグループ ※Red Hat Enterprise Linux をサーバ用途で使用する場合の基本的なインストールパッケージ • ランレベル 3 (テキストログインモード)
ソフトウェアインストール	<ul style="list-style-type: none"> • VMware Tools (仮想化ユーティリティ) 	<ul style="list-style-type: none"> • Open VMware Tools (仮想化ユーティリティ)
その他	<ul style="list-style-type: none"> • SNP 無効化 • デフラグ無効化 	<ul style="list-style-type: none"> • Ctrl + Alt + Del によるリブート動作の制限

上記内容に記載が無い内容については既定値で設定。

引き渡し時のゲスト OS に含まれない設定、ソフトウェア/パッケージ追加は、業務システム運用保守業者でおこなうこと。

表5-5 パーティション構成

パーティション	サイズ	ファイルシステム	備考
/boot	1GB	ext4/vfs	最小限のサイズを設定(OS により異なる)
/boot/efi	200MB		RedHat Enterprise Linux8 以降
swap	8GB	swap	割り当てメモリ容量に応じて設定 <ul style="list-style-type: none"> ・2GB 未満 : メモリの2倍 ・2GB～8GB : メモリに同じ ・8GB 以上 : 4GB 以上 ⇒サーバ仮想化基盤では 8GB を設定する
/ (ルート)	別途調整	ext4/vfs	OS・データ領域を含む

5.2.2. 同一構成の仮想マシンに関する払い出しについて

業務システムで同一構成の仮想マシンを複数構築する場合、業務システム側で事前に必要なインストール、設定をおこなった仮想マシンをもとに、サーバ仮想化基盤にてクローニングサービスを提供する。

サービス利用にあたっては、業務所管課からの申請により個別対応となる。

その場合の責任分界点として、通常の仮想マシンの払い出しと異なり、クローニングした仮想マシンの基本動作以外の確認は実施しない。

(同一構成の仮想マシンのクローニングを実施する場合、Microsoft Windows サーバに対しては sysprep による SID の再生成、ホスト名、IP アドレス設定のみの実施となる)

5.3. 仮想ネットワーク機能

5.3.1. 仮想ネットワークの構成概要

ゲスト OS のネットワーク設定については、下記セグメント構成となる。

表5-6 ネットワークセグメント構成

セグメント	用途
情報系ネットワーク/ 基幹系ネットワーク/ 独立系ネットワーク	業務システムのサービスを提供するためのネットワークセグメント ※ヒアリングシートを元に決定。

※負荷分散対象サーバについては、仮想ロードバランサに仮想 IP アドレスを別途付与する。

※各ネットワークのインターネット接続はできません。インターネット接続の必要がある機器との通信については、特殊な方法で行う必要があるため、直接デジタル戦略部にご相談ください。

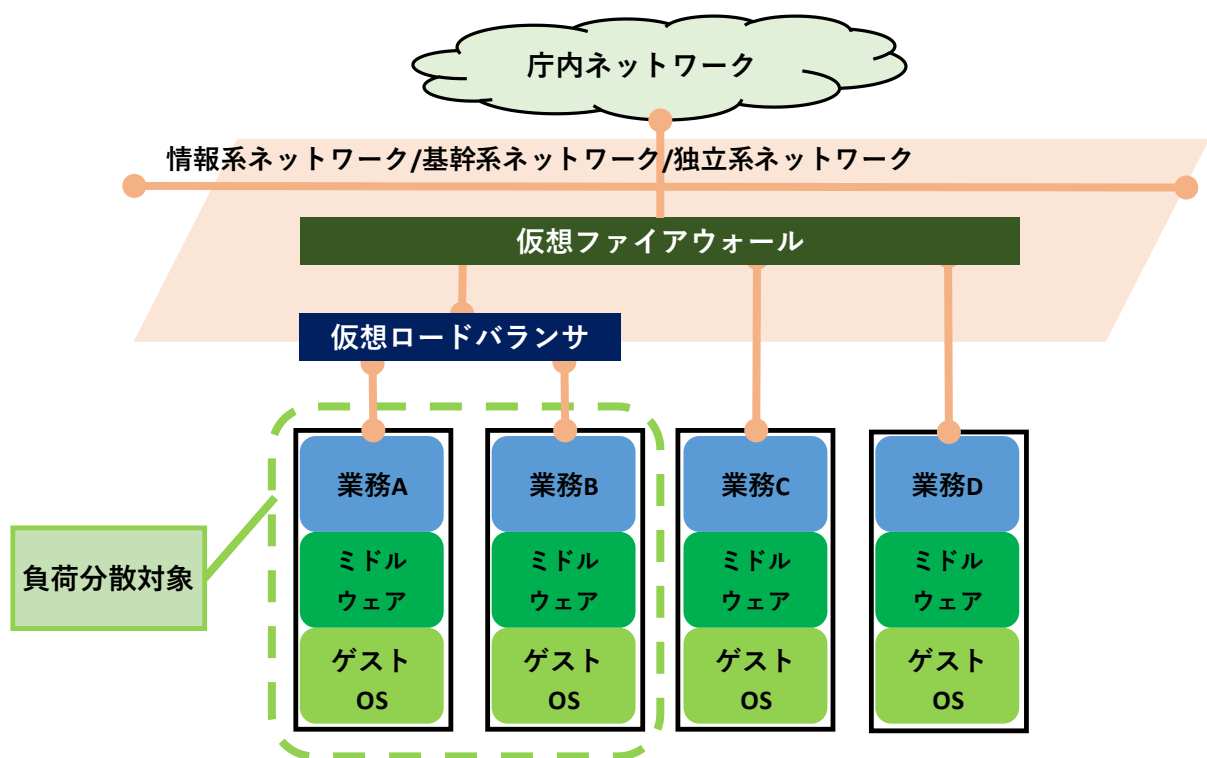


図5-1 仮想マシンと仮想ロードバランサの関連図

5.3.2. 仮想ファイアウォール

仮想ファイアウォールについては、以下のとおりである。

- サーバ仮想化基盤ネットワークに配置する仮想ファイアウォールでファイアウォール機能を提供する。
- 庁内 LAN クライアント端末からサーバ仮想化基盤上で稼動する業務システムへのアクセスについて通信制限を実施。

※仮想ファイアウォールの設定は、業務システム運用保守業者がサーバ仮想化基盤 FW_LB 設定ポータルにて実施。

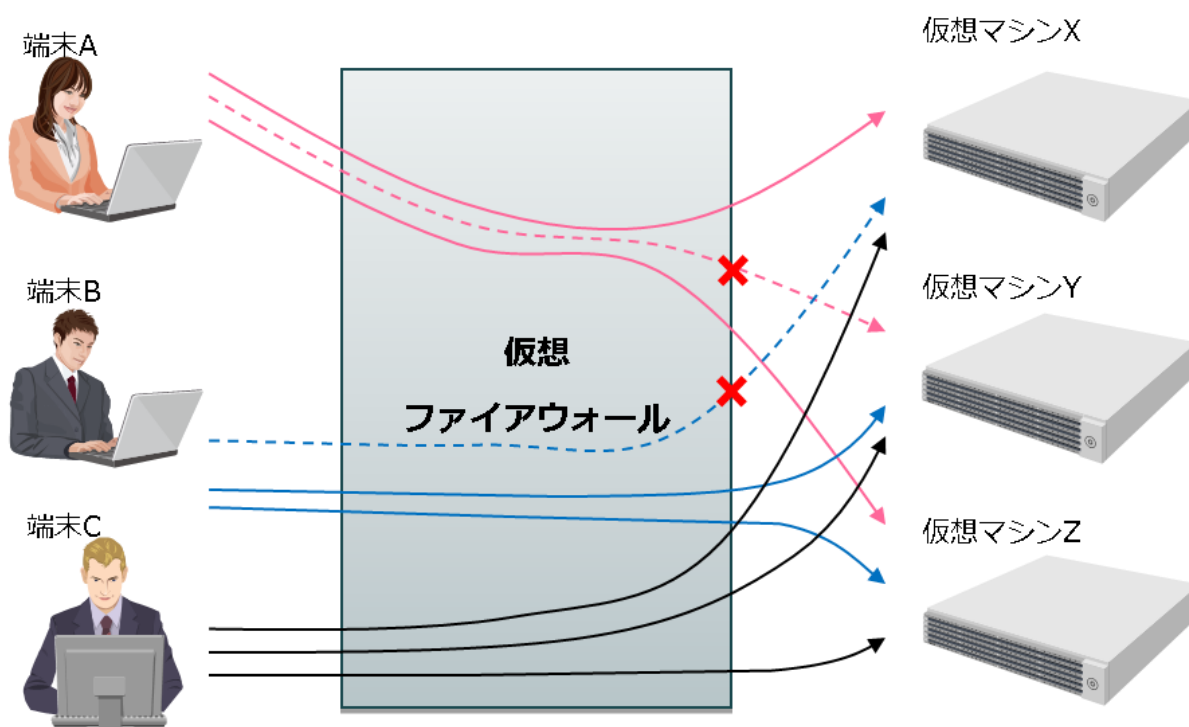


図5-2 仮想ファイアウォールの動き

#	対象仮想マシン	アクセス許可
1	仮想マシン X	端末 A、端末 C
2	仮想マシン Y	端末 B、端末 C
3	仮想マシン Z	全て

5.3.3. 仮想ロードバランサ

仮想ロードバランサについては、以下のとおりである。

- サーバ仮想化基盤ネットワークに配置する仮想ロードバランサで負荷分散機能を提供する。

※負荷分散機能

- (1) レイヤー4/レイヤー7
 - TCP/UDP/HTTP/HTTPS
 - L7 LB Rules
 - (2) パーシステンス
 - 送信元 IP/cookie
 - (3) SSL Termination
 - オフロード/Proxy
 - TLS 相互認証
 - (4) ヘルスチェック
- 庁内 LAN クライアント端末から、サーバ仮想化基盤上で稼働する業務システムへのアクセスについて、同じ機能を有する複数の仮想マシンへ通信を分散させる。
 - 分散先の仮想マシンを複数設定することで冗長性を持たせることができる。

※仮想ロードバランサの設定は、業務システム運用保守業者がサーバ仮想化基盤 FW_LB 設定ポータルにて実施。

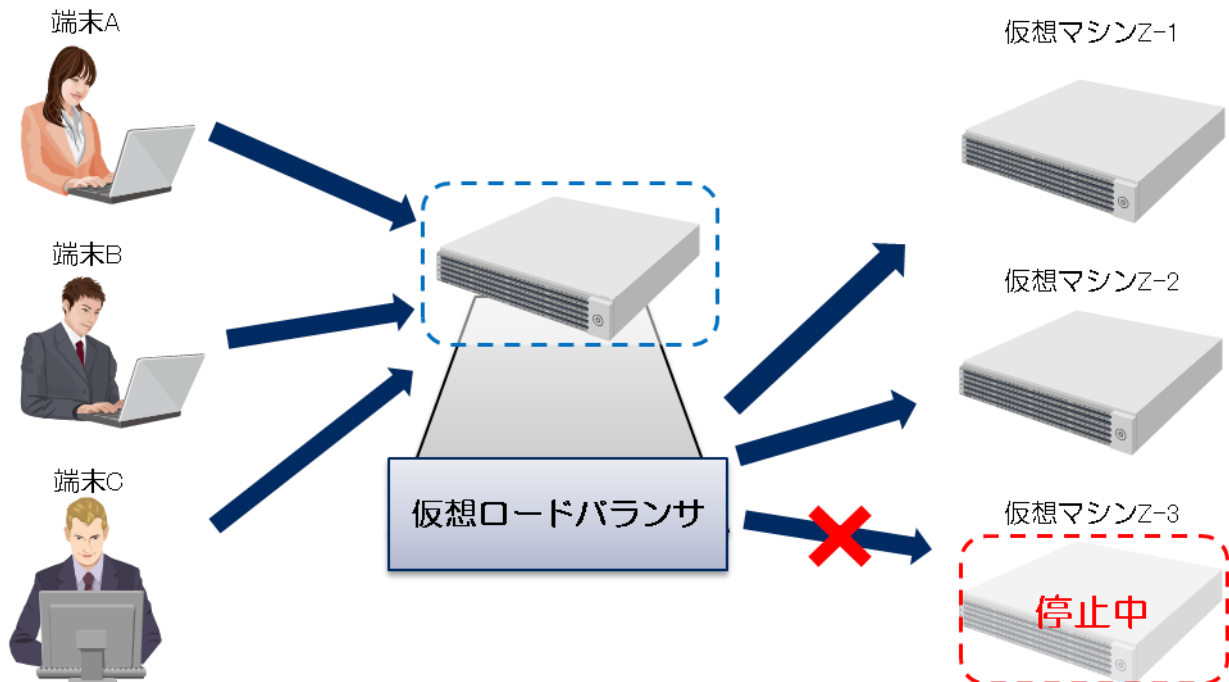


図5-3 仮想ロードバランサの動き

5.3.4. サーバ仮想化基盤 FW_LB 設定ポータル

サーバ仮想化基盤において、業務システムで仮想ファイアウォール、仮想ロードバランサを利用するためには、業務システム運用保守業者で設定する必要がある。
そのため、サーバ仮想化基盤では仮想ファイアウォール、仮想ロードバランサを設定する専用のポータル機能である、サーバ仮想化基盤 FW_LB 設定ポータルを提供する。

