

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。

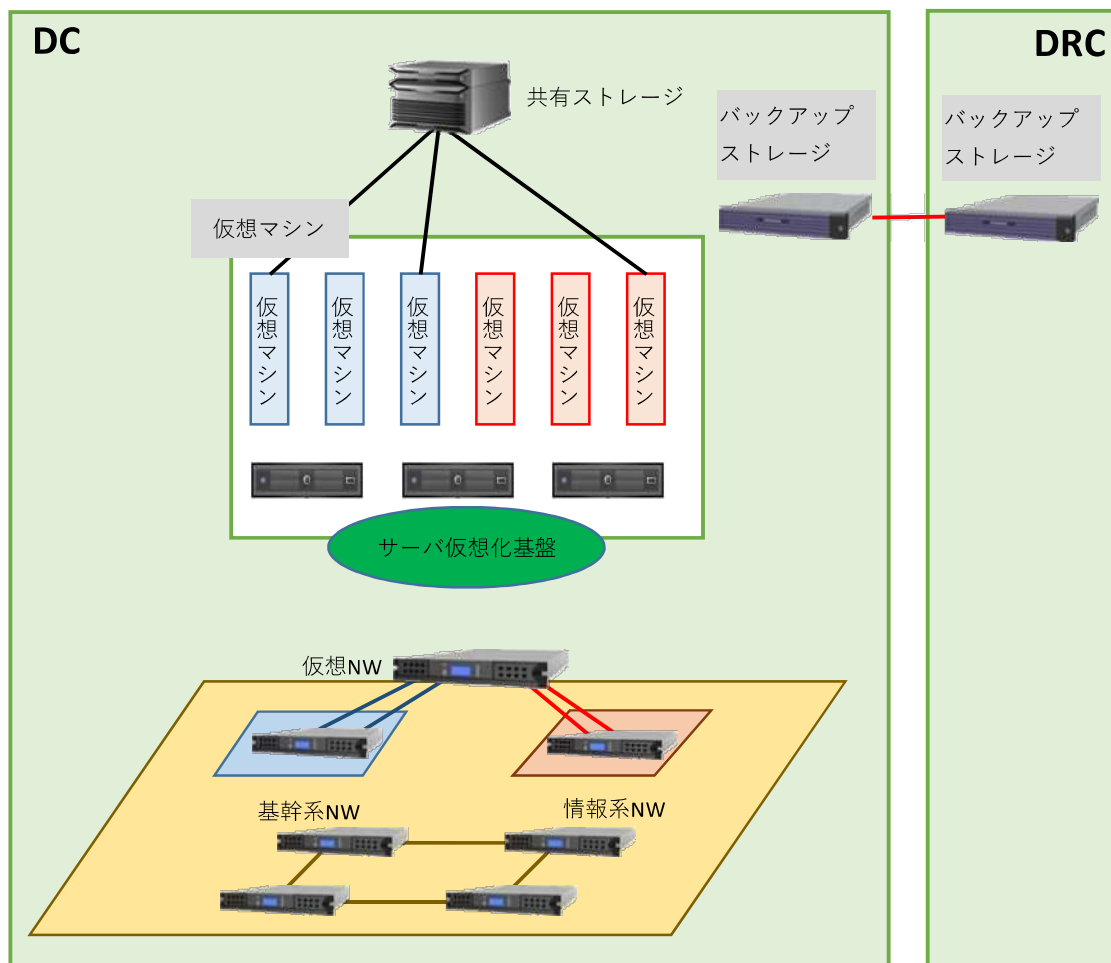


図2-1 サーバ仮想化基盤システム構成図（概要）

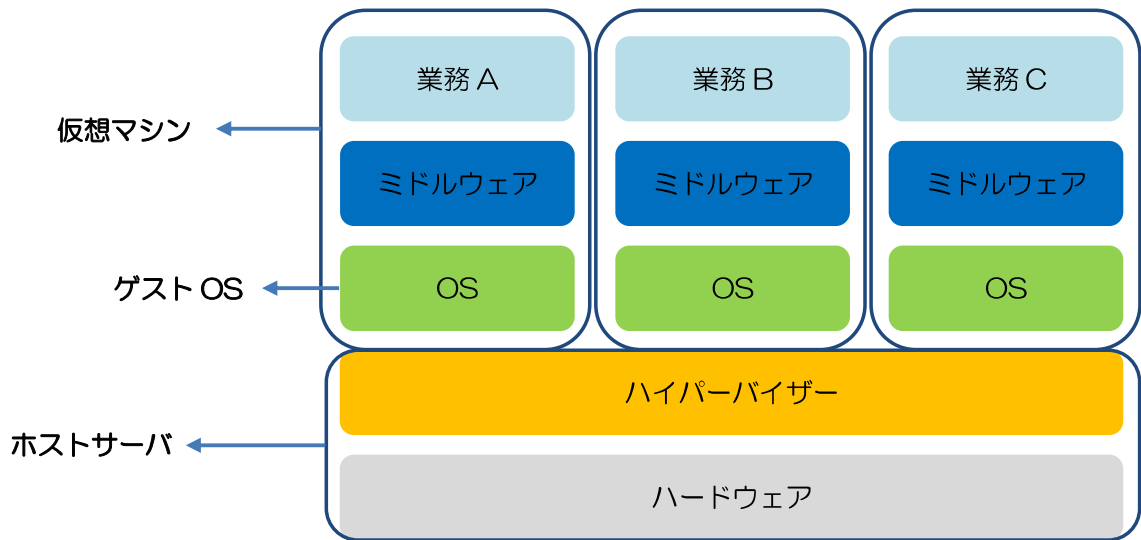


図2-2 ホストサーバと仮想マシンの関係

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。

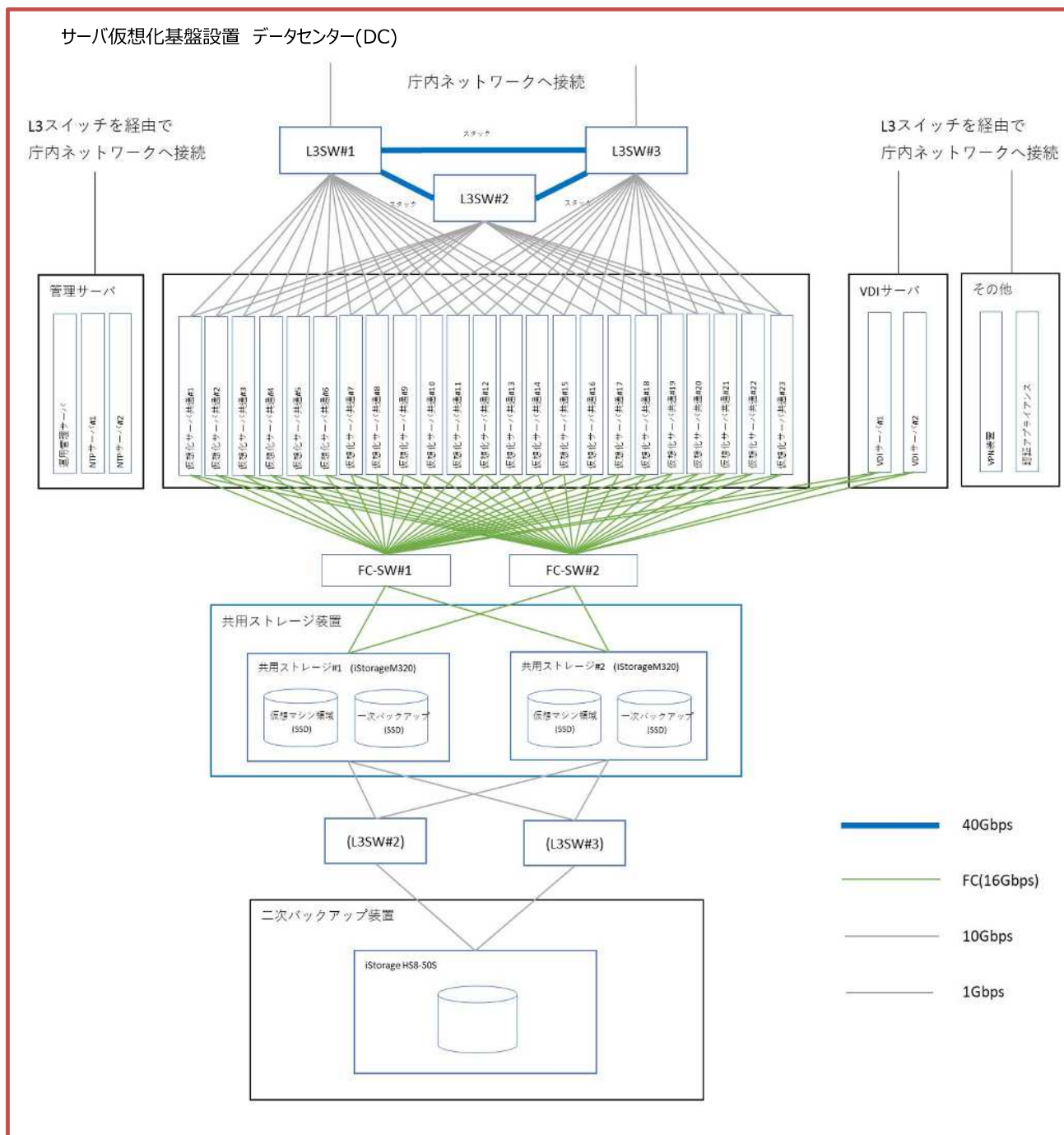


図 3-1 DC 構成

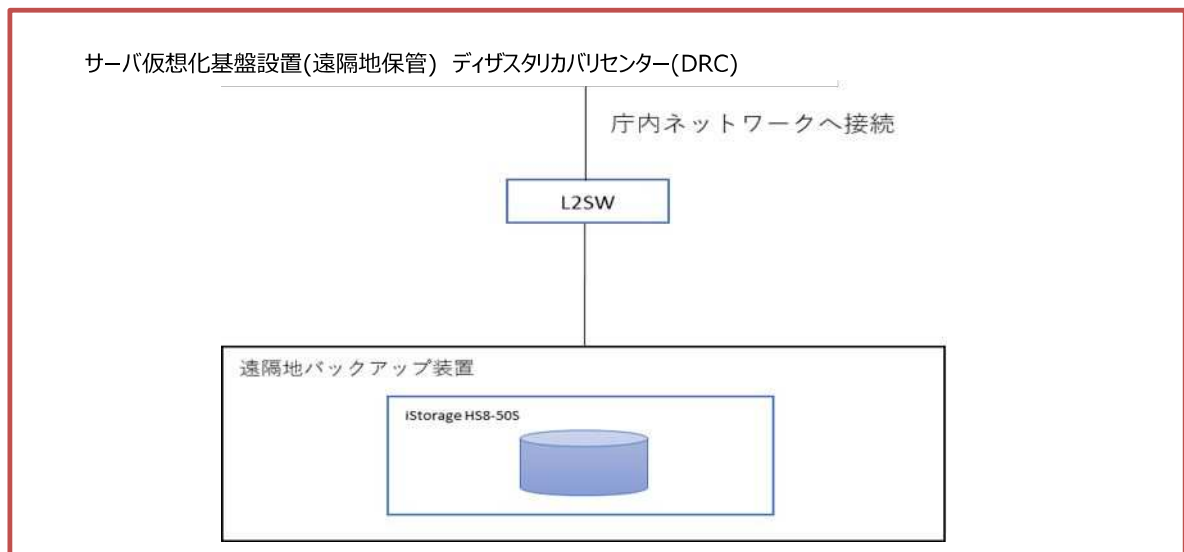


図3-2 DRC 構成

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

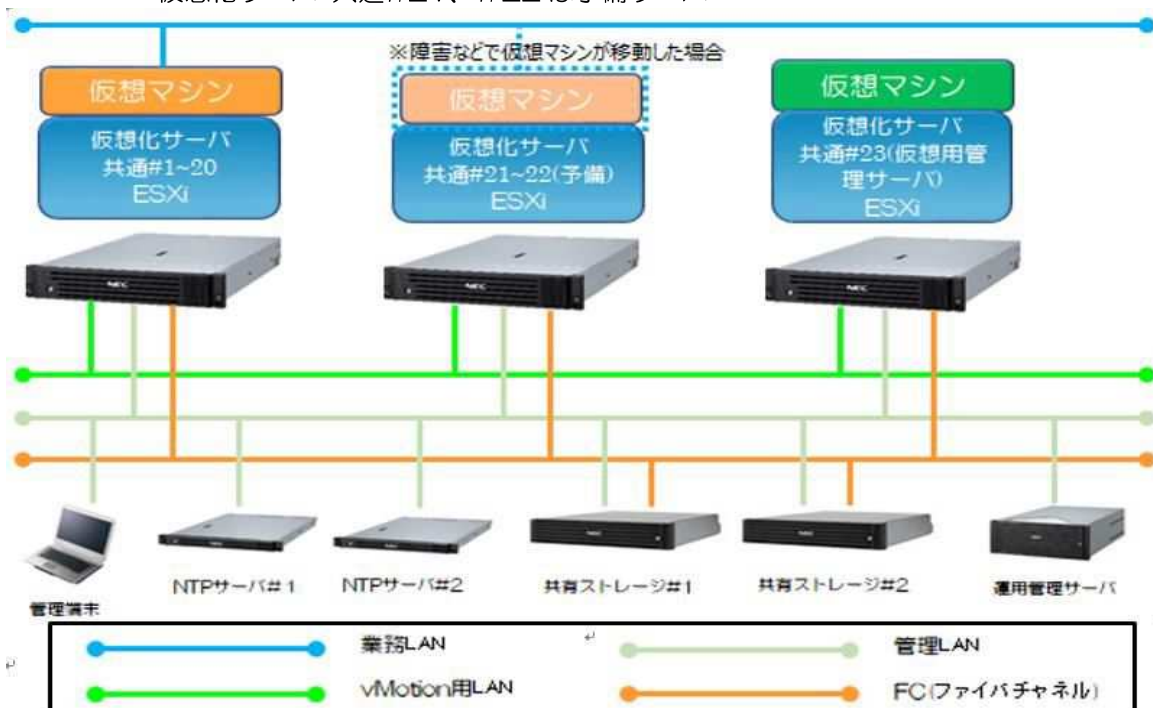


図3-3 仮想化サーバ共通用エリア

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

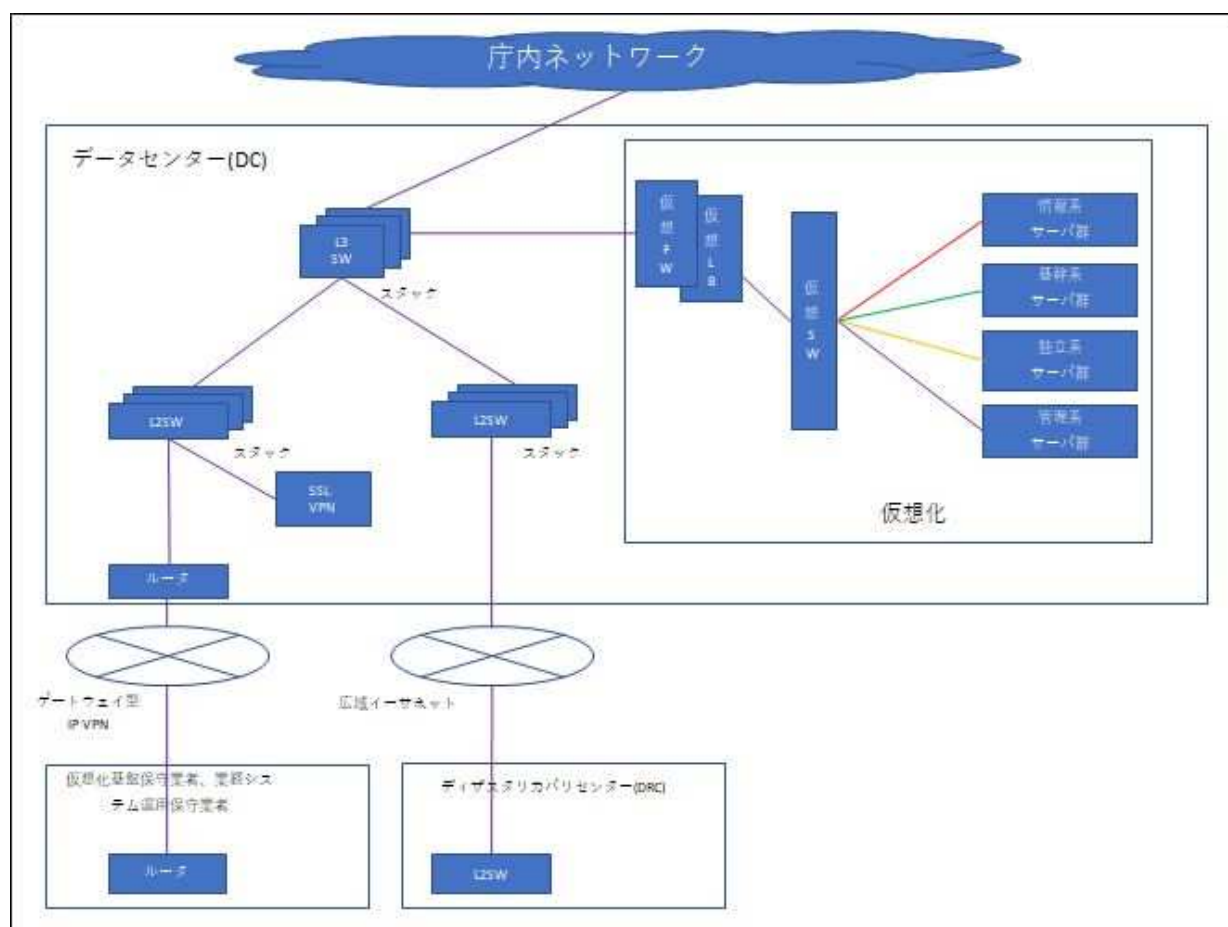


図4-1 ネットワーク構成図

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、最適ナリ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	ヒアリングシートに記載された容量、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 によるリポート動作の制限

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 ・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。

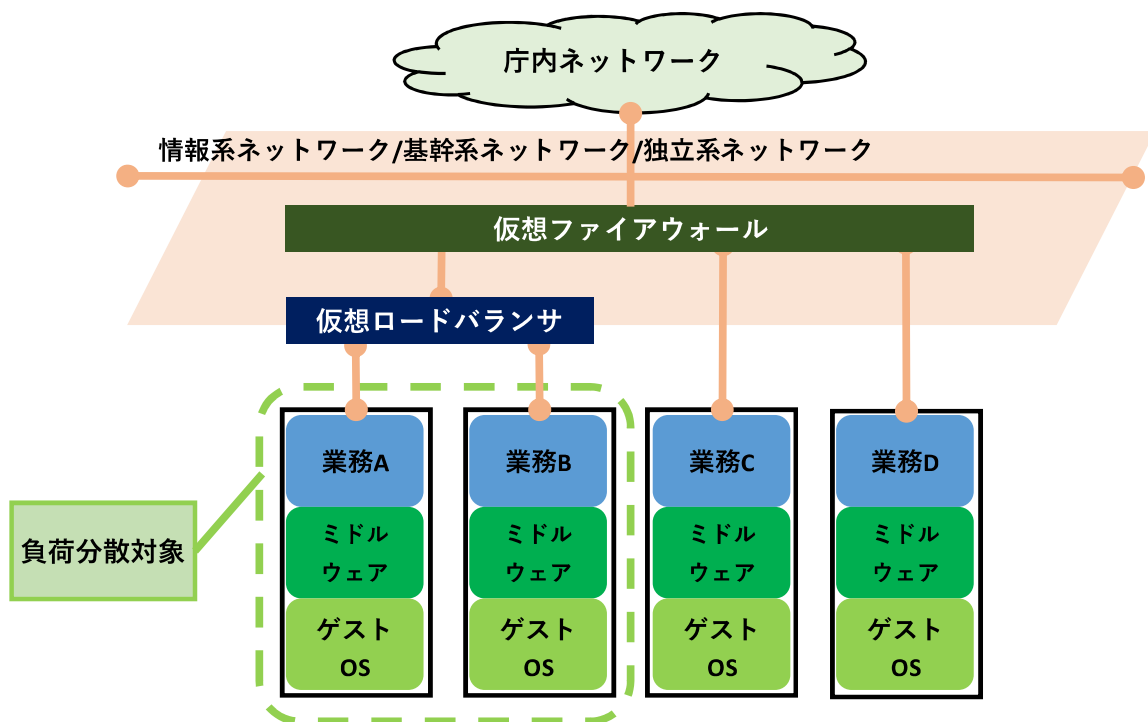


図5-1 仮想マシンと仮想ロードバランサの関連図

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。

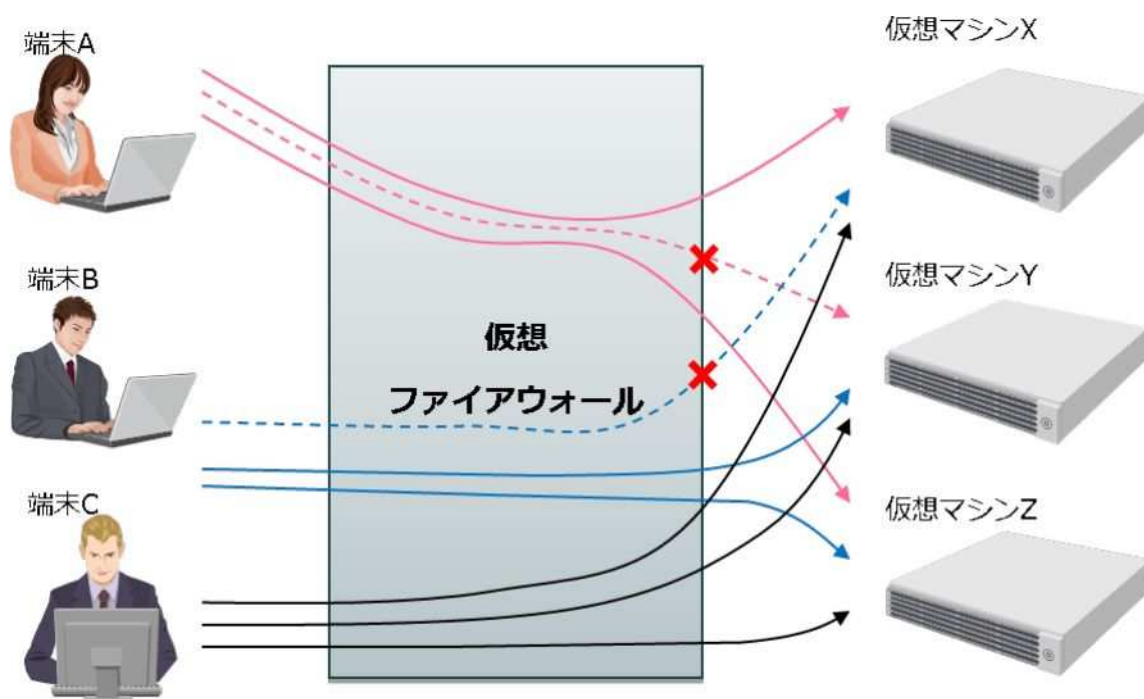


図5-2 仮想ファイアウォールの動き

#	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。

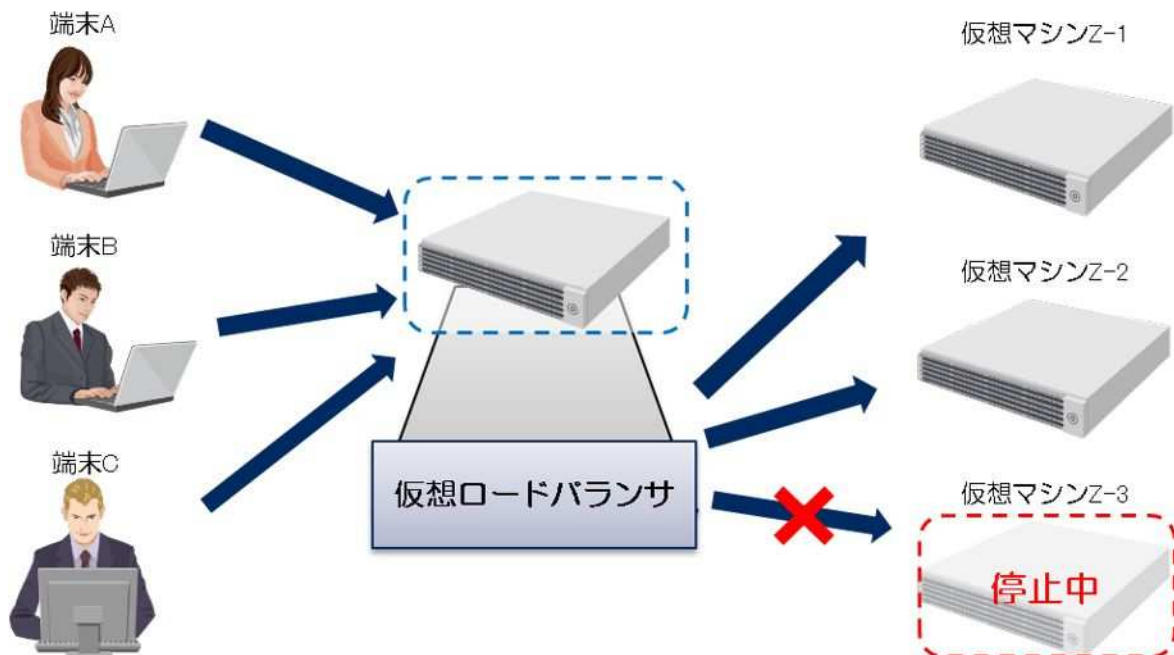


図5-3 仮想ロードバランサの動き

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、それぞれのシステムの既存の 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

