

高専統一業務システム用ハウジング 一式

**Housing Service for Unified Business Systems
for National Institute of Technology**

1 set

仕 様 書

令和4年1月



独立行政法人 国立高等専門学校機構

目 次

I. 仕様概要説明	- 2 -
1. 調達の背景及び目的	- 2 -
2. 契約期間	- 2 -
3. 現在のシステム構成	- 2 -
4. 調達物品名及び構成内訳	- 11 -
4.1 概要	- 11 -
4.2 ハウジング調達の範囲	- 11 -
5. 技術的要件の概要	- 11 -
II. 調達物品に備えるべき要件	- 12 -
1. 性能、機能に関する要件	- 12 -
1.1 データセンター	- 12 -
1.2 サーバ	- 13 -
1.3 ネットワーク機器	- 16 -
1.4 通信回線	- 18 -
1.5 その他機器	- 18 -
1.6 補足事項	- 18 -
2. 性能、機能以外に関する要件	- 19 -
2.1 受注条件	- 19 -
2.2 設置条件等	- 19 -
2.3 導入構築	- 20 -
2.4 保守・運用サポート	- 22 -
2.5 提出物及び提出期限	- 23 -
2.6 操作教育	- 24 -
2.7 機密保持	- 24 -
2.8 検査及び検収	- 24 -
2.9 損害賠償	- 24 -
2.10 サプライチェーンリスクマネジメントについて	- 25 -
2.11 ワーク・ライフ・バランス等の推進に関する評価について	- 25 -
2.12 その他	- 25 -

I. 仕様概要説明

1. 調達の背景及び目的

独立行政法人国立高等専門学校機構（以下「機構」という）において運用している、高専統一業務システム（以下、業務システム）を稼働するためのハウジング（以下、ハウジング）を調達するものである。

2. 契約期間

契約期間は、契約締結日から令和9年11月30日までとする。

なお、下記の賃貸借期間の開始までに本調達物品に係る構築作業及びデータ移行作業をすべて完了させ、運用可能な状態にすること。

賃貸借期間：令和4年12月1日～令和9年11月30日〔60ヵ月間〕

3. 現在のシステム構成

3.1 業務システム一覧

現在稼働している業務システムの内訳は以下の通りである。

- (1) 人事給与統合システム
- (2) 勤怠管理システム
- (3) 給与明細システム
- (4) ファイル共有システム
- (5) 旅費システム
- (6) 特許管理システム
- (7) 研究情報ポータルシステム
- (8) 教職員向け情報 Web システム
- (9) 内部専用システム
- (10) 財務会計システム
- (11) マルウェア対策システム
- (12) 包括ライセンス用 OS イメージ配信システム
- (13) 授業料債権管理・免除システム

3.2 仮想基盤サーバ

機器の名称：Nutanix NX-3060-G5×2 台

機器の名称：Nutanix NX-6155-G5×3 台

機器の名称：Nutanix NX-1175S-G5×2 台(記憶領域のみ利用)

構成：上記7台のハイパーコンバージドインフラストラクチャー構成

合計物理 CPP 数：10

合計 vCPU 数：560

合計メモリ：2400 GB

合計記憶領域：68.2 TiB

各ネットワークインターフェース：10GBaseT×2ポート 1000BaseT×1ポート

仮想基盤サーバの上にゲスト OS として表 1 の業務系システムを運用している。

表 1. 仮想基盤サーバ上のゲスト OS の一覧

項番	役割	OS	vCPU	vRAM (GB)	vHDD	
					OS 領域	データ領域
					容量 (GB)	容量 (GB)
ファイル共有システム						
1	アプリケーションサーバ#1	Red Hat Enterprise Linux 7	12	16	120	-
2	アプリケーションサーバ#2	Red Hat Enterprise Linux 7	12	16	120	-
3	アプリケーションサーバ#3	Red Hat Enterprise Linux 7		16	120	-
4	データベースサーバ#1	Red Hat Enterprise Linux 7	12	32	120	800
5	データベースサーバ#2	Red Hat Enterprise Linux 7	12	32	120	800
6	NFSサーバ#1	Red Hat Enterprise Linux 7	6	16	120	12000
給与明細システム						
1	アプリケーションサーバ#1	Windows Server 2012R2	6	12	120	50
2	アプリケーションサーバ#2	Windows Server 2012R2	6	12	120	50
3	アプリケーションサーバ#3	Windows Server 2012R2	6	12	120	50
4	データベースサーバ#1	Windows Server 2012R2	6	32	120	400
旅費システム						
1	アプリケーションサーバ#1	Red Hat Enterprise Linux 7	8	16	120	180
2	アプリケーションサーバ#2	Red Hat Enterprise Linux 7	8	16	120	180
3	アプリケーションサーバ#3	Red Hat Enterprise Linux 7	2	16	120	180
4	データベースサーバ#1	Red Hat Enterprise Linux 7	10	48	120	480
5	データベースサーバ#2	Red Hat Enterprise Linux 7	2	32	120	180
授業料債権管理・免除システム						
1	アプリケーションサーバ#1	Windows Server 2016	2	16	100	50
2	アプリケーションサーバ#2	Windows Server 2016	2	16	100	50
3	アプリケーションサーバ#3	Windows Server 2016	2	16	100	50
4	データベースサーバ#1	Windows Server 2016	4	32	100	150
財務会計システム						
1	データベースサーバ#1	Windows Server 2016	4	16	200	800
2	データベースサーバ#2	Windows Server 2016	4	16	200	800
3	データベースサーバ#3	Windows Server 2016	4	16	200	800
2	データベースサーバ#4	Windows Server 2016	4	16	200	800
2	アプリケーションサーバ#1	Windows Server 2016	4	8	200	-
3	アプリケーションサーバ#2	Windows Server 2016	4	8	200	-
2	アプリケーションサーバ#3	Windows Server 2016	4	8	200	-
3	アプリケーションサーバ#4	Windows Server 2016	4	8	200	-
2	アプリケーションサーバ#5	Windows Server 2016	4	8	200	-
3	アプリケーションサーバ#6	Windows Server 2016	4	8	200	-
2	アプリケーションサーバ#7	Windows Server 2016	4	8	200	-