5.4. 時刻同期

サーバ仮想化基盤の機器類に時刻同期をおこなうため、NTP サーバを 2 台設置する。
本 NTP サーバは、上位の既設の NTP サーバと時刻同期する。
時刻同期の対象機器にて、上記 2 台の NTP サーバを設定することで、1 台の NTP サーバで障害が発生しても時刻同期は可能である。

基幹系システム、情報系システムについては、本 NTP サーバを使用せず、それぞれの系統の既存の NTP サーバと時刻同期する。

表 5-7 時刻同期の方法

時刻同期の対象	同期先	備考
情報系 LAN 上の仮想マシン	情報系 LAN 上の NTP サーバ	仮想マシン起動時 VMware Tools 経由で時刻同期するが、起動過程で、仮想マシンで設定した NTP サーバの時刻同期で上書きする。
基幹系 LAN 上の仮想マシン	基幹系 LAN 上の NTP サーバ	仮想マシン起動時 VMware Tools 経由で時刻同期するが、起動過程で、仮想マシンで設定した NTP サーバの時刻同期で上書きする。
独立系 LAN 上の仮想マシン	独自の NTP サーバまたはホストサーバ (VMware Tools 経由)	仮想マシン起動時 VMware Tools 経由で時刻同期するが、起動過程で、仮想マシンで設定した業務システム内独自の NTP サーバの時刻同期で上書きする。 ※独自の NTP サーバが存在しない場合、上書きされない。
管理用 LAN 上の機器	サーバ仮想化基盤 LAN 上の NTP サーバ	上位の NTP サーバと時刻同期する必要がある。

<補足>

VMware Tools は下記の特定の操作を実行時、時刻同期が行われます。

- ・再起動やパワーオン操作などで VMware Tools デーモンを開始するとき
- ・サスペンド状態の仮想マシンをレジュームするとき
- ・仮想マシンをパワーオン状態で取得されたスナップショットへ戻したとき

5.5. バックアップ機能

サーバ仮想化基盤で提供するバックアップ機能は下記のとおりである。

5.5.1. 提供するバックアップ機能

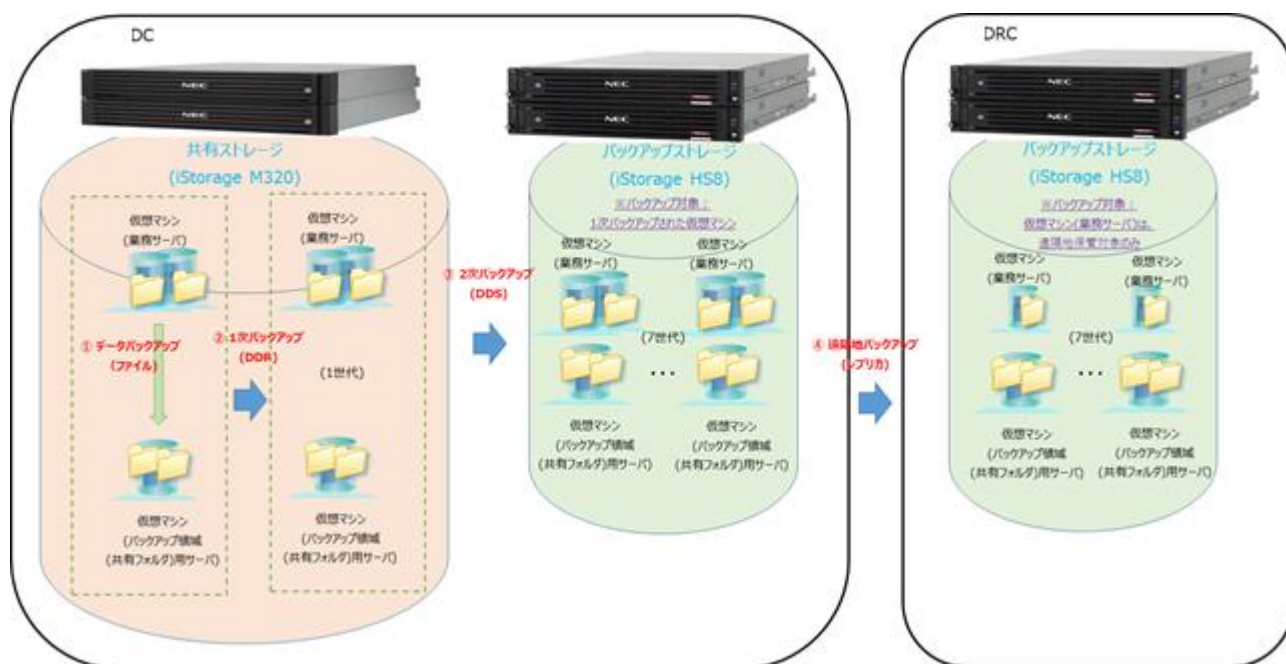


図5-4 提供するバックアップ機能

サーバ仮想化基盤上で稼動する仮想マシンのバックアップは、大きく以下の4通りに分類される。

(1) 業務データバックアップ・・・【日中～3：00】

- ・ 業務システム運用保守業者が実施する、サーバ仮想化基盤が提供するバックアップ領域（共有フォルダ）へのバックアップ（Disk to Disk）

(2) 1次バックアップ・・・・・・【3：00～7：00】

- ・ サーバ仮想化基盤運用保守業者が実施する、バックアップ領域（共有フォルダ）用サーバのイメージバックアップ（Disk to Disk）
- ・ サーバ仮想化基盤運用保守業者が実施する、仮想マシン（業務サーバ）のイメージバックアップ（Disk to Disk）

(3) 2次バックアップ・・・・・・【9：00～15：00】

- ・ サーバ仮想化基盤運用保守業者が実施する、1次バックアップイメージのバックアップ（Disk to Disk）

(4) 遠隔地バックアップ・・・・・・【16：00～24：00（終了まで）】

- ・ サーバ仮想化基盤運用保守業者が実施する、2次バックアップイメージのバックアップ（Disk to Disk）
※バックアップ対象は、遠隔地保管用バックアップ領域（共有フォルダ）用サーバ、およびデジタル戦略部と個別調整で許可された仮想マシン（業務サーバ）が対象となる。

5.5.2. 各バックアップで実施する処理について

表5-8 バックアップ及びリストアの実施内容

#	項目	業務データバックアップ	1 次バックアップ		2 次バックアップ	遠隔地バックアップ
		業務所管課	サーバ仮想化基盤運用保守業者			
1	バックアップ対象（ソース）	データファイル	バックアップ領域（共有フォルダ）用サーバ（仮想マシン）	仮想マシン	1 次バックアップデータ	一部の 2 次バックアップデータ
2	バックアップ先（ディスティネーション）	バックアップ領域（共有フォルダ）	バックアップ格納領域（サーバ仮想化基盤内）		2 次バックアップ用サーバ	遠隔地バックアップ用サーバ
3	バックアップ実施者	業務システム運用保守業者	サーバ仮想化基盤運用保守業者		サーバ仮想化基盤運用保守業者	サーバ仮想化基盤運用保守業者
4	バックアップタイミング	業務システムの運用による	自動スケジュールによる		自動スケジュールによる	自動スケジュールによる
5	バックアップツール	業務システム運用保守業者が準備（スクリプト等）	ストレージの機能		ストレージの機能	ストレージの機能
6	リストア実施者	業務システム運用保守業者（タイミングは任意）	リストア対象を確認の上、サーバ仮想化基盤運用保守業者が実施		リストア対象を確認の上、サーバ仮想化基盤運用保守業者が実施	リストア対象を確認の上、サーバ仮想化基盤運用保守業者が実施
7	リストアタイミング	任意なタイミング	リストア依頼により手動にて実施		リストア依頼により手動にて実施	リストア依頼により手動にて実施
8	リストアツール	業務システム運用保守業者が準備（スクリプト等）	ストレージの機能（DDR）		ストレージの機能（DDS）	ストレージの機能（レプリカ）

※仮想マシンのリストアは、既存の仮想マシンへの上書きおよび新規仮想マシンとしてリストア可能である。

5.5.3. 業務データバックアップの詳細

(1) データバックアップ(ファイル)

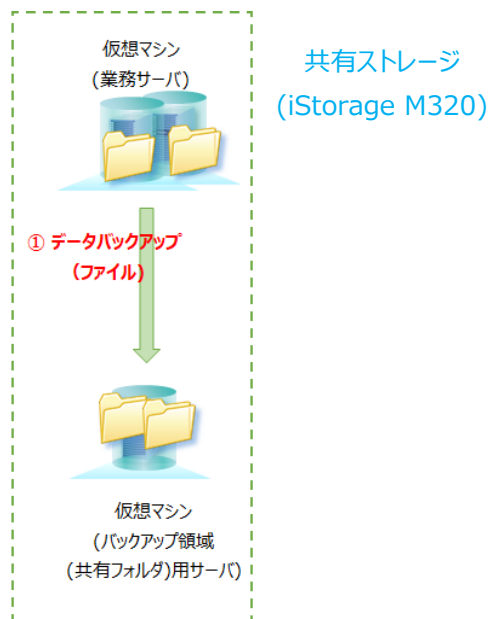


図5-5 データバックアップ

- データバックアップ（ファイル）は、業務システム運用保守業者で実施する。
- サーバ仮想化基盤は、バックアップ領域（共有フォルダ）のみを提供する。
- 業務システム運用保守業者は、バックアップ領域（共有フォルダ）内に業務システムで利用する業務データをバックアップすることができる。
- 業務システム運用保守業者は、バックアップ領域（共有フォルダ）内にバックアップされた業務データをリストアすることができる。
- バックアップ領域（共有フォルダ）に対する業務データのバックアップ・リストアは、業務システム運用保守業者が任意のタイミングで実施できる。
- データを格納するためのツール（スクリプト等）は、業務システム運用保守業者にて準備する。（Microsoft Windows：xcopy、robocopy 等、Linux：cp、rsync 等）

5.5.4. 1次バックアップの詳細

(1) イメージバックアップ (仮想マシン)



図5-6 イメージバックアップ (仮想マシン) のバックアップイメージ

- 1次バックアップ(DDR)は、サーバ仮想化基盤で実施する。
- 1次バックアップ(DDR)は、仮想マシン(業務サーバ)およびバックアップ領域（共有フォルダ）用サーバの仮想マシンのイメージをバックアップする。
- イメージバックアップの取得は、iStorageの筐体内複製機能であるDDR機能を使用するため、仮想マシンの停止は不要であり、ディスク負荷などの業務影響を最小限としている。
- 1次バックアップは、1日1回自動スケジュールで実行する。
- 1次バックアップしたバックアップデータは1世代保管される。
- 1次バックアップでは、バックアップデータは全量保存されるため、リストアするためのベースとして問題なく復旧が可能である。
- 1次バックアップでは、データの圧縮、重複排除の機能はない。
- 1次バックアップでは、更新（差分）のみのレプリケーションがおこなわれる。

5.5.5. 2次バックアップの詳細

(1) イメージバックアップ(仮想マシン)

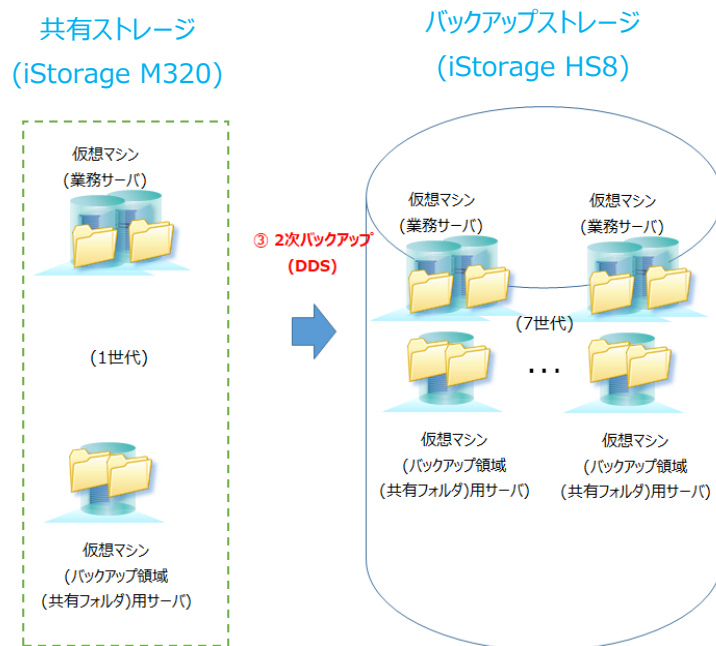


図5-7 2次バックアップ

- 2次バックアップは、1次バックアップされた仮想マシン(業務サーバ)やバックアップ領域(共有フォルダ)用サーバの仮想マシンのイメージを2次バックアップ装置へバックアップする。
- 共有ストレージから2次バックアップ装置へのバックアップは、バックアップ専用LAN (iSCSI)を使用するため、転送時のディスク負荷などの業務影響を最小限としている。
- 2次バックアップは、1日1回自動スケジュールで実行する。
- 2次バックアップしたバックアップデータは7世代保管される。
- 2次バックアップでは、バックアップデータは全量保存されるため、リストアするためのベースとして問題なく復旧が可能である。
- 2次バックアップでは、重複排除の機能はない。
- 2次バックアップでは、データの圧縮がおこなわれる。
- 2次バックアップでは、更新(差分)のみのレプリケーションがおこなわれる。