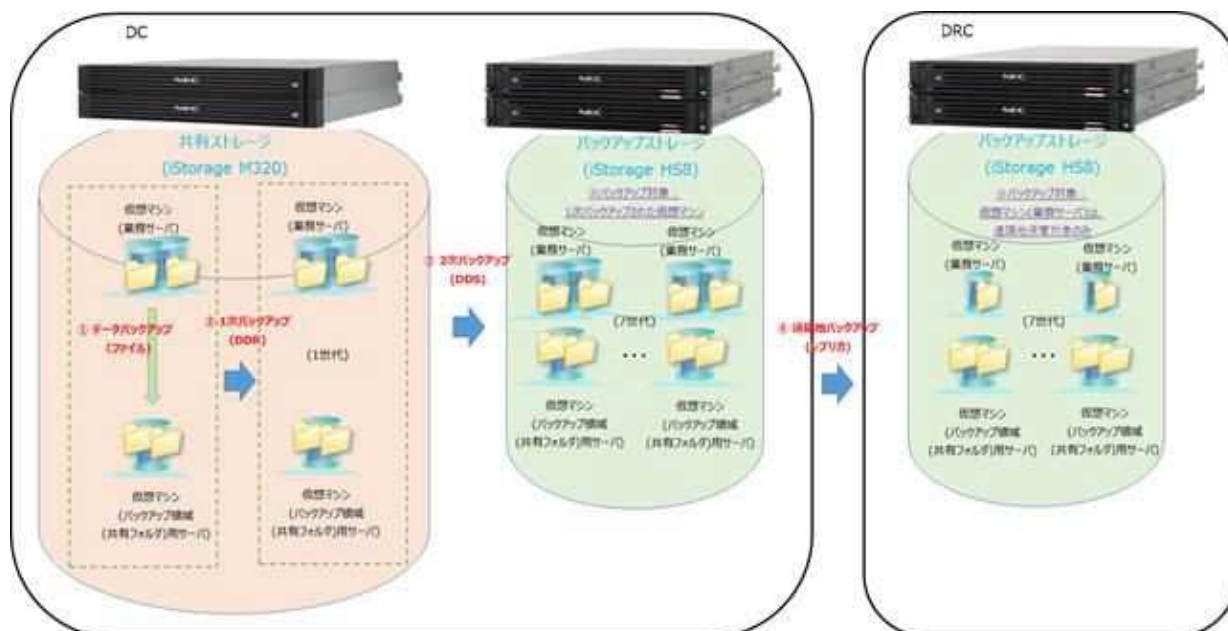


図5-4 提供するバックアップ機能

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)

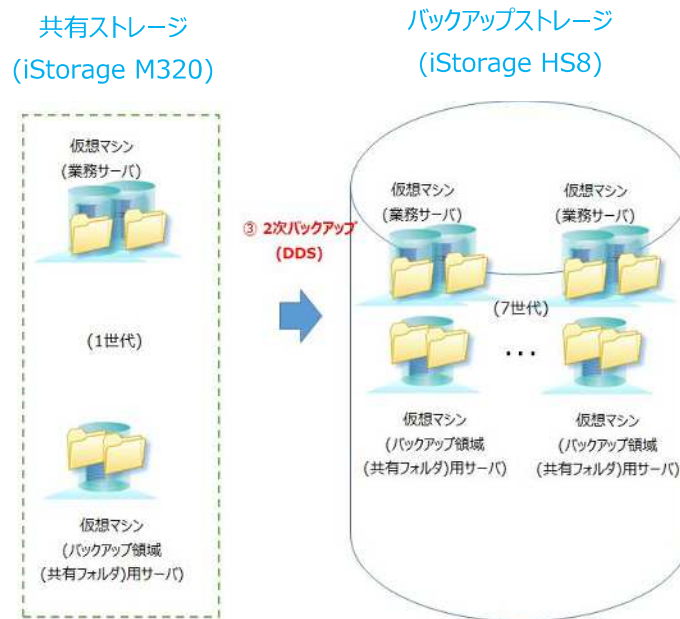


図5-7 2次バックアップ

- 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)

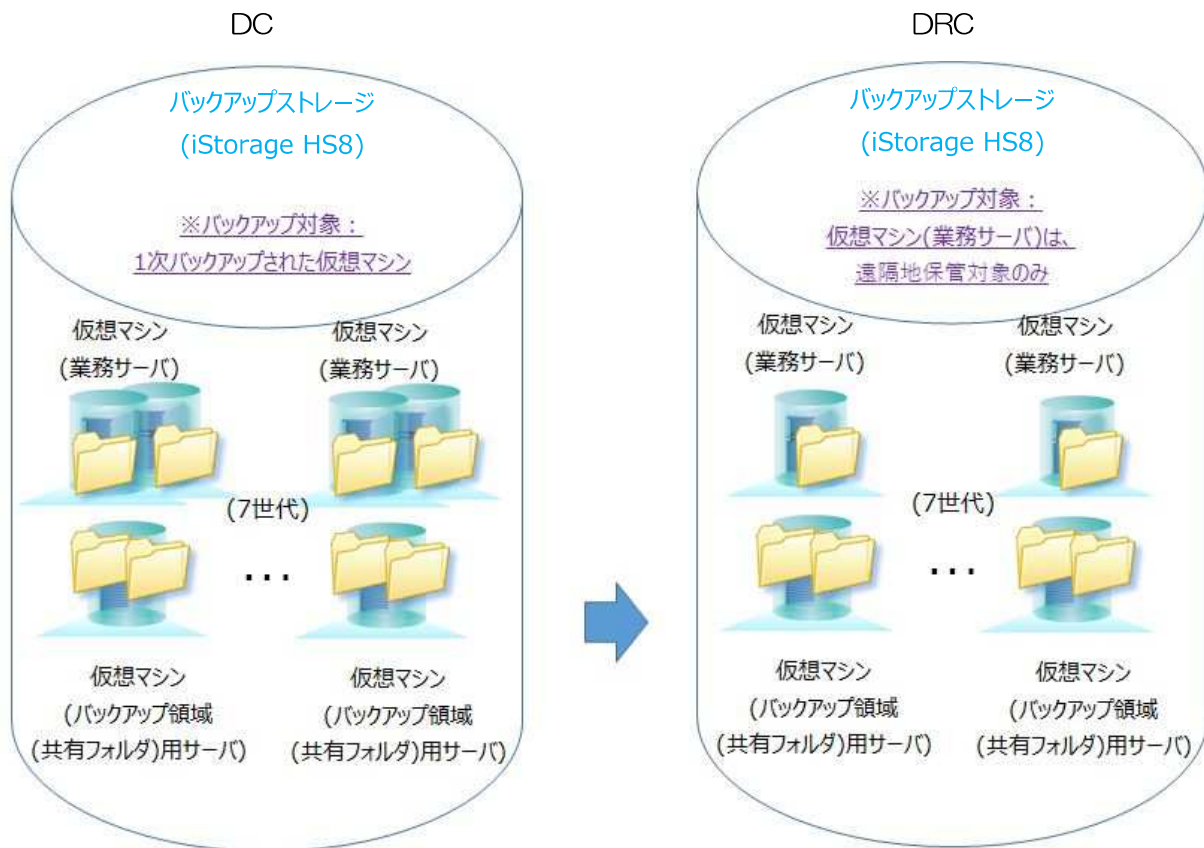


図5-8 遠隔地バックアップ

- ・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

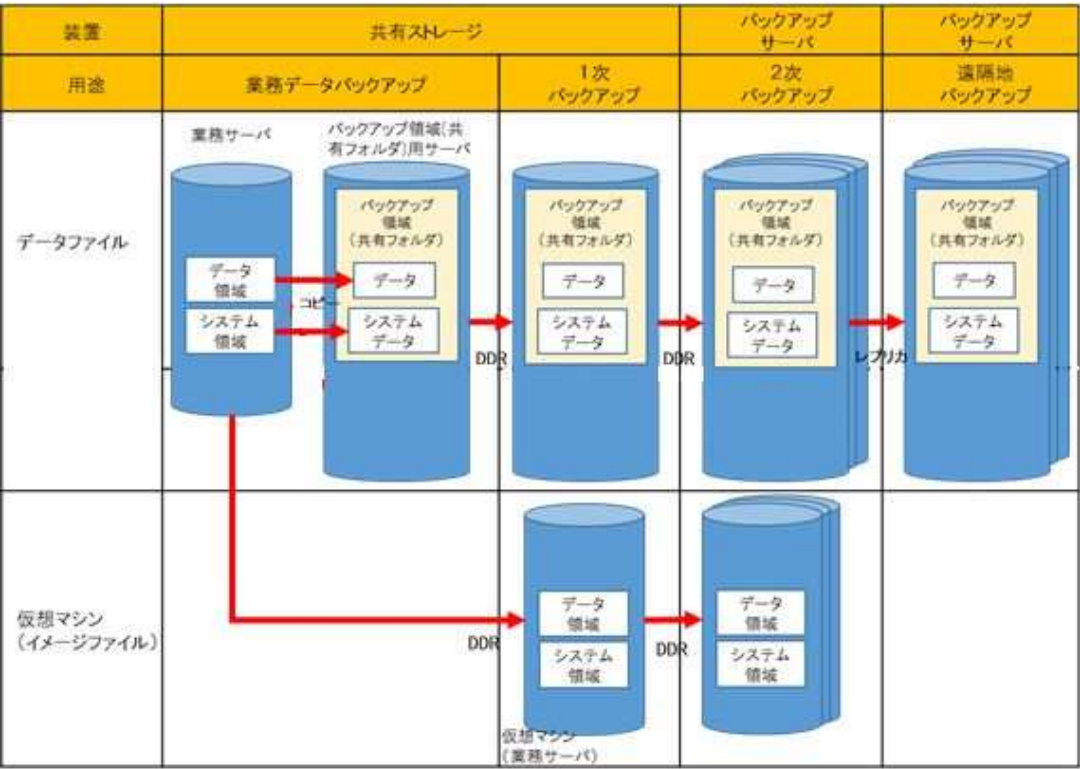


図5-9 バックアップ単位

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。

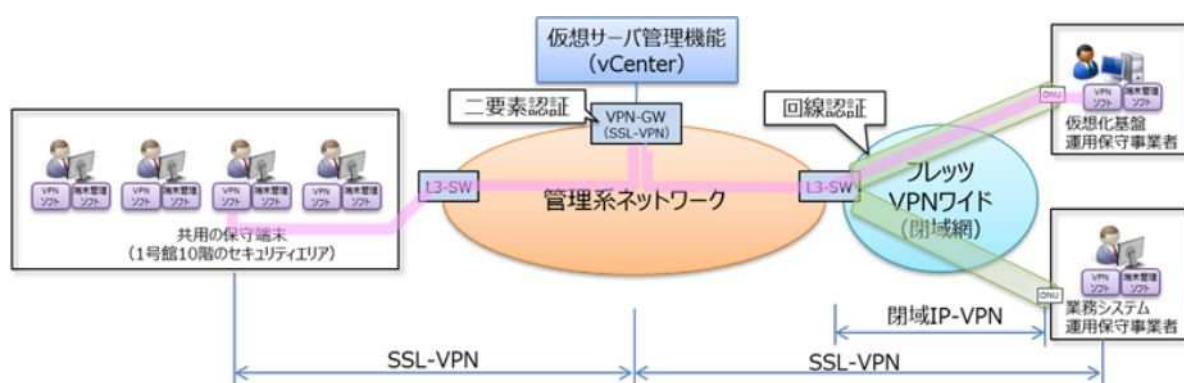
- ① (光回線を新設する場合のみ) 光回線の手配 (業務システム運用保守業者)
光回線を新設する場合は、NTT 西日本へ回線の手配をおこなう。
(注) 保守環境を利用できる回線は、最大 100Mbps 又は 200Mbps の
ファミリータイプ、マンションタイプ、ファミリー・ハイスピードタイプ、
マンションハイスピードタイプのフレッツアクセスサービスのみ。
(フレッツ光ネクストの「ファミリー・スーパーハイスピードタイプ隼」、「マ
ンション・スーパーハイスピードタイプ隼」及び「ビジネスタイプ」は対象
外。)
※詳細は、NTT 西日本に確認すること。
- ② 保守用回線申込申請書及び同意書の提出 (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。



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. アフィニティールールの設定

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ー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、アフィニティールールを設定する。