3	アプリケーションサーバ#8	Windows Server 2016	4	8	200	-
4	検証用サーバ兼バックアップサーバ	Windows Server 2016	4	8	400	-
マルウェア対策システム						
1	TCCM サーバ#1	Windows Server 2016	6	8	150	-
2	TCCM 用 SQL サーバ#1	Windows Server 2016	4	16	240	-
3	TMMS サーバ#1	Windows Server 2016	2	4	80	-
4	スタンドアロン SPS サーバ#1	CentOS 7(専用仮想アプライアンス)	4	4	60	-
5	スタンドアロン SPS サーバ#2	CentOS 7(専用仮想アプライアンス)	4	4	60	-
6	スタンドアロン SPS サーバ#3	CentOS 7(専用仮想アプライアンス)	4	4	60	-
7	スタンドアロン SPS サーバ#4	CentOS 7(専用仮想アプライアンス)	4	4	60	-
8	スタンドアロン SPS サーバ#5	CentOS 7(専用仮想アプライアンス)	4	4	60	-
9	スタンドアロン SPS サーバ#6	CentOS 7(専用仮想アプライアンス)	4	4	60	-
10	スタンドアロン SPS サーバ#7	CentOS 7(専用仮想アプライアンス)	4	4	60	-
11	VBcorp+TMSM サーバ#1	Windows Server 2016	3	4	80	-
12	VBcorp+TMSM サーバ#2	Windows Server 2016	3	4	80	-
13	VBcorp+TMSM サーバ#3	Windows Server 2016	3	6	80	-
14	VBcorp+TMSM サーバ#4	Windows Server 2016	3	4	80	-
15	VBcorp+TMSM サーバ#5	Windows Server 2016	3	4	80	-
16	VBcorp+TMSM サーバ#6	Windows Server 2016	3	4	80	-
17	VBcorp+TMSM サーバ#7	Windows Server 2016	4	4	80	-
18	VBcorp+TMSM サーバ#8	Windows Server 2016	3	4	80	-
19	VBcorp+TMSM サーバ#9	Windows Server 2016	3	4	80	-
20	VBcorp+TMSM サーバ#10	Windows Server 2016	3	4	80	-
21	VBcorp+TMSM サーバ#11	Windows Server 2016	3	4	80	-
22	VBcorp+TMSM サーバ#12	Windows Server 2016	3	4	80	-
23	VBcorp+TMSM サーバ#13	Windows Server 2016	3	4	80	-
24	VBcorp+TMSM サーバ#14	Windows Server 2016	3	4	80	-
25	VBcorp+TMSM サーバ#15	Windows Server 2016	3	4	80	-
26	VBcorp+TMSM サーバ#16	Windows Server 2016	3	4	80	-
27	VBcorp+TMSM サーバ#17	Windows Server 2016	4	4	80	-
28	VBcorp+TMSM サーバ#18	Windows Server 2016	3	4	80	-
29	VBcorp+TMSM サーバ#19	Windows Server 2016	3	4	80	-
30	VBcorp+TMSM サーバ#20	Windows Server 2016	3	4	80	-
31	VBcorp+TMSM サーバ#21	Windows Server 2016	3	4	80	-
32	VBcorp+TMSM サーバ#22	Windows Server 2016	3	4	80	-
33	VBcorp+TMSM サーバ#23	Windows Server 2016	3	4	80	-
34	VBcorp+TMSM サーバ#24	Windows Server 2016	3	4	80	-
35	VBcorp+TMSM サーバ#25	Windows Server 2016	3	4	80	-
36	VBcorp+TMSM サーバ#26	Windows Server 2016	3	4	80	-
37	VBcorp+TMSM サーバ#27	Windows Server 2016	3	4	80	-
38	VBcorp+TMSM サーバ#28	Windows Server 2016	3	4	80	-
39	VBcorp+TMSM サーバ#29	Windows Server 2016	3	4	80	-
40	VBcorp+TMSM サーバ#30	Windows Server 2016	3	4	80	-

41	VBcorp+TMSM サーバ#31	Windows Server 2016	3	4	80	-
42	VBcorp+TMSM サーバ#32	Windows Server 2016	3	4	80	-
43	VBcorp+TMSM サーバ#33	Windows Server 2016	3	4	80	-
44	VBcorp+TMSM サーバ#34	Windows Server 2016	3	4	80	-
45	VBcorp+TMSM サーバ#35	Windows Server 2016	3	4	80	-
46	VBcorp+TMSM サーバ#36	Windows Server 2016	3	4	80	-
47	VBcorp+TMSM サーバ#37	Windows Server 2016	3	4	80	-
48	VBcorp+TMSM サーバ#38	Windows Server 2016	3	4	80	-
49	VBcorp+TMSM サーバ#39	Windows Server 2016	4	4	80	-
50	VBcorp+TMSM サーバ#40	Windows Server 2016	3	4	80	-
51	VBcorp+TMSM サーバ#41	Windows Server 2016	3	4	80	-
52	VBcorp+TMSM サーバ#42	Windows Server 2016	3	4	80	-
53	VBcorp+TMSM サーバ#43	Windows Server 2016	3	4	80	-
54	VBcorp+TMSM サーバ#44	Windows Server 2016	3	4	80	-
55	VBcorp+TMSM サーバ#45	Windows Server 2016	3	4	80	-
56	VBcorp+TMSM サーバ#46	Windows Server 2016	3	4	80	-
57	VBcorp+TMSM サーバ#47	Windows Server 2016	4	4	80	-
58	VBcorp+TMSM サーバ#48	Windows Server 2016	3	4	80	-
59	VBcorp+TMSM サーバ#49	Windows Server 2016	3	4	80	-
60	VBcorp+TMSM サーバ#50	Windows Server 2016	3	4	80	-
61	VBcorp+TMSM サーバ#51	Windows Server 2016	3	4	80	-
62	VBcorp+TMSM サーバ#52	Windows Server 2016	3	8	80	-
63	VBcorp+TMSM サーバ#53	Windows Server 2016	2	4	100	-
64	VBcorp+TMSM サーバ#54	Windows Server 2016	2	4	100	-
研究情報ポータルシステム用サーバ						
1	研究情報ポータルシステム用サーバ#1	Red Hat Enterprise Linux 7	6	32	120	380
教職員向け情報 Web システム用サーバ						
1	教職員向け情報 Web システム用サーバ#1	Red Hat Enterprise Linux 7	6	32	120	380
各種 Web サーバ						
1	Web サーバ#1 (ms-ees)	Red Hat Enterprise Linux 7	1	4	150	-
人事給与統合システム						
1	アプリケーションサーバ#1	Windows Server 2012R2	6	12	100	50
2	アプリケーションサーバ#2	Windows Server 2012R2	6	12	100	50
3	アプリケーションサーバ#3	Windows Server 2012R2	6	12	100	50
4	アプリケーションサーバ#4	Windows Server 2012R2	6	12	100	50
5	アプリケーションサーバ#5	Windows Server 2012R2	6	12	100	50
6	アプリケーションサーバ#6	Windows Server 2012R2	6	12	100	50
7	アプリケーションサーバ#7	Windows Server 2012R2	6	12	100	50