5.5.6. 遠隔地バックアップの詳細

(1) イメージバックアップ(仮想マシン)

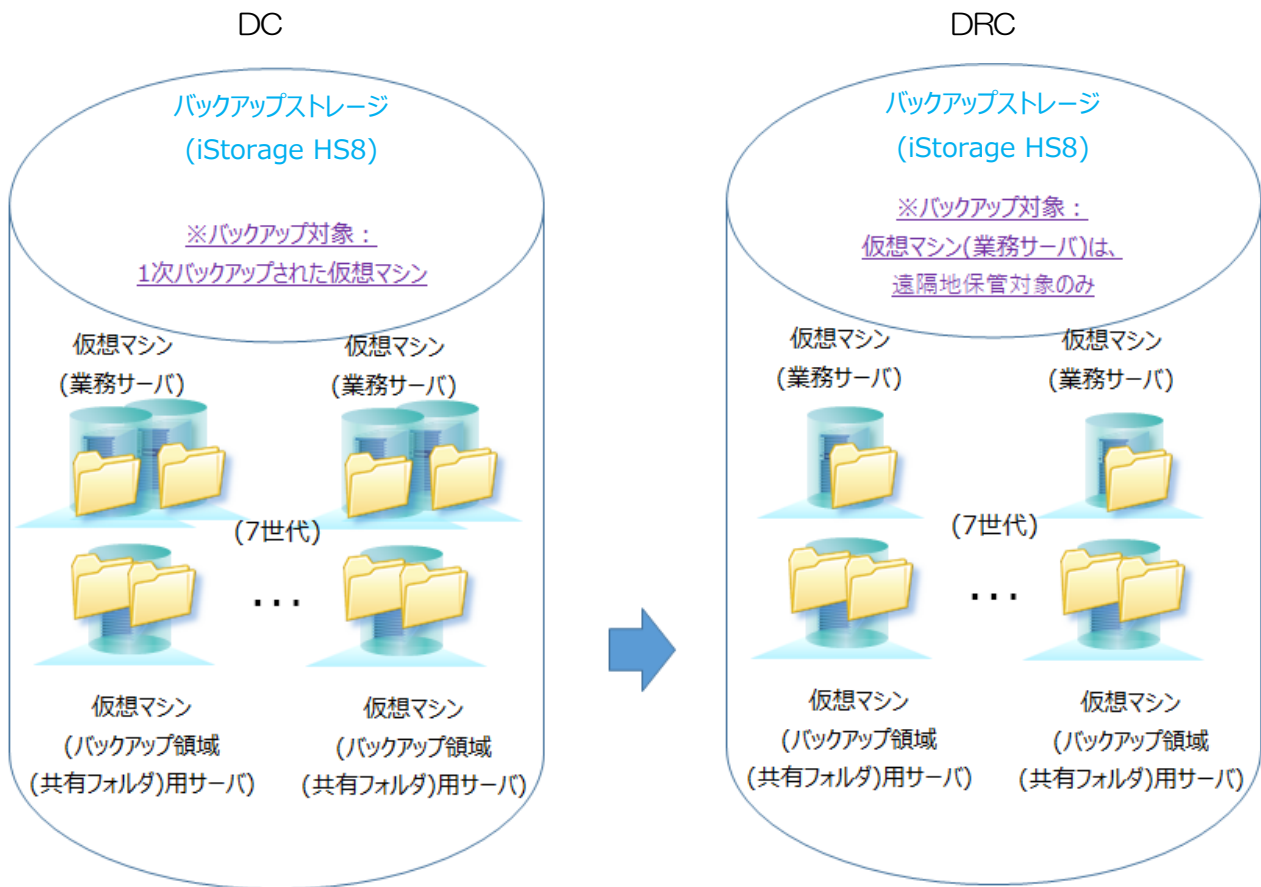


図5-8 遠隔地バックアップ

- 遠隔地バックアップは、2次バックアップされたバックアップ領域（共有フォルダ）用サーバの仮想マシンや、デジタル戦略部と個別調整で許可された仮想マシン（業務サーバ）のイメージを遠隔地バックアップ装置へバックアップする。
- 仮想マシンのイメージバックアップは、1日1回自動スケジュールで転送する。
- イメージバックアップで取得したバックアップデータは7世代保管される。
- バックアップの対象は、遠隔地保管用バックアップ領域（共有フォルダ）用サーバの仮想マシンおよび遠隔地保管が必要な仮想マシンのみをバックアップ対象とする。
- 遠隔地バックアップでは、バックアップデータは全量保存されるため、リストアするためのベースとして問題なく復旧が可能である。
- 遠隔地バックアップでは、重複排除の機能はない。
- 遠隔地バックアップでは、データの圧縮がおこなわれる。
- 遠隔地バックアップでは、更新（差分）のみのレプリケーションがおこなわれる。

5.5.7. バックアップ機能

サーバ仮想化基盤で提供するバックアップは下記のとおりである。

表5-9 バックアップ機能

	業務データ バックアップ	1 次 バックアップ	2 次 バックアップ	遠隔地 バックアップ
バックアップ 単位	バックアップ 領域(共有フォルダ)	仮想マシン	仮想マシン	仮想マシン
バックアップ 頻度	業務システム 側で随時 (日中～3:00)	日次 (3:00 ～ 7:00)	日次 (9:00 ～ 15:00)	日次 (16:00 ～ 24:00 (終了まで))
管理する 世代数	—	1 世代	7 世代	7 世代