表5-13 アフィニティールールの種類

アフィニティールール	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

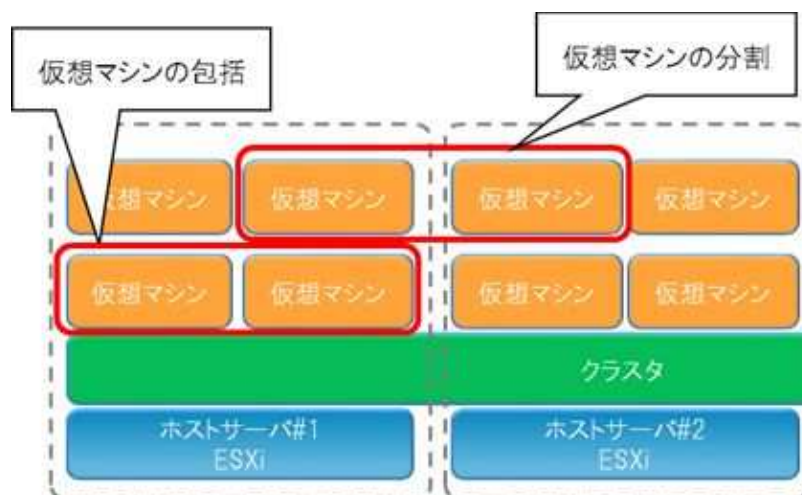


図5-13 アフィニティールールの種類

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。

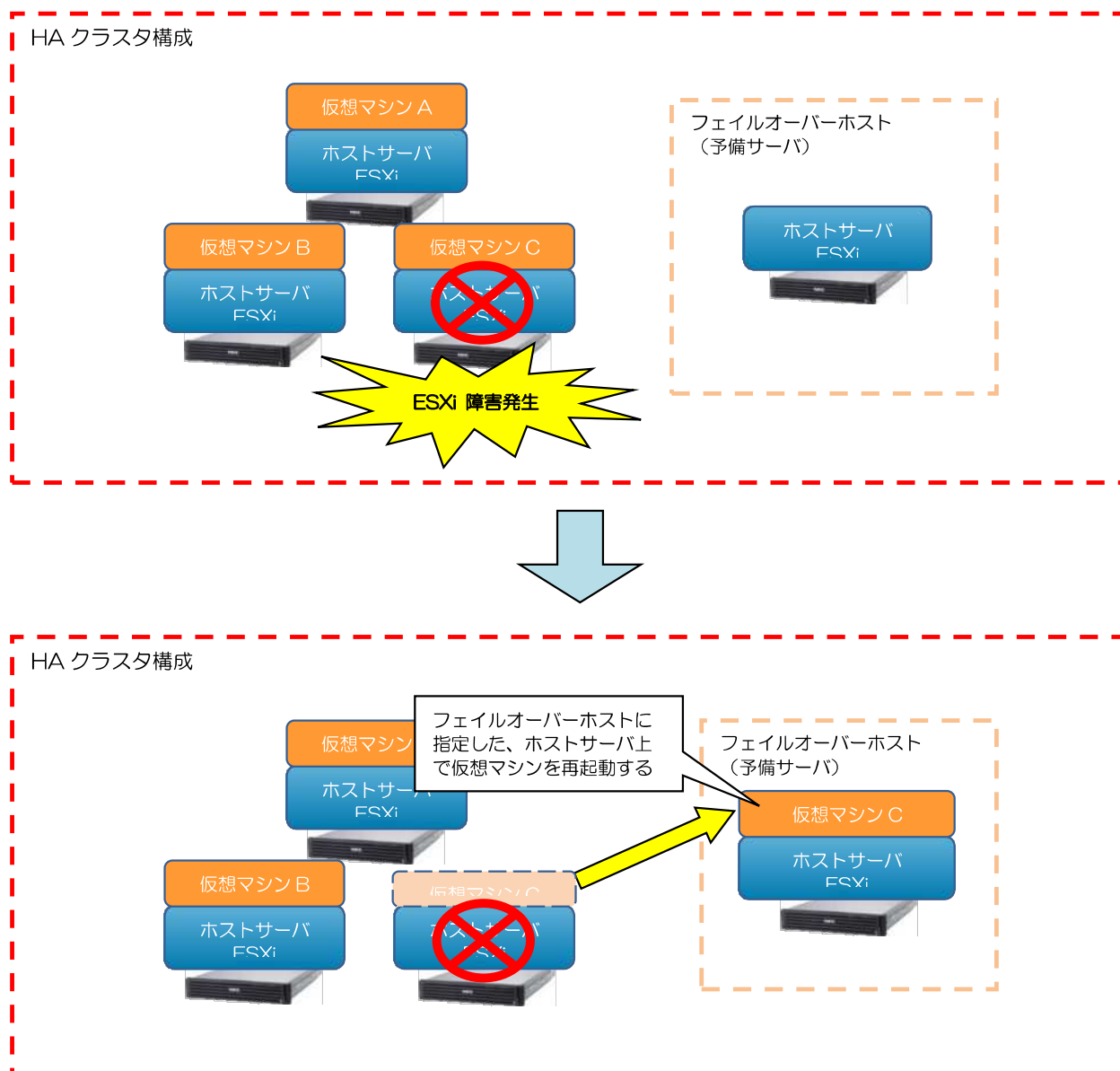


図5-14 vSphere HA の動き

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。

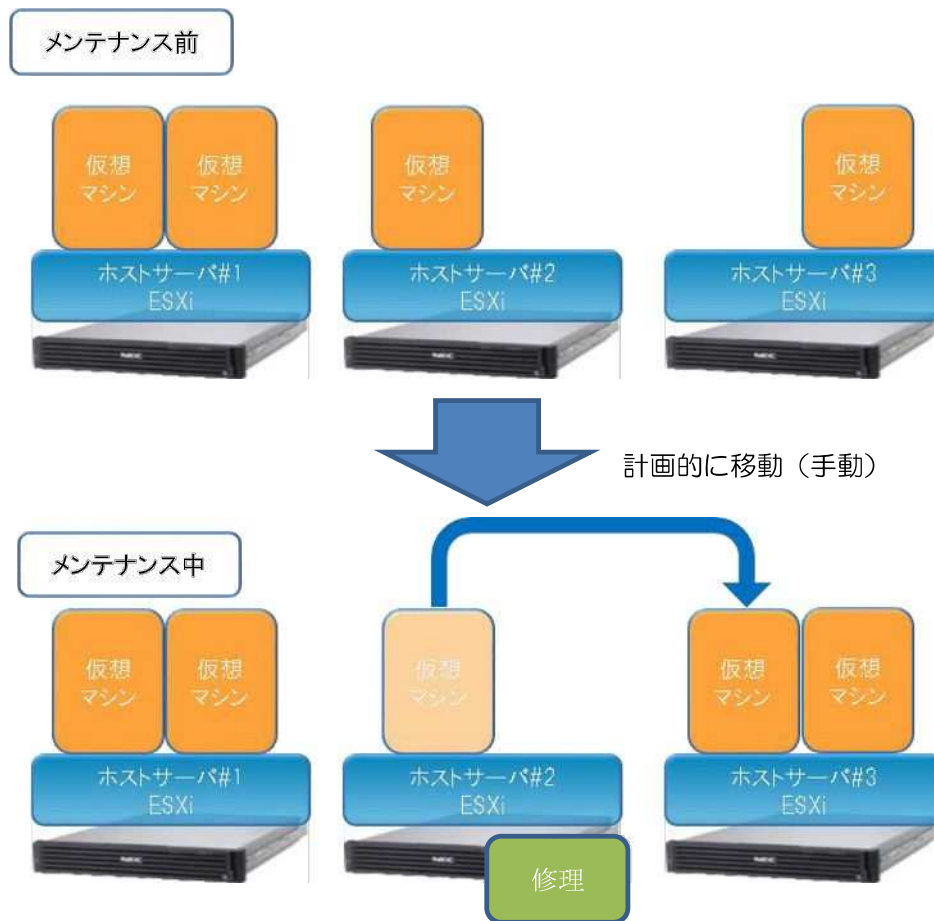


図5-15 vMotion の動き

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>

5.11.1.1. 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）

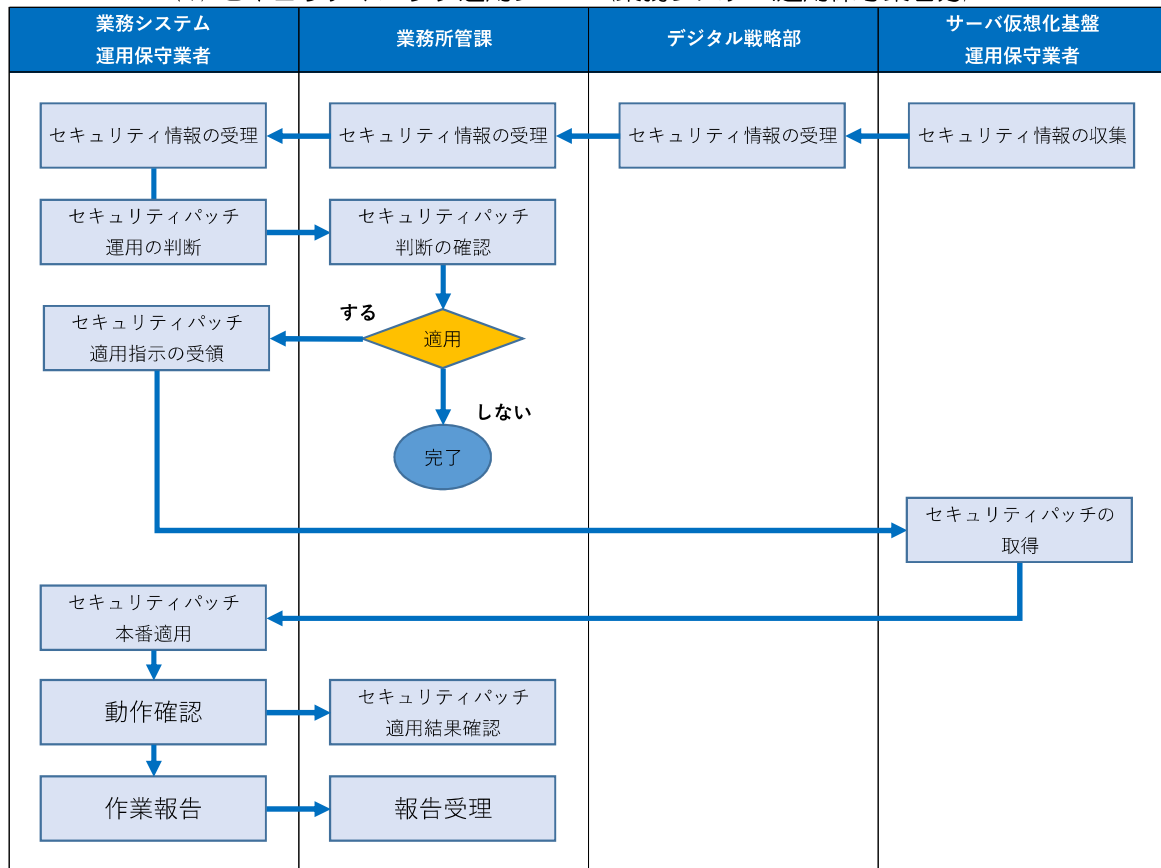


図5-16 セキュリティパッチ適用フロー（業務システム運用保守業者分）

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）

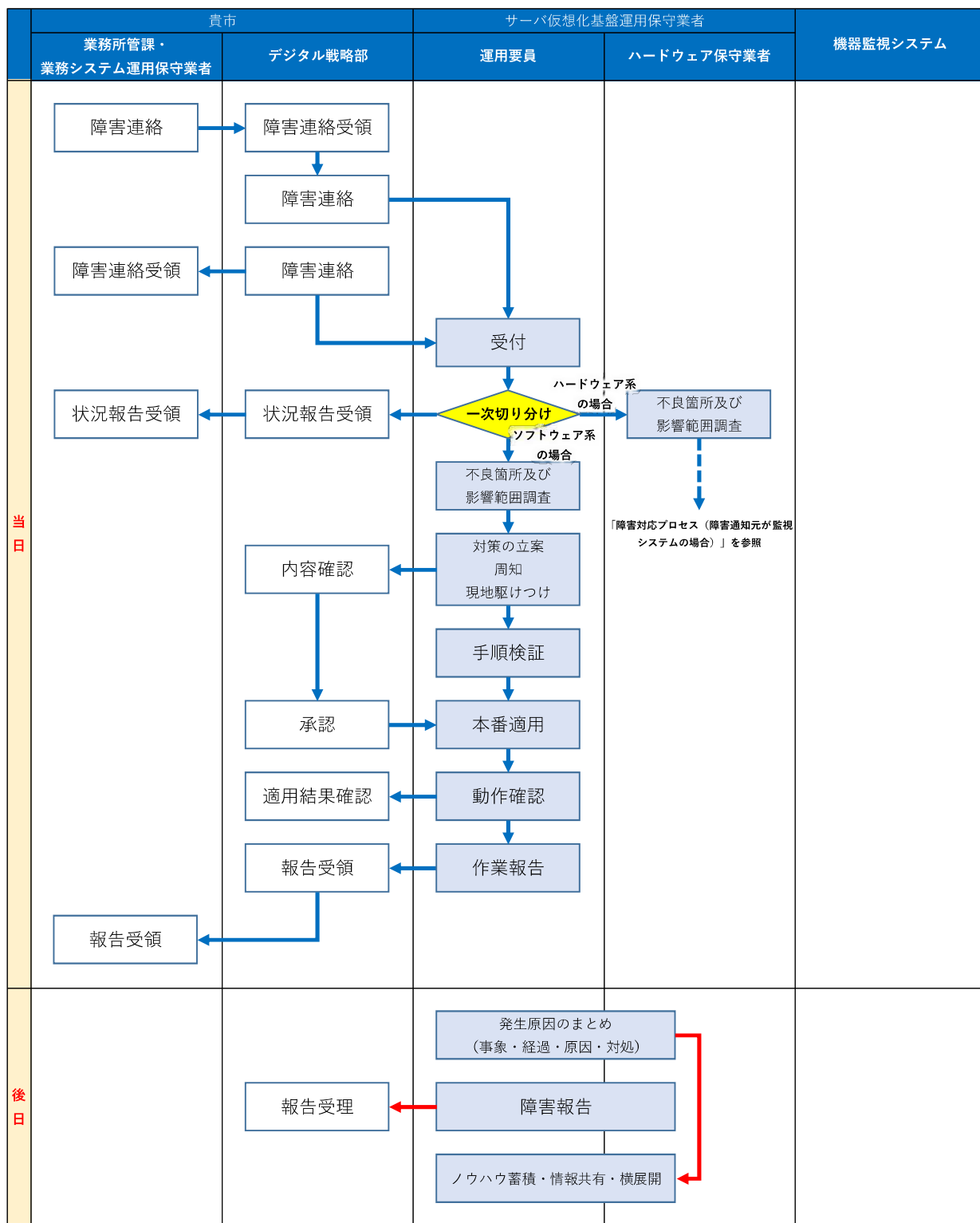


図5-17 障害対応プロセス（開庁日業務時間内）

5.13.2. 障害対応プロセス（開庁日夜間及び休日）

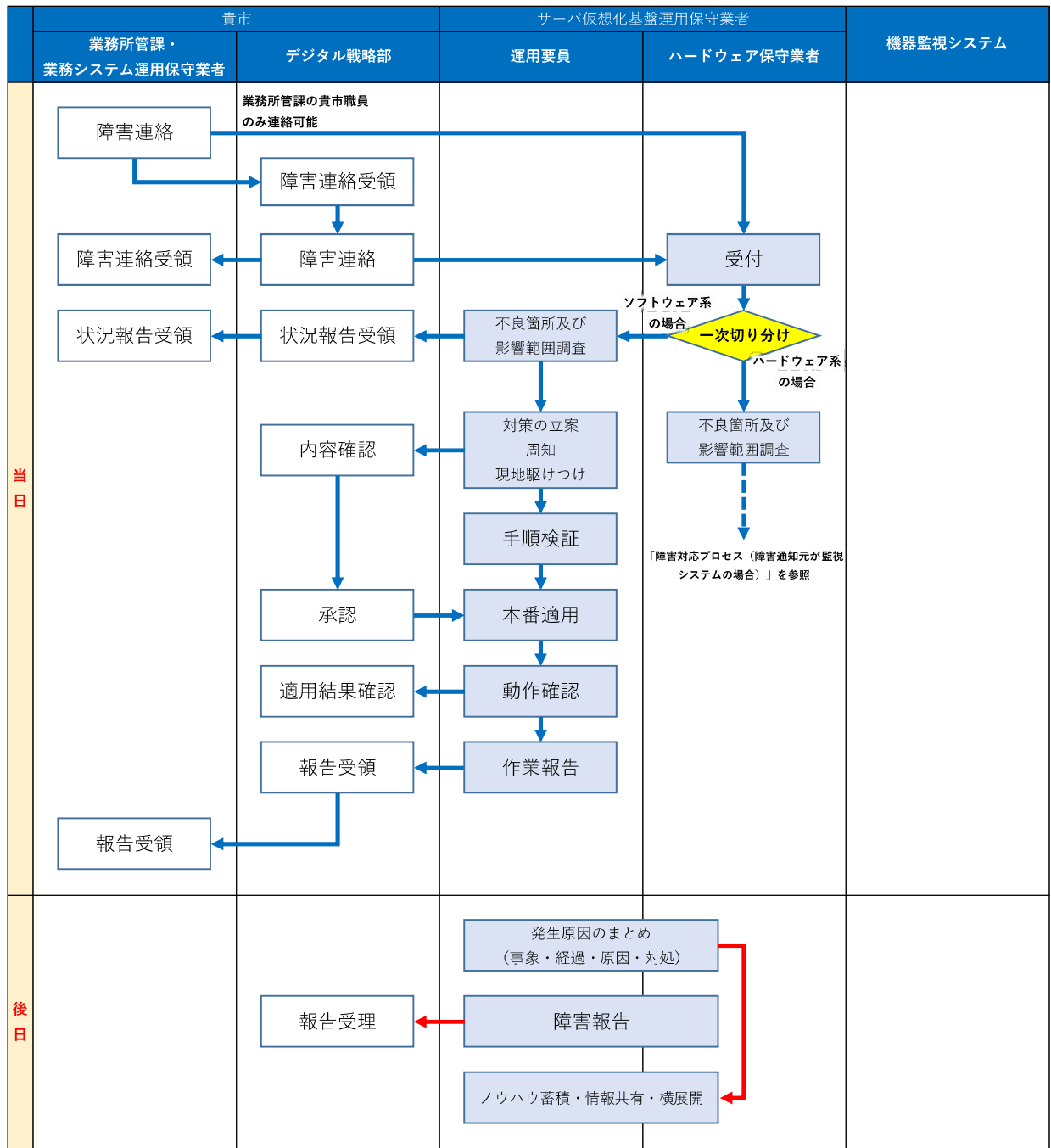


図5-18 障害対応プロセス（開庁日夜間及び休日）

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）

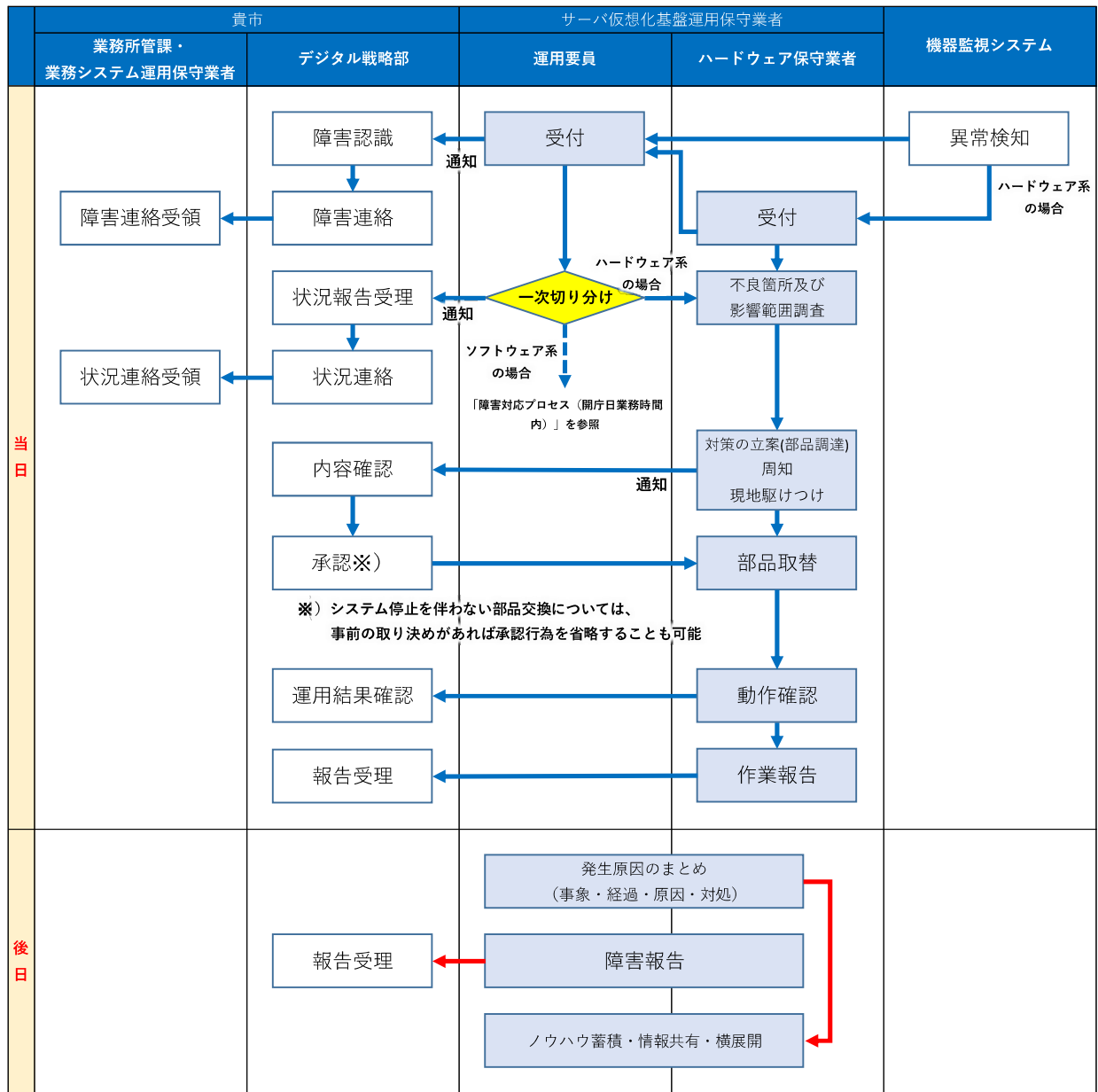


図5-19 障害対応プロセス（障害検知元が監視システムの場合）

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。

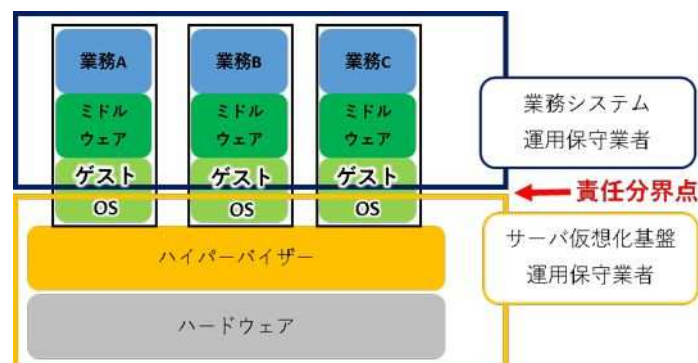


図6-1 仮想マシン引き渡し時の責任分界点（業務システム導入前）

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）

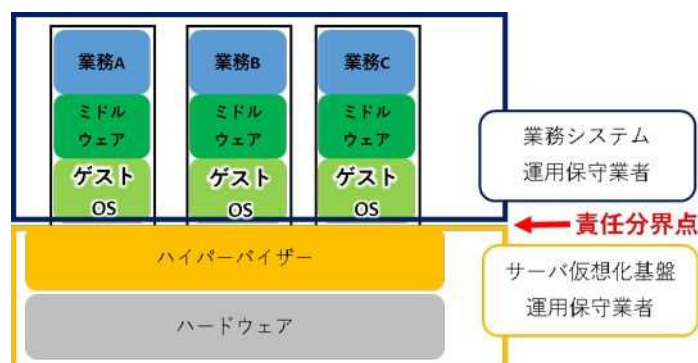


図6-2 仮想マシン引き渡し後の責任分界点

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	ウィルス定義ファイルの取得適用、 ウィルス検知の確認	○ (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。

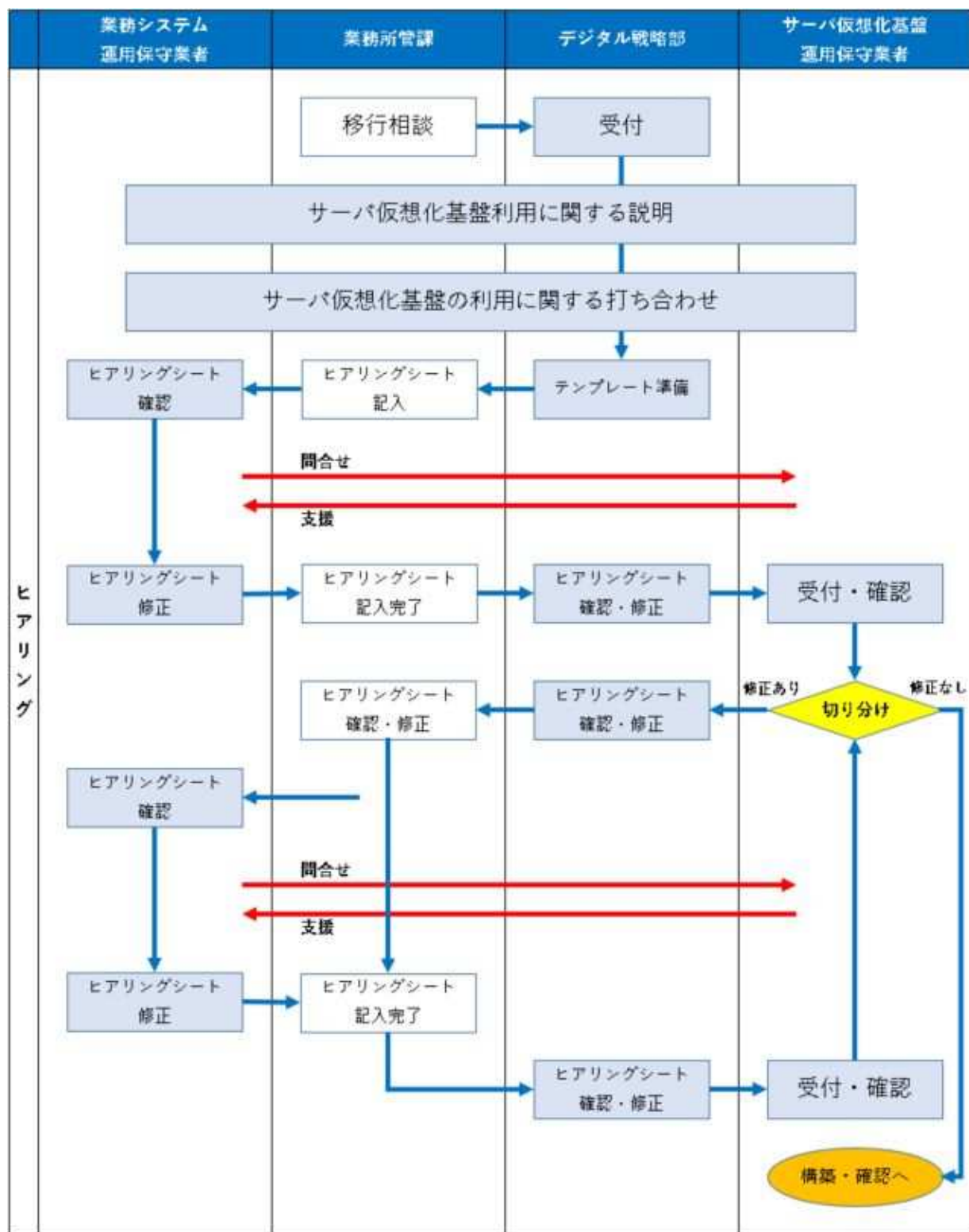


図7-1 工程の時系列（ヒアリング）

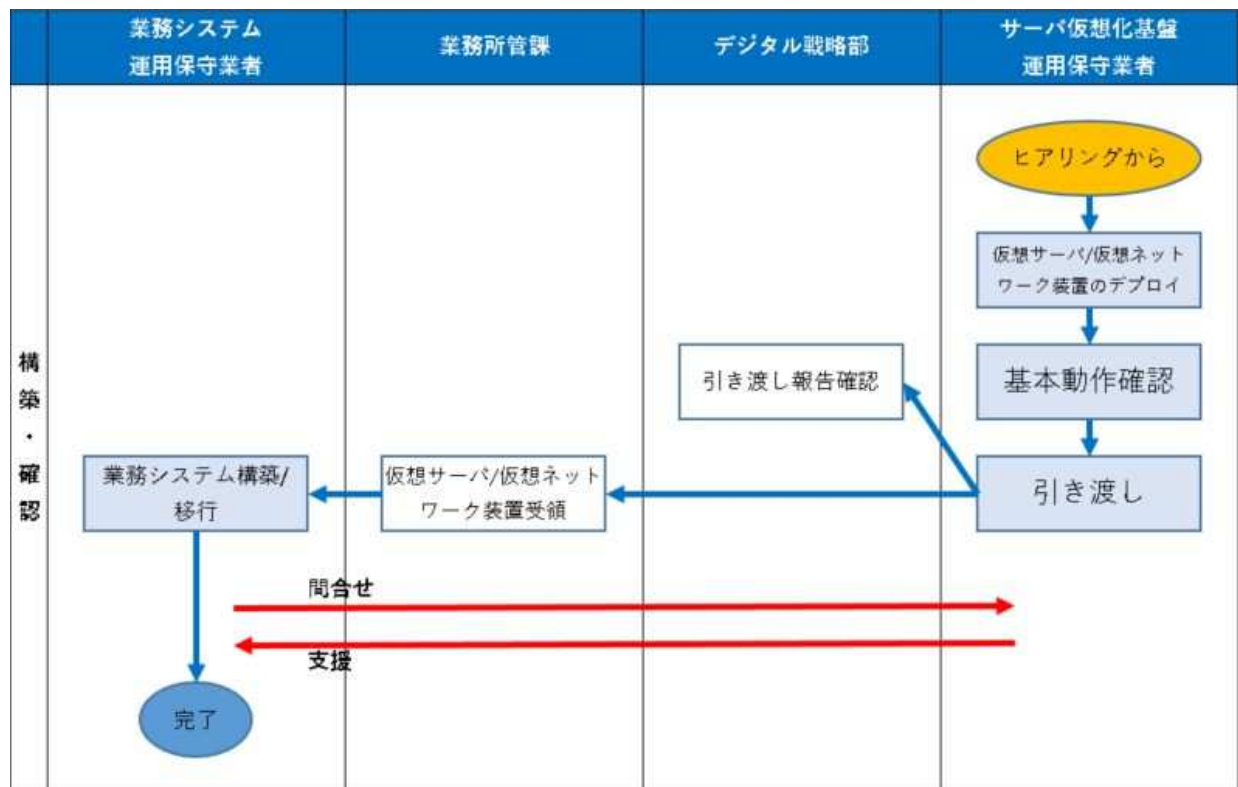


図7-2 工程の時系列（構築・確認）

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)で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 ver.
☐ SQL Server 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

台

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)

■【別紙】サーバー一覧

サーバー管理 仮想マシン														
名前	タイプ	OS	仮想マシン名	仮想マシンID	仮想マシンタイプ	仮想マシンサイズ	仮想マシンステータス	仮想マシン作成日時	仮想マシン更新日時	仮想マシン削除日時	仮想マシン削除理由	仮想マシン削除ステータス	仮想マシン削除日時	仮想マシン削除理由
WebAPサーバ	VD000MB001	Windows Server 2012 R2	WebAPサーバ	0001	仮想マシン	4GB	起動中	2012/12/12	2012/12/12					
DNSサーバ	VD000MB001	Windows Server 2012 R2	DNSサーバ	0002	仮想マシン	4GB	起動中	2012/12/12	2012/12/12					
1														
2														
3														
4														
5														
6														
7														
8														
9														
10														

■【別紙】サーバー一覧(2)

サーバー管理 仮想マシン				
名前	タイプ	OS	仮想マシン名	仮想マシンID
WebAPサーバ	VD000MB001	Windows Server 2012 R2	WebAPサーバ	0001
DNSサーバ	VD000MB001	Windows Server 2012 R2	DNSサーバ	0002
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

■【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／運用時に使用する(社内接続)PCのIPアドレス(★1つ以上必須)

構築時	台	運用時	台
-----	---	-----	---

項目	IPアドレス	備考
①	1	ページ
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。

神戸市庁内情報システムの
導入に関する手引き
(第 6 版)

令和 5 年 9 月

神戸市 企画調整局デジタル戦略部

- Microsoft, Windows, Windows 10, Windows Server, Active Directory, Internet Explorer, .NET Framework, Microsoft Office, Word, Excel, PowerPoint, Access, Microsoft IME, Visual Basic は、米国 Microsoft Corporation の米国および各国における登録商標または商標です。
- Adobe Reader, Acrobat は、アドビシステムズ社の米国および各国における登録商標または商標です。
- Linux は、Linus Torvalds の米国および各国における登録商標または商標です。
- UNIX は、X/Open Company Ltd. がライセンスしている米国及び各国における登録商標です。
- その他、本書に記載されている製品名は各社の登録商標または商標です。
- 本文中に®及びTMマークは明記しておりません。
- 本文中においては、文書の体裁上の都合等により会社名、製品名の表記において、商標登録表示、その他の商標表示を省略している場合があります。

改訂履歴

変更日付	改訂内容等
平成 29 年 4 月 1 日	初版発行
平成 30 年 4 月 1 日	第 2 版発行
平成 31 年 4 月 1 日	第 3 版発行
令和 2 年 4 月 6 日	第 4 版発行
令和 3 年 7 月 5 日	第 5 版発行
令和 5 年 9 月 5 日	第 6 版発行

目 次

1	はじめに.....	1
2	サーバ室.....	2
2.1	サーバ室の概要.....	2
2.2	新規機器設置時のルール	2
2.2.1	機器の設置方法等	2
2.2.2	設置機器(ラックを含む)の搬入作業	2
2.2.3	機器設置の附帯工事.....	3
2.2.4	提出書類	3
2.3	機器撤去時のルール.....	4
2.3.1	原状復旧工事	4
2.3.2	提出書類	5
2.4	サーバ室の運用ルール	5
2.4.1	搭載機器変更時のルール.....	5
2.4.2	サーバ室入退室のルール.....	5
2.4.3	その他	5
3	ネットワーク.....	6
3.1	基幹系ネットワーク.....	6
3.1.1	背景と目的.....	6
3.1.2	ネットワーク構成(WAN)	6
3.1.3	ネットワーク構成(LAN)	7
3.1.4	利用にあたってのルール.....	8
3.1.5	提供サービス	10
3.1.6	利用にあたってのルールと提供サービスの関係	11
3.1.7	利用にあたっての手続き概要.....	12
3.1.8	留意事項	13
3.2	情報系ネットワーク.....	14
3.2.1	背景と目的.....	14
3.2.2	構成	14
3.2.3	LAN(本庁舎・各拠点).....	15
3.2.4	WAN.....	16
3.2.5	サーバ	17
3.2.6	対外接続点.....	20
3.2.7	利用にあたっての手続き概要.....	20

3.2.8	留意事項	20
3.3	独自プロバイダとの契約	21
3.3.1	手順	21
4	情報系端末(事務処理用 PC)	21
4.1	ハードウェアの基本構成	21
4.2	標準ソフトウェア(※)	22
5	共通サービス.....	23
5.1	サーバ仮想化基盤(基幹系・情報系).....	23
5.1.1	構築の背景	23
5.1.2	サーバ仮想化基盤の全体概要(構成, 提供サービス).....	23
5.1.3	仮想マシン機能.....	23
5.1.4	仮想ネットワーク機能	23
5.1.5	統合バックアップ機能	23
5.1.6	仮想デスクトップ機能	23
5.1.7	提供サービス説明	24
5.1.8	サーバ仮想化基盤の利用手続き	25
5.1.9	事業者の保守環境	26
5.2	共通基盤システム(基幹系)	26
5.2.1	構築の背景と目的	26
5.2.2	共通基盤システムの機能構成.....	27
5.2.3	文字コード変換.....	28
5.2.4	共通基盤システム利用にあたっての手続き概要	29
5.3	統合宛名システム(基幹系)	29
5.3.1	構築の背景.....	29
5.3.2	統合宛名システム概要	29
5.3.3	主な機能の概要.....	30
5.3.4	統合宛名システムの機能構成.....	30
5.3.5	番号制度への対応について	31
5.3.6	統合宛名システム利用にあたっての手続き概要	34
5.4	文字情報基盤システム(基幹系)	35
5.4.1	構築の背景.....	35
5.4.2	文字情報基盤システムの目的.....	35
5.4.3	文字統合基盤の構成概要.....	35
5.4.4	神戸市外字フォントについて.....	36
5.4.5	文字統合基盤利用にあたっての手続き概要.....	37

5.5	サーバ職員認証基盤（情報系）.....	38
5.5.1	システムの概要と目的	38
5.5.2	システムの機能概要.....	38
5.5.3	利用ガイドラインの提供.....	39
6	ライセンス	40
6.1	マイクロソフト社製品に関する包括契約ライセンスの考え方	40
6.1.1	＜利用できる機器＞	40
6.1.2	＜職員及び外部委託業者等＞	40
6.1.3	＜利用できるライセンス＞	40
6.2	仮想環境におけるライセンスに関する注意事項	41
7	関連ドキュメント	43
7.1	詳細説明資料	43
7.2	申請書.....	43
8	参考ドキュメント	45
8.1	神戸市情報セキュリティポリシー	45
8.2	神戸市の個人情報保護制度	45

1 はじめに

神戸市庁内情報システムの導入に関する手引き(以下、「本書」という。)は、本市において新たに庁内情報システムを導入するにあたり必要となる情報を一括で提供するためのものです。

詳細については「7. 関連ドキュメント」を各管理者から入手してください。

2 サーバ室

2.1 サーバ室の概要

サーバ室の概要を表 2-1 に示します。

※ 本庁舎 1 号館のサーバ室が利用できるのは、令和 8 年度末までの予定です。

別途 4 号館にデジタル戦略部が管理するラックを設置しており、空きユニットを利用することが可能です。本章とは条件が異なりますので、事前にデジタル戦略部に相談してください。

項目	内容	
所在地	場所	神戸市本庁舎 1 号館
サーバ室構造	床面積	約 327 m ²
	耐荷重	500 kg/m ² (搭載機器重量+ラック重量)
	床構造	フリーアクセス床(床高 0.4m)
	消火設備	ハロン消火設備
電源	CVCF	常時インバータ給電方式
		停電時より供給時間 10 分以上
	使用可能電力	計 6kVA/架
	配電方式	単相三線式
	計画停電	年 3 日程度
空調	空調設備	床下型空冷空調機(PAC+セントラル)
	運用	常時室内温度湿度監視
セキュリティ	セキュリティ設備	物理鍵, 防犯カメラ
機器搬入	搬入可能サイズ	W1.35m×D1.4m×H2.1m 以下
	エレベータ	耐荷重 1600kg 以下