8	データベースサーバ#1	Windows Server 2012R2	6	32	100	900
9	データベースサーバ#2	Windows Server 2012R2	6	32	100	900
勤怠管理システム						
1	アプリケーションサーバ#1	Windows Server 2012R2	6	12	150	50
2	アプリケーションサーバ#2	Windows Server 2012R2	6	12	150	50
3	データベースサーバ#1	Windows Server 2012R2	6	32	150	400
特許管理システム						
1	アプリケーションサーバ#1 兼データベースサーバ#1	Windows Server 2012R2	6	8	100	100
ロードバランサー						
1	ロードバランサー	F5-BIG-LTM-VE-10GV16	8	16	129	20
合計			485	1114	34599	

3. 3 バックアップサーバ#1・仮想基盤管理サーバ

・主データセンター（所在地：埼玉県さいたま市）

機器の名称 : HP ProLiant DL380 Gen9

台数 : 1台

CPU数 : 8

メモリ : 24GB

記憶領域 : OS領域 300GB : データ領域 60TB

ネットワークインターフェース : 10GBaseT×2ポート 1000BaseT×4ポート

OS : Windows Server 2016

3. 4 バックアップサーバ#2

・副データセンター（所在地：北海道札幌市）

機器の名称 : HP ProLiant DL380 Gen9

台数 : 1台

CPU数 : 8

メモリ : 24GB

記憶領域 : OS領域 300GB : データ領域 60TB

ネットワークインターフェース : 10GBaseT×2ポート 1000BaseT×4ポート

OS : Windows Server 2016

3. 5 一時バックアップ・内部専用DNS/NTP/SMTP/Syslog/監視/プロキシサーバ

機器の名称 : HP ProLiant DL380 Gen9

台数 : 1台

CPU数 : 8

メモリ : 24GB

記憶領域 : OS領域 300GB : データ領域 10TB

ネットワークインターフェース : 10GBaseT×2ポート 1000BaseT×4ポート

OS : CentOS 7

3. 6 ネットワーク機器

3. 6. 1 SINET ノード接続用 L2 スイッチ#1

・主データセンター（所在地：埼玉県さいたま市）

機器の名称 : HPE Aruba 2920 24G

台数 : 2 台(スタック構成/Active-Active 冗長構成)

3. 6. 2 サーバ接続用 L2 スイッチ

機器の名称 : HP 5700-32XT-8XG-2QSFP+

台数 : 2 台(スタック構成/Active-Active 冗長構成)

3. 6. 3 ファイヤーウォール

機器の名称 : Fortigate 600D

台数 : 2 台(HA 構成/Active-Standby 冗長構成)

3. 6. 4 SINET ノード接続用 L2 スイッチ#2

・副データセンター（所在地：北海道札幌市）

機器の名称 : HPE Aruba 2920 24G

台数 : 2 台(スタック構成/Active-Active 冗長構成)

3. 7 通信回線

3. 7. 1 SINET 接続用回線

回線の名称 : SINET5

3. 7. 2 バックアップ用回線

主センターと副センター間でバックアップ用の SINET 回線を用いている。

3. 8 その他機器

3. 8. 1 KVM コンソール

機器の名称 : LCD 8500 コンソール

台数 : 1 台

3. 9 ラック構成図及びネットワーク構成図

図 1 に、現在のサーバ及びスイッチのラック構成図を示す。また、図 2 に現在の主データセンターのネットワーク構成図を、図 3 に現在の副データセンターのネットワーク構成図を示す。