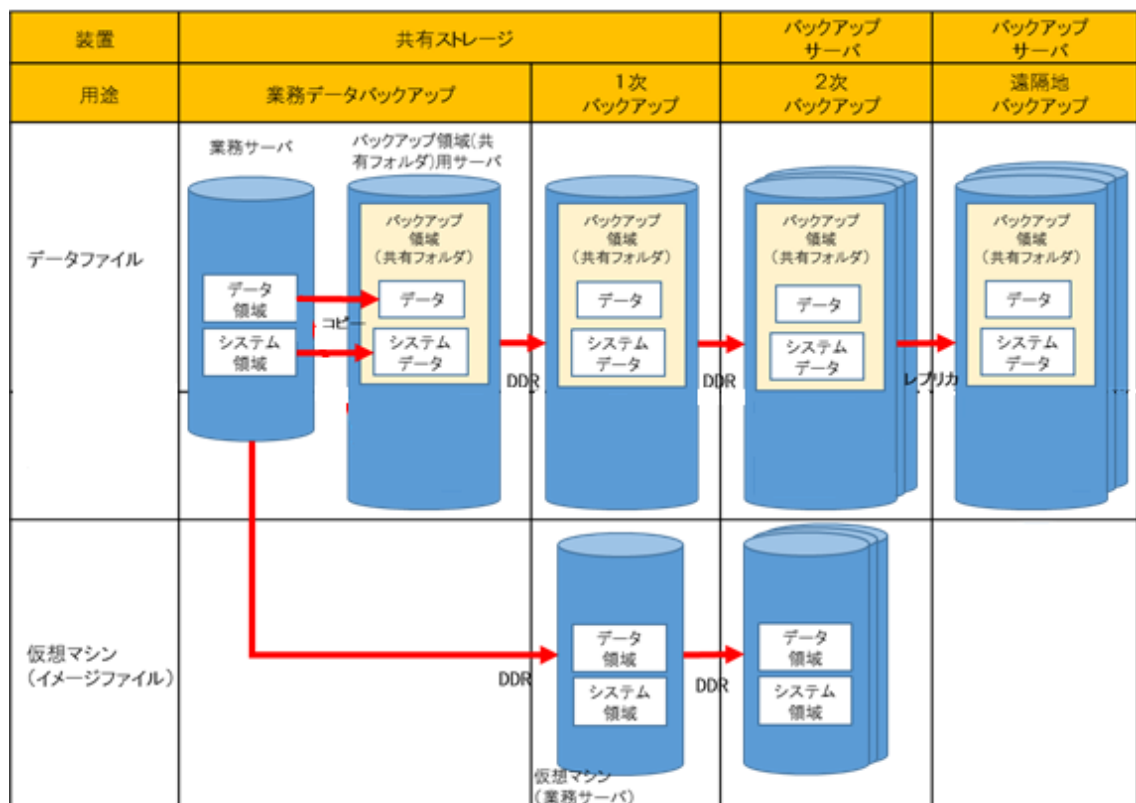


図5-9 バックアップ単位

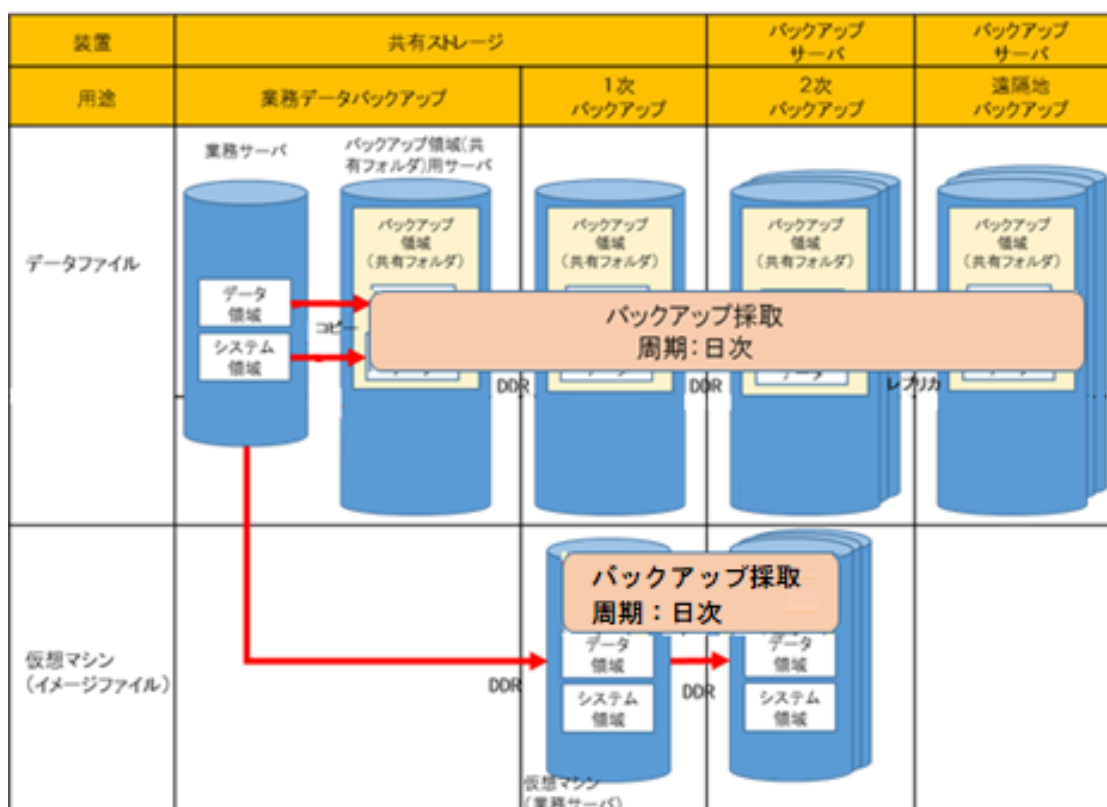


図5-10 バックアップ頻度

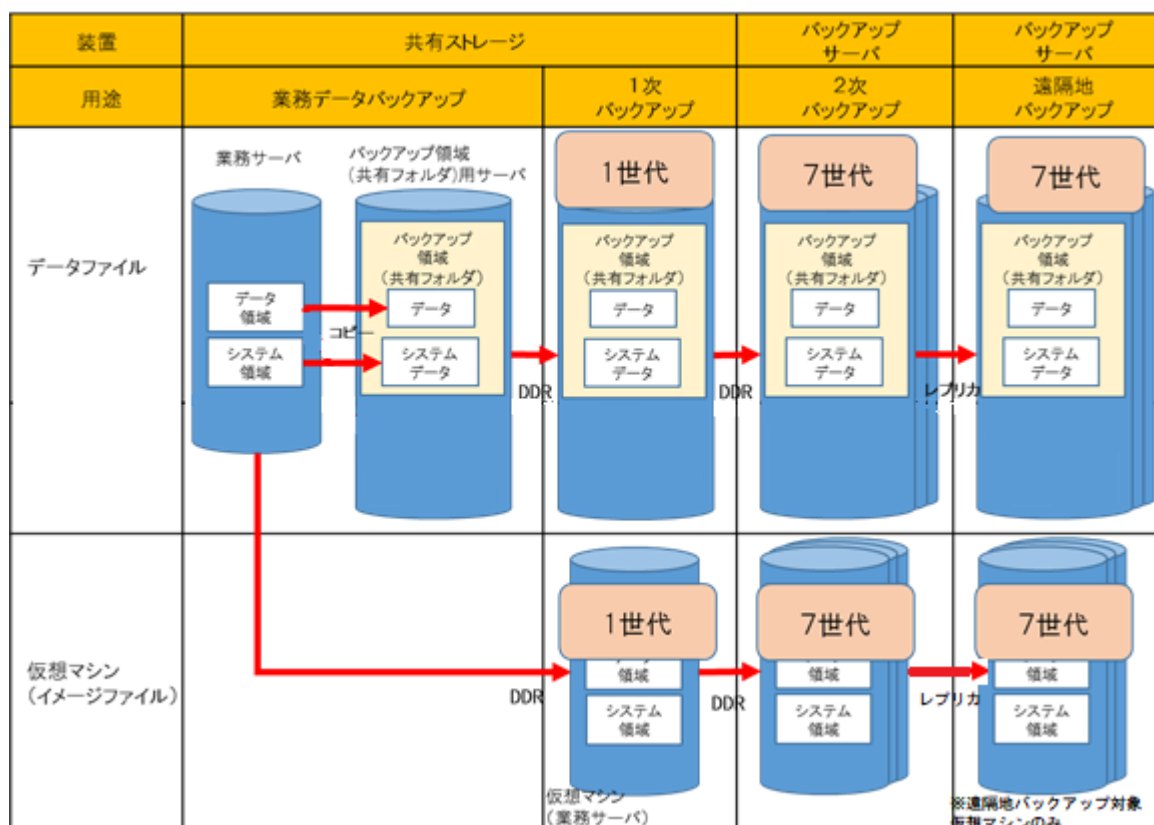


図5-11 バックアップ管理世代

5.6. クローン機能

サーバ仮想化基盤運用保守管理者は、業務システム運用所管課の依頼で仮想マシンのクローンを取得する。取得した仮想マシンのクローンは依頼に応じて利用可能な状態にする。

【使用想定】

- 仮想マシン自体の保守作業時(パッチ適用、ソフトウェアバージョンアップなど)。

なお、仮想マシンのクローンは原則として 1 週間保持した後、削除する。

5.7. 保守機能

5.7.1. 保守環境

サーバ仮想化基盤の仮想マシンの保守環境は以下のとおりである。

- ゲートウェイ型閉鎖 IP-VPN 網を利用したリモート保守端末
(各業務システムでは運用保守に必要な台数を設置可能)
- 庁内に設置された保守用端末 (1 号館サーバ室内 L2 スイッチを接続点として管理系ネットワークに接続)
1 号館 10 階のセキュリティエリアに共有端末を 6 台設置

いずれの端末も SSL-VPN を利用して保守環境に接続する必要があるため、事前にデジタル戦略部に SSL-VPN 利用申請を提出。

申請を受理した後、個人単位にワンタイムパスワードトークンの払い出しをおこなう。

※庁内のネットワーク環境などから、リモートデスクトップでの仮想マシンへのアクセスはおこなわないこと。但し、接続元の端末、接続先の仮想サーバともに、操作者を特定したうえでの操作ログの取得ができていない場合はこの限りではない。

5.7.2. 保守回線

サーバ仮想化基盤の仮想マシンの保守をおこなうための保守回線として、NTT 西日本の「フレッツ・VPN ワイド」を提供する。業務システム運用保守業者が利用するためのフローは以下のとおりである。

なお、現在は NTT 西日本のサービス提供地域からのみ接続が可能であり、NTT 東日本のサービス提供地域からの接続はできない。

- ① (光回線を新設する場合のみ) 光回線の手配 (業務システム運用保守業者)
光回線を新設する場合は、NTT 西日本へ回線の手配をおこなう。
(注) 保守環境を利用できる回線は、最大 100Mbps 又は 200Mbps のファミリータイプ、マンションタイプ、ファミリー・ハイスピードタイプ、マンションハイスピードタイプのフレッツアクセスサービスのみ。
(フレッツ光ネクストの「ファミリー・スーパーハイスピードタイプ集」、「マンション・スーパーハイスピードタイプ集」及び「ビジネスタイプ」は対象外。)
※詳細は、NTT 西日本に確認すること。

- ② 保守用回線申込申請書及び同意書の提出 (業務所管課)
所定の様式 (デジタル戦略部から提供) にてデジタル戦略部へ申請書を提出する。
なお、申請に必要な項目は以下のとおりである。
 - 利用開始希望日
 - 対象システム (情報システムコード、システム名称)
 - 保守事業者 (会社名、責任者、連絡担当者、電話番号、E-mail)
 - 保守回線情報 (契約名義、回線利用場所、利用回線の回線 ID)

上記の申請書と併せて、「フレッツ・VPN ワイド」の利用にかかる同意書 (業務システム運用保守業者の署名および押印が必要) を提出する。

- ③ 申請書の受付（デジタル戦略部）
デジタル戦略部から（業務所管課を経由し）業務システム運用保守業者へ申請受付連絡をおこなう。
- ④ フレッツ・VPNワイドの工事手配・実施（NTT西日本）
保守回線の工事手配を実施する。
工事手配から工事完了まで2週間程度かかる。
- ⑤ 回線認証情報の提供（デジタル戦略部）
業務システム運用保守業者から VPN を利用するための以下の回線認証情報を（業務所管課を経由し）業務システム運用保守業者へ提供する。
 - ・ユーザID
 - ・ユーザPW
 - ・VPN 暗証番号
 - ・企業識別子
 - ・IPアドレス

なお、保守回線利用料、VPN 利用料（月額 1,800 円）及び保守端末については、業務システム運用保守業者の費用負担となる。

（注）保守ネットワークは複数の事業者が共用するので、通信の許可範囲をサーバ仮想化基盤のサーバ群に限定するようフィルタリング設定をおこなうこと。

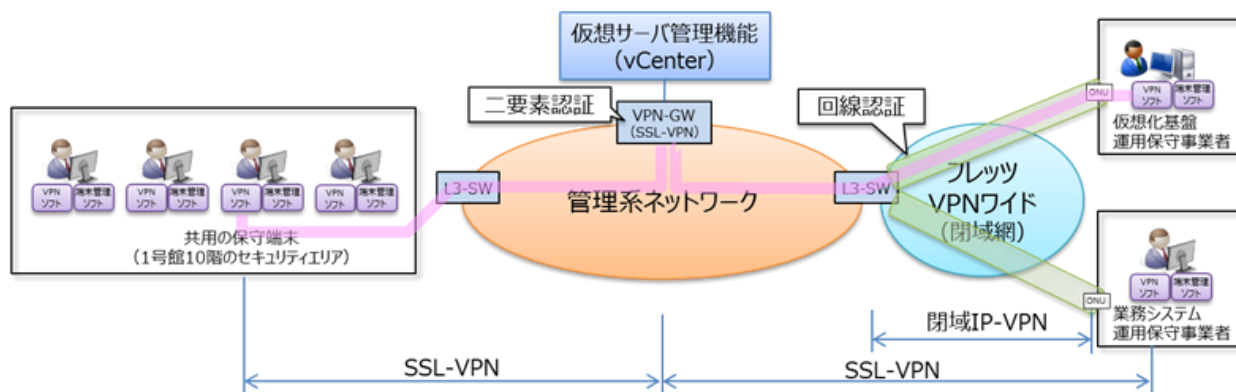


図5-12 保守機能の概要

5.7.3. 保守端末

保守端末を使用する場合、標準機能、フリーソフトウェアあるいはサーバ仮想化基盤がライセンスを保有する以下のソフトウェアを提供するので、端末に導入すること。
対象 OS は Microsoft Windows10 もしくは Microsoft Windows11 とする。

表5-10 導入が必要なソフトウェア

導入が必要なソフト	説明
CISCO Any Connect	VPN 接続用
Microsoft Edge	vCenter Server に接続するためのブラウザ
VMware Remote Console	vCenter Server に接続する際のコンソール機能
Windows Defender	ウイルス対策ソフト
SKYSEA Client View	セキュリティ監視 保守端末に接続するデバイスの制御

※vCenter Server に接続するためのブラウザとして、Mozilla FireFox、Google Chrome を使用することもできるが、使用する場合は業務システム運用保守業者側で準備すること。

保守端末からは、VMware vCenter Server またはサーバ仮想化基盤 FW_LB 設定ポータルへ接続し、操作をおこなう。
利用可能な主な機能は、以下のとおり。

vCenter Server

- (1) コンソールの起動 (ゲスト OS へのログイン)
- (2) 仮想マシンの起動/停止
- (3) スナップショットの作成/削除
- (4) USB デバイスの利用
- (5) 仮想マシンのハードウェア情報の参照
- (6) 仮想マシンのパフォーマンス(CPU、メモリ、ディスク、ネットワークなど)の参照
- (7) タスク、イベントの参照
- (8) 監視(アラーム定義)の個別設定

サーバ仮想化基盤 FW_LB 設定ポータル

- (1) ゲートウェイファイアウォールの設定、確認
- (2) ロードバランサの設定、確認

保守端末は以下のとおり管理すること。

- ・情報の取り扱いは神戸市情報セキュリティ基本方針、神戸市情報セキュリティ対策基準に準拠する。
- ・情報漏えい等を防止するために、保守端末及び付属機器を適切な場所に設置する。
- ・ネットワークは保守を実施するための専用回線とすること。インターネットへの接続や企業内 LAN との接続をしないこと。
- ・保守端末自体をリモート保守の目的以外に利用しない。

5.8. パフォーマンス管理

サーバ仮想化基盤上のホストサーバにかかる負荷を平準化し、サーバリソースの最適化と仮想マシンのパフォーマンス劣化の防止をおこなう機能について記載する。

5.8.1. vSphere DRS

表 5-11 vSphere DRS の実装内容

ツール	実装内容
vSphere DRS	特定のホストサーバに負荷が集中した場合、その上で稼働する仮想マシンを別のホストサーバ上に再配置し負荷分散を図る。 再配置の実施方法については、以下のとおりである。 <ul style="list-style-type: none">• 自動化レベル• アフィニティルール

5.8.2. vSphere DRS の自動化レベル

起動時および起動後の仮想マシンを配置する際に自動化する範囲を、以下 3 種類の自動化レベルから設定する。

サーバ仮想化基盤の vSphere DRS の自動化レベルについては、仮想マシンの起動時にクラスタ内ホストサーバ間のリソースの最適化を図るため、「一部自動化」である。

表 5-12 vSphere DRS の自動化レベル

自動化レベル	仮想マシン起動時の配置	仮想マシン起動後の移行
手動	推奨する移行先を表示	推奨する移行先を表示
一部自動化	自動で配置	推奨する移行先を表示
完全自動化	自動で配置	自動で配置

(1) 手動

仮想マシンの起動時に、推奨する移行先のホストサーバを表示する。

(2) 一部自動化

仮想マシンの起動時に、適切なホストサーバに仮想マシンを自動的に配置する。
クラスタ内のホストサーバ間でリソースにばらつきが発生した場合、
推奨する移行先のホストサーバを表示する。

(3) 完全自動化

仮想マシンの起動時に、適切なホストサーバに仮想マシンを自動的に配置する。
クラスタ内のホストサーバ間でリソースにばらつきが発生した場合、
自動的に最適なホストサーバへ仮想マシンが再配置される。

5.8.3. アフィニティルールの設定

ホストサーバと仮想マシン、または仮想マシン間で依存関係を定義し、仮想マシンの配置をどのようにおこなうか、以下 2 種類のアフィニティルールにて設定する
サーバ仮想化基盤では、業務システム運用保守業者からヒアリングシートによる申請があった場合のみ、アフィニティルールを設定する。

表5-13 アフィニティルールの種類

アフィニティルール	説明
仮想マシンの包括	仮想マシンを同じホストサーバ内で稼働させたい場合に利用
仮想マシンの分割	仮想マシンを別のホストサーバで稼働させたい場合に利用