表 2-1 サーバ室の概要

2.2 新規機器設置時のルール

2.2.1 機器の設置方法等

設置機器は全て 19 インチラック内に収めてください。現在、既設ラックはありませんので、機器納入業者がラックを用意してください。

2.2.2 設置機器(ラックを含む)の搬入作業

設置機器の搬入作業は、原則、平日の業務時間内(8時45分～17時30分)に行ってください。平日の業務時間内に行えない事情がありましたら、業務システム所管課を通じて、デジタル戦略部に相談してください。

搬入用エレベータの専有使用や駐車場の専有使用を希望する場合は、業務システム所管課を通じて、行財政局庁舎課(庁舎管理係)に相談してください。ただし、専有使用が認められない場合もあります。

2.2.3 機器設置の附帯工事

2.2.3.1 耐震工事

ラックを設置する際は、耐震工事が必須となります。機器納入業者の責任において耐震工事を行ってください。

アンカーボルトを使用して、サーバとフリーアクセス下のコンクリートスラブを固定してください。工事例を「図 2-1. 耐震工事例」に示します。

サーバの幅を超える耐震補強は禁止しています。

耐震工事は、原則、休前日を除く平日の業務時間外(17 時 30 分以降)に施工してください。

2.2.3.2 電源工事

サーバから分電盤までの電源配線工事は、機器納入業者の責任において行ってください(最長 10m 程度)。

サーバ 1 架につき使用可能電力 6kVA の分電盤を 1 つ提供します。

分電盤には、主幹ブレーカ (60A) と分岐ブレーカ (20A×2) (30A×2) を設置しています。詳細は、

「図 2-2. 提供分電盤」を参照してください。

分岐ブレーカが足りない場合は、機器納入業者の施工により、増設することが可能です。

電源工事は、原則、休前日を除く平日の業務時間外(17 時 30 分以降)に施工してください。

2.2.3.3 LAN 配線工事

本市が管理している通信機器からサーバまでの LAN 配線工事は、機器納入業者の責任において行ってください。(最長 100m 程度)

本市が管理している通信機器のインタフェースは「RJ45」です。

LAN ケーブルの色は、接続するネットワークにより、次の通りとしてください。

- 基幹系ネットワークに接続する場合は水色
- 情報系ネットワークに接続する場合は緑色

その他のネットワークに接続する場合や、色の詳細については、業務システム所管課を通じてデジタル戦略部まで相談してください。

LAN ケーブルの起点と終点に、「システム名」、「業務システム所管課名」、「ラック内接続機器名及びポート番号～本市が管理している通信機器名及びポート番号」を記載した線札を付けてください。

本市が管理している通信機器名及びポート番号は、施工前までに業務システム所管課を通じて連絡します。

LAN 工事は、原則、休前日を除く平日の業務時間外(17 時 30 分以降)に施工してください。施工内容によってデジタル戦略部が認めた場合に限り、平日の業務時間内に施工が可能です。

2.2.4 提出書類

ラック設置予定日の 2 週間前までに、業務システム所管課を通じて「サーバ設置予定書」、「ラック搭載機器図(重量及び消費電力等記載されたもの)」をデジタル戦略部まで提出してください。

各提出書類の様式は業務システム所管課を通じて入手してください。

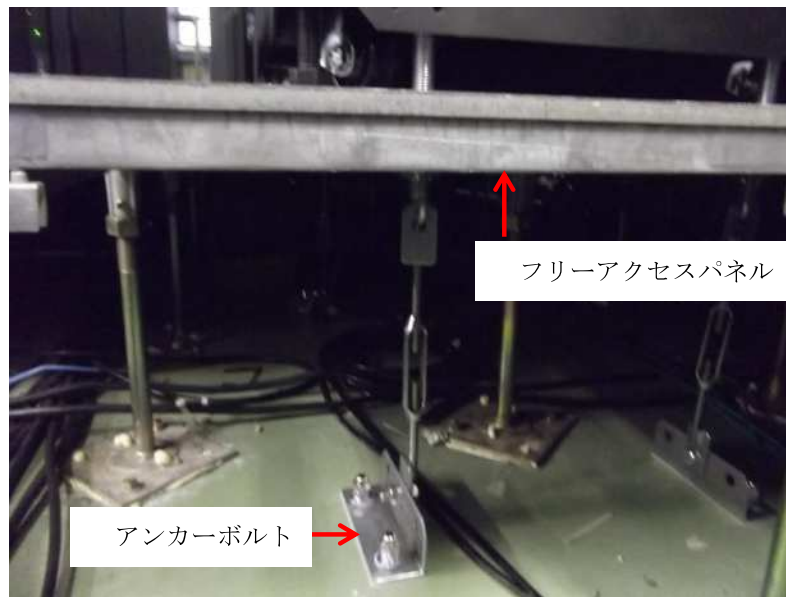


図 2-1 耐震工事例

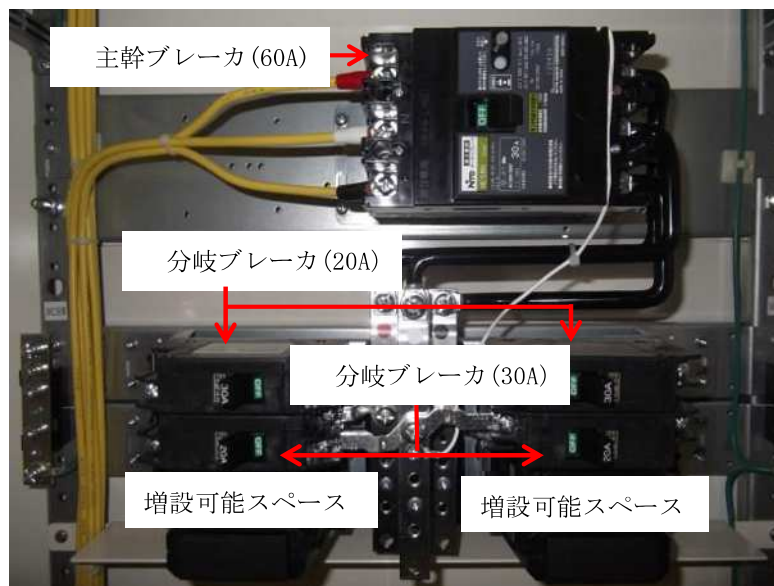


図 2-2 提供分電盤

2.3 機器撤去時のルール

2.3.1 原状復旧工事

2.3.1.1 耐震工事

機器撤去時は、機器納入業者の責任においてラック耐震施工の撤去工事を行ってください。

施工は、原則、休前日を除く平日の業務時間外(17時30分以降)に行ってください。

2.3.1.2 電源工事

機器撤去時は、機器納入業者の責任においてサーバから分電盤までの電源配線の撤去工事を行ってください。

分電盤に分岐ブレーカを増設している場合は、ブレーカの撤去工事も行ってください。

施工は、原則、休前日を除く平日の業務時間外(17時30分以降)に行ってください。

2.3.1.3 LAN 配線工事

機器撤去時は、機器納入業者の責任において本市が管理している通信機器からサーバまでの LAN 配線の撤去工事を行ってください。

施工は、原則、休前日を除く平日の業務時間外(17 時 30 分以降)に行ってください。施工内容によってデジタル戦略部が認めた場合に限り、平日の業務時間内に施工が可能です。

2.3.2 提出書類

撤去予定日の2 週間前までに、業務システム所管課を通じて、「サーバ撤去予定書」をデジタル戦略部まで提出してください。

サーバ撤去作業が完了しましたら、業務システム所管課を通じて速やかに「サーバ撤去終了報告書」をデジタル戦略部まで提出してください。

2.4 サーバ室の運用ルール

2.4.1 搭載機器変更時のルール

サーバ内に搭載された機器を追加又は撤去する場合は、業務システム所管課を通じて「ラック搭載機器図(重量及び消費電力等記載されたもの)」をデジタル戦略部まで提出してください。

機器の追加または撤去の際に工事が必要な場合は、業務システム所管課を通じて工事予定日の2 週間前までにデジタル戦略部まで連絡してください。

2.4.2 サーバ室入退室のルール

サーバ室への入室が必要な場合は、業務システム所管課の職員とともにデジタル戦略部まで入室証の貸与手続きに来てください。入室者 1 名につき入室証を 1 枚貸与します。

平日の業務時間外にサーバ室へ入室する場合は、当日の業務時間内に手続きに来てください。

休日にサーバ室へ入室する場合は、前開庁日の業務時間内に手続きに来てください。

サーバ室での作業は、業務システム所管課の職員の監督の下で行ってください。業者の方のみでのサーバ室への入室は禁止しています。

2.4.3 その他

サーバ室はサーバを設置することが目的のため、サーバ室内でのシステム開発作業は禁止しています。

3 ネットワーク

3.1 基幹系ネットワーク

3.1.1 背景と目的

平成 25 年 5 月に「行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）」（以下、「番号法」という。）が成立したことに伴い、本市では「個人番号に関連するシステム」のみを対象とし、利用にあたっての厳格なルールを設定した「基幹系ネットワーク」を構築しています。これは個人番号利用事務等のインターネットリスクからの分離、住民情報の流出防止を徹底することを目的としています。

なお、対象システムである「個人番号に関連するシステム」は、具体的には下記の2つの事務を取り扱うシステムです。

- 1) 個人番号利用事務（番号法の別表 1 に記載されている事務）又は情報提供者となりうる事務（番号法の別表 2 に記載されている事務）
- 2) 1) と経常的にデータ連携を行っている事務

3.1.2 ネットワーク構成(WAN)

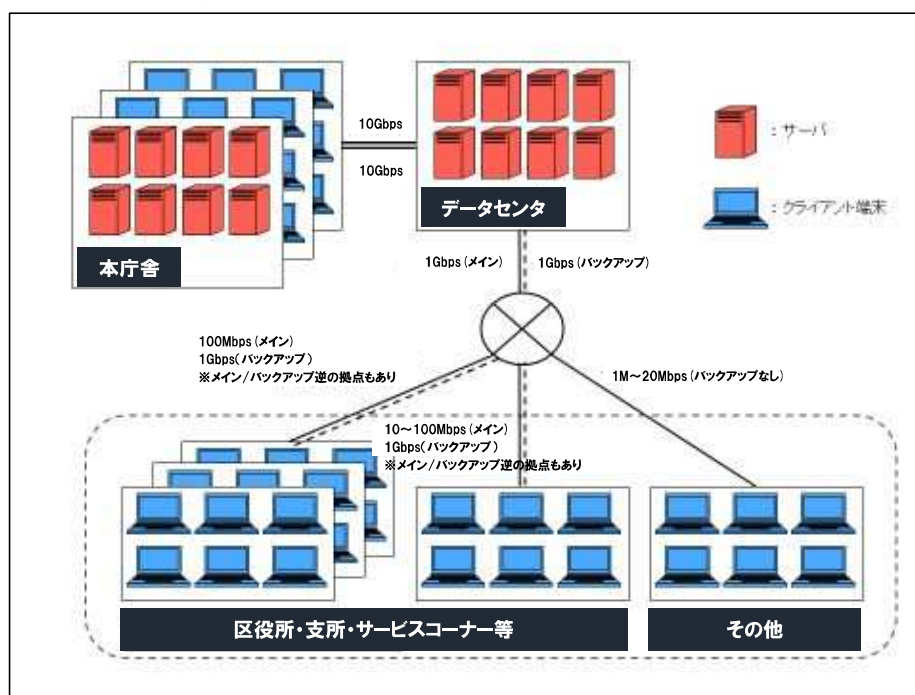


図 3-1 WAN 構成概要図

サーバの設置場所は、サーバ室（本庁舎１号館（令和８年度末まで））又はデータセンタ等とし、事務室への設置は禁止します。ただし、業務データを保存していないプリンタサーバ等については除きます。

区役所、支所、出張所等、重要拠点の WAN 回線は冗長化されています。

障害時に迅速に対応するため、重要拠点の WAN 回線はデジタル戦略部が管理しています。WAN 回線の新規契約及び変更契約を締結する場合は、事前にデジタル戦略部へ連絡してください。

3.1.3 ネットワーク構成(LAN)

3.1.3.1 本庁舎及び拠点

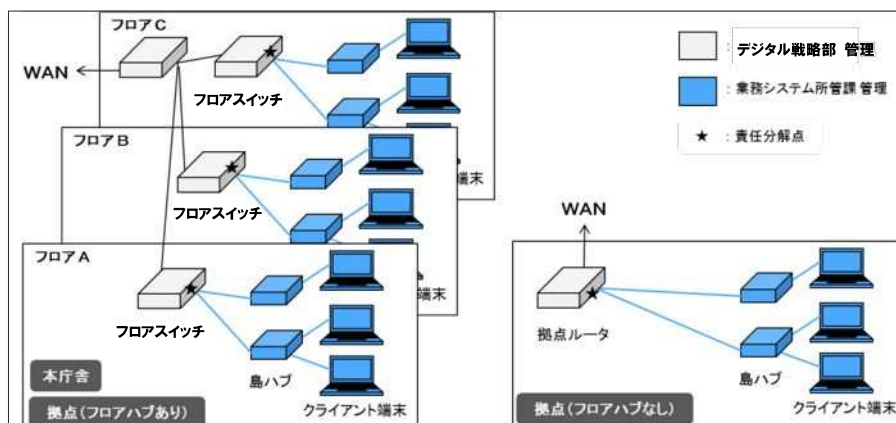


図 3-2 LAN 構成概要図（本庁舎及び拠点）

拠点のフロア毎にフロアスイッチ 2 台を設置しています。フロアスイッチの指定ポートに島ハブを接続し、島ハブを経由して業務システムのクライアント端末を接続してください。

区役所等の拠点においては、業務継続性の観点から、業務窓口クライアント端末を設置する際は、接続先ができるだけ1つのフロアハブに偏らないよう考慮してください。

フロアスイッチがない拠点については拠点ルータに島ハブを接続してください。

責任分界点は「フロアスイッチのポート」又は「拠点ルータのポート」となります。

3.1.3.2 サーバ室

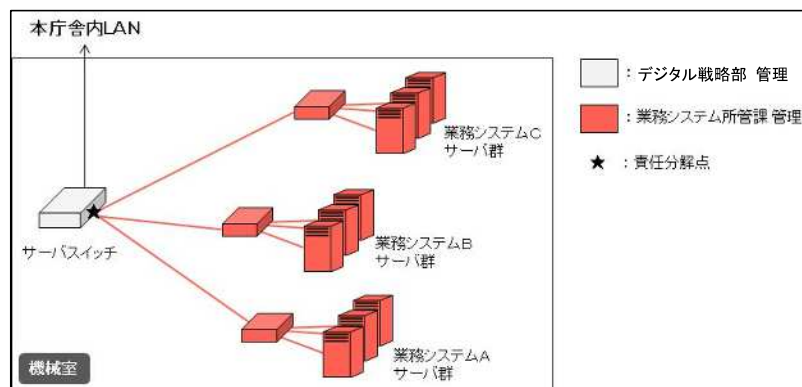


図 3-3 LAN 構成概要図（サーバ室）

サーバ室に業務システムを接続するためのスイッチ（以下、「サーバスイッチ」という。）を設置しています。サーバスイッチの指定ポートに業務システムのサーバ群を接続してください。

責任分界点は「サーバスイッチのポート」となります。

3.1.4 利用にあたってのルール

「インターネットリスクからの分離」「住民情報の流出防止」を徹底するため、以下のルールを遵守してください。

3.1.4.1 データベースへのアクセスログ管理の実施

業務データが格納されているデータベースへのアクセスログを業務システム側で収集・管理してください。

なお、収集・管理用のソフトウェアとして SKYSEA Client View（以下、「SKYSEA」という。）を提供します。対応 OS（※）の業務システムのサーバ・クライアント端末（以下、「機器」という。）については、SKYSEA をインストールしてください。ライセンス調達は、デジタル戦略部で一括で行っていますが、急遽必要となった場合はデジタル戦略部に連絡のうえ、業務システム側で調達してください。

※ 対応 OS は Windows, Mac 及び Red Hat Linux サーバです。対応していないバージョンもありますので、最新の対応状況については、デジタル戦略部までお問い合わせください。

3.1.4.2 操作ログ管理の実施

全ての機器の操作ログ（※）を業務システム側で収集・管理してください。

なお、デジタル戦略部が提供する SKYSEA で操作ログの収集・管理が可能です。SKYSEA が利用 OS に対応していない等、SKYSEA での操作ログの収集・管理が不可能な場合は業務システム側で操作ログの収集・管理を実施してください。

※ ファイル操作記録（作成、削除、コピー）、外部媒体のアクセス記録、プリンタ出力記録等

3.1.4.3 外部媒体の利用制限

全ての機器に対して、不必要な外部媒体利用がないよう制限を実施してください。**特に外部媒体への書き出しについては原則禁止**とします。

ただし、国への報告等で外部媒体に書き出す必要がある場合は、毎年操作ログ等により実績を報告することを条件として、例外的に許可することがあります。業務システム所管課を通してデジタル戦略部ネットワーク担当へ相談してください。

※ 操作ログ管理用にインストールする SKYSEA の機能として「デバイス管理」機能があります。この機能を利用すれば外部媒体への利用制限が可能となります。

3.1.4.4 2要素認証の導入

業務システムへの認証にあたっては2要素認証を実施してください。

2要素認証とは下記の3要素のうち、異なる2つを組み合わせで認証することを意味します。

- 1) ユーザが知っていること（パスワード等） .. 知識情報認証
- 2) ユーザが持っているもの（IC カード等） .. 所有情報認証
- 3) ユーザの身体的特性（指紋、静脈等） .. 生体情報認証

※ 操作ログ管理用にインストールする SKYSEA の機能として「USB メモリによるコンピュータ使用制限」機能があります。各個人毎に個別の USB メモリを準備する等により、上記2)の要素として利用することが可能となります。

3.1.4.5 外部ネットワークとの接続禁止

外部のネットワークとの接続を原則禁止とします。

やむを得ず外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス) 及びアプリケーションプロトコル(ポート番号) のレベルでの限定を行わなければなりません。また、その外部接続先についてもインターネット等と接続してはなりません。

ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先として本市情報セキュリティ統括責任者が認めるものについては、この限りではなく、LGWAN を経由して、インターネット等と基幹系ネットワークとの双方向通信でのデータの移送を可能とします。

3.1.4.6 ウイルス対策の実施

全ての機器に対して、ウイルス対策ソフトをインストールし、定期的にパターンファイルを更新してください。

特別な事情がない限り、クライアント端末については Symantec Endpoint Protection (以下、「SEP」という。) に指定します。インストーラはデジタル戦略部が用意しますので、ライセンスの調達及びインストール作業は業務システム側で行ってください。SEP が利用 OS に対応していない等、特別な事情がある場合はデジタル戦略部ネットワーク担当に相談のうえ、業務システム側でウイルス対策を実施してください。

3.1.4.7 業務システム用ファイアウォールの設置

業務システムのサーバセグメントを不正なアクセスから守るため、必ずファイアウォールを設置してください。

3.1.4.8 業務システム時刻の同期

業務システム内の時刻については、デジタル戦略部が設置している基幹系ネットワーク内の標準時間を定めたサーバ(NTP サーバ)と同期を取ってください。NTP サーバの利用を希望する場合は、業務システム所管課を通してデジタル戦略部ネットワーク担当に申請書を提出してください。

3.1.4.9 インベントリ情報報告

本市ではソフトウェアライセンスを厳格に管理するため、全市的にライセンス管理システムを導入しています。業務システム所管課により下記の作業が必要となりますので、情報の提供をお願いします。なお、作業時の報告項目等の詳細情報については業務システム所管課にお問い合わせください。

実施時期	作業内容
機器導入時	機器とソフトウェアの登録作業
年 1 回	機器とソフトウェアの棚卸作業 (各機器にインストールされているソフトウェアの情報収集など)

表 3-1 インベントリ情報報告作業

※ 操作ログ管理用にインストールする SKYSEA の機能として「資産管理」機能があります。この機能を利用することも可能です。

3.1.4.10 SKYSEA の導入について

ログ管理機能等の利用にあたっては、管理用クライアントが 1 台以上必要になりますので、業務システム側で準備をお願いします。

サーバへのインストールについては、他ソフトウェアとの相性等で誤作動の原因となる可能性

もありますので、事前に業務システム側でベンダーや委託業者に確認していただき、インストールの可否を判断してください。

3.1.5 提供サービス

基幹系ネットワークでは以下のサービスを提供しています。【必須】と記載したサービスについては 3.1.4. で提示したルール遵守のため、必ず利用してください。またそれ以外のサービスについても、セキュリティ向上、コスト削減につながりますので積極的に利用してください。

3.1.5.1 機器管理用サーバ【必須】

機器管理用 SKYSEA サーバを提供します。機器の操作ログは全てこのサーバに蓄積され、業務システム側で準備する管理機により、自システム内の機器に対してのみ閲覧・制御が可能です。

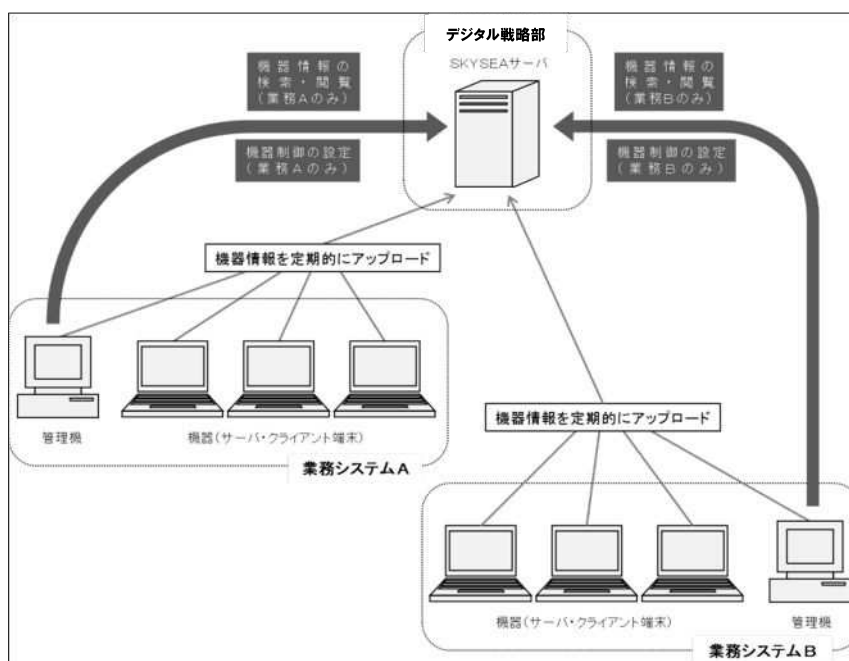


図 3-4 機器管理サービス構成概要

3.1.5.2 ウイルス対策ソフト配信【必須】

SEP 用のウイルスパターンファイルを配信するサーバを提供します。

概要は以下のとおりです。

3.1.5.2.1 配信の仕組み

ネットワーク負荷を軽減させるため、SEP の「グループ更新プロバイダ (GUP)」と呼ばれる機能を利用し、各機器に対して GUP 経由でパターンファイルを配信します。

デジタル戦略部の機器がない拠点等については、業務システムの端末に対して GUP の役割をお願いすることがあります。GUP の設定に関して、業務システム側での作業は特に必要ありませんが、端末のハードディスク容量を 1 GB 程度使用させていただきます。

3.1.5.2.2 インストール方法

インストール用 CD を提供します（ライセンスは提供しません）ので、業務システム側でインストール作業を実施してください。

3.1.5.2.3 不具合時の対応

SEP に関するトラブルについては、原則として業務システム側で対応してください。ただし、デジタル戦略部もトラブル解決に向けてサポートします。

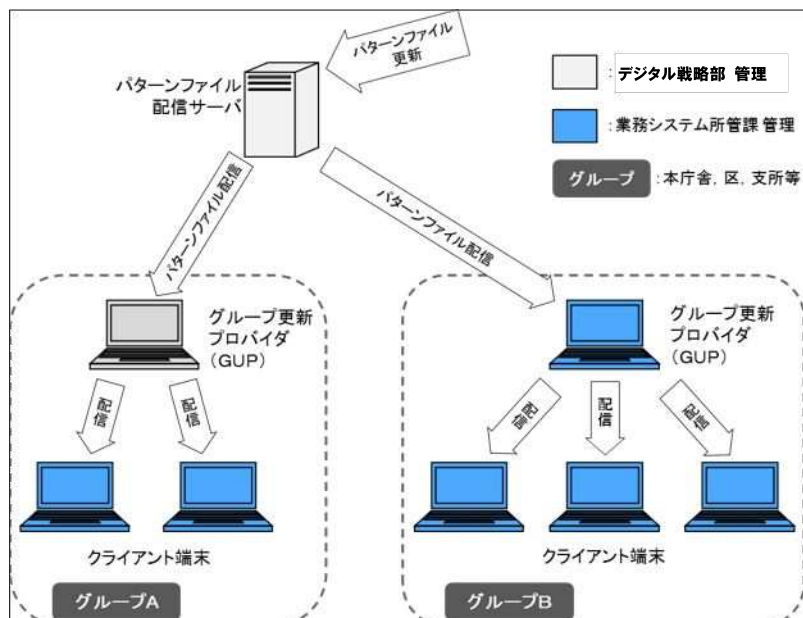


図 3-5 ウイルス対策ソフトパターンファイル配信の仕組み

3.1.5.3 NTP サーバ【必須】

基幹系ネットワーク内の標準時間と同期するための NTP サーバを提供します。

3.1.5.4 Windows Server Update Services (WSUS) サーバ

デジタル戦略部により WSUS サーバを設置しています (WSUS 構成概要は、図 3-9 のとおり)。業務システム所管課を通してデジタル戦略部ネットワーク担当へ申請書を提出することにより、業務システムから利用可能です。

3.1.5.5 障害通報用メールサーバ

デジタル戦略部で障害通報用メールサーバを構築しています。利用を希望する場合は、送信元 IP アドレス・送信元メールアドレス・送信先メールアドレスを定め、業務システム所管課を通してデジタル戦略部ネットワーク担当へ申請してください。