主データセンター

副データセンター

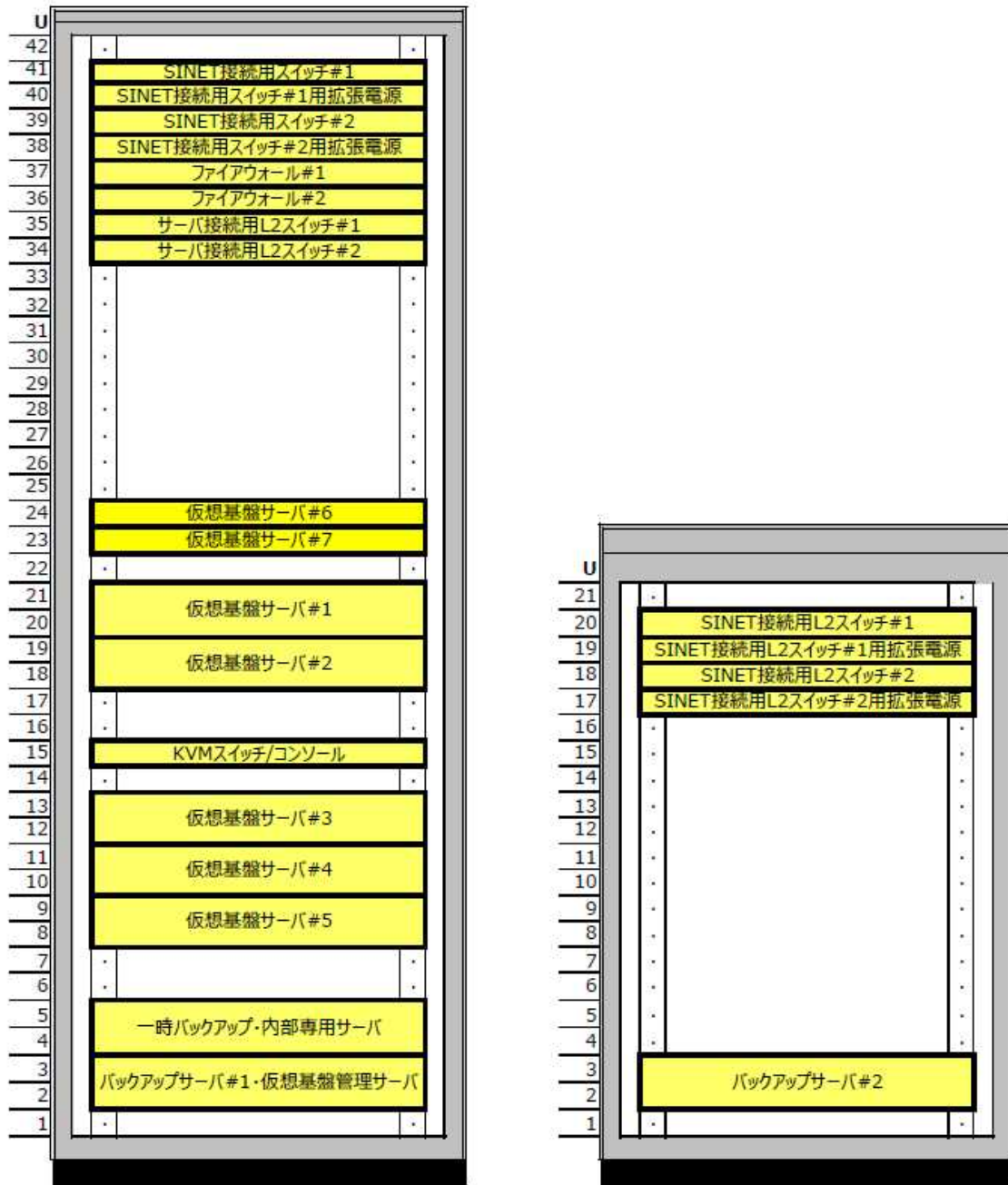


図 1. ラックマウント構成図

主データセンター

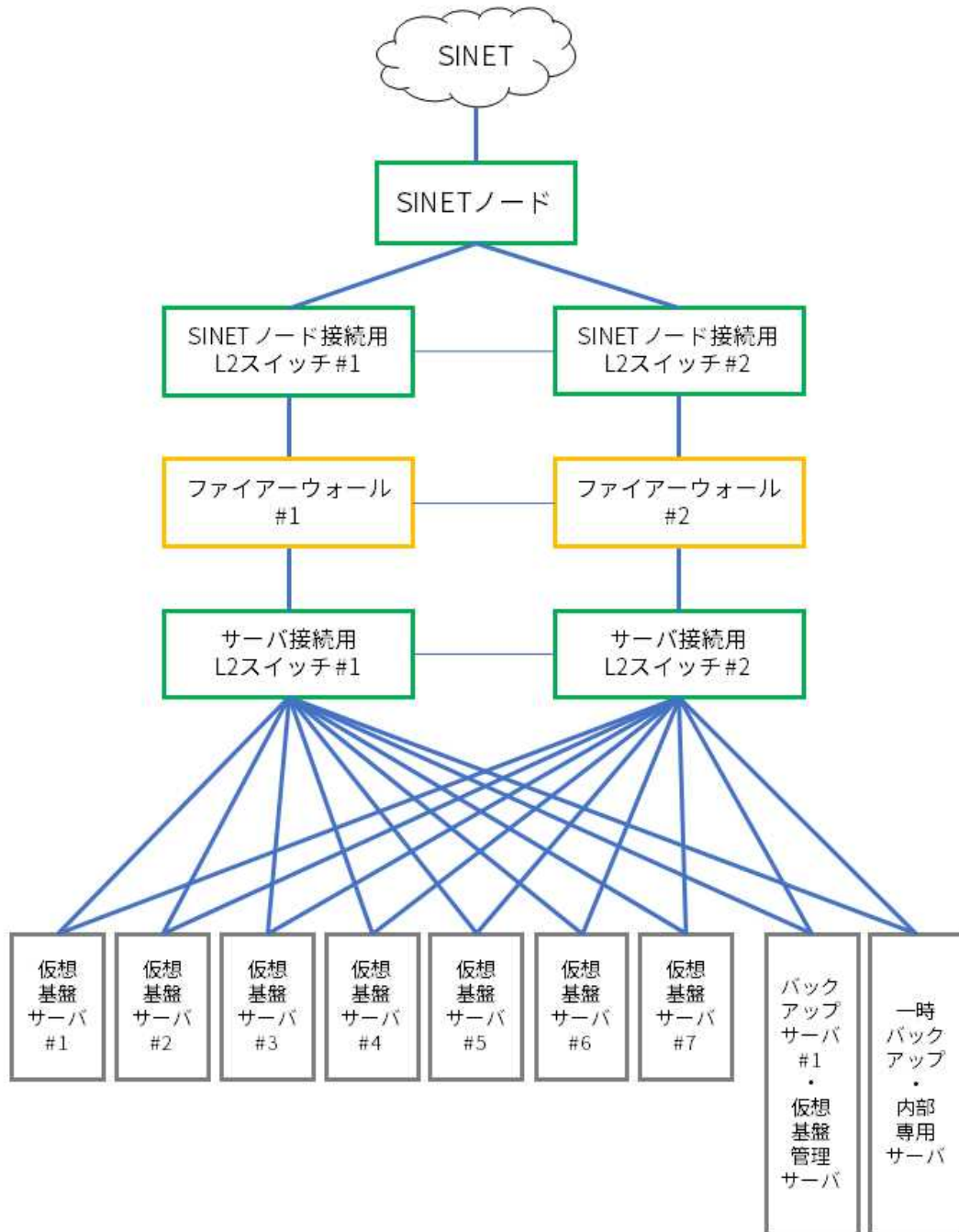


図2. 主データセンターのネットワーク構成図

副データセンター

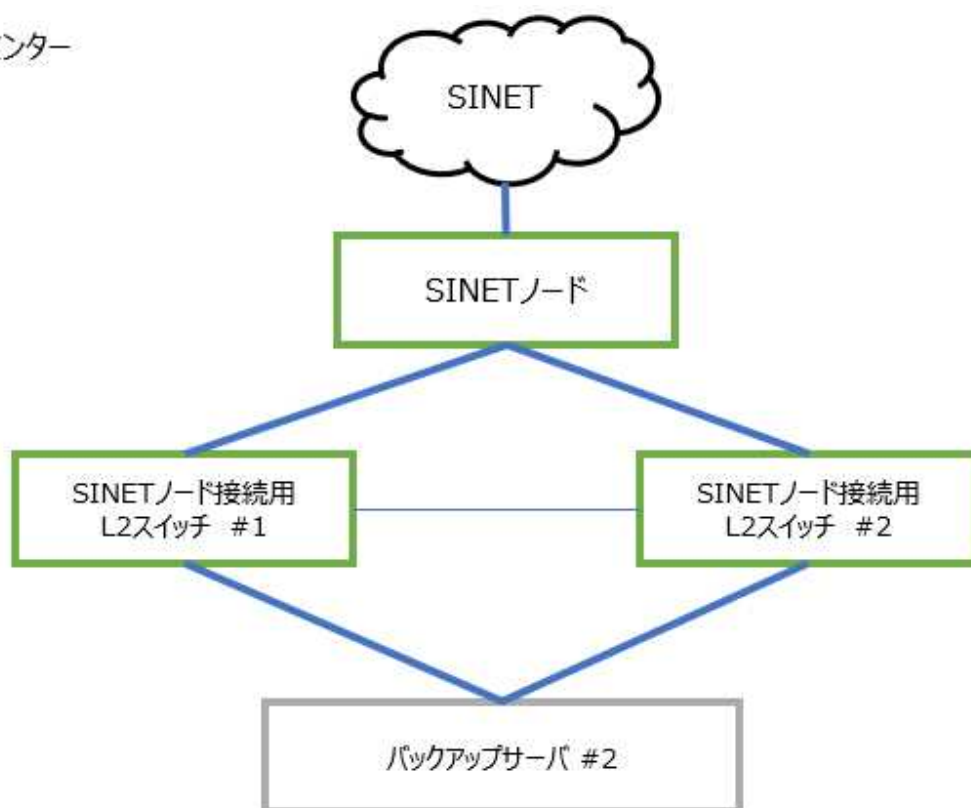


図3. 副データセンターのネットワーク構成図

4. 調達物品名及び構成内訳

4. 1 概要

ハウジングは、安全性に優れたデータセンターに設置するものとし、導入するハウジングは、仕様書の要件をすべて満たすこと。ただし、仮想基盤をサービスとして提供する場合、業務システムを運用するにあたり必要とされる仮想基盤管理機能を提供すること。