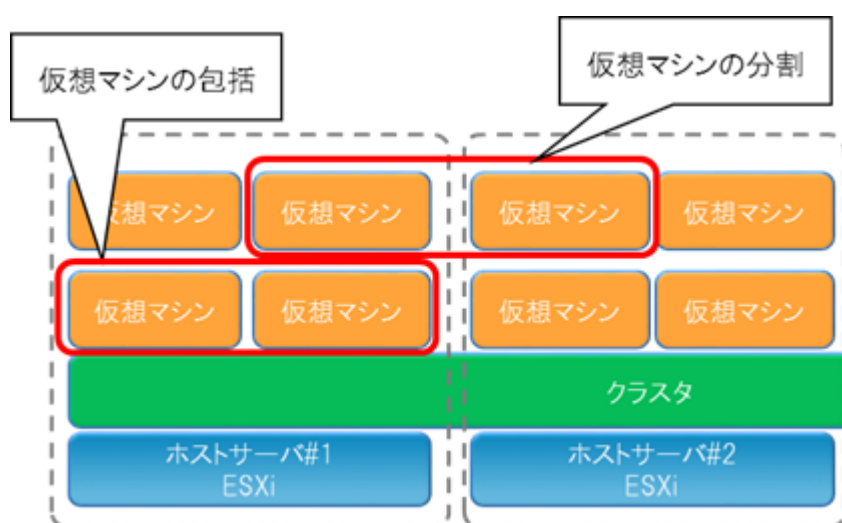


図5-13 アフィニティルールの種類

各ルールの利用ケースは以下のとおりである。

(1) 仮想マシンの包括

仮想マシン間のネットワーク通信が同じホストサーバ上の仮想スイッチのポートグループ内で閉じ、ネットワーク通信の性能とセキュリティの向上が期待できる場合

(2) 仮想マシンの分割

複数の仮想マシンがクラスタソフトにより構成されており、可用性の観点から別々のホストサーバ上で稼働させる必要がある場合

5.9. ホストサーバの冗長化

ホストサーバに障害が発生した場合、その上で稼働していた仮想マシンを自動的に他のホストサーバ上で再起動させ、業務のダウンタイムを最小限に抑えるホストサーバの冗長化機能について記載する。なお、vSphere HA 発生時、数分のダウンタイムがあり、仮想マシンの再起動までにタイムラグが発生する。

5.9.1. vSphere HA

表 5-14 vSphere HA の実装内容

ツール	実装内容
vSphere HA	仮想化サーバ共通用エリアで HA クラスタを構成する。 フェイルオーバーホストには、予備サーバを設定する。

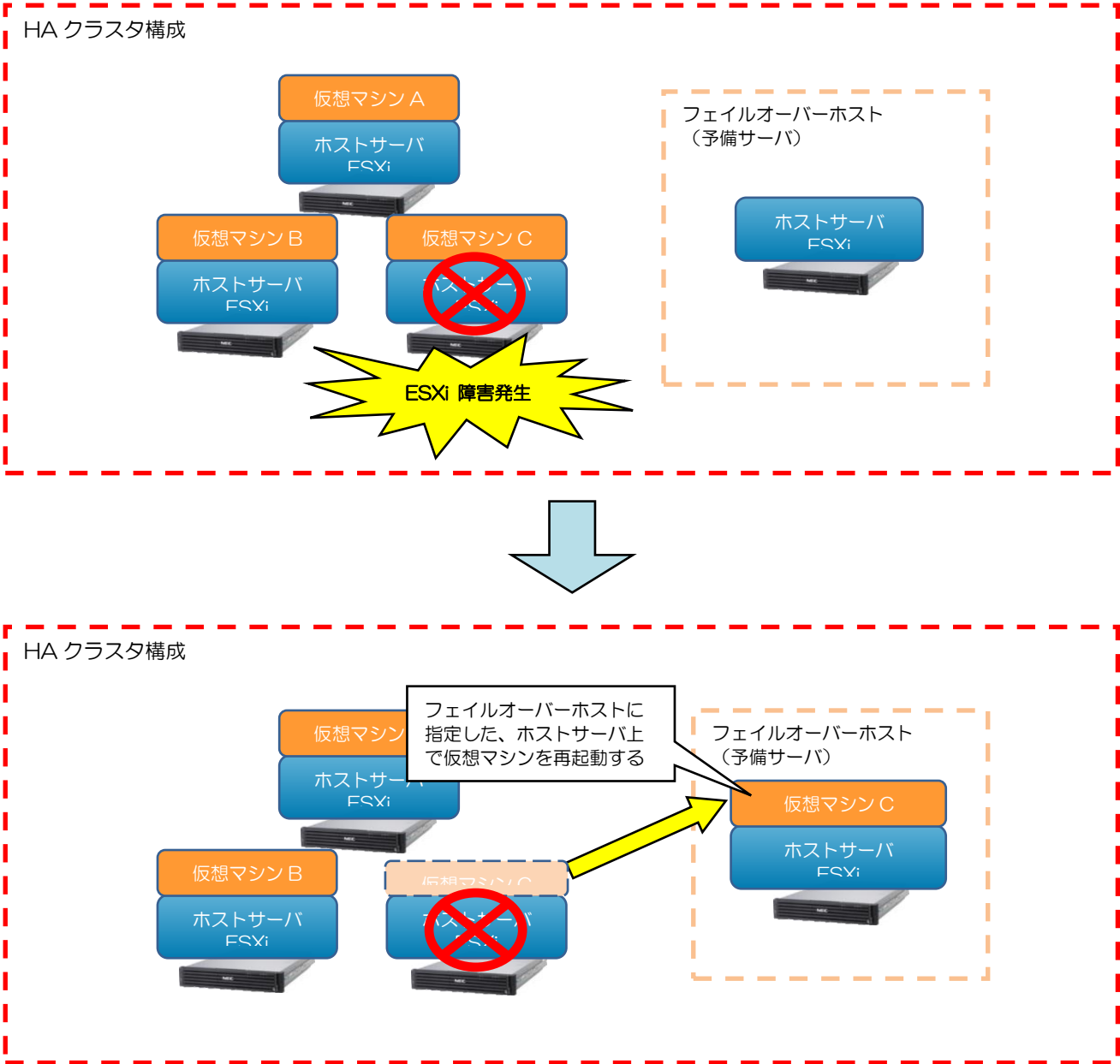


図 5-14 vSphere HA の動き

ホストサーバ23台を1つのクラスタに配置する構成とし、フェイルオーバーホストして2台の予備機サーバ(可変)を配置する。

表5-15 ホストサーバの役割

ホストサーバ	クラスタ	vSphere HA/DRS	役割
仮想化サーバ共通#1～#20	仮想化サーバ 共通 クラスタ	HA：有効 DRS：一部自動 化	業務システム用
仮想化サーバ共通#21、#22			予備機
仮想化サーバ共通#23			サーバ仮想化基盤管理用

5.10. ライブマイグレーション機能

サーバ仮想化基盤では、以下の機能を利用して、ホストサーバのメンテナンス時等に仮想マシン停止せず別のホストマシンへ移動させるライブマイグレーション機能について記載する。

5.10.1. vMotion

表 5-16 vMotion の実装内容

ツール	実装内容
vMotion	ホストサーバのメンテナンス時や負荷分散が必要となった場合に、仮想マシンを停止せず別のホストマシンへ移動させる。

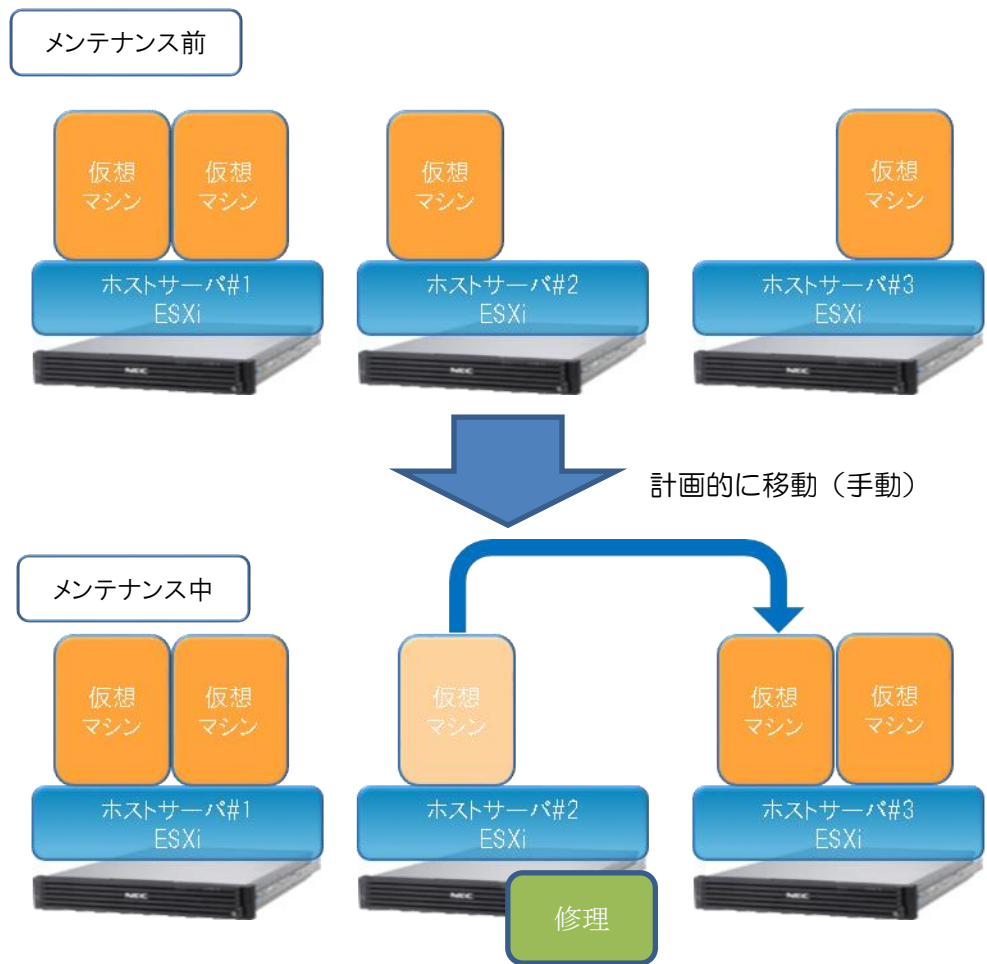


図5-15 vMotion の動き

5.11. 運用監視機能

サーバ仮想化基盤の運用監視機能について記載する。

5.11.1. サーバ仮想化基盤としての運用監視

サーバ仮想化基盤の運用監視は、機能提供するハードウェア、ソフトウェアの障害あるいは仮想化基盤全体の性能などを運用監視ソフトウェアで自動的に監視し、問題発生時にサーバ仮想化基盤運用保守業者へ電話あるいは電子メールで通報することで迅速な対応をおこなうための機能となる。

主な運用監視は以下のとおりである。

表5-17 運用監視

監視項目	監視対象	備考
死活監視	サーバ仮想化基盤を構成するハードウェア ・サーバ ・共有ストレージ ・ネットワーク機器 ・仮想マシン(サーバ仮想化基盤管理用) など	
障害監視	サーバ仮想化基盤を構成するハードウェア、ソフトウェア ・サーバ ・共有ストレージ ・ネットワーク機器 ・サーバ仮想化基盤関連(vCenter) など	
性能監視	サーバ仮想化基盤を構成するハードウェア ・CPU 使用率 ・メモリ使用率 ・ストレージ負荷状況 など	
リソース監視	サーバ仮想化基盤を構成するハードウェア ・CPU 使用率 ・メモリ使用率 ・ストレージ使用率 など	
セキュリティ監視	SEP を使用している仮想マシン ・ウイルス発生状況	Windows Defender を使用している仮想マシンは対象外
バックアップ監視	サーバ仮想化基盤の仮想マシン ・1 次バックアップ ・2 次バックアップ ・遠隔地バックアップ	

表5-18 サーバ仮想化基盤の監視機能

監視対象	通報方式	通報方法
サーバ仮想化基盤のハードウェアに対する監視	メール	<p>サーバ仮想化基盤で使用しているハードウェア機器の障害については、エクスプレス通報にて、ネットワークで提供する SMTP サーバ経由で通報メールを保守センターに送信する。</p> <p>vCenter Server で検知した障害については、ネットワークで提供する SMTP サーバ経由で通報メールを自動電話通報サービス（Automatic Message Call（以下、AMC））もしくはサーバ仮想化基盤運用保守業者へ送信する。</p> <p>AMC は、送付された通報メールを仕分けて、自動的にサーバ仮想化基盤運用保守業者に電話通報する。</p>