3.1.6 利用にあたってのルールと提供サービスの関係

「3.1.4. 利用にあたってのルール」の各項目に対応する「3.1.5. 提供サービス」の項目は以下のとおりです。提供サービスの利用種別欄に「必須」と記載されたものについては必ずサービスを利用してください。「任意」と記載されたものについては必要に応じて利用してください。

3.1.4. 利用にあたってのルール		3.1.5. 提供サービス		
項番	内容	項番	内容	利用種別
1	データベースのアクセスログの収集・管理	1	SKYSEA サーバ	△ 任意
2	機器の操作ログの収集・管理 ・SKYSEA のインストール ・管理機の準備	1	SKYSEA サーバ	◎ 必須
3	外部媒体の利用制限（書き出し禁止）	1	SKYSEA サーバ	△ 任意
4	2要素認証の導入	1	SKYSEA サーバ	△ 任意
5	外部ネットワークとの接続禁止	対応する提供サービスなし		
6	ウイルス対策の実施 ・SEP インストール	2	パターンファイル 配信サーバ	◎ 必須
8	業務システム時刻の同期 ・基幹系ネットワーク標準時刻との同期	3	NTP サーバ	◎ 必須
9	インベントリ情報報告	1	SKYSEA サーバ	△ 任意

表 3-2 利用にあたってのルール及び提供サービス

3.1.7 利用にあたっての手続き概要

基幹系ネットワークに加入する際に必要な申請は以下のとおりです。

様式	申請書
様式 1	基幹系ネットワーク利用申請書
様式 2	IP アドレス配布申請書
様式 3	IP アドレス返却申請書
様式 4	NTP サーバ接続申請書
様式 5	SEP 追加配信依頼書
様式 6	SKYSEA 利用申請書
様式 7	障害通報用メールサーバ利用申請書
様式 8	ネットワーク設定依頼書
—	保守業者用 VPN 利用申請書

※ 保守業者用 VPN は、デジタル戦略部が指定するネットワークサービスを経由し、業務システム保守事業者の拠点に設置した専用の保守端末からサーバの保守を行う環境です。アクセス回線、VPN ルータ及び保守端末の費用については、業務システム側の負担となります。また、不正なアクセスを防止するため、基幹系ネットワーク内に保守業者接続用ファイアウォールを設置しています。使用する IP アドレス、ポート番号について業務システム所管課を通してデジタル戦略部ネットワーク担当まで申請してください。本保守環境は「3.1.4.5 外部ネットワークとの接続禁止」の例外事項として提供します。「インターネットリスクからの分離」「住民情報の流出防止」の観点から、「操作ログの管理」「外部媒体の利用制限」をデジタル戦略部側で実施します。必要なソフトウェア等を提供しますので保守端末への

インストール作業等を行ってください。

3.1.8 留意事項

各業務システムで利用する機器は、各業務システム所管課で調達、管理してください。

基幹系ネットワークにて端末認証を実施しているため、各業務システムで利用する機器についてはデジタル戦略部ネットワーク担当への登録が必要になります。故障時等で機器が変更になった際にも再登録が必要になるので注意してください。

基幹系ネットワークは固定 IP アドレス制であり、業務システム所管課を通してデジタル戦略部ネットワーク担当に申請書を提出することにより IP アドレスを付与します。業務システム側にてクライアント端末に設定を行ってください。

他のシステムに迷惑をかけるような通信（大量の FTP 通信等）は避けてください。止むを得ない場合は事前に、業務システム所管課を通してデジタル戦略部ネットワーク担当に相談してください。

各業務システム間のデータ連携についてはデジタル戦略部が提供する共通サービスである共通基盤システムを利用してください。なお、詳細については「5.2 共通基盤システム（基幹系）」を参照してください。

大量データ印刷環境についてはデジタル戦略部では提供しません。業務システム側でアウトソーシング等にて対応してください。

3.2 情報系ネットワーク

情報系ネットワークとは、国が示した「自治体情報システム強靱性向上モデル」におけるインターネット接続系ネットワークと LGWAN 接続系ネットワークに接続するネットワークを指します。

3.2.1 背景と目的

情報系ネットワークは、内部事務の効率化を目的としたシステム群と事務処理用 PC が配置されたネットワークです。

3.2.2 構成

WAN, LAN（本庁舎・各拠点）を含めたネットワーク全体の物理構成図及び論理構成図を次に示します。

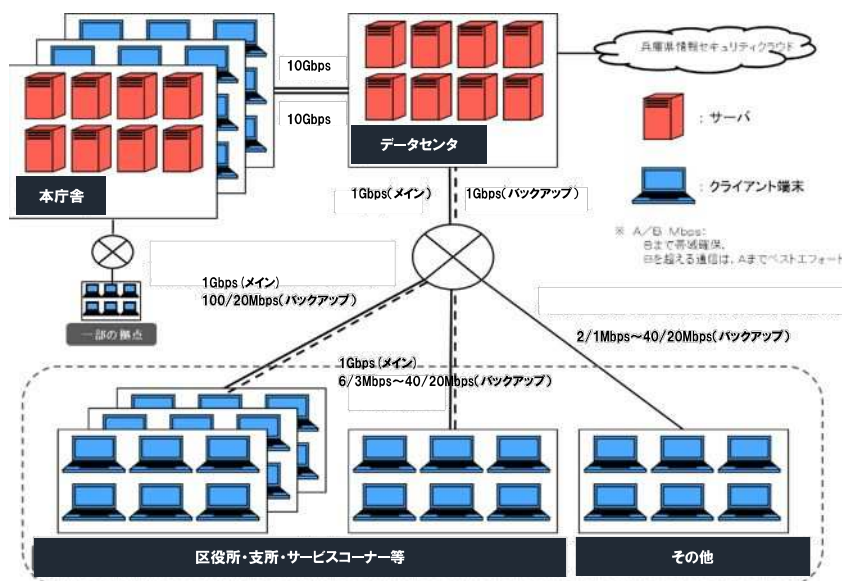


図 3-6 ネットワーク全体の物理構成図

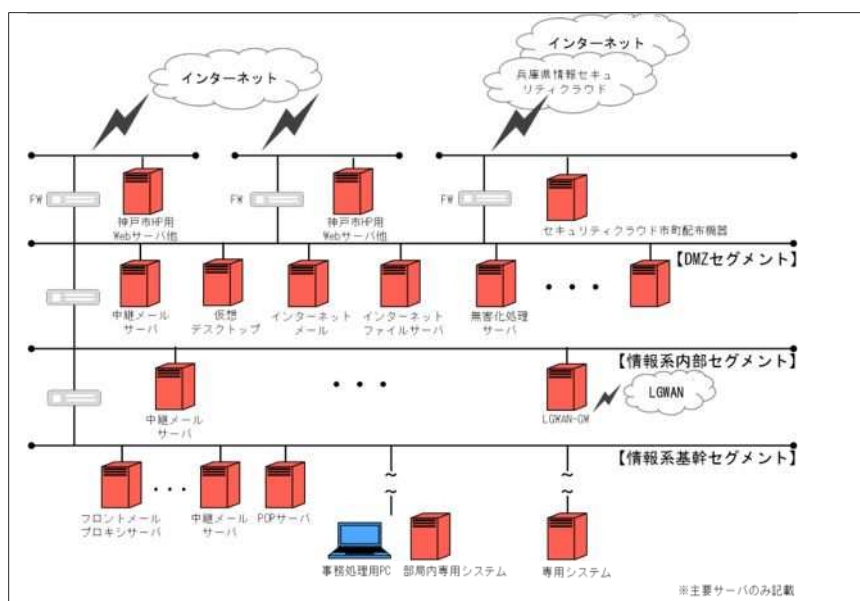


図 3-7 ネットワーク全体の論理構成図

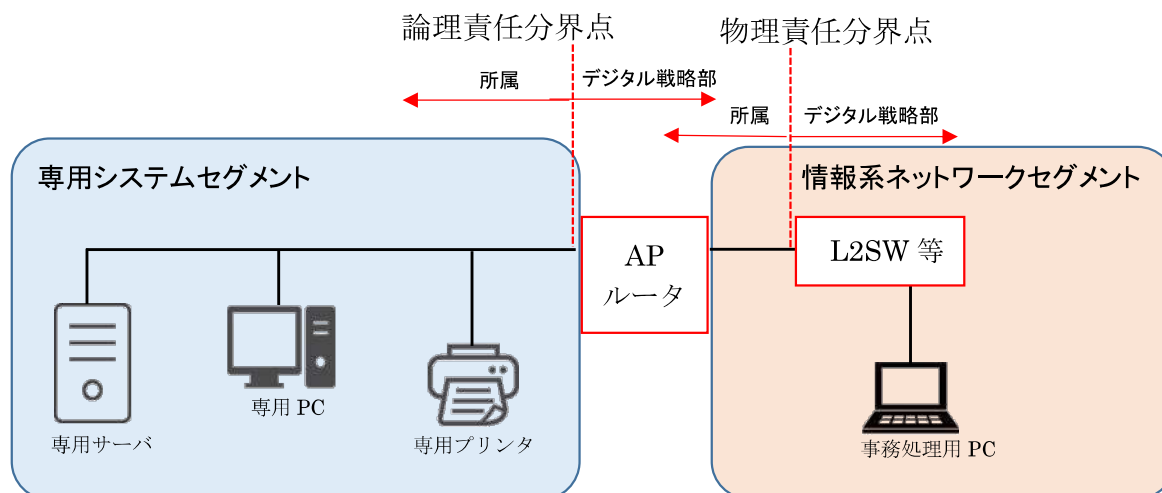
3.2.3 LAN(本庁舎・各拠点)

情報系ネットワーク上では、財務会計システム、文書管理・電子決裁システム、庶務事務システム等の全庁的に事務処理用 PC で処理を行うシステム群のほか、各種の専用システムが稼働しており、市役所本庁舎、区役所、支所、出張所、保育所、クリーンセンター、消防署、建設事務所等約 250 か所の拠点がつながっています。

専用システムを情報系ネットワークに接続する場合の手続については、3.2.7 に記載しています。責任分界点は、以下のとおりです。

3.2.3.1 責任分界点

サーバ等を設置する専用システムセグメントを情報系ネットワークに接続する場合、本市が管理する L2SW 等接続口(RJ-45 コネクタ)に本市指定のルータ（以下 AP ルータ）を介して UTP ケーブルで接続するものとし、考え方は次のとおりです。なお、AP ルータについては、所管課の職員を通じてデジタル戦略部ネットワーク担当に確認してください。



項番	責任分界点	考え方
1	物理的責任分界点	本市が指定する L2SW 接続口を物理的責任分界点とする。
2	論理的責任分界点	AP ルータは専用システム側の調達範囲であるが、設定作業はデジタル戦略部で実施するものとし、ここを論理的責任分界点とする。

表 3-3 責任分界点

3.2.4 WAN

WAN 回線は、データセンタ（DC）（一部を除く）に集約しています。

メイン回線は、区役所・支所・出張所等は、1 Gbps の帯域確保型の回線（基幹系ネットワークのバックアップ回線との統合網）、その他の拠点は、一部帯域確保型（確保帯域を超える場合は、契約帯域までベストエフォートとなる。）の回線を利用しています。

バックアップ回線は、区役所、支所、出張所等のみで一部帯域確保型の回線を利用しています。

メイン回線とバックアップ回線とは、キャリアを分散しています。

WAN 構成の概要は下図のとおりです。

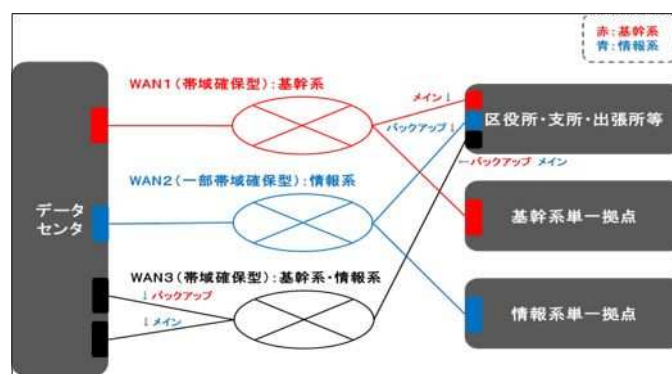


図 3-8 WAN 構成概要

3.2.5 サーバ

情報系ネットワークが基幹サーバで各システムに提供している主な機能は、次のとおりです。

項番	サーバ名	提供機能
1	NTP サーバ	本市情報系ネットワークの NTP サーバは、各業務システムで利用することができる。
2	DNS サーバ	<p>情報系ネットワークの DNS サーバは、各業務システムで利用することができる。登録できるドメイン名は1システム1つで、任意のサブドメイン（http(s)://〇〇〇.〇〇〇.city.kobe.lg.jp の〇〇〇の部分で使用できる文字は半角英数字）を登録する場合は、既存の他システムとのドメイン名の重複、使用文字制限等を確認するため、所管課の職員を通じてデジタル戦略部ネットワーク担当に必ず相談すること。</p> <p>ドメイン名が複数必要な場合は、割り当てられているネットワークセグメント内に自ら DNS サーバを構築すること。</p>
3	DHCP サーバ	情報系ネットワークの DHCP サーバは、事務処理用 PC 及び庁内 LAN 接続端末に対して機能を提供するものであり、各業務システムセグメント内の IP アドレス割り当てには利用することができない。必要に応じて、割り当てられているネットワークセグメント内に自ら DHCP サーバを構築すること。
4	SMTP サーバ	情報系ネットワークの SMTP サーバは、各業務システムで利用することができる。ただし、発信専用のメールアドレスは割り当てない。
5	POP サーバ	情報系ネットワークの POP サーバは、各業務システムが利用することはできない。必要に応じて、割り当てられているネットワークセグメント内に自ら POP サーバを構築すること。
6	WSUS	<p>各業務システムでアップストリームサーバ及びダウンストリームサーバを利用することができる。各業務システムでダウンストリームサーバを構築し、サーバ及び端末に配信すること。</p> <p>WSUS の更新プログラムは日本語版のみとし、製品とクラス (※) は、以下のとおり。</p>

項番	サーバ名	提供機能
		<u>Office</u> Office 2013, 2016, 365 Client <u>Silverlight</u> Silverlight <u>SQL Server</u> SQL Server 2014, 2016, 2017 SQL Server Management Studio v17, v18 SQL Server 2014-2016 Product Updates for Setup SQL Server Feature Pack <u>Windows</u> Windows 10, 10 Language Packs Windows 8.1, 8.1 Language Packs Windows Defender Antivirus Windows Server 2016, 2019, version 1903 and later Windows Server 2012 R2, R2 Language Packs Windows Server 2012, Language Packs ※カテゴリ : Service Packs, Upgrades セキュリティ問題の修正プログラム, 修正プログラム集 重要な更新, 定義更新プログラム WSUS 構成の概要は, 図 3-9 のとおり。
7	ウイルス定義配布サーバ	SEP (Symantec Endpoint Protection) のウイルス定義ファイル配信サーバを利用することができる。SEP 構成の概要は, 図 3-10 のとおり。

表 3-4 提供機能一覧

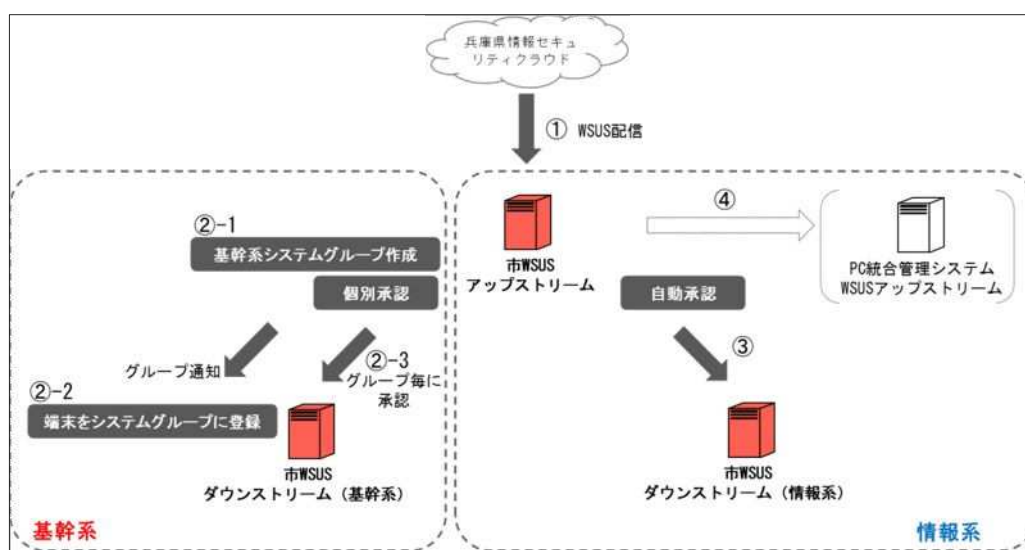


図 3-9 WSUS 構成概要

- 1) 市 WSUS アップストリームサーバは、兵庫県情報セキュリティクラウドより、更新プログラムを取得します。
- 2) -1 市 WSUS アップストリームサーバでは、基幹系ネットワークのシステムグループをあらかじめ作成します。
 -2 市 WSUS ダウンストリームサーバ（基幹系）では、あらかじめシステム端末をシステムグループに登録しておきます。
 -3 市 WSUS アップストリームサーバでは、基幹系システムグループ毎に配信承認を行います。承認された更新プログラムは、市 WSUS ダウンストリームサーバ（基幹系）で配信されます。
- 3) 市 WSUS アップストリームサーバから、市 WSUS ダウンストリームサーバ（情報系）へは、承認なしで配信されます。
- 4) PC 統合管理システムの WSUS アップストリームサーバは、市 WSUS アップストリームサーバを参照し、更新プログラムを取得します。

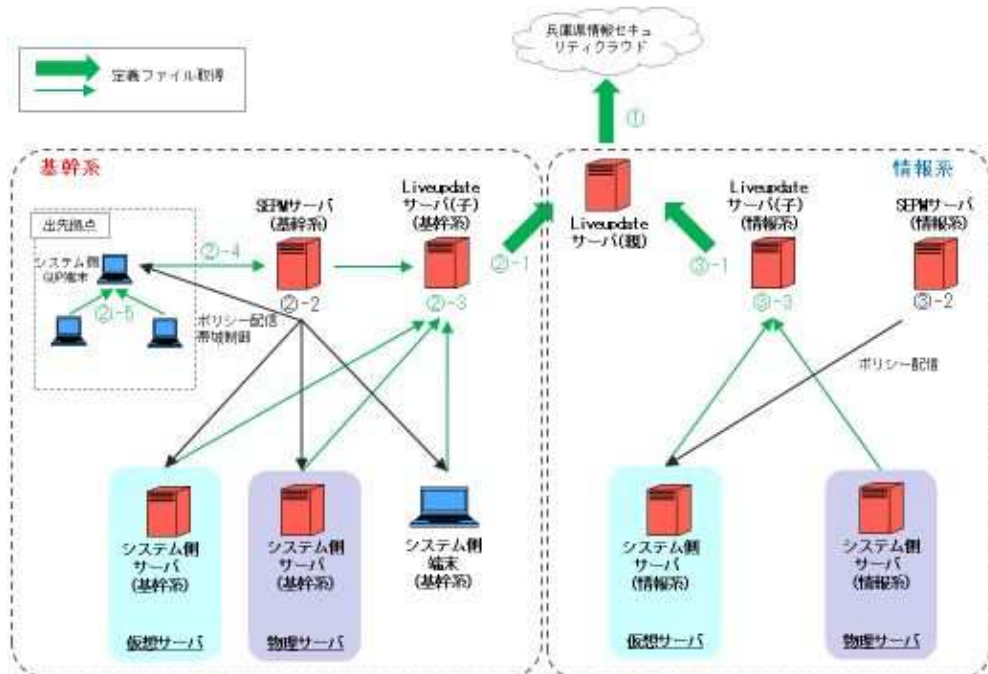


図 3-10 SEP 構成概要

- 1) Liveupdate サーバ（親）は、兵庫県情報セキュリティクラウドより、定義ファイルを取得します。
- 2) -1 Liveupdate サーバ（子）（基幹系）は、Liveupdate サーバ（親）から定義ファイルを取得します。
 -2 SEPM サーバ（基幹系）では、システム側サーバ（基幹系）及び端末（基幹系）にポリシー配信を行います。出先拠点については、事前に登録した情報を基に GUP ポリシーによる帯域制御を行います。
 -3 出先拠点以外のシステム側サーバ（基幹系）及び端末（基幹系）は、Liveupdate サーバ（子）（基幹系）から定義ファイルを取得します。
 -4 出先拠点の GUP 端末は、出先拠点の代表として SEPM サーバ（基幹系）から定義ファイルを取得します。
 -5 出先拠点の GUP 端末以外の端末は、出先拠点の代表端末から定義ファイルを取得しま

す。

- 3) -1 Liveupdate サーバ(子) (情報系) は、Liveupdate サーバ(親)から定義ファイルを取得します。
- 2 SEPM サーバ (情報系) では、仮想化基盤上のシステム側サーバ (情報系) にポリシー配信を行います。
- 3 システム側サーバ (情報系) は、Liveupdate サーバ(子) (情報系) から定義ファイルを取得します。

3.2.6 対外接続点

情報系ネットワークから LGWAN 等の外部ネットワークへ接続可能ですが、接続方法等については、所管課の職員を通じてデジタル戦略部ネットワーク担当に相談してください。

3.2.7 利用にあたっての手続き概要

規定や依頼書等は表 3-5、検討相談を要する事項については表 3-6 をご確認ください。

文書名	内容
ネットワーク設定依頼書	利用目的や接続にあたり必要な設定を記入し、提出いただく様式です。
ネットワーク設定依頼書 別紙 ネットワーク接続設定内容	システムの論理構成図と使用する通信プロトコル等を記入し、「情報系・基幹系ネットワーク設定依頼書」とともに提出してください。

表 3-5 文書一覧

項番	事項	必須	確認等
1	通信プロトコル・ポート番号		○
2	神戸市が指定するルータ機種		○
3	情報系ネットワークに専用システムセグメントを接続する場合の神戸市指定ルータの設置	○	
4	DNS サーバに登録するドメイン名		○
5	SEPM(SymantecEndpointProtectionManager)の設置	○	
6	SEPM が設置できない場合の対応方法		○
7	専用システムでの外部 (インターネット) 接続		○
8	専用システムでのメール通知		○
9	専用システム間のデータ連携機能の作成	○	

表 3-6 準備必須/確認相談事項一覧

3.2.8 留意事項

帳票印刷は、情報系ネットワークに接続している所属の共用プリンタで行ってください。

情報系ネットワーク上に新たに専用システムを構築又は国等が作成したシステム (パッケージシステムを含む) を導入することを検討する場合は、以下を参考にしてください。

「5.1 サーバ仮想化基盤 (基幹系・情報系)」に記載しているサーバ仮想化基盤が利用できないか調査検討してください。

その結果、サーバ仮想化基盤を利用できる場合は、利用に必要な手続をとってください。

構築又は導入予定の専用システムが何らかの理由により、サーバ仮想化基盤を利用できないことが判明した場合は、独自にサーバ等を設置する必要があります。

独自にサーバ等を情報系ネットワーク上に設置する場合には、デジタル戦略部ネットワーク担当が専用システム用セグメントを割り当てますので、当該専用システムセグメントと情報系ネットワークとの境界に本市指定のルータを必ず設置してください。責任分解点については、3.2.3.1を参照してください。

原則として、専用システムからインターネットへ接続できません。業務上必要な場合は、所管課の職員を通じてデジタル戦略部ネットワーク担当に相談してください。また、専用システムが情報系ネットワーク上の他網の専用システムに接続する場合は、サーバ間で通信を行うようにしてください。詳細は、所管課の職員を通じてデジタル戦略部ネットワーク担当に確認してください。

情報系ネットワーク上にはデータ連携基盤がないため、データ連携が必要な場合は、各関係システム所管課を通じてデジタル戦略部ネットワーク担当と協議を行い、独自に仕組みを構築してください。

専用システムで処理結果等をメールで通知する場合の方法等については、所管課の職員を通じてデジタル戦略部ネットワーク担当に相談してください。

3.3 独自プロバイダとの契約

国等が構築したシステムの利用等のために、デジタル戦略部が管理するイントラネット回線以外に、独自でインターネットを利用するためのプロバイダ契約を行う場合は、事前に申請手続が必要です。

3.3.1 手順

- 1) 契約するプロバイダの情報を収集する。
- 2) 新たに専用パソコンを調達する場合は、情報システムコードの付与を受けてから、専用パソコン調達の申請手続を行う。
- 3) プロバイダ契約を行う。

4 情報系端末(事務処理用 PC)

事務処理用 PC は、必要最小限のハードウェア仕様及び標準ソフトウェア構成を基にデジタル戦略部が調達仕様書を作成し、一括で調達しています。調達した実機は、年度ごとに様々であり、下表には、その最低スペックを掲げています。なお、設定内容は変更できません。OS, Microsoft Edge, Office, Adobe Acrobat Reader, +Lhaca, レジストリ, BIOS の標準設定について、必要な場合は、所管課の職員を通じて、デジタル戦略部 PC・基盤システム担当に相談してください。

4.1 ハードウェアの基本構成

項番	項目	事務処理用 PC (推奨スペック (64BIT))
1	基本形式	A4 サイズのノートパソコンを基本とする
2	CPU	2 ギガヘルツ (GHz) 程度の 64 ビットプロセッサ
3	メモリ	8 ギガバイト

項番	項目	事務処理用 PC（推奨スペック（64BIT））
4	ストレージ（SSD）	128GB 容量には空き容量を含む。
5	有線ネットワーク	※ 1000BASE-T/100BASE-TX 対応
	無線ネットワーク	IEEE802.11ac, Bluetooth
6	表示機能	TFT カラー液晶ディスプレイ
7	インタフェース	USB ポート×2（USB インタフェース Ver2.0）以上

表 4-1 ハードウェアの基本構成一覧

4.2 標準ソフトウェア(※)