業務システムの内訳は 3.1 業務システム一覧 の通りである。

設計、搬入、設置、据付、配線、調整、接続、保守、搬出、撤去を含む
(詳細については、「Ⅱ. 調達物品に備えるべき要件」に示す)

4. 2 ハウジング調達の範囲

業務システムが稼動するために、以下のハウジングを提供すること。

- (1) データセンター
- (2) サーバ
- (3) 仮想基盤システム
- (4) バックアップシステム
- (5) 監視システム
- (6) ストレージシステム
- (7) ネットワーク機器
- (8) 通信回線
- (9) その他機器
- (10) 上記項目提供のための設計、搬入、設置、据付、配線、調整、接続、
- (11) 上記項目に関わる監視・保守
- (12) 現在稼働している、現クラウド基盤からのサーバ移行

5. 技術的要件の概要

- (1) 本調達物品に係る性能、機能及び技術等（以下「性能等」という。）の要求要件（以下「技術的要件」という。）は、「Ⅱ 調達物品に備えるべき要件」に示すとおりである。
- (2) 技術的要件はすべて必須の要求要件である。
- (3) 必須の要求要件は機構が必要とする最低要件を示しており、入札物品の性能等がこれらを満たしていないとの判定がなされた場合には不合格となり、落札決定の対象から除外する。
- (4) 入札物品の性能等が技術的要件を満たしているか否かの判定は、技術審査委員会において、入札物品にかかる技術仕様書その他の入札説明書で求める提案資料の内容を審査して行う。
- (5) 機構の指定する日時・場所において、提案内容についてのプレゼンテーションを行うこと。

Ⅱ. 調達物品に備えるべき要件

1. 性能、機能に関する要件

1. 1 データセンター

機構外のデータセンターにサーバ等を設置することにより、機構の停電や災害時の事業継続性を強化するとともに、省電力化を図るものである。

データセンターは、主データセンター及び副データセンターとして2か所に設置し、主データセンターで業務システムを稼働し、副データセンターで業務システムのバックアップを行う耐障害性の高いシステムとする。

1. 1. 1 設置要件

- (1) 主データセンターの設置場所は、機構本部より直線で100km圏内とする。副データセンターは災害対策を目的とするため、主データセンターから250km以上の遠隔地とする。
- (2) 自治体のHPで公開しているハザードマップ（液状化・浸水等）において危険度が低い（5段階評価の場合1または2相当）地域となっていること。ただし、想定される災害に対し有効とみとめられる対策が施されている場合は、危険度が低いとみなす。
- (3) 半径100m以内に消防法によるところの指定数量以上の危険物製造設備、火薬製造設備、高圧ガス設備がないこと。
- (4) 建物への受電方式は複数の受電経路が確保されていること。
- (5) 無停電電源装置、非常用電源設備が整備され、無瞬断での電源供給が可能なこと。さらに、主データセンターの無停電電源装置、非常用電源設備はいずれもN+1を含む冗長構成となっていること。
- (6) 非常用電源設備はデータセンター敷地に備蓄された燃料の追加供給を含めて40時間以上の給電が可能であること。
- (7) 法定点検や設備更改等による供給電源の停電がないこと。
- (8) 無停電電源装置の蓄電池は、停電発生時においても非常用電源設備からの給電を開始するまでの時間の3倍以上の時間、または5分以上、電源供給が可能なこと。
- (9) 発電機は燃料を補給することによって連続運転が可能であり、災害時の燃料補給ルートも予め策定されたコンティンジェンシープランにより確保されていること（万が一災害発生により電力会社からの供給が長期間停止になった場合においても、センタ設備については停止することなく稼働することが可能であることを考慮）。
- (10) 機器類が適切に冷却可能な空調設備を有すること。
- (11) 空調設備はN+1を含む冗長構成とし、24時間365日連続して空調稼働していること。
- (12) 空調機排水廻りに漏水検知システムを設置していること。
- (13) ラック外の周囲温度を適正に保ち、結露の発生しない温湿度設定が可能な空調であること。
- (14) データセンターでは温湿度情報と空調機の運用状態を一元的に管理し、温湿度の変化、漏水、空調機故障などのアラーム情報を24時間365日監視し、万が一の場合に備え万全の対策を確保してあること。
- (15) 通信、電力配線は電気誘導障害が起こらないよう、通信、電力配線が重ならないようにすること。
- (16) 機器設置室は物理的に隔離された管理区域であること。

- (17) データセンターの出入口には施錠機能を設け、入退出管理機能またはこれに類する機能を有すること。
- (18) 主データセンターの建物は、震度 6 強の地震に耐える、制震構造、免震構造いずれかであり、副データセンターの建物は、震度 6 強の地震に耐える耐震構造、制震構造、免震構造いずれかであること。主データセンターは建築基準法に規定する耐火性能を有し、副データセンターは建築基準法に規定する準耐火性能以上を有すること。
- (19) 機器設置室内の消火システムは水を利用しない人体に影響の少ない新ガス系の消火システムであること。
- (20) 所定の火災検知システムに加えて超高感度煙探知センサーシステムを設置していること。
- (21) 建物への回線引き込み部分が物理的に十分余裕があり、将来の回線数の増加にも対応可能であること。
- (22) 回線の引き込みにおいて引き込み可能なキャリア等の制限がないこと。
- (23) 機器設置室には監視カメラが設置され、過去 1 週間以上録画を残すとともに常時有人監視が行われていること。
- (24) 機器設置室から外部に通じる全ての出入り口は、専用 ID カード等による入室確認、監視カメラ設置、24 時間×365 日有人による監視体制が整備されていること。
- (25) 緊急時については、事前登録されている担当者の機器設置室への 24 時間 365 日の入室が可能であること。
- (26) 事前の申請に基づき、主データセンター及び副データセンターへ 24 時間 365 日の入館が可能であること。また、主データセンター及び副データセンター入館時には顔写真付きの身分証明書（運転免許証・パスポート・社員証等）による本人確認を行うこと。
- (27) ラックの鍵については、主データセンター及び副データセンター内にて管理すること。
- (28) 主データセンター及び副データセンターに避雷設備があること。
- (29) データセンターは、ISO27001/ISMS の認証を取得していること。