5.11.1. 業務システムにおける運用監視

業務システムにおける運用監視は、主に業務システムの仮想サーバに対する障害や運用状況を監視するための機能となる。

業務システムにおける主な運用監視機能は以下のとおりである。

表5-19 業務システムの監視機能

監視対象	通報方式	通報方法
vCenter Server のアラート設定による監視	メール	<p>サーバ仮想化基盤では、vCenter Server でフォルダ、仮想サーバ単位で個別にアラート設定する機能を提供する。</p> <p>上記機能を使用することで、アラート発生時に vCenter Server から SMTP サーバを経由して通報メールを業務システム運用保守業者へ送信することができる。</p>
業務システムで独自の障害監視サーバによる監視	メール	<p>業務システムで独自に構築した障害監視サーバから、ネットワークで提供する SMTP サーバ経由で通報メールを業務システム運用保守業者へ送信することができる。</p>

vCenter Server で設定できる代表的なアラートの種類には以下のものがある。

- 仮想マシンの状態(起動、停止、再起動、レジュームなど)
- 仮想マシンの使用率(CPU、メモリ、ネットワーク)
- vSphere HA 関連 など

5.12. セキュリティ管理

5.12.1. セキュリティパッチ

セキュリティパッチに関するサーバ仮想化基盤の運用は以下のとおりである。

表5-20 セキュリティパッチの運用

作業項目	作業内容
セキュリティパッチの情報の収集	各メーカーから提供される各ソフトウェアに対するセキュリティパッチの情報を収集する。
セキュリティパッチの取得・提供	OS (Windows、Linux)、ミドルウェアのセキュリティパッチを取得し、必要に応じて共有フォルダ上へ提供する。 (Windows 関連のセキュリティパッチは、WSUS で自動取得する。)
セキュリティパッチの適用	業務システムの仮想サーバに対しては、業務システム運用保守業者にて必要に応じて手動でセキュリティパッチを適用する。 (Windows 関連のセキュリティパッチは、WSUS からの適用を可能とする。) サーバ仮想化基盤関連のサーバに対しては、サーバ仮想化基盤運用保守業者にてセキュリティパッチを適用する。 保守端末については、最新のセキュリティパッチが WSUS を経由して自動的に適用される。

(1) セキュリティパッチ適用フロー (業務システム運用保守業者分)

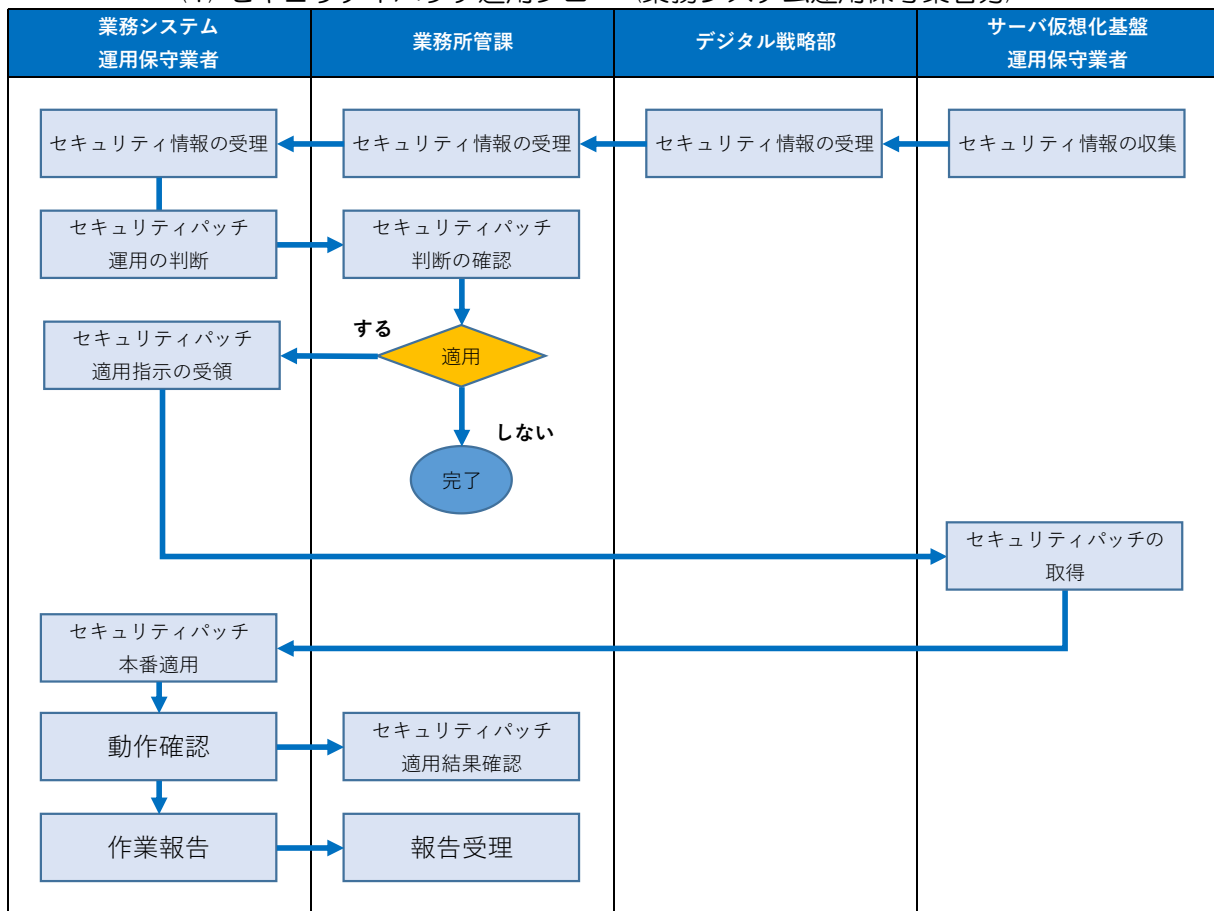


図5-16 セキュリティパッチ適用フロー (業務システム運用保守業者分)

5.12.2. ウイルス定義ファイルの更新

ウイルス定義ファイルの更新に関するサーバ仮想化基盤の運用は以下のとおりである。

表5-21 ウイルスパターンファイルの更新

種類	更新方法
業務システム用仮想マシン	Windows Defender では、定期的に WSUS サーバへ確認、適用する。 SEP は定期的に、SEP サーバよりパターンファイルが配信される。前回更新時からの差分更新となる。
保守端末	Windows Defender では、定期的に WSUS サーバへ確認、適用する。