項番	ソフトウェア名称	機能	備考
1	Windows 10 Enterprise (64bit)	OS	Future Update は年 1 回実施する。 最新バージョンは、デジタル戦略部に確認すること。
2	Microsoft Edge Google Chrome	ブラウザ	
3	Microsoft Office professional Plus 2016 (32bit)	オフィス統合製品	Word, Excel, PowerPoint, Access, Outlook, Onenote, Publisher, Visio Viewer, Office ツール (Office 共有機能含む)
4	.NET Framework	AP 実行環境	最新バージョンはデジタル戦略部に確認すること。
5	Windows Defender	ウイルス対策	
6	NFC Port Software	認証関連	
7	日立指静脈認証管理	認証関連	
8	インターネット用 PC インストールパック	インターネット分割	
9	Adobe Acrobat Reader DC	PDF ファイル表示	
10	CubePDF	PDF ファイル作成	職員が任意でインストール
11	+Lhaca	解凍・圧縮	職員が任意でインストール
12	FFFTP	ファイル転送	職員が任意でインストール
13	VLC media player	動画再生	職員が任意でインストール
14	SFCard Viewer 2	Felica 読取	職員が任意でインストール

表 4-2 標準ソフトウェア一覧

【注意】

事務処理用 PC は、職務上、常時使用する職員の人数分の台数を払い出すことを基本としています。人員増に伴う台数増については、前年度から把握していた場合のみ認め、当該年度途中での増は認められません。やむを得ない事情により、当該年度途中で事務処理用 PC の払出しが必要となる場合や、所属の職員数以上の PC の払出しが必要となる場合は、事前に期間的余裕を持ってデジタル戦略部に相談してください。その場合は、所属に費用負担を求める場合があります。

また、原則として職員以外（委託事業者等）の使用は認めていません。事業者が委託業務を遂

行する上で事務処理用 PC が必要な場合は、必ず事前にデジタル戦略部に相談してください。

5 共通サービス

5.1 サーバ仮想化基盤(基幹系・情報系)

5.1.1 構築の背景

本市においては、ホストオープン化や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、維持管理コストの増大や設置スペースの枯渇が課題となっています。

これらの課題を解決するため、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することにより全体最適化を図っています。

5.1.2 サーバ仮想化基盤の全体概要(構成, 提供サービス)

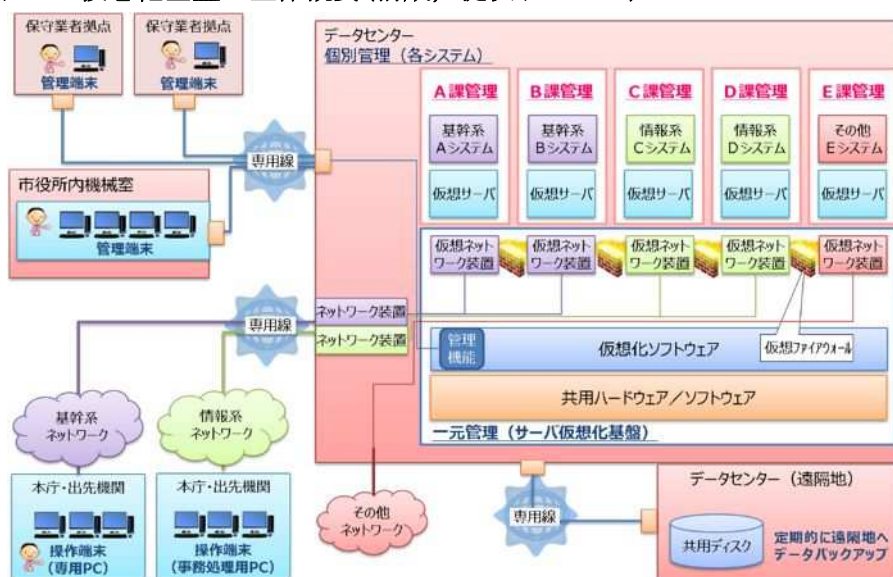


図 5-1 サーバ仮想化基盤システム構成図概要

5.1.3 仮想マシン機能

業務システムの仮想サーバの機能を提供します。（インターネットへ直接接続することはできません）

5.1.4 仮想ネットワーク機能

仮想ファイアウォール、仮想ロードバランサの機能を提供します。

5.1.5 統合バックアップ機能

業務システムのイメージおよび業務データのバックアップ機能を提供します。

5.1.6 仮想デスクトップ機能

基幹系の業務システムを情報系の事務処理用 PC から操作することができる仮想デスクトップ環境を提供します。詳細は神戸市仮想デスクトップ環境構築利用ガイドラインを参照すること。

5.1.7 提供サービス説明

5.1.7.1 仮想マシン機能

以下の環境(OS・ミドルウェア)を提供します。サポート期限が切れた OS・ミドルウェアのバージョンについては提供対象外とします。

5.1.7.1.1 提供可能な OS

Windows	Windows Server 2022
	Windows Server 2019
	Windows Server 2016
	Windows Server 2012, Windows Server 2012 R2
Linux	Red Hat Enterprise Linux 8(CentOS 8)
	Red Hat Enterprise Linux 7(CentOS 7)

5.1.7.1.2 提供可能なミドルウェア

データベース	Oracle Database 19c
	Oracle Database 18c
	Oracle Database 12c Release 2 Standard Edition
	Oracle Database 12c Release 1 Standard Edition
	Microsoft SQL Server 2019
	Microsoft SQL Server 2016
	Microsoft SQL Server 2014

5.1.7.1.3 提供する共通ソフトウェア

仮想化ユーティリティ	VMware Tools
ウイルス対策ソフト	Symantec Endpoint Protection (Linux のみ提供) (Microsoft Defender については、基幹系及び情報系ネットワークのWSUSサーバから更新ファイルの取得が可能)

5.1.7.2 仮想ネットワーク機能

「仮想ロードバランサ」、「仮想ファイアウォール」の機能を業務システムに提供します。

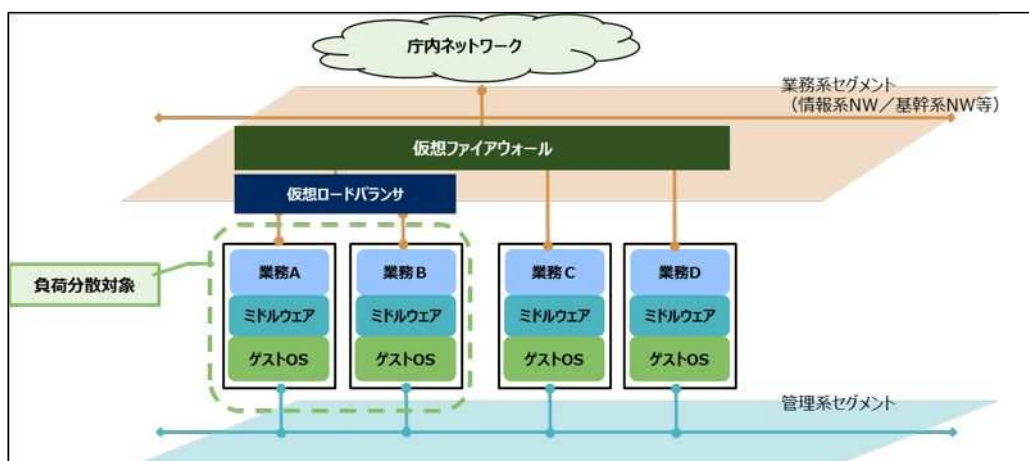


図 5-2 仮想ネットワーク機能概要

5.1.7.3 統合バックアップ機能

仮想マシンのイメージ保管、世代管理、遠隔地保管の機能を提供します。業務データのバックアップは、業務システムの運用保守事業者により、本市が提供するバックアップ領域(共有フォルダ)にデータを格納していただくことが前提となります。

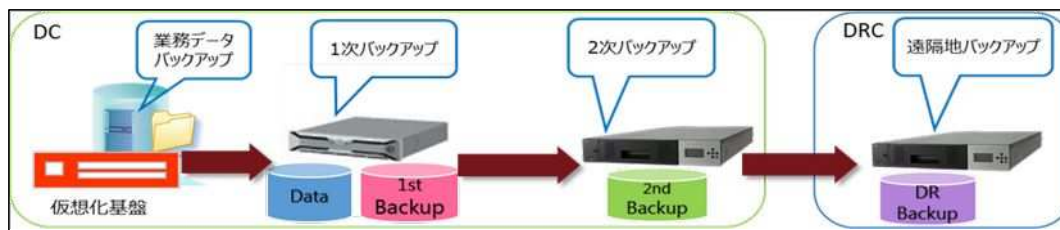


図 5-3 統合バックアップ機能概要

1次バックアップ	サーバ仮想化基盤の運用保守事業者が実施する仮想マシンのイメージバックアップ、サーバ仮想化基盤内に設定され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を指す。
2次バックアップ	サーバ仮想化基盤の運用保守事業者が実施するバックアップ領域から2次バックアップ用サーバへのバックアップを指す。
遠隔地バックアップ 重要システムに限定	サーバ仮想化基盤の運用保守事業者が実施する2次バックアップサーバからDRCへのバックアップを指す。

5.1.8 サーバ仮想化基盤の利用手続き

サーバ仮想化基盤の利用にあたっては、業務システム所管課を通じて以下の申請書を提出してください。

文書名	内容
様式 1-1	仮想サーバ利用申請書
様式 1-4	リソース割り当て変更申請書
様式 1-5	廃止申請書
様式 2-1	ヒアリングシート(サーバ仮想化基盤)
様式 3-1	保守アカウント交付及びOTP トークン借用申請書(神戸市用)
様式 3-2	保守アカウント交付及びOTP トークン借用申請書(事業者用)
様式 3-5	OTP トークンの事故報告書(紛失・盗難・破損)
様式 4-1	保守回線及び保守端末接続申請書
様式 5-1	仮想化基盤管理端末利用申請書
様式 6-1	仮想サーバクローン取得申請書
様式 6-2	仮想サーバクローン置き換え申請書
様式 6-3	仮想サーバリストア申請書
様式 6-4	仮想サーバスナップショット機能利用申請書

表 5-1 サーバ仮想化基盤の利用申請様式

5.1.9 事業者の保守環境

サーバ仮想化基盤の仮想サーバ保守環境として、以下の2種類の方法を提供します。仮想サーバの保守環境とは管理系ネットワークを経由した vCenter への接続環境であり、telnet や ssh 等により仮想サーバへ接続できる環境ではありません。

- 庁内のセキュリティエリアに設置した共用の保守端末から仮想サーバの保守を行う環境
- NTT 西日本の「フレッツ・VPN ワイド」を経由し、業務システム保守事業者の拠点に設置した専用の保守端末から仮想サーバのリモート保守を行う環境

※ フレッツ・VPN ワイド経由のリモート保守環境を構築する場合のアクセス回線、VPN 利用料、保守端末の費用については、業務システム側の負担となります。

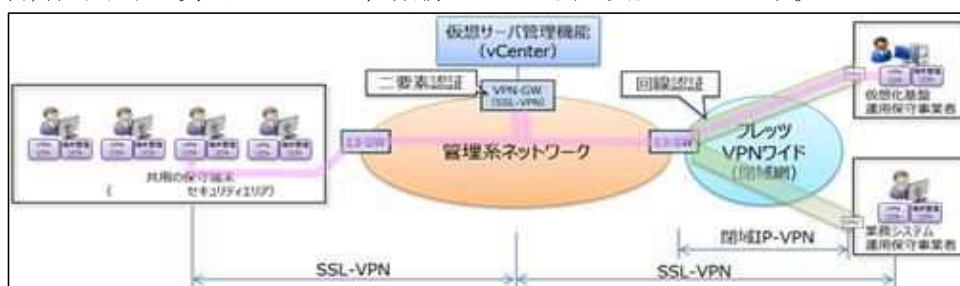


図 5-4 仮想サーバ保守環境

5.2 共通基盤システム(基幹系)

5.2.1 構築の背景と目的

5.2.1.1 ファイル連携の標準化による統一制御

従来、業務システムごとのインタフェース仕様により個別に行っていたファイル連携や、外部媒体でのデータ受け渡しによる非効率な連携方法を、マルチベンダ環境による共通インタフェース、本市標準のデータ連携仕様を策定することにより、システム連携の簡素化と業務の独立性を確保した制御を行います。

5.2.1.2 文字コード変換処理の集約

文字コード変換には、各業務システム間のコード体系が異なることにより、仕様・フォーマット調整、改修作業にかかる時間・費用等に関する課題が残存します。共通基盤システムでファイル連携を行う工程において、文字コード変換処理を一手に制御することで解消を図ります。なお、業務システムの文字コードは UTF-8 へ統一することを目指しており、統一後は共通基盤システムの文字コード変換機能は廃止する予定です。

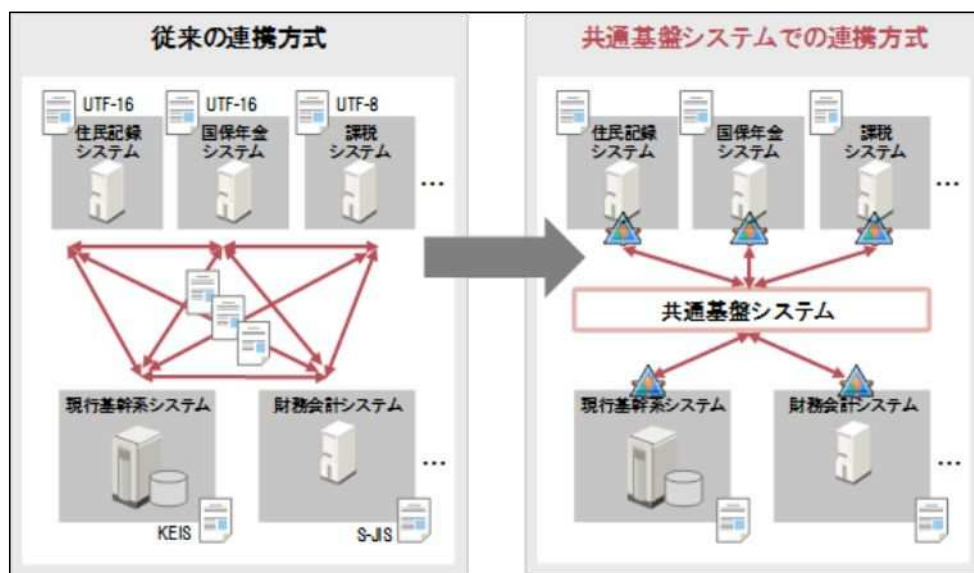


図 5-5 連携方式概要図

5.2.1.3 住記データ利用について

共通基盤システムの住記データ（参照用住記 DB）を直接参照する I/F を構築し、個人情報、世帯情報を参照可能としています。共通基盤システムは令和 7 年 5 月にガバメントクラウドに移行予定となっており、移行後、一定期間は参照用住記 DB は存続しますが、将来的には廃止となります。

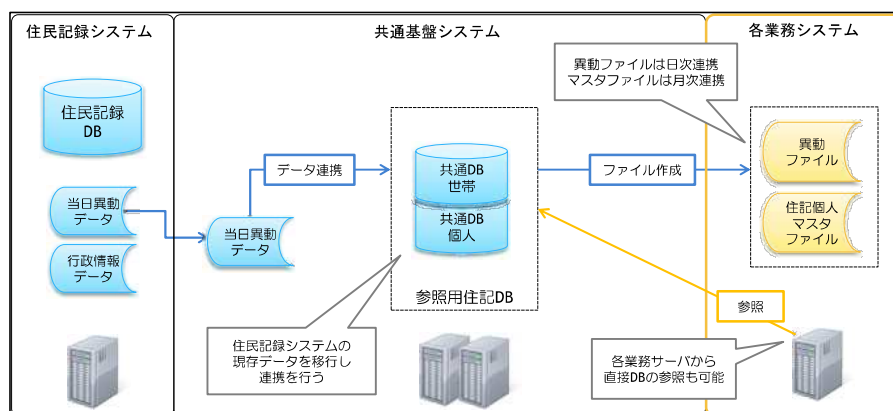


図 5-6 共通 DB 概要図

5.2.2 共通基盤システムの機能構成

5.2.2.1 ファイル連携機能

ファイル連携機能では、共通基盤システムを通じて、各業務システム間のファイル連携を行います。業務システム間で行われるデータファイルの授受は、本機能を通じて実行され、情報の発生源となる連携元システムから連携先システムへ、データ連携するための仕組みを実装してい

ます。

5.2.2.2 文字コード変換機能

共通基盤システムは、業務所管課が準備した文字コード管理テーブルに従い、文字コード変換のみを行います。

共通基盤システムでは、本市住民記録システム(新住記システム)の UTF-16 を基準とした文字コード管理テーブル(UTF-16⇔UTF-8)を提供しています。(この「UTF-16⇔UTF-8」の変換テーブルについては、神戸市外字フォントの利用が前提となります。)それ以外のマッピングについては、提供側業務所管課と利用側業務所管課で協議の上、作成いただきます。

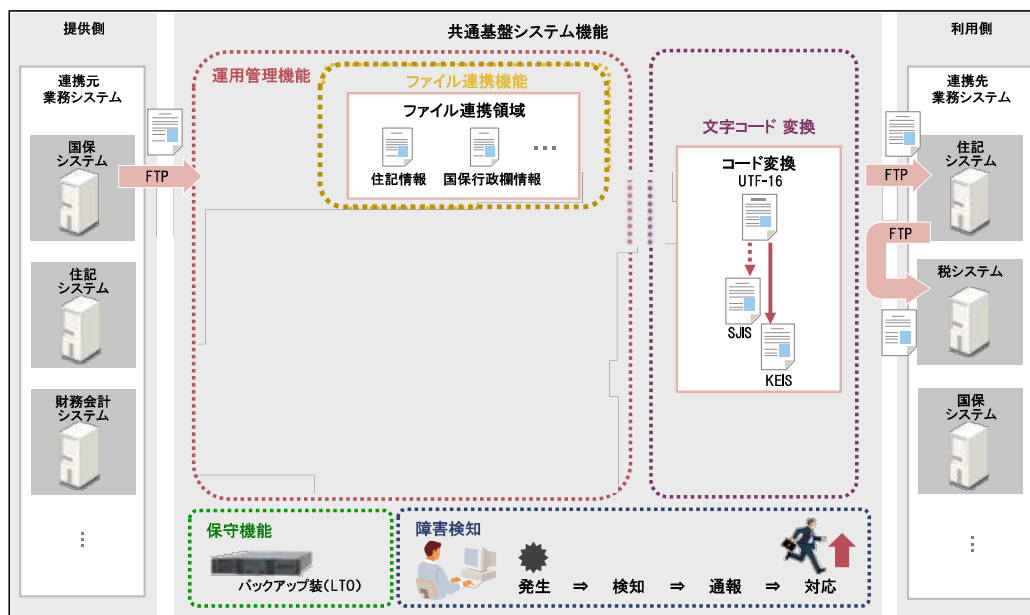


図 5-7 共通基盤システム全体概要

5.2.3 文字コード変換

文字コード管理テーブルに重複レコードが存在する場合や、文字コード変換前のファイルに文字コード管理テーブルに存在しない文字コード(未定義コード)が含まれる場合、共通基盤システムは置換文字(半角：*，全角：◎)に置き換えて変換後のファイルを出力します。

文字コード変換を行う連携ファイルの形式は、以下の通りです。

No.	項目	説明
1	形式	TXT, CSV, 固定長
2	エンディアン	UTF-8, UTF-16 の場合、ビッグエンディアン(BE)またはリトルエンディアン(LE)を指定する。
3	BOM(Byte Order Mark)	UTF-8, UTF-16 の場合、BOM の有無を指定する。 BOM 無し→BOM 有り, BOM 有り→BOM 無し にする変換は実施しない。
4	EOF(End Of File)	任意

表 5-2 文字コード変換時の連携ファイル形式

その他、文字コード範囲の詳細や文字コード管理テーブルの作成方法等については、「共通基盤利用ガイドライン」を参照してください。

5.2.4 共通基盤システム利用にあたっての手続き概要

ファイル連携機能および共通テーブル機能の申請で使用する様式を以下の表に示します。共通基盤システムを初めて利用する際には、【様式 1】、【様式 2】をデジタル戦略部 PC・基盤システム担当へ提出してください。

様式内の項目の説明や記入例、注意点は、「共通基盤利用ガイドライン」及び、各様式を参照してください。

なお、各所管課が管理するデータの利用にあたっては、事前に所管課にデータ利用承認を得ていただき、その利用目的やスケジュールなどを沿えてデジタル戦略部 PC・基盤システム担当に申し込んでいただく必要があります。

No.	様式	ドキュメント名	申請の種類			
			新規	停止	再開	変更
1	様式 1	共通基盤システム利用申請書	要	要	要	要
2	様式 2	業務情報申請書	要	要	要	要
3	様式 3	ファイル連携・共通テーブル利用申請書	要	要	要	要
4	様式 4	ファイル定義情報申請書	要	要	要	要
5	様式 5	文字コード管理テーブル申請書	要	—	—	要

表 5-3 共通基盤システムの利用申請様式

No.	様式	ドキュメント名	申請の種類			
			新規	停止	再開	変更
1	様式 1	共通基盤システム利用申請書	要	要	要	要
2	様式 6	Oracle 利用業務情報申請書	要	要	要	要
3	様式 8	INDEX_VIEW_項目追加申請書	要	要	—	—

表 5-4 共通 DB の利用申請様式

5.3 統合宛名システム(基幹系)

5.3.1 構築の背景

番号法に基づく社会保障・税番号制度(以下、「番号制度」という。)に対応するため、統合宛名システムを導入しています。改修費用の低減や導入後の運用の簡素化等を考慮し、統合宛名システムは共通基盤システムを介して各業務システムと連携する方式としています。

5.3.2 統合宛名システム概要

統合宛名システム概要を次図に示します。

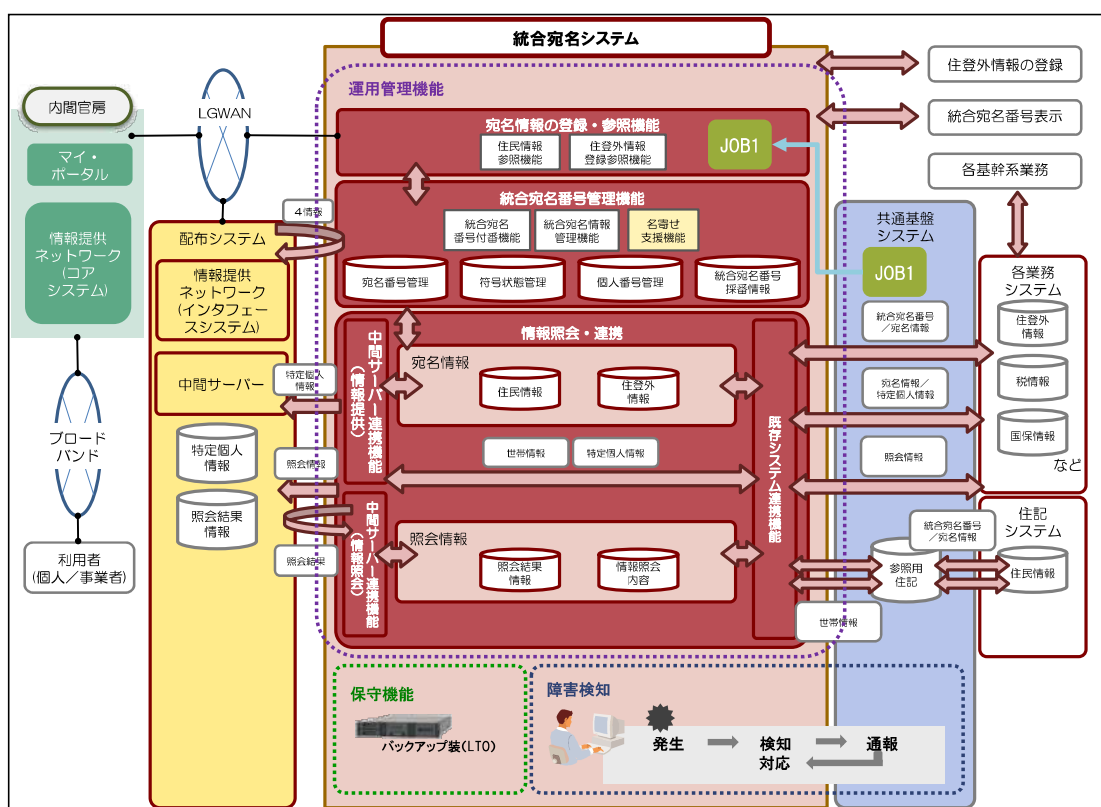


図 5-8 統合宛名システムを中心とした情報システム

5.3.3 主な機能の概要

統合宛名システムでは中間サーバ連携機能及び特定個人情報の登録・照会機能を構築しています。中間サーバへの副本登録を行うためには、必ず統合宛名システムを利用する必要があります。

各番号利用事務で保有する宛名情報、個人番号及び統合宛名番号の紐付けと管理を統合宛名システムで行います。なお、各業務システムで宛名情報と紐づく個人番号を管理する必要があります。

統合宛名システムで管理する宛名情報は、特定個人情報の登録・照会の対象となるものとし、統合宛名番号と紐付ける必要が無い宛名情報については、統合宛名システムに連携する必要はなく、各業務システムで管理します。

5.3.4 統合宛名システムの機能構成

統合宛名システムが提供している機能は、次表の通りです。

なお、番号制度への対応として、①統合宛名システムでは共通基盤システム連携を利用する方式と②統合宛名仮想端末から中間サーバ接続機能を利用する方式を提供しています。

No.	機能名 (大分類)	機能名 (中分類)	機能内容
1	宛名情報管理機能	宛名情報登録	本市の住民基本台帳に登録されている者(住登者)および住登外者の個人番号、宛名情報を登録する。
2		統合宛名番号採番	統合宛名番号が未付番の個人に