1. 2 サーバ

1. 2. 1 共通要件

ハウジング上で業務システムを稼働させるサーバ（アプリケーションサーバ・データベースサーバ）の共通要件は、以下のとおりとする。

ただし、バックアップサーバの仕様は共通要件を満たさなくてもよいものとする。

1. 日本語または英語の Web インタフェースを使って、遠隔地から OS の稼働状況に依存することなく、サーバの管理・監視（CPU、メモリ、ディスク、LAN インタフェースおよび物理サーバの場合は、電源、ファン、温度センサー等の稼働状況や障害管理等）が可能であること。また、複数のサーバを一元管理・監視ができること。
2. 各サーバの CPU については、現在機構で運用している業務システムで稼働している各サーバの性能以上であること。
3. 各サーバのログを 1 年以上取得し保存すること。
4. 各サーバのアップデートを一年に一度以上の間隔で行うこと。また、アップデートの際、業務系システムの停止を行わないこと。

1. 2. 2 仮想基盤システム

以下の性能を有する機器を主データセンターに設置すること。

1.2.2.1 仮想基盤サーバ

導入する仮想基盤サーバは、以下の仕様を満たすこと。

1. 現在、稼働中の業務システムをゲスト OS として運用すること。
2. vCPU を必要リソース分搭載すること。
3. 合計物理 CPU 数は、8～10 個とすること。
4. メモリを必要リソース分搭載すること。
5. ストレージは、合計で実効容量 80TiB 以上であること。
6. ストレージの一部または全部が SSD であること。
7. ネットワークインタフェースを冗長化すること。
8. 電源を冗長化すること。
9. 導入するハイパーバイザーは、現在使用している VMware vSphere ESXi 上で稼働しているゲスト OS をコピー又は移動して稼働できるものとする。また、構築時において、安定動作する最新版のバージョンのものを導入すること。
10. 複数台の物理サーバで冗長化すること。
11. 仮想基盤システムでは、仮想マシンを動作させるリソースを用意すること。
12. 仮想基盤サーバ 1 台に障害が発生しても必要リソース (CPU、メモリ、ストレージ) を賄え、さらに 30%以上のリソース (CPU、メモリ、ストレージ) に余裕がある構成とすること。
13. 仮想化基盤はハイパーコンバージドインフラストラクチャー構成とすること。

1.2.2.2 仮想基盤管理サーバ

導入する仮想基盤管理サーバは、仮想基盤サーバ上のゲスト OS を管理する機能を有すること。

1. 2. 3 バックアップシステム

以下の性能を有する機器をデータセンターに設置すること。

1.2.3.1 バックアップサーバ

1. CPU を 8 コア以上搭載すること。
2. メモリを 48GB 以上搭載すること。
3. ハードディスクの実効容量を合計で 60TB 以上用意すること。
4. ハードディスクを RAID6 で冗長化すること。
5. ネットワークインタフェースを 1 ポート以上有すること。
6. ネットワークインタフェースを冗長化すること。
7. 導入する OS は Windows Server 2019 相当以上とすること。
8. 主データセンター、副データセンターに必要数の筐体をそれぞれ導入すること。
9. 主データセンターに仮想基盤サーバ、仮想基盤管理サーバ、バックアップサーバ、一時バックアップサーバ、監視サーバ以外の全サーバの一次バックアップを取得すること。

10. スケジューリングバックアップを可能とすること。
11. ファイルレベルリストア機能を有すること。
12. 世代管理をすること。
13. 増分、永久増分、バックアップが可能であること。
14. バックアップ対象が仮想マシンの場合、エージェントレスによるバックアップ、および復元を可能とすること。
15. バックアップ対象が仮想マシンの場合、構成ファイルをバックアップから復元できる機能を有すること。
16. バックアップ対象が仮想マシンの場合、仮想マシンのディスク単位でバックアップから復元できる機能を有すること。
17. バックアップ対象が仮想マシンの場合、バックアップから仮想マシンを復元する際に、オリジナルの仮想マシンを上書きするか新しい仮想マシンを作成するか選択が可能なこと。
18. 重複排除、圧縮によりバックアップのサイズ削減、レプリケーション時の転送量削減が可能であること。
19. 管理サーバ、処理実行サーバ、保存先サーバを分割して配置することが可能であること。
20. バックアップ、レプリケーションを行う際に、使用するネットワーク帯域幅を設定、帯域制限を行う時間帯を設定可能であること。
21. バックアップ内の仮想マシンをハイパーバイザに転送せずに直接起動が可能であること。
22. バックアップファイルから Azure VM としてや Amazon EC2 としてリストアできること。
23. 初回レプリケーション時にバックアップファイルから複製仮想マシンを作成可能であること。
24. レプリケーション時にバックアップファイルをデータソースとすることが可能であること。
25. 保守拠点を日本国内に有し、問い合わせ時に日本語で迅速に回答できうる体制を有していること。
26. 製品専用のナレッジベース(日本語)の提供可能であること。
27. 副データセンターに仮想基盤サーバ、仮想基盤管理サーバ、バックアップサーバ、一時バックアップサーバ、監視サーバ以外の全サーバの二次バックアップを取得すること。また、取得のためのサーバについても本調達に含むこと。主データセンター用のバックアップサーバと副データセンター用のバックアップサーバは同一の製品とすること。

1.2.3.2 一時バックアップサーバ

以下の性能を有する機器を主データセンターに設置すること。

1. ハードディスクの実効容量を 10TB 以上搭載すること。
2. ハードディスクを冗長化すること。
3. ネットワークインタフェースを 1 ポート以上有すること。
4. ネットワークインタフェースを冗長化すること。
5. 電源を冗長化すること。
6. NFS サービスを提供すること。
7. CIFS サービスを提供すること。
8. 高専機構本部 syslog サーバで取得されているログのバックアップを取得するこ

と。

1. 2. 4 監視システム（監視サーバ）

以下の性能を有する機器を主データセンターに設置すること。

1. 各システムを監視すること。
2. ネットワーク機器を監視すること。
3. 監視サーバが動作するのに必要な推奨スペック以上で稼働させること。
4. 異常を検知したらアラートメールを送信すること。
5. 1.2.3.2の一時バックアップサーバと兼用も可とする。