5.13. 障害時切り分け

サーバ仮想化基盤における障害発生時の対応プロセスについて記載する。

5.13.1. 障害対応プロセス（開庁日業務時間内）

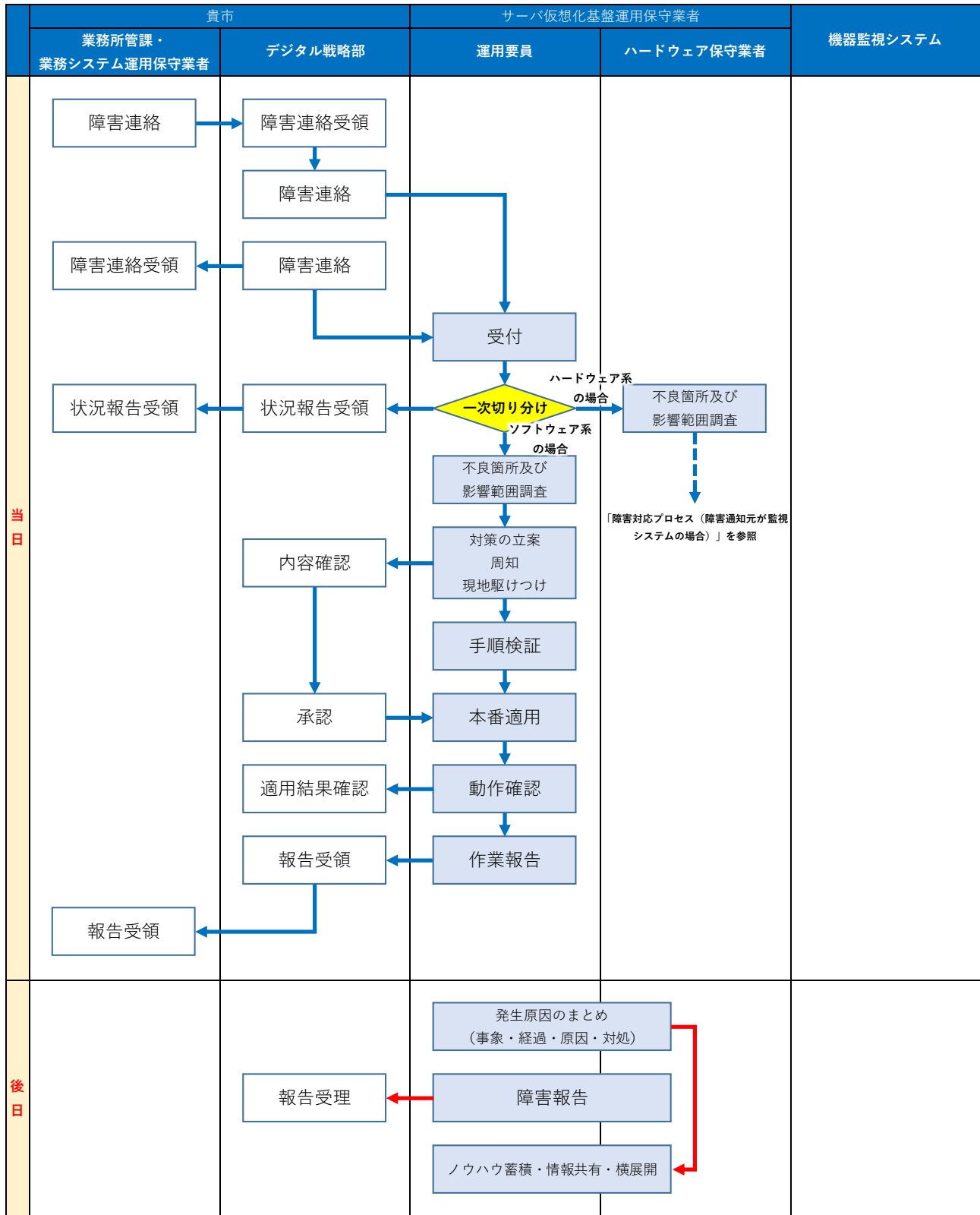


図5-17 障害対応プロセス（開庁日業務時間内）

5.13.2. 障害対応プロセス（開庁日夜間及び休日）

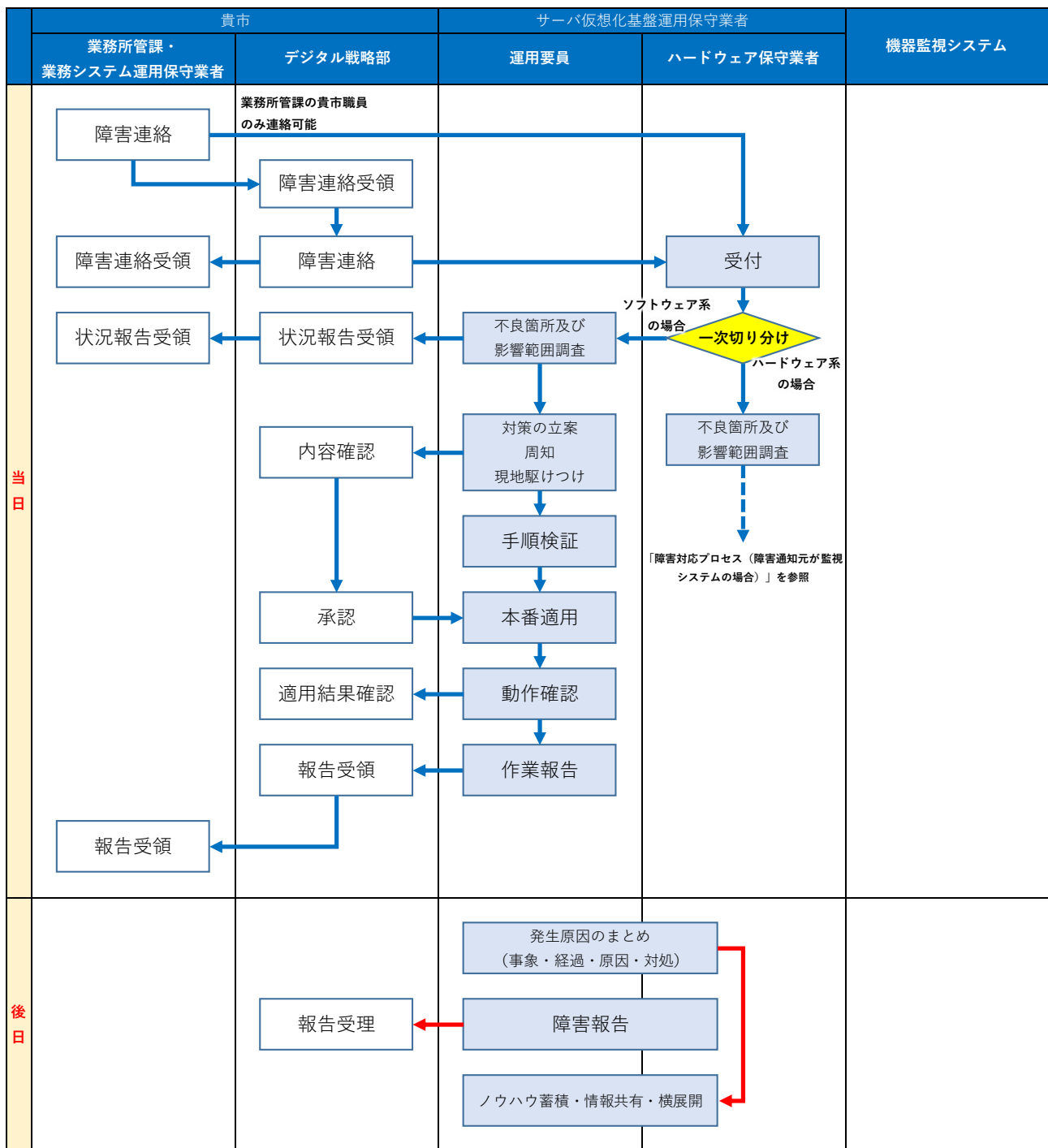


図5-18 障害対応プロセス（開庁日夜間及び休日）

5.13.3. 障害対応プロセス（障害検知元が監視システムの場合）

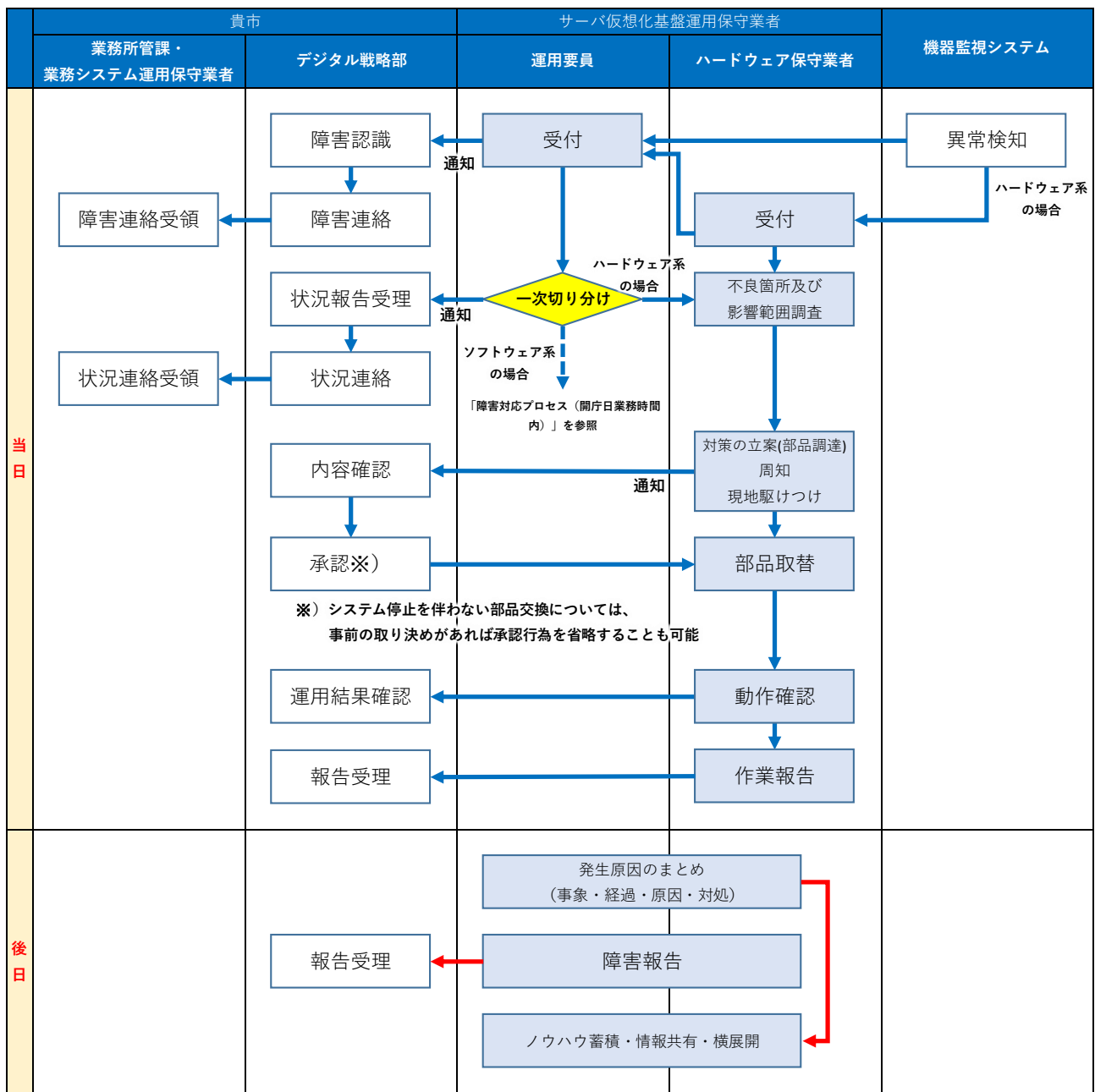


図5-19 障害対応プロセス（障害検知元が監視システムの場合）

6. 責任分界点

サーバ仮想化基盤における仮想マシンに関する責任分界点について記載する。

6.1. 仮想マシン払い出しにおける責任分界点

サーバ仮想化基盤が提供する仮想マシンに対しては、仮想マシン引き渡し前後で責任分界点が以下のように異なる。

6.1.1. 仮想マシン引き渡し時（業務システム導入前）

仮想マシン引き渡し時(業務システム導入前)は、環境変更前に業務システム運用保守業者にて仮想マシンのゲスト OS の動作に問題がないか確認する。発生した問題に関しては、サーバ仮想化基盤運用保守業者にて対応する。

※ 引き渡し直後は、ゲスト OS 部分は責任範囲が重複。

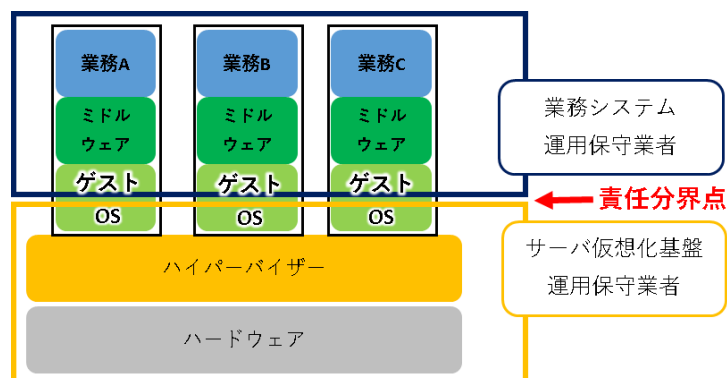


図6-1 仮想マシン引き渡し時の責任分界点（業務システム導入前）

6.1.2. 仮想マシン引き渡し後

業務システム導入後の仮想マシンのゲスト OS、は業務システム運用保守業者の責任範囲となる。

（業務システム導入にあたり、ゲスト OS の環境変更を業務システム運用保守業者が実施するため、サーバ仮想化基盤としてはトラブルシューティングの対応スコープから外れるため）

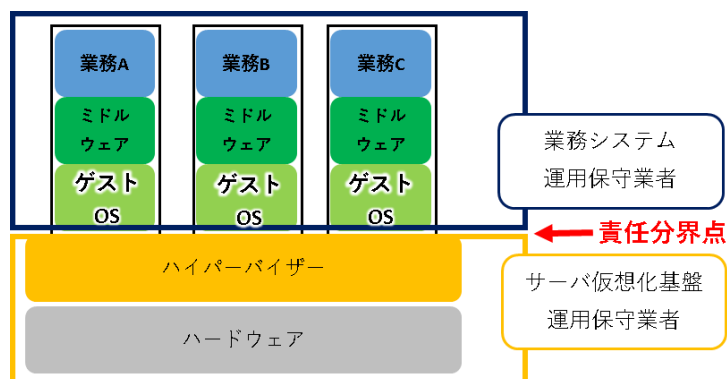


図6-2 仮想マシン引き渡し後の責任分界点

6.2. 運用時の責任分界点

サーバ仮想化基盤の運用・保守における責任分界点は以下のとおりである。

表6-1 運用時の責任分界点 ○：主担当、▲：作業支援

分類	概要	業務所管課・ 業務システム 運用保守業者	デジタル 戦略部	サーバ仮想化 基盤運用保守 業者
定常運用	システム運用	監視（ホストの監視）		○
		バックアップ（データファイル）	○	
		バックアップ（仮想マシン）		○
		仮想マシンの作成 （テンプレートから デプロイした仮想マシン）		○
		仮想マシンの作成 （業務システム運用保守業者で 作成した業務サーバを デプロイした仮想マシン）	▲	○
	問合せ対応	デジタル戦略部からの問い合わせ対応		○
	セキュリティ対策	ウイルス定義ファイルの取得適用、 ウイルス検知の確認	○ (Windows)	○ (Linux)
		セキュリティパッチ情報の収集		○
		セキュリティパッチの取得提供		○
		セキュリティパッチの運用	○	○
障害対応	事前対応	監視機能で障害の前兆が見込まれた場合、 ハードウェア保守業者からの 連絡を受け対応する		○
	発生時対応	発生した障害について、一次切り分け作業 応急処置の実施	▲	○
		発生した障害の原因について、 二次切り分け作業 本格的な復旧作業	▲	○
システム保守	ソフトウェア保守	サーバ仮想化基盤についてバグ対応、 パラメータ更新	▲	○
	機能改修	機能改修要望に対する方針案の検討 方針決定後の改修作業	▲	○
	バージョンアップ	適用を実施するかの方針検討	▲	○
	ハードウェア保守	不具合時の部品交換、定期健診、予防交換 パッチ情報提示、パッチ適用必要性の調査、 パッチ適用作業の実施	▲	○
	ネットワーク保守	N/W構成の維持、 N/W機器（スイッチなど）の保守	▲	○
	ファシリティ保守	電源、空調機などの維持管理	○	
	稼働状況分析	システム性能の情報を収集分析し、 最適なシステム状態を保持する、 または保持するための提案をする		○

7. サーバ仮想化基盤利用時の手続き

7.1. 役割分担

工程ごとの役割分担は以下のとおりである。

表7-1 工程ごとの役割分担 <●：実施 ○：支援 ◎：承認>

	各工程	役割（担当）			
		業務所管課	デジタル戦略部	業務システム 運用保守業者	サーバ仮想化基盤 運用保守業者
①	サーバ仮想化基盤利用に関する説明 （利用ガイドライン）		●		○
②	サーバ仮想化基盤利用に関する打ち合わせ	●	○	●	○
③	引き渡し日程の調整	◎	○	●	○
④	ヒアリングシート（利用申請）の作成、承認	◎	○	●	○
⑤	仮想マシンのデプロイ、動作確認	◎		○	●
⑥	仮想ネットワーク装置のデプロイ、動作確認	◎		○	●
⑦	業務システム構築	◎		●	○
⑧	旧システムからのデータ移行	◎		●	○
⑨	業務システム動作テスト、本番稼働	●		●	○
⑩	サーバ仮想化基盤利用に関する問い合わせ	●	○	●	○

7.2. 支援内容

工程ごとのサーバ仮想化基盤運用保守業者がおこなう支援内容は、以下のとおりである。

表 7-2 支援内容

	各工程	支援内容
①	サーバ仮想化基盤利用に関する説明 (利用ガイドライン)	デジタル戦略部にて、サーバ仮想化基盤を利用する業務所管課及び業務システム運用保守業者向けにサーバ仮想化基盤利用に関する説明を実施する際に、必要に応じて説明の支援を実施する。
②	サーバ仮想化基盤利用に関する打ち合わせ	サーバ仮想化基盤利用に関する調整。要件確定をおこなうために、デジタル戦略部からの依頼に基づき、業務所管課及び業務システム運用保守業者との打ち合わせに同席し、技術的な支援を実施する。
③	引き渡し日程の調整	業務システム運用保守業者にて作成した業務システム構築（移行スケジュール）を基に、業務所管課、デジタル戦略部と協議の上で引き渡し日程の調整を実施する。
④	ヒアリングシート（利用申請）の作成、承認	業務所管課もしくは業務システム運用保守業者で作成するヒアリングシート（利用申請）に関する問い合わせ対応を実施する。
⑤	仮想マシンのデプロイ、動作確認	ヒアリングシート（利用申請）を元に、仮想マシンのデプロイを実施する。また、デプロイ後に基本動作確認を実施する。
⑥	仮想ネットワーク装置のデプロイ、動作確認	ヒアリングシート（利用申請）を元に、仮想ネットワーク装置のデプロイを実施する、また、デプロイ後に基本動作の確認を実施する。
⑦	業務システム構築	業務システム運用保守業者にて業務システムを構築する際のサーバ仮想化基盤に関する問い合わせ対応を実施する。
⑧	旧システムからのデータ移行	業務システム運用保守業者が旧システムからデータ移行する際のサーバ仮想化基盤に関する問い合わせ対応を実施する。
⑨	業務システム動作テスト、本番稼働	業務システムの動作テスト、本番稼働時のサーバ仮想化基盤に関する問い合わせ対応を実施する。
⑩	サーバ仮想化基盤利用に関する問い合わせ	サーバ仮想化基盤利用に関する全般的な問い合わせ対応を実施する。