No.	機能名(大分類)	機能名(中分類)	機能内容
			ついて、新規に統合宛名番号を付番する。
3		宛名情報更新	住登外者の宛名情報を更新する。
4		宛名情報表示	番号情報表示において、ユーザ権限によってログイン制御、及び、表示項目制限を実施する。
5			個人番号、統合宛名番号または業務宛名番号に紐付く宛名情報を検索、表示する。
6			検索したユーザ、宛名情報等をログ出力する。
7	中間サーバ連携機能	情報提供データの登録	他団体へ提供する特定個人情報を中間サーバに連携する。
8		情報照会内容の登録	団体内での要求に応じ、中間サーバへ他団体への照会を実施する。
9		情報提供内容の取得	中間サーバから、他団体からの情報照会結果を受信する。

表 5-5 統合宛名システムの機能一覧

5.3.5 番号制度への対応について

統合宛名システムでは、「住記(住登者)テーブル」と「住登外者テーブル」で統合宛名番号等を管理しています。住登者、住登外者でそれぞれ対応方法が異なるので、システム構築・運用の際は注意してください。なお、詳細は、「統合宛名システム利用ガイドライン」及び「情報照会・情報提供（副本登録）機能説明書」を参照してください。

5.3.5.1 統合宛名番号の付番について

5.3.5.1.1 住登者の場合

住登者に統合宛名番号を付番し、共通基盤システムを通じて個人番号、統合宛名番号及び住記個人番号をファイル出力し、各業務システムに提供します。

各番号利用事務所管課における住登者の宛名情報と個人番号との紐付けのイメージは下図のとおりです。

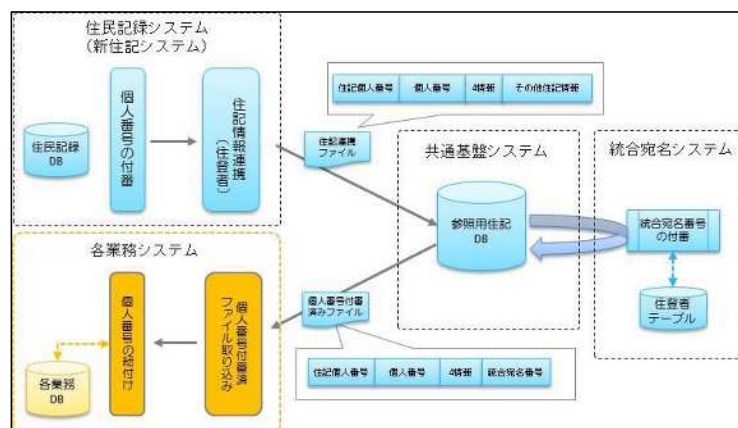


図 5-9 各業務システムへの付番連携概念図（住登者）

出生等により新たに個人番号が付番される場合は、共通基盤システムと連携している業務システムに対して、バッチ処理(日次)にて個人番号と統合宛名番号を含めた異動ファイルを各業務システムへ連携します。

各業務システムは、提供されたファイルを基に宛名情報と個人番号及び統合宛名番号の紐付けを実施する必要があります。

各番号利用事務で管理する住登者の宛名情報と個人番号の紐付けの整合性については各番号利用事務所管課で確認する必要があります。

5.3.5.1.2 住登外者の場合

1) 当初セットアップ時

各業務所管課では、各業務システムから統合宛名システムに連携する宛名情報を原則「1個人1宛名情報」となるように、宛名情報のクレンジングを行う必要があります。

また、各番号利用事務で管理する宛名情報の実態に応じて、各番号利用事務所管課の責任で実施していただく必要があります。

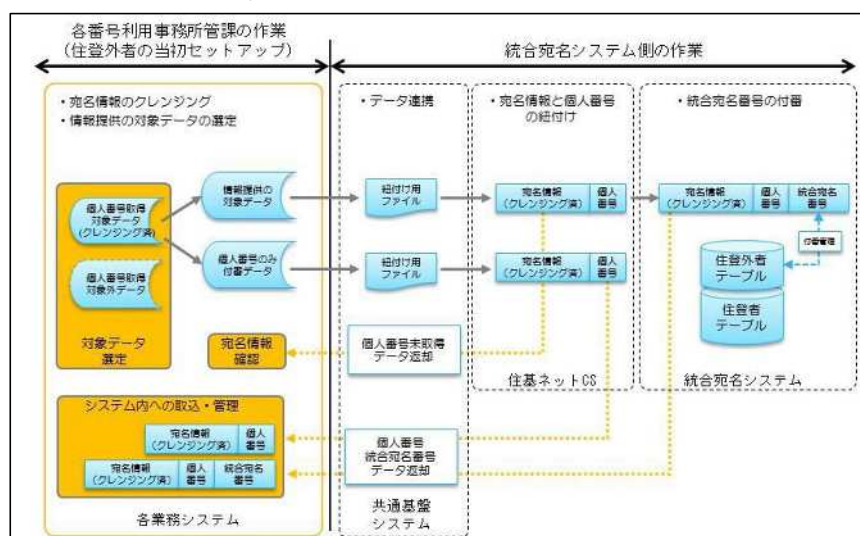


図 5-10 当初セットアップ時の付番の流れ（住登外者）

2) 運用開始後

運用開始後の住登外者の登録方法は、①統合宛名端末を使用して直接登録する方法と、②夜間バッチ処理で業務システムからファイル連携により登録する方法を用意しています。詳細は「統合宛名システム利用ガイドライン」を参照してください。

5.3.5.2 中間サーバへの連携について

5.3.5.2.1 副本登録の概要

副本登録が必要な業務システムは、定められたフォーマットに従って特定個人情報を含む連携データを共通基盤システムへ送信し、統合宛名システムを介して中間サーバに連携します。副本登録の流れについての概要を下記に示します。

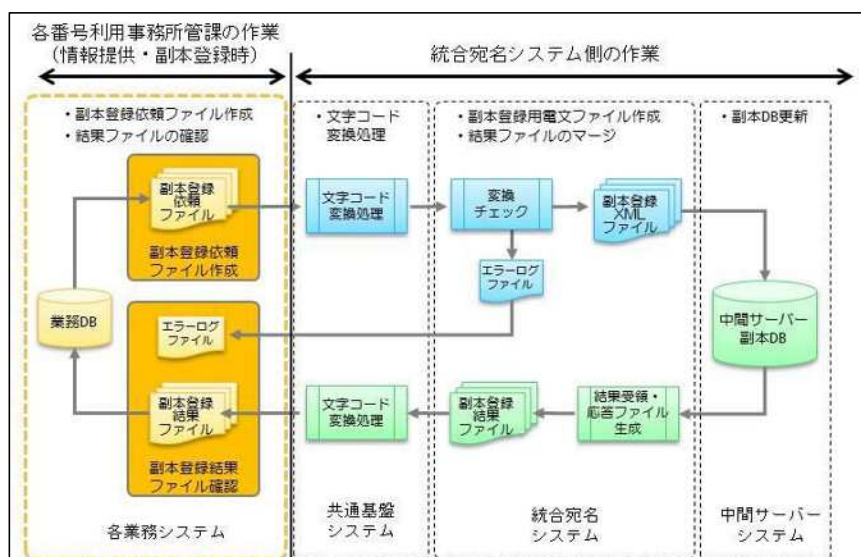


図 5-11 中間サーバへの副本登録の概要

特定個人情報を中間サーバへ連携するため、一時的に統合宛名システムに特定個人情報を登録しますが、中間サーバとの連携が完了した後は、統合宛名システムに登録された特定個人情報は削除します。統合宛名システムでは特定個人情報を管理しないことから、各業務所管課にて管理してください。

5.3.5.2.2 情報照会の概要

本市では、情報照会するための方法を2パターン準備しています。

単件照会する場合は、中間サーバ接続端末を利用して情報照会を推奨します。この場合、中間サーバと直接通信するため、共通基盤システムや統合宛名システムを連携しません。

複数件数を一括で照会及び日次・月次処理など経常的な運用を想定している場合は、業務システム側で情報照会データをCSVファイル形式で作成し、共通基盤システムにFTP転送いただき、統合宛名システムがそのファイルを中間サーバへ連携する方式を推奨します。

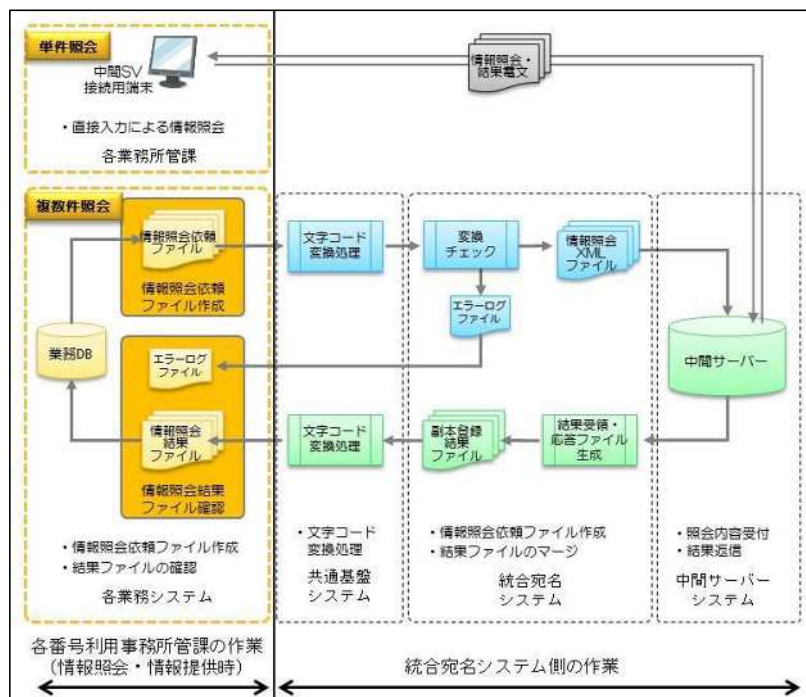


図 5-12 情報照会の概要

5.3.5.2.3 中間サーバへの連携方法

1) 連携方法

業務システムから情報照会依頼ファイルを連携する際は、各業務システムから共通基盤システムに対してFTP転送を行いますので、事前に「共通基盤利用ガイドライン」を参照し、下記利用申請をデジタル戦略部PC・基盤システム担当へ行ってください。

No.	様式	ドキュメント名	申請の種類			
			新規	停止	再開	変更
1	様式 1	共通基盤システム利用申請書	要	要	要	要
2	様式 2	業務情報申請書	要	要	要	要
3	様式 9	中間サーバ連携申請書	要	要	要	要

表 5-6 中間サーバ連携の申請様式

2) データ項目

情報照会を行う場合、副本登録と同様に、メッセージの種類やシステム識別子等の電文制御に係るデータを設定する「メッセージヘッダ部」と、情報提供（副本登録）で使用するデータを設定する「メッセージボディ部」で構成されたcsvファイルの生成が必要です。

メッセージボディ部は中間サーバI/Fに準じますが、機密事項が含まれますので、機密保持契約の締結や誓約書を提示した後に開示します。

5.3.6 統合宛名システム利用にあたっての手続き概要

統合宛名システムの利用にあたっては、共通基盤システムを経由したデータ連携が必要となります。そのため、「5.2.4. 共通基盤システム利用にあたっての手続き概要」から申請を行ってください。

5.4 文字情報基盤システム(基幹系)

5.4.1 構築の背景

番号制度においては、情報システムの文字管理の観点から考えると、今まで以上にそれぞれのシステムの文字情報を標準化・共通化していかなければ、利便性の高い情報システムの構築や情報連携が困難になることが予想されます。

また、「情報提供ネットワークシステム」の中継役を担う中間サーバでは、使用する文字を UTF8 の文字コード体系で JIS の第一水準から第四水準に含まれる文字とし、外字を取り扱わない仕様となっています。

これらの背景から、中間サーバとの特定個人情報の連携のため文字縮退変換を実現することを主目的とし、更には既存業務システム間の文字統合管理を目指すため、文字情報基盤システムを構築することとしました。

5.4.2 文字情報基盤システムの目的

文字情報基盤システムでは、既存業務システムの文字情報を統合管理するために、本市で使用される文字情報を文字の字形も含め、LGWAN-ASP サービス上での管理を実施しています。

5.4.3 文字統合基盤の構成概要

文字管理の概要を次図に示します。

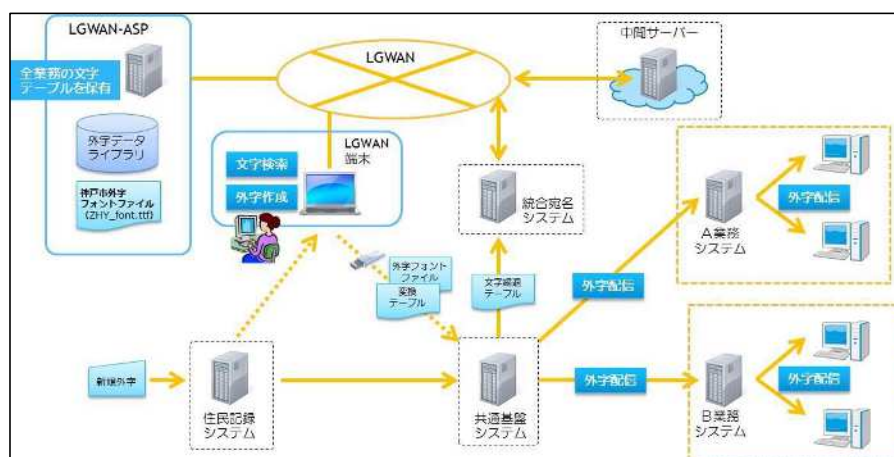


図 5-13 本紙の文字管理の概要

デジタル戦略部で運用管理する文字情報基盤システムで、「神戸市外字フォントファイル」を作成しています。この外字フォントファイルは神戸市全システムの範囲内で使用することができます。

住民記録システムで使用可能な約 4,800 文字の外字のうち、神戸市外字フォントでは約 2,200 文字のみを使用できますが、共通基盤システムで管理する参照用住記 DB に格納されている全ての外字を表示できるよう整備しています。

住民記録システムで新規外字が発生した場合、新規外字を LGWAN-ASP の文字情報基盤システムで検索し、外字データライブラリに登録します。辞書に登録されていない文字の場合は、新規作成後に登録します。

新規外字を含むフォントと文字コード変換テーブルを共通基盤システムに登録することで、各業務システムへ共通基盤システム経由で配信します。

中間サーバ向けの文字縮退も、文字縮退テーブルを作成し、共通基盤システムに登録することで対応しています。

5.4.4 神戸市外字フォントについて

神戸市外字フォントは JIS X 0213:2004 を基本とし、内字部分は Windows に標準搭載されている「MS 明朝」、ユーザ外字部分に文字情報基盤システムから提供する「SS 明朝」を使用することで、参照用住記 DB(共通基盤システム内)に収録されている文字のほとんどの字形を表示することができます。

5.4.4.1 神戸市外字フォントの使用可能な範囲

本市が文字情報基盤システムの利用を継続している限りは、本市の全ての業務システムで使うことができます。

また、外部印刷業者に帳票等の印刷を委託する場合には、その印刷業務に必要な期間内に限り使用していただく事も可能です。

5.4.4.2 制約事項

神戸市外字フォントを使用するにあたり下記の制約事項があります。

No.	分類	設定値
1	対応 OS	Windows10
2	住記関連提供ファイル仕様 (住記異動ファイル・住記 マスタファイル共通)	文字コード：UTF-8(サロゲート面未使用) 形 式：CSV 形式
3	出力できない外字	①参照住記データベース当初移行時に「◎」であった文字 →「◎」で出力されます。 ②住民記録システムでの不要外字削除対応後、住民記録システムで復活させた文字の一部(233 文字) →縮退文字で出力されます。 ③文字情報基盤システムが保有していない文字 →「◎」で出力されます。

表 5-7 神戸市外字フォントの制約事項

5.4.4.3 神戸市外字フォントの連携方法

神戸市外字フォントは、LGWAN-ASP よりデジタル戦略部担当者がダウンロードし、共通基盤システムから各業務システムに対して FTP で連携する方法を標準方式とします。

なお、現時点において、神戸市外字フォントは、住記情報を利用する基幹系業務システムにのみ提供することを想定しています。

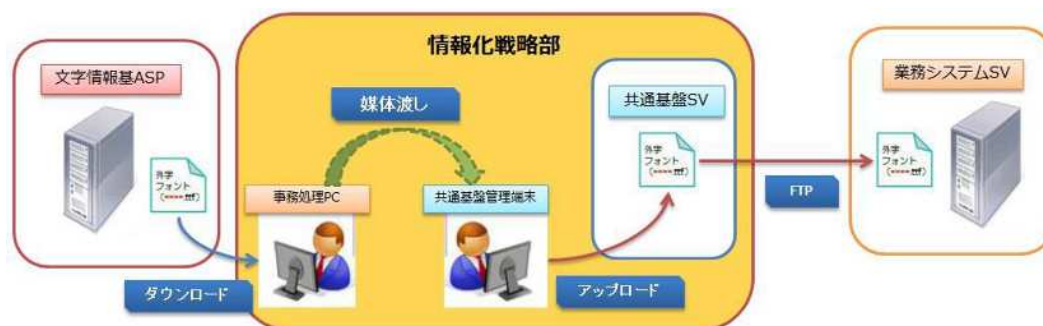


図 5-14 フォントファイル連携の流れ

5.4.4.4 神戸市外字フォントの更新頻度

住民記録システムでの追加外字が発生した際に、随時フォントファイルを更新します。ファイル名 (ZHY_font.ttf) の変更はありません。(更新は不定期です。月 1 回程度の更新を想定しています。)

5.4.4.5 神戸市外字フォントの連携方法

サーバや端末に外字フォントを適用するために、「外字活性化ツール」と「フォント適用バッチファイル」を各業務システムに提供します。

5.4.4.6 フォント適用バッチファイルについて

外字フォントを使用できるようにするためには、レジストリエディタを使用したレジストリ値(ユーザー外字領域の参照先)の変更や、コマンドプロンプトから外字適用コマンドの投入等の操作が必要になります。これらの操作を、フォント適用バッチファイルで一括実行可能です。

バッチファイルの適用方法は、①PC 起動時のスタートアクションでフォント適用バッチファイルの実行する方法、又は、②ダブルクリック(手動)の適応操作を行う方法を推奨しています。

外字フォントファイルは、業務システムサーバから端末の所定のディレクトリに配信・格納していただく必要があります。(配信方法は、各システムの仕様に合わせて設計してください。)

フォント適用バッチファイルの設定値は下記のとおりです。設定値(手順)を変更する場合は、バッチファイルの書き換えが必要になります。

No.	分類	設定値
1	外字フォント名称	ZHY_font.ttf
2	外字フォント格納先	D:\%kuho_font
3	外字活性化ツール格納先 (FontActivationWin.exe)	D:\%kuho_font

表 5-8 フォントファイル連携の流れ

5.4.4.7 文字コード変換について

システム間の文字コード変換は、共通基盤システムで実施します。文字コード変換テーブルは各業務所管課でご準備ください。共通基盤システムの文字コード変換については、「5.2.3 文字コード変換」を参照してください。

5.4.5 文字統合基盤利用にあたっての手続き概要

ファイル連携機能および共通テーブル機能の申請で使用する様式は以下のとおりです。

神戸市外字フォントを初めて利用する際には、共通基盤システムと共通の「ファイル定義情報申請書」をデジタル戦略部 PC・基盤システム担当へ提出してください。様式内の項目の説明や記入例、注意点は各様式を参照してください。

No.	ドキュメント名	申請の種類			
		新規	停止	再開	変更
1	ファイル定義情報申請書	要	要	要	要

表 5-9 神戸市外字フォント利用の申請様式
(共通基盤システムのファイル定義情報申請書)

5.5 サーバ職員認証基盤（情報系）

5.5.1 システムの概要と目的

事務処理用 PC で操作する業務システム向けに、職員認証機能を提供します。

事務処理用 PC のログイン（Windows ログオン）情報によるシングルサインオンを実現
人事・給与システム、情報管理システムからの職員情報を連携（プロビジョニング機能）

5.5.2 システムの機能概要

5.5.2.1 シングルサインオン機能

本システムでは、シングルサインオンソフトウェア（OpenAM）を利用してシングルサインオン連携を行います。職員が事務処理用 PC に IC カードとパスワードを入力してサインインしたのち、グループウェアや業務システムへのパスワード再入力是不要となります。シングルサインオン連携方式は業務システム側のインタフェースに合わせて、SAML2.0、統合 Windows 認証及びリバースプロキシから選択できます。

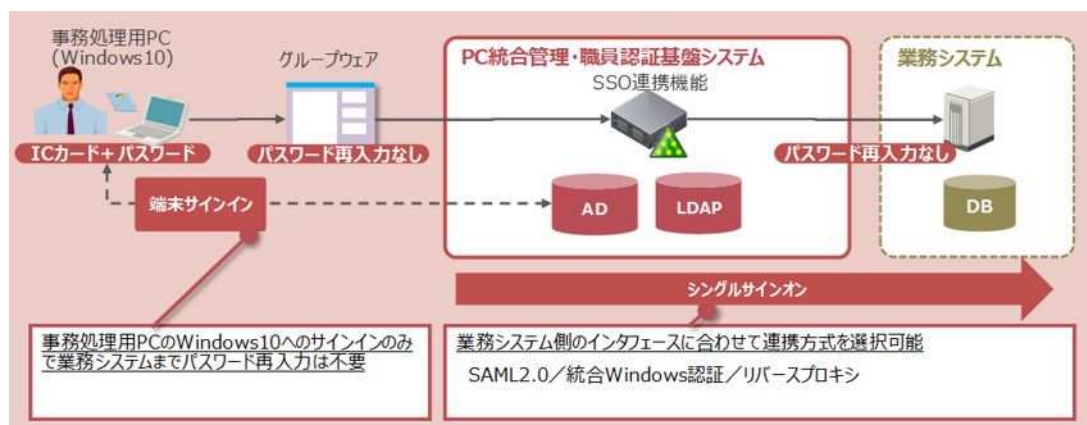


図 5-15 シングルサインオン連携機能の概要

5.5.2.2 プロビジョニング機能

本システムでは、ID 管理ソフトウェア（LDAP Manager）を利用してプロビジョニングを行います。入力処理機能では、人事・給与システム及び情報管理システムから PC 統合管理・職員認証基盤システムの LDAP に職員情報（人事異動情報・メールアドレス情報）の取込みを行います。出力処理機能では、PC 統合管理・職員認証基盤システムで所持する職員情報を業務システム向けに出力し、プロビジョニング処理を行います。プロビジョニング方法は、業務システムの DB

の種類によって選択可能であり、職員データ等を直接更新する方法またはファイル連携（CSV）での連携も可能です。

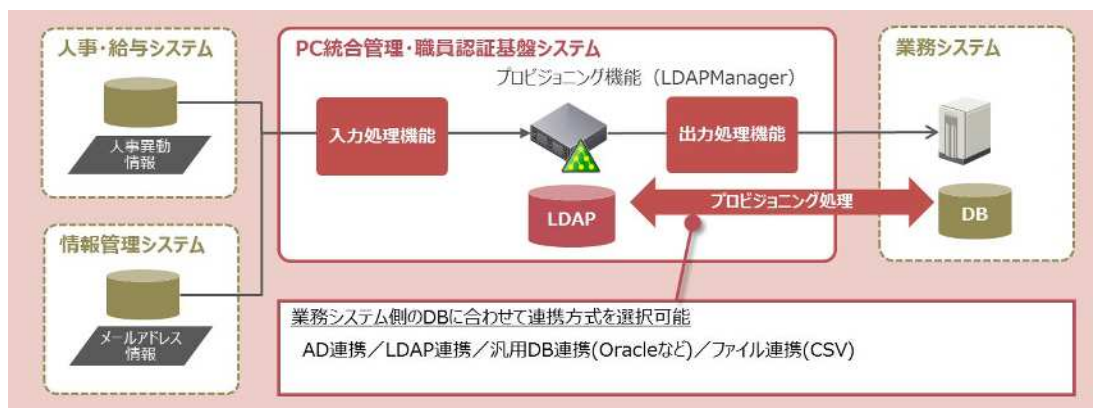


図 5-16 プロビジョニング機能の概要

5.5.3 利用ガイドラインの提供

5.5.3.1 契約締結前の提供資料

本市の職員認証基盤を利用したい場合は、情報提供依頼(RFI)、入札(RFP)等の際に、調達仕様書の一部として、デジタル戦略部が提供する「職員認証基盤利用ガイドライン（概要編）」を添付してください。対象事業者は本ガイドラインにより、構築しようとしている業務システムが本市の職員認証基盤に適合するかどうかを確認することができます。

なお、本ガイドラインを提供する際には、必ず提供先の事業者から機密保持の誓約書を受領してください。

5.5.3.2 契約締結後の提供資料

本市の職員認証基盤を利用することになった場合は、事業者選定後のシステム設計前に、デジタル戦略部が提供する「職員認証基盤利用ガイドライン（詳細編）」を構築事業者に提供してください。構築事業者は本ガイドラインにより、本市の職員認証基盤を前提にしたシステム設計、構築をすることができます。

なお、本ガイドラインを提供する際には、提供先の事業者と機密保持契約を締結しておく必要があります。

6 ライセンス

神戸市では、マイクロソフト社の一部ライセンスやシマンテック社のライセンスについて、神戸市職員が使用できる契約を締結しています。

6.1 マイクロソフト社製品に関する包括契約ライセンスの考え方

マイクロソフト社と以下の内容で包括契約を締結しています。契約内容が変更される場合がありますので、ライセンスの使用を前提とする場合は、所管課の職員を通じて最新情報をデジタル戦略部 PC・基盤システム担当に確認してください。ライセンスの利用範囲等は以下のとおりです。