1. 2. 5 内部専用 DNS/NTP/SMTP/プロキシサーバ

以下の性能を有する機器を主データセンターに設置すること。

1. 本調達用で構築するサーバ用として、DNS/NTP/SMTP/プロキシの機能を提供するサーバを構築すること。
2. 他のサーバとの兼用も可とする。
3. 仮想基盤サーバ内にゲスト OS としての提供も可とする。

1. 2. 6 内部専用 syslog サーバ

以下の性能を有する機器を主データセンターに設置すること。

以下の機器からのログを収集し保存する機能を持っていること。

なお、保存するログは、以下の機器が収集しているすべてのログとする。

また、収集したログを1年以上保存する機能を持っていること。

1. ハイパーバイザー
2. ファイアウォール
3. スイッチ
4. バックアップサーバ
5. 一時バックアップサーバ
6. 監視システム（監視サーバ）
7. 内部専用 DNS/NTP/SMTP/プロキシサーバ

1. 3 ネットワーク機器

1. 3. 1 ロードバランサー

以下の性能を有する機器を主データセンターに設置し、冗長構成とすること。

1. L4、L7の負荷分散が可能であること。
2. ヘルスチェック機能として負荷分散対象の機器の監視が可能であること。
3. セッション維持機能として、IP アドレス情報、HTTP Cookie 情報、HTTP ヘッダ情報、SSL セッション ID 情報でのパーシステンス機能をサポートしていること。
4. L7のデータペイロードの情報をもとにして、トラフィック制御が可能であること。

5. HTTP ヘッダの変更/挿入/削除ができること。
6. HTTP Cookie 暗号化による、なりすまし防御機能を備えること。
7. 脆弱性につながる特定の文字列（サーバの情報など）をレスポンスから遮断するリソースクロッキング機能を備えること。
8. コンテンツキャッシュ機能と HTTP 圧縮機能を備えること。
9. 設定情報のバックアップ及びリストア機能を有すること。
10. SSL サーバ証明書をバックアップできること。
11. SSL サーバ証明書はバックアップから復元できること。
12. 機器に対応が必要な異常が発生した場合、SNMP 及びメールで警告を送信できること。
13. ネットワーク経由で、電源オン、オフ、リセットを実行できる管理機能を有すること。
14. 一意性保証情報を冗長構成で利用できること。
15. Web ブラウザより HTTPS で GUI 管理/設定を行う機能を有すること。
16. SSH により CLI 管理/設定を行う機能を有すること。
17. パケットキャプチャを取得する機能を有すること。
18. 仮想基盤サーバ内に仮想アプライアンスとして構成しても構わない。

1. 3. 2 スイッチ

以下の性能を有する機器をデータセンターに全システムが稼働するための必要なだけ設置すること。主データセンターのサーバ接続用とストレージ接続用は用途別に物理的または論理的に独立させ、それぞれ冗長化すること。

1. 10 GbE スイッチであること。
2. 本システムの機器類等の 10Gbps のインタフェースを接続するポート数以上の 10GBASE-T 対応ポートを有していること。
3. 1000BASE-T に対応した管理用イーサネットポートを 1 ポート以上有していること。
4. スイッチ筐体をまたいで複数のポートを論理的に 1 つのポートに構成する機能を有すること。また対象のポート全てを利用して同時に通信できること。
5. 冗長化された電源共有ユニットを有すること。
6. 主データセンターのサーバ接続用スイッチは、全二重でのスイッチファブリック容量が 640Gbps 以上であること。
7. 上記全ての機能はライセンス等の追加を必要とすることなく、サポートすること。

1. 3. 3 ファイアウォール

以下の性能を有する機器を主データセンターに設置し、冗長構成とすること。

1. 物理的な機器の場合は、GbE インタフェースを 2 ポート以上搭載すること。
2. 物理的な機器の場合は、シリアルコンソール用のインタフェースを 1 ポート有すること。
3. 最大同時セッションは 500,000 セッション以上であること。
4. ステートフルインスペクションによるアクセス制御が可能なこと。
5. WebUI、CLI から設定管理が可能なこと。
6. SNMP に対応していること。
7. Telnet、SSH によるリモートアクセス管理に対応可能であること。

8. アンチマルウェア、不正侵入防御、Web フィルタリング、アンチスパム機能を搭載すること。
9. FW を通過する、外側から内側及び内側から外側の通信のポリシーで、アンチマルウェア、不正侵入防御、Web フィルタリング、アンチスパム機能を有効化すること。
10. すべての通信ログを 1 年以上保存すること。Syslog サーバに保存しても構わない。

1. 4 通信回線

1. 4. 1 SINET6 接続用回線

1. 国立情報学研究所の運営する学術情報ネットワーク (SINET6) の接続拠点 (以下、NOC) と主データセンター間、及び、NOC と副データセンター間の回線を用意すること。
2. 1. の回線については占有型 10Gbps 以上の回線とし、回線を冗長化すること。
3. 機構本部・各高専から主データセンター間の接続、及び、主データセンターから副データセンター間の接続を、SINET6 の L2VPN サービスを利用して行うこと。
4. 主データセンター及び副データセンターから SINET6 の NOC への接続に係る初期導入費用及び利用料を本調達に含めること。
5. 本機構本部及び各高専から SINET6 への接続に係るアクセス回線は本調達の範囲外とする。
6. 本機構本部及び各高専から SINET6 への接続に係る L2VPN 設定は本調達の範囲外とする。

1. 5 その他機器

1. 5. 1 KVM コンソール

1. KVM コンソールとして、機器類に適したディスプレイ、日本語キーボード及びポインティングデバイスが提供されていること。

1. 6 補足事項

1. 6. 1 ミドルウェアライセンス

機構では Oracle Database Standard Edition 2 を 10 ライセンス保有しており、本調達納期の時点では、10 ライセンスが本調達のシステムで利用可能である。

契約開始時点では、本調達に含む以下サーバで Oracle を使用する。

また、サーバ構築及び並行稼働期間中に必要な Oracle ライセンスは、受注者が用意すること。

1. 人事給与統合システム用データベースサーバ	2 台
2. 勤怠管理システム用データベースサーバ	1 台
3. 給与明細システム用データベースサーバ	1 台
4. 旅費システム用データベースサーバ	2 台
5. 特許管理システムデータベースサーバ	1 台

1. 6. 2 OS および仮想基盤ソフトウェア

各サーバに必要となるOSのライセンスは、本調達に含むものとする。また、業務システムを稼働するために必要となる仮想基盤のハイパーバイザーや管理用ソフトウェア等も本調達に含むものとする。