【期間】

概ね初回説明から 1 カ月程度で仮想マシンの払い出しをおこなう。

（工程①～④：約 3 週間 、 工程⑤～⑥：約 1 週間）

7.3. 時系列

時系列で整理した工程は以下のとおりである。

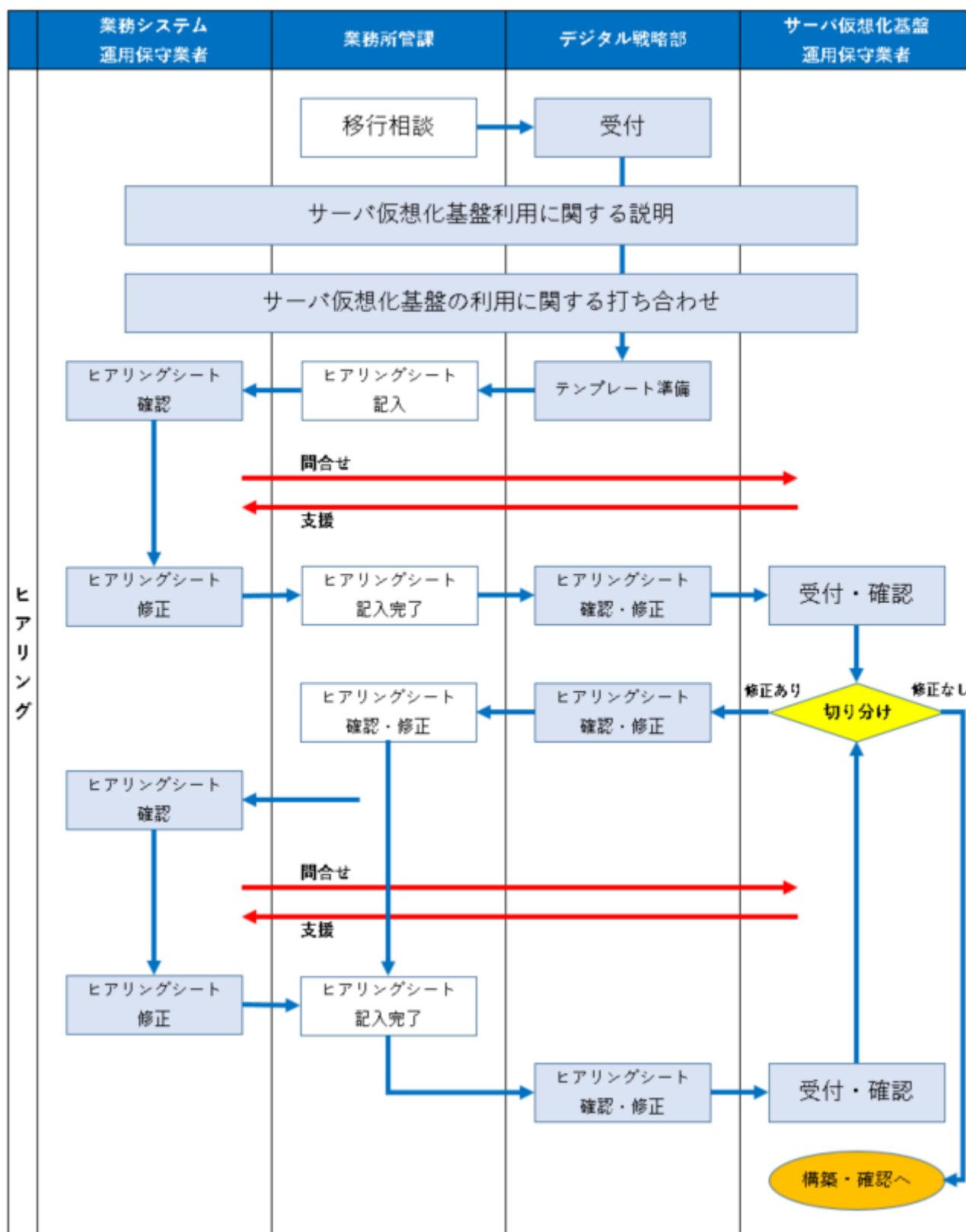


図7-1 工程の時系列（ヒアリング）

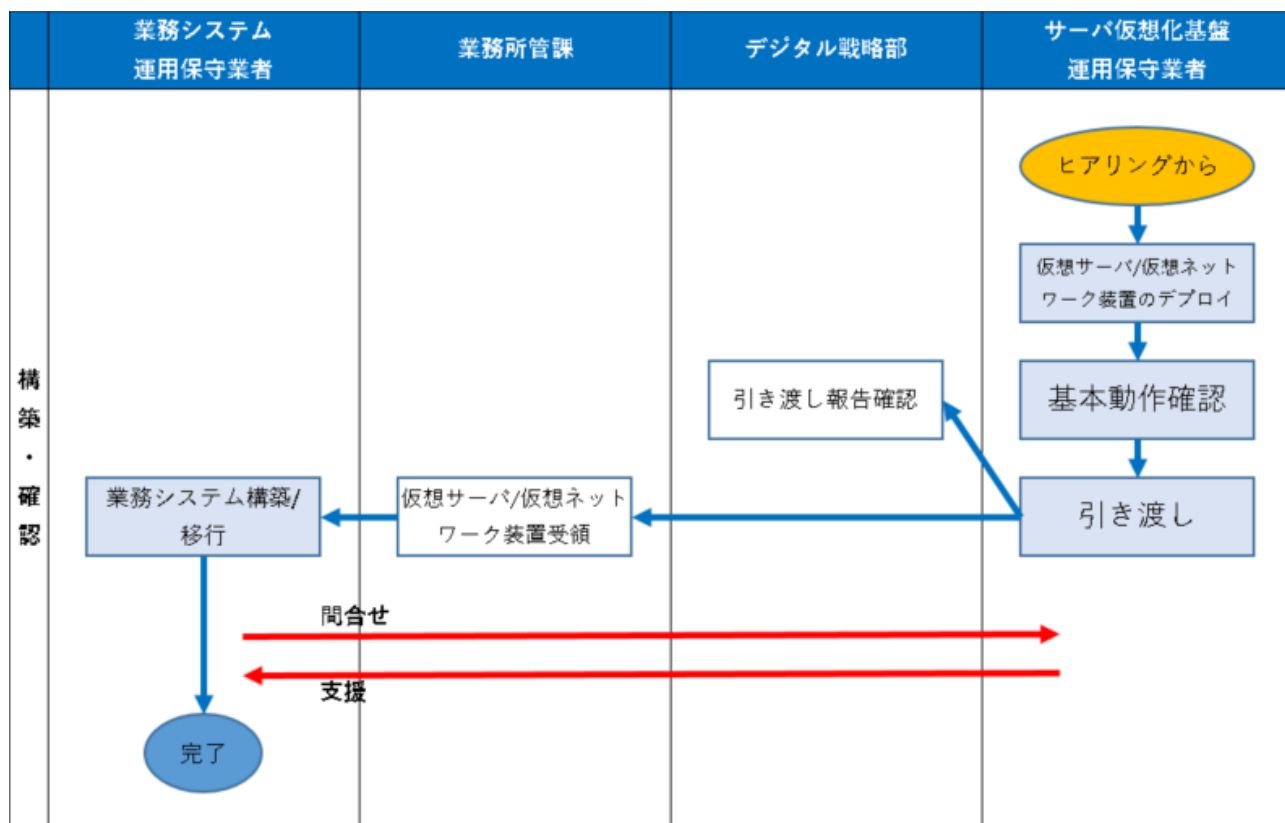


図7-2 工程の時系列（構築・確認）

7.4. サーバ仮想化基盤利用時に提供いただく情報

7.4.1. ヒアリングシート（利用申請）の作成、承認

サーバ仮想化基盤利用にあたって、別紙のヒアリングシートに記入の上、デジタル戦略部に提出する。

ヒアリング内容は、主に以下の3つの項目である。

表7-3 ヒアリング項目

	ヒアリング項目	内容
1	サーバの基本項目	払い出すサーバの OS、利用用途、バックアップに必要な容量などサーバ構築に必要な基本項目
2	サーバのリソース	払い出しが必要なサーバの CPU コア数、メモリ容量、ディスク容量などリソース
3	保守回線接続 PC 台数	保守回線接続を利用する PC の台数

下記は、ヒアリングシートのイメージである。

■ヒアリングシート(全体)

サーバ仮想化基盤 ヒアリングシート

【システム名記入】

システム名

サブシステム名:

【依頼箇所記入欄】 ※サーバ毎に記入願います。

依頼区分

☐ 新規
☐ 変更

変更概要

■バックアップ設定

データバックアップ(ファイル)に必要なサイズ

[GB]

データ想定使用量を元に、バックアップ用領域(共有フォルダ)に必要な容量を記入願います。
※乖離がある場合は、別途確認させていただきます。

■インストールメディアの貸出希望 ※貸出可能なインストールメディアが必要な場合、記入願います。

☐ Oracle
☐ SQL Server

ver:

ver:

■ロードバランサの利用有無 ※ロードバランサの使用有無を記入願います。
記入がない場合は、「使用しない」とみなします。

☐ 使用する
☐ 使用しない

特記事項

例:IPアドレスが複数必要等

■検証用仮想端末の要否

☐ 使用する
☐ 使用しない

→ 台数

OS

※最大3台となります。(1台のスペック CPU: 2vCPU、メモリ: 8GB、ディスク: 100GB)

49

■【別紙】サーバー一覧

[illegible]

■【別紙】サーバー一覧(2)

サーバ仮想化基盤 ヒアリングシート

業務/システム運用保守業務 記入項目

装置	サーバ名称	ホスト名	アフィニティルール	組み合わせ	仮想マシン 格納ストレージ
サーバの用途等がわかるサーバ名称を記入して下さい。 ホスト名を記入して下さい。 適用したいアフィニティルールを指定する。 適用したい仮想マシン格納一番号を指定する。					
<div> <div> 10台以上のサーバがある場合は、既存の行をコピーして増やして下さい。 </div> <div> 【仮想マシンの包括】 仮想マシンを包括したい場合 </div> <div> 【仮想マシンの分割】 仮想マシンを分割したい場合 </div> <div> ※アフィニティルールを使用しない場合は空白にする。 </div> <div> 【装置1】 共有ストレージ装置1に配置 【装置2】 共有ストレージ装置2に配置 【-】 使用する共有ストレージ装置性、仮想マシンを、共有ストレージ装置に付けない場合に指定 </div> <div> ※選択がない場合は、【-】とみなします。 </div> </div>					
例1 Webサーバ	VD00XWE001	仮想マシンの分割	1	装置1	
例2 DNSサーバ	VD00XWE001	仮想マシンの分割	1	装置2	
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

仮想マシンの包括

仮想マシンの分割

■【別紙】保守回線接続 PC

サーバ仮想化基盤 ヒアリングシート 保守回線接続PCの台数【システム毎に記入】

■システム構築／運用時に利用する（庁内接続）PCのIPアドレス（★1つ以上必須）

構築時	台	運用時	台
-----	---	-----	---

項番	IPアドレス	備考
①		
②		
③		

※ 保守回線を利用してリモートアクセスする場合のPC台数を記入願います。
サーバ仮想化基盤運用保守業者より、PC台数分のIPアドレスの払い出しをお願いします。

※ 本項目を指定していない場合、ゲストOSの起動やWebからのゲストOSコンソールアクセスができません。

図7-3 ヒアリングシート（イメージ）

8. サーバ仮想化基盤に関する問い合わせ

8.1. サーバ仮想化基盤に関する一般的な問合せ

サーバ仮想化基盤に関する一般的な問合せは、電子メール（フリーフォーマット）にておこなう。

電子メール送付先：kasoukakiban@office.city.kobe.lg.jp

サーバ仮想化基盤運用保守業者の問合せ受付は、開庁日の8：45～17：30のため、定時後の問合せは、翌開庁日の受付となる。

8.2. 業務共通利用ソフトウェアに関する問合せ

サーバ仮想化基盤で提供する業務共通利用ソフトウェア（VMware 製品、Microsoft 製品（Windows、SQL Server）、Linux、Oracle、SEP）に関する問合せは、電子メール（フリーフォーマット）にておこなう。

問合せの内容により、別途情報提供を要請する場合がある。

9. 費用の考え方

9.1. 費用負担

サーバ仮想化基盤の利用において、一般会計のシステムについて負担金は不要である。

ただし、企業会計のシステムについては、会計間の独立性を踏まえ、負担金を徴収する必要があるため、次表に定めるリソース単価で計算された金額の費用負担を求める。

表9-1 費用負担額

項目		課金単位	年間利用料	備考
①仮想マシン	vCPU	1vCPU	31,700 円	
	メモリ	1GB	3,100 円	
	ストレージ	1GB	113 円	
	Microsoft SQL server	1vCPU	57,000 円	

※仮想化基盤で提供する業務用バックアップ領域についても課金対象（ストレージ）とする。

9.2. 効果額算定

サーバ仮想化基盤の導入に伴う費用対効果を算定するため、下記の情報を提供すること。

既存システムの機器更新：現在の機器リース費用を提示すること。

システムの新規構築：システム構築事業者からハードウェアに関する見積を取得している場合は、見積資料を提出すること。見積を取得していない場合は、当該システムに要求されるCPU、メモリ、ストレージのリソースに基づき、サーバ仮想化基盤を利用しない場合に要する費用を算定する方針である。