6.1.1 <利用できる機器>

項目	内容
機器	事務処理用 PC, 専用 PC, サーバを問わず利用可能

表 6-1 本市でマイクロソフト社ライセンスを利用可能な機器

6.1.2 <職員及び外部委託業者等>

項目	内容
利用可	① 一般職員（任期付職員を含む） ② 技術労務職員（前年度に実施される利用者数調査の回答に含まれる者） ③ 再任用職員 ④ その他パソコン業務が必要な以下(1)～(3)のもの (1) 会計年度任用職員（嘱託職員，臨時的任用職員） (2) 人材派遣職員 (3) 神戸市と委託契約を締結した事業者で事務処理用 PC を使用しなければ委託業務が遂行できない者
利用不可	① 技術労務職員（前年度に実施される利用者数調査の回答に含まれない者） ② 教育委員会事務局職員及び学校園職員 ※ 別途、包括契約を締結していますので、教育委員会事務局まで確認してください。 ③ 外郭団体又は地方独立行政法人へ出向中の職員

表 6-2 本市でマイクロソフト社ライセンスを利用できる職員等

6.1.3 <利用できるライセンス>

区分	名称
アプリケーション関係	Microsoft Office Professional
サーバ関係	Core CAL
	Windows Server - User CAL
	Exchange Server Standard CAL - User CAL
	SharePoint Server Standard CAL - User CAL
	Skype for Business Server Standard User CAL
	System Center Configuration Manager Client ML
	System Center Endpoint Protection

区分	名称
システム関係	Windows10（フルライセンスではありません）

表 6-3 本市で利用可能なマイクロソフト社ライセンス

上記ソフトウェアについては、最新版へのアップグレードの権利とダウングレードの権利を有しているため、あらゆるバージョンで使用が可能です。

マイクロソフト社との包括契約ライセンスには、サーバ上で仮想 Windows クライアントを稼働させ、当該仮想 OS を Windows クライアントの OEM ライセンスを有する端末から遠隔実行する権利が含まれております。

VDI 環境において、包括契約ライセンスを使用したい場合には、所管課の職員を通じて、デジタル戦略部 PC・基盤システム担当へ相談してください。

企業会計については、費用負担が必要となります。また、外部委託事業者等にライセンスを使用させる場合は、事前に使用人数の報告をお願いします。この場合、費用負担が必要となる場合があります。詳細については、デジタル戦略部 PC・基盤システム担当へ事前に相談してください。

6.1.3.1 Microsoft Office Professional について

Office Standard は、Office Professional とは別の製品ファミリーになるため、ライセンスの範囲には含まれません。また、Office を使用できる OS は、基本的には Windows のみです。

6.1.3.2 Core CAL について

開発期間中は、外部事業者の CAL 又は神戸市が当初から調達した CAL のどちらでも可です。

CAL は、それぞれのサーバのサービスを享受する場合に必要です。認証で拒否される等、サーバ内部にアクセスできない仕組みがあれば不要です。

6.1.3.3 Windows について

Windows は、Professional 等のビジネスモデルがプレインストールされている場合に、Enterprise 等へアップグレードできる権利のみを保有しています。

6.1.3.4 VDI について

サーバ側で複数の仮想クライアント OS を実行し、それぞれの仮想 OS を PC などの物理端末から遠隔実行する形式

6.2 仮想環境におけるライセンスに関する注意事項

仮想環境においては、構築する環境の組み合わせやソフトウェアの使用許諾条件によって、様々なライセンスの考え方が存在します。

以下の「表 6-4. 確認項目例」に、SAMAC（一般社団法人 IT 資産管理評価認定協会）及び JIPDEC（一般財団法人日本情報経済社会推進協会）IT マネジメント評価検討委員会の考えを参考に、仮想サーバや CPU ライセンスにおける確認項目例を示しますので、これらを参考しながら構築を行ってください。

ただし、これらは、あくまでも必要最低限の項目であり、調達の際には使用許諾条件に従って、必要な項目を適宜追加してご確認ください。

項目	内容
ライセンス種別	プロセッサライセンス、ユーザライセンス、サイトライセンス等、使用するソフトウェアのライセンスの利用数（利用範囲）をどのように算定する条件になっているかを確認する。
仮想化方式	仮想環境を構築しているソフトウェア（Microsoft 社 Hyper-V, VMware 社 vSphere, Citrix 社 Xen 等）を確認し記録する。
ハードウェアの稼働状況とライセンスの要否	待機系（Hot Standby, Warm Standby, Cold Standby 等）の状態の差異によるライセンスの要否を確認する。なお、待機系の意味については、パブリッシャーやソフトウェアにより異なる場合があるので、留意すること。また、開発環境か本番環境かによって要求されるライセンスが異なるので、併せて確認する。
保守契約	保守契約は初年度には必ず付加されてくるライセンスが多いが、過去に調達したライセンスの保守契約を継続していない場合に、新規で調達した保守契約の権利が行使できないケースもある。調達する保守契約の権利内容について、確認し記録する。
その他	<ul style="list-style-type: none"> ・プロセッサライセンスについて 必要なライセンスを選定するために CPU の型番ごとに係数を設定している場合がある。ソフトウェアをインストールする予定のハードウェアのプロセッサ情報を確認した上で、必要なライセンスを選定する。 ・指定監視ツールについて 使用許諾条件の中には、リソースの監視ツールを導入し、定期的な記録を保管することを要求しているもの（IBM の DB2 など）もある。 利用状況をモニタリングすることが義務付けられていないか、義務付けられている場合には、どのようなモニタリングが必要かを確認する。 ・パーティショニングについて ハードウェアのリソースを分割する技術としてパーティショニングがあり、パーティショニングの方式によって、ライセンスが異なるもの（Oracle など）がある。パーティショニングの違いによるライセンス条件の差異の有無を確認する。 ・接続ライセンスについて 仮想化方式によっては RDSCAL 等も所属で調達が必要な場合があります。

表 6-4 確認項目例

7 関連ドキュメント

7.1 詳細説明資料

本書記載の各内容について詳細を説明した以下の資料が存在します。配付分類に従い、所管課の職員を通じて管理者より入手してください。

No.	分類	資料名	配付分類	管理者
1	サーバ室	セキュリティエリア運用要綱	④本契約締結後	ネットワーク担当
2		サーバ仮想化基盤利用ガイドライン	②公開(要手続)	ネットワーク担当
3	共通基盤システム	共通基盤利用ガイドライン	①公開	PC・基盤システム担当
4	統合宛名システム	統合宛名システム利用ガイドライン	③非公開(要手続)	PC・基盤システム担当
5	文字基盤システム	神戸市外字フォントファイル概要	②公開(要手続)	PC・基盤システム担当
6	職員認証基盤システム	職員認証基盤利用ガイドライン(概要編)	③非公開(要手続)	PC・基盤システム担当
7		職員認証基盤利用ガイドライン(詳細編)	④本契約締結後	PC・基盤システム担当
8	包括契約ライセンス【関連6.2】	仮想環境におけるライセンスの考え方について	③非公開(要手続)	PC・基盤システム担当

表 7-1 詳細説明資料一覧

[凡例]

- ① 公開 本市 HP に公開可能な資料。庁内イントラに掲載。
- ② 公開(要手続) 本市 HP での公開は不可だが、RFI や RFP 等において事業者に配付可能な資料。提供にあたりデジタル戦略部への手続が必要。
- ③ 非公開(要手続) 機密保持契約の締結や誓約書を提示した事業者にのみ配付可能な資料。
提供にあたりデジタル戦略部への手続が必要。
- ④ 本契約締結後 本市との開発委託契約を締結後、別途、機密保持契約の締結や誓約書を提示した事業者にのみ配付可能な資料。提供にあたりデジタル戦略部への手続が必要。

7.2 申請書

本書記載の各システムの利用にあたっての申請書は以下のとおりです。本市との契約締結後、所管課の職員を通じて、入手先より申請書を入手してください。また、申請にあたっては、申請書に記載の指示に従ってください。

No.	分類	様式	ドキュメント名	入手先
1	サーバ室	様式 1	サーバ設置許可申請書	ネットワーク担当へ依頼
2		様式 2	サーバ撤去予定書	
3		様式 3	サーバ撤去終了報告書	
4	基幹系ネットワーク	様式 1	基幹系ネットワーク利用申請書	
5		様式 2	IP アドレス配布申請書	

神戸市庁内情報システムの導入に関する手引き

No.	分類	様式	ドキュメント名	入手先
6		様式 3	IP アドレス返却申請書	イントラネットよりダウンロード
7		様式 4	NTP サーバ接続申請書	
8		様式 5	SEP 追加配信依頼書	
9		様式 6	SKYSEA 利用申請書	
10		様式 7	障害通報用メールサーバ利用申請書	
11		—	保守業者用 VPN 利用申請書	ネットワーク担当へ依頼
12	情報系ネットワーク	様式 8	ネットワーク設定依頼書	イントラネットよりダウンロード
13	サーバ仮想化基盤	様式 1-1	仮想サーバ利用申請書	イントラネットよりダウンロード
14		様式 1-4	リソース割り当て変更申請書	
15		様式 1-5	廃止申請書	
16		様式 2-1	ヒアリングシート(サーバ仮想化基盤)	
17		様式 3-1	保守アカウント交付及び OTP トークン借用申請書(神戸市用)	
18		様式 3-2	保守アカウント交付及び OTP トークン借用申請書(事業者用)	
19		様式 3-5	OTP トークンの事故報告書(紛失・盗難・破損)	
20		様式 4-1	保守回線及び保守端末の接続申請書	
21		様式 5-1	仮想化基盤管理端末利用申請書	
22		様式 6-1	仮想サーバクローン取得申請書	
23		様式 6-2	仮想サーバクローン置き換え申請書	
24		様式 6-3	仮想サーバリストア申請書	
25		様式 6-4	仮想サーバスナップショット機能利用申請書	
32	共通基盤システム	様式 1	共通基盤システム利用申請書	PC・基盤システム担当へ依頼
33		様式 2	業務情報申請書	
34		様式 3	ファイル連携・共通テーブル利用申請書	
35		様式 4	ファイル定義情報申請書	
36		様式 5	文字コード管理テーブル申請書	
37	共通 DB	様式 1	共通基盤システム利用申請書	
38		様式 6	Oracle 利用業務情報申請書	
39		様式 7	CSV 連携利用申請書	
40		様式 8	INDEX_VIEW_項目追加申請書	
41	中間サーバ連携	様式 1	共通基盤システム利用申請書	
42		様式 2	業務情報申請書	
43		様式 3	中間サーバ連携申請書	

表 7-2 申請書一覧

8 参考ドキュメント

8.1 神戸市情報セキュリティポリシー

<https://www.city.kobe.lg.jp/a06814/shise/jore/youkou/0400/policy.html>

8.2 神戸市の個人情報保護制度

<https://www.city.kobe.lg.jp/information/public/hogo/kojinjouhouhogoseidotop.html>

機密を要する情報システムでインターネット回線の利用を認める基準

令和 2 年 3 月 16 日
 情報セキュリティ統括責任者決定
 （企画調整局長）
 令和 4 年 3 月 30 日
 情報セキュリティ統括責任者改定
 （デジタル戦略部長）
 令和 5 年 4 月 1 日
 情報セキュリティ統括責任者改定
 （デジタル戦略部長）
 令和 7 年 4 月 1 日
 情報セキュリティ統括責任者改定
 （デジタル戦略部長）

「物理的・技術的セキュリティ管理基準」3.3.3 に規定するインターネット VPN（IP Sec-VPN 又は SSL-VPN）及び TLS 通信に関する基準とは、次のとおりとする。

3.3.3 機密を要する情報システムで使用する回線【対策基準 6.3.5】

ア 対策基準 6.3.4 における「適正な回線」とは、閉域イーサネット、専用線、IP-VPN 等の閉域網をいう。

イ 次の条件にあてはまるときは、情報セキュリティ管理者が許可した場合に限り、自治体機密性 2 以上の情報を取り扱うことができるものとする。

- (1) インターネット VPN を利用してシステムまたはクラウドサービスを利用する場合
- (2) ファイアウォール、WAF、IP アドレス制限等の付加的なセキュリティ対策を施したシステムまたはクラウドサービスとの通信にインターネット回線（TLS 通信）を利用する場合

【インターネット VPN の利用について】

以下の 1～2 の項目をすべて満たすものについて、インターネット VPN の利用を認めることとする。

1 インターネット VPN の設定が確実に行われること

インターネット VPN は設定ミスから脆弱性が生まれるリスクがあるとされているため、VPN の設定が確実に行われるものでなければ利用を認められない。

2 インターネット VPN の適性が認められること

次に掲げる前提条件、通信の品質、効率性、セキュリティ要件、コストメリットのすべての事項についてインターネット VPN の適性が認められなければならない。

(1) 前提条件

- ① 当該回線の接続先である特定の Web サーバに格納又は格納予定のデータ以外のデータを当該回線に取り扱わないこと
- ② 当該回線の接続先のサーバ側及び接続元側の双方に VPN 装置が設置可能であること（リモートアクセスの場合は基本的に接続先のサーバ側のみで可）
- ③ インターネット VPN により制限のあるプロトコルの通信がないこと
- ④ 接続先又は接続元的一方又は双方がインターネット環境にあること
- ⑤ マイナンバー利用系ネットワークから接続するものではないこと

(2) 通信の品質

- ① 回線速度を保証する必要がある用途で利用すること
- ② BCP に係る通信用途ではないこと
- ③ 通信経路の断絶等による通信障害の責任を問う必要がないこと

(3) 効率性

- ① アクセスする PC の特定が可能であること（リモートアクセス型の場合）
- ② アクセスする PC に専用ソフトを導入することが可能であること（SSL-VPN の場合は一部の特殊な事例を除き導入不要）
- ③ アクセスする PC への通信のための要求事項が明確であり、対応できること

(4) セキュリティ要件

- ① ログイン時に原則として二要素以上の認証を実施すること
- ② 許可された端末以外がアクセスできないユーザ認証・アクセス制御のしくみを採用すること（クライアント証明書等）
- ③ 世界標準の暗号化技術のうちその時点で最も強度の高い暗号化技術を採用すること（標準技術に依存することで問題ない）なお、運用段階において当該技術に致命的な脆弱性が発見された場合は、可及的速やかに措置を講じること。

(5) コストメリット

- ① インターネット VPN を用いた場合のコストが、IP-VPN 等を用いた場合のコストと比較して明らかに有利であること
（双方のコスト算出を行っていること）

【インターネット回線（TLS 通信）の利用について】

以下の 1～2 の項目をすべて満たすものについて、インターネット回線（TLS 通信）の利用を認めることとする。

- 1 TLS 1.2 以上を使用すること。
- 2 管理基準 3.3.2 に規定する付加的なセキュリティ対策(IP アドレス制限、多要素認証等、

WAF（Web Application Firewall）や FW（ファイアウォール）の設置等）を施すこと。

情報セキュリティ遵守特記事項

(趣旨)

第1条 この契約で定める情報セキュリティ遵守特記事項（以下「特記事項」という。）は、次の各号の契約（以下、「委託契約等」という。）の約款の特記条項として、個人情報を取り扱う業務又はネットワーク又は情報システムの開発、保守又はデータ処理その他情報処理に係る業務（ただし、業務遂行のための連絡用ツールとしてクラウドサービス等の外部サービスを利用する場合は除く。以下「情報処理業務」という。）の委託契約等に関する情報の取扱いについて、必要な事項を定めるものである。

- (1) 物品売買契約
- (2) 物品賃貸借契約
- (3) 製造その他請負契約
- (4) 委託契約（企業会計も含む）

(定義)

第2条 この特記事項において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

- (1) 個人情報
個人情報の保護に関する法律（平成 15 年法律第 57 号）第 2 条第 1 項に規定する個人情報をいう。
- (2) 特定個人情報
行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）第 2 条第 9 項に規定する特定個人情報をいう。
- (3) 第 1 号及び前号以外の秘密等に係る情報
法令の規定により秘密を守る義務を課されている情報、部外に知られることが適当でない法人その他の団体に関する情報及び部外に漏れた場合に行政の信頼を著しく害するおそれのある情報をいう。
- (4) 重要情報
第 1 号から前号までに規定する情報及び神戸市（以下「甲」という。）が指定する情報をいう。
- (5) 情報
重要情報及び重要情報以外の情報をいう。

(基本的事項)

第3条 この契約により甲から業務を受託または請負し情報を取り扱う者（以下「乙」という。）は、個人情報の保護に関する法律（平成 15 年法律第 57 号）、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）、神戸市個人情報保護法の施行等に関する条例（令和 4 年 12 月条例第 17 号）、神戸市会の個人情報の保護に関する条例（令和 5 年 2 月条例第 18 号）、神戸市会の個人情報の保護に関する条例施行規則（令和 5 年 3 月規則第 1 号）及び神戸市情報セキュリティポリシーその他関係法令を遵守し、この契約による業務（以下「委託業務等」という。）を通じて知り得た情報の保護の重要性を認識し、委託業務等を履行するため

に必要な情報の取扱いにあたっては、甲の業務に支障が生じることがないように、適正に取り扱わなければならない。

- 2 乙は、委託業務等を通じて知り得た情報を正当な理由なく他人に知らせ、又は不当な目的に使用してはならない。
- 3 乙は、委託業務等を履行するにあたって、情報の漏えい、滅失、き損及び改ざんの防止その他情報の適正な管理のために必要な措置を講じなければならない。

(管理体制の整備等)

第4条 乙は、情報の適正な管理を実施する者として業務責任者を選定して管理組織を整備するとともに、前条第3項の措置に係る管理規程又は情報の具体的な取扱い内容を規定しなければならない。

- 2 乙は、前項に定める管理体制を書面により速やかに甲に通知しなければならない。管理体制を変更するときも同様とする。
- 3 乙は、情報処理業務を行う場所及び情報を保管する施設その他情報を取り扱う場所において、入退室の規制及び防災防犯対策その他必要な情報セキュリティ対策を講じなければならない。

(従事者の監督)

第5条 乙は、乙の業務責任者に、乙の従業員その他委託業務等に従事する者（以下「従事者」という。）に対し、委託業務等を通じて知り得た重要情報を正当な理由なく他人に知らせ、又は不当な目的に使用しないよう、並びに委託業務等に関する重要情報を安全に管理するよう、必要かつ適切な監督を行わせなければならない。この契約が終了し、又は解除された後においても同様とする。

(教育の実施)

第6条 乙は、乙の業務責任者及び従事者に対し、委託業務等に関する情報を取り扱う場合に遵守すべき事項、関係法令に基づく罰則の内容及び民事上の責任その他委託業務等の適切な履行のために必要な事項に関する研修等の教育を実施しなければならない。

(作業場所及び従事者の届出)

第7条 乙は、委託業務等に関する仕様書において委託業務等の履行に係る作業場所が定められていない場合、当該作業場所を書面により速やかに甲に届け出なければならない。作業場所を変更するときも同様とする。

- 2 乙は、委託業務等を履行するにあたって、作業場所ごとに従事者の所属（特定個人情報を取り扱う場合は従事者の氏名及び役職も必要）その他必要な事項を書面により速やかに甲に届け出なければならない。従事者を変更するときも同様とする。

(収集の制限)

第8条 乙は、委託業務等を履行するにあたって情報を収集するときは、委託業務等を履行するために必要な範囲内で、適正かつ公正な手段により収集しなければならない。

(目的外利用及び第三者への提供の禁止)

第9条 乙は、委託業務等を履行するにあたって知り得た情報を、甲の書面による事前の承諾を得ることなく委託業務等を履行する目的以外の目的で利用し、又は第三者に提供してはならない。

(複写及び複製の禁止)

第10条 乙は、委託業務等を履行するにあたって甲から貸与された重要情報が記載又は記録された文書及び資料その他ファイル等を、甲の指示又は承諾を得ることなく複写し、又は複製してはならない。

(重要情報の管理)

第11条 乙は、委託業務等に関する重要情報を安全に管理するため、次の各号に定める事項を遵守しなければならない。

- (1) 重要情報を作業場所以外に持ち出さないこと。やむを得ず持ち出さなければならないときは、甲の承諾を得たうえで、持ち出しの状況に関する記録を作成し、確実に保管すること。
- (2) 重要情報が記載された文書が第三者の利用に供されることのないよう施錠管理すること。また、重要情報が格納された電子計算機又は電磁的記録媒体が第三者の利用に供されることのないよう、記憶領域の暗号化又はファイルへのパスワード設定を施したうえで施錠管理すること。
- (3) 重要情報の格納又は処理を行うにあたって、個人のパーソナルコンピュータ等の電子計算機又は電磁的記録媒体を使用しないこと。
- (4) 重要情報を処理する電子計算機について、OS・アプリケーションの最新化やウィルス対策(ウィルス対策ソフトウェアのインストール及び定期的なウィルススキャンの実施等)等の適切なセキュリティ対策を実施すること。

(再委託先等の監督等)

第12条 乙は、委託業務等を遂行するために得た重要情報を自ら取り扱うものとし、第三者に取り扱わせてはならない。ただし、甲の書面による事前の承諾を得た場合は、この限りではない。

- 2 乙は、前項ただし書の規定により重要情報を取り扱う業務を第三者に再委託または下請負(以下「再委託等」という。)する場合、当該再委託等を受ける者(以下「再委託先等」という。)に対し、この契約に基づく一切の義務を遵守させなければならない。
- 3 乙は、再委託先等の当該業務に関する行為及びその結果について、乙と再委託先等との契約(以下「再委託契約等」という。)の内容にかかわらず、甲に対して責任を負うものとする。
- 4 乙は、第2項の再委託等を行う場合、再委託契約等において、再委託先等が委託契約約款及び製造その他請負契約約款並びに特記事項を遵守するために必要な事項その他甲が指示する事項を規定するとともに、再委託先等に対する必要かつ適切な監督、重要情報に関する適正な管理及び情報セキュリティ対策について、具体的に規定しなければならない。
- 5 乙は、第2項の再委託等を行った場合、再委託先等による当該業務の履行を監督するとともに、甲の求めに応じて、履行の状況を甲に対して適宜報告しなければならない。
- 6 乙は、再委託先等に対し、甲の書面による事前の承諾なくして、重要情報をさらなる委託等(以下「再々委託等」という。)により第三者(以下「再々委託先等」という。)に取り扱わせることを禁止し、その旨を再委託先等と約定しなければならない。

- 7 第1項から前項までの規定は、前項の規定による甲の承諾を得て重要情報を取り扱う業務を再々委託等する場合について準用する。

(提供文書等の返還及び廃棄等)

- 第13条 乙は、委託業務等を履行するにあたって甲から貸与され、又は乙が収集し、複製し、若しくは作成した重要情報が記載又は記録された文書及びファイル等を善良な管理者の注意をもって管理し、この契約が終了し、又は解除された後直ちに甲に返還し、又は引き渡さなければならない。ただし、甲が別に指示したときは、当該方法によるものとする。
- 2 前項ただし書の場合において、重要情報が記録されたファイル又はファイルが格納された電磁的記録媒体（以下「ファイル等」という。）の廃棄等を甲が指示した場合、乙は、ファイル等からすべての情報を消去し、復元不可能な状態にする措置を講じなければならない。また、甲は、職員による立ち会い又は証拠書面の提出により当該措置の履行確認を確実に行わなければならない。
- 3 第1項の場合において、乙が乙の電子計算機を使用して重要情報を処理し、同項ただし書の規定により当該電子計算機（以下「機器」という。）に格納された当該重要情報の消去を甲が指示した場合、乙は、機器からすべての情報を消去し、復元不可能な状態にする措置を講じなければならない。また、甲は、職員による立ち会い又は証拠書面の提出により当該措置の履行確認を確実に行わなければならない。

(報告及び検査)

- 第14条 甲は、乙に対し、契約開始時に委託業務等に関する情報の管理状況及び情報セキュリティ対策の実施状況についての報告書を提出させなければならない。又、必要があると認めるときは、検査をすることができる。
- 2 甲は、必要があると認めるときは、乙に対し、委託業務等である情報処理業務を行う場所及び情報を保管する施設その他情報を取り扱う場所で検査をすることができる。
- 3 乙は、甲から前2項の指示があったときは、速やかにこれに従わなければならない。

(事故発生時等における報告等)

- 第15条 乙は、甲の提供した情報並びに乙、再委託先等又は再々委託先等が委託業務等の履行のために収集した情報について、火災その他の災害、盗難、紛失、漏えい、改ざん、破壊、コンピュータウイルスによる被害、不正な利用、不正アクセスその他の情報セキュリティ事故が発生したとき、又は発生するおそれがあることを知ったときは、速やかに甲に報告し、甲の指示に従わなければならない。
- 2 乙は、前項の場合において、次の各号に定める事項を行わなければならない。
- (1) 直ちに被害を最小限に抑えるための措置を講じること。
- (2) 甲の求めに応じて、当該事故の原因を分析すること。
- (3) 甲の求めに応じて、当該事故の再発防止策を策定し、実施すること。
- (4) 甲の求めに応じて、当該事故の経緯等の記録を書面で提出すること。
- 3 乙は、第1項の場合に備え、同項及び前項に定める報告等必要な事項を速やかに行うことができるよう、緊急時連絡体制を整備しなければならない。

(契約の解除及び損害の賠償)

第 16 条 甲は、次の各号のいずれかに該当するときは、乙に対してこの契約の解除及び損害賠償の請求をすることができる。

- (1) 委託業務等を履行するために乙、再委託先等又は再々委託先等が取り扱う重要情報について、乙、再委託先等又は再々委託先等の責に帰すべき理由による漏えい、滅失、き損又は改ざんがあったとき。
- (2) 前号に掲げる場合のほか、特記事項に違反し、委託業務等の目的を達成することができないと認められるとき。

(留意事項)

- 1 委託業務等が情報処理業務に該当する場合は、下記 3 の場合を除き、原則としてこの特記事項をそのまま適用する。
- 2 委託業務等が情報処理業務に該当しないが個人情報を取り扱う業務に該当する場合も、この特記事項を適用する。ただし、委託業務等の実態に即して、明らかに該当しない条項（例：紙媒体以外を使用しないときは、電子計算機や電磁的記録媒体に係る条項など）を削除しても構わない。
- 3 契約書又は仕様書等において再委託等を一切禁止している条項を規定している場合は、第 12 条第 1 項のただし書及び第 2 項から第 7 項までを削除しても構わない。また、再委託等及び再々委託等という文言がある第 15 条及び第 16 条の当該文言を削除しても構わない。