なお、機構が別途契約する包括ライセンスにより Core CAL Suite は使用可能である。

2. 性能、機能以外に関する要件

2. 1 受注条件

受注者は一般社団法人情報マネジメントシステム認定センター、公益財団法人日本適合性認定協会若しくはその他認定機関により認定された審査登録機関によるISO/IEC27001又はJIS Q 27001の認証を受けていること。

また、一般財団法人日本情報経済社会推進協会からプライバシーマーク制度によるプライバシーマーク（JISQ15001）使用許諾の認証を受けていること。

2. 2 設置条件等

1. 作業日程は、機構担当者と協議の上決定すること。
2. 本契約に、設計、搬入、設置、据付、配線、調整、接続、保守、搬出、撤去に要する全ての費用は本調達に含むこと。
3. 設置や導入構築等の際は作業日程と体制を前もって掲示し、受注者及び機構の作業を明確にし、機構担当者の承諾を得ること。また、作業の実施時間帯は、原則「平日（国民の祝日に関する法律第3条に規定する休日を除く月曜日～金曜日）の9時～17時」とするが、状況によっては土日祝・夜間となることも想定されることから、具体的な作業日時については、機構担当者と協議の上決定すること。
4. 受注者が提供するデータセンターへ、必要に応じて搬入、設置、据付、配線、調整、接続を行うこと。なお、必要なサーバラック及び電源設備はデータセンター側で別途用意すること。
5. 機器間及びネットワーク等の構成に必要とする消耗品等（UTP ケーブルなど）、及びサーバラック内に収容するためのラックマウントキットやネジ・金具類も全て本調達に含めること。
6. 導入した物理機器のホスト名、IP アドレス、ハードウェア固有情報等を物理機器にシール等をはり付けること。
7. 本調達物品に接続される物理配線については、すべて配線番号や行き先等を表示したシール等をはり付ける、もしくはタグ等を取り付けること。
8. 導入時に生じる梱包材等は、受注者が責任を持って引き取ること。
9. 契約満了時は、ハードディスクなどに残るデータを完全消去し、機構へ報告書を提出すること。

2. 3 導入構築

2. 3. 1 システム共通事項

1. 本調達物品において、本調達物品以外の他システム等との連携が多くあることから、これを一体化させ運用を円滑に行うため、機構担当者及びその他システム等納入業者・保守業者と連携し綿密な調整を行い、支障なく稼働できるよう導入構築を行うこと。また、契約期間中は、必要に応じて機構担当者とはシステム等納入業者・保守業者との打ち合わせ等に参画すること。

本調達物品上で稼働予定の他システム等一覧

- (A) 人事給与統合システム用ソフトウェア
 - (B) 勤怠管理システム用ソフトウェア
 - (C) 給与明細システム用ソフトウェア
 - (D) ファイル共有システム用ソフトウェア
 - (E) 旅費システム用ソフトウェア
 - (F) 財務会計システム
 - (G) 特許管理システム用ソフトウェア
 - (H) 研究情報ポータルシステム用ソフトウェア
 - (I) 教職員向け情報 Web システム用ソフトウェア
 - (J) 上位のネットワーク機器
2. 導入構築にあたり、作業日程と体制に基づき、機構との調整を密にしながら、各種管理（進捗、課題、品質、セキュリティ、障害）を実施すること。
 3. 本調達物品以外の他システム等との連携について不具合が発生した場合は、原因の切り分けを行い、本調達物品に起因する問題については速やかに対処し、これに連携する他システム等に起因する問題については、積極的な技術支援及びアドバイスをを行い、必要に応じて立ち会うこと。なお、立ち会いの要請は令和4年11月末まで応じ、本調達物品以外のシステム等における設定作業等は、機構担当者又はシステム等納入業者・保守業者が行う。
 4. ソフトウェア移行作業は他システム等納入業者・保守業者が行うが、その作業に必要な設計書及び構築における各種パラメータ値がわかる設定書を提出すること。
 5. 試験設計に基づき検証を行い、動作、品質、パフォーマンス、セキュリティ等を確認し、機構担当者の承諾を得ること。
 6. 導入構築に関して、本仕様書に明示されていない詳細設定については、機構担当者との協議の上決定すること。

2. 3. 2 設計

1. 機構担当者及び他システム等納入業者・保守業者と連携し綿密な調整を行い、支障なく稼働できるよう各種設計を行うこと。
2. 設計に必要な各種情報等について、機構及び他システム等納入業者・保守業者にヒアリングするためのヒアリングシートを作成し機構担当者の承諾を得ること。なお、他システム等納入業者・保守業者へのヒアリングシート送付及び収集は、機構担当者が行い受注者に提供する。
3. 機構及びシステム等納入業者・保守業者から収集したヒアリングシートを精査し、詳細設計、運用設計、試験設計等を行い、機構担当者の承諾を得ること。

2. 3. 3 各種サーバ

1. 設計時に作成及び収集するヒアリングシートをもとに、各サーバの OS インストールや設定等を行うこと。
2. 項 1. 2. 5 の内部専用 DNS/NTP/SMTP/プロキシサーバに、現行設定を移行すること。
3. 項 1. 2. 6 の内部専用 syslog サーバに、現行設定を移行すること。
4. 全サーバのハードウェアに異常を検出した場合は、メールで管理者に通知する構成にすること。なお、通知設定に SMTP サーバが必要な場合は、本調達物品にある SMTP サーバと連携させること。
5. 機構担当者が指定するサーバに、別途調達するマルウェア対策システムの納入業者と協調し、マルウェア対策ソフトウェアをインストールすること。
6. マルウェア対策ソフトウェアを導入した際は、マルウェア定義ファイル等を自動更新する設定とし、また、導入時に必ずシステムに影響のないテストマルウェアファイルで実際にマルウェアを検知することを確認すること。
7. 監視サーバを構築し、各システムを監視すること。監視内容は項 2. 3. 6 に記載する。

2. 3. 4 仮想基盤システム

1. 仮想基盤システム用ハイパーバイザー「VMware vSphere 6.5 相当以上」の各機能が支障なく使用できるよう導入構築を行うこと。
2. ハードウェアのリソース配分 (CPU、メモリ、ディスク容量等) などの詳細設定は、現クラウド基盤環境に準拠すること。
3. 仮想基盤管理用ソフトウェアおよび関連するソフトウェア類の各機能が支障なく使用できるよう導入構築および提供を行うこと。

2. 3. 5 バックアップシステム

1. 全サーバのバックアップを取得し、復元できるように設定すること。
2. 機構が指定するサーバについては、スケジューリングバックアップによって定期的にバックアップを取得すること。
3. 一時バックアップサーバについては NFS、CIFS サービスを設定すること。

2. 3. 6 監視システム

1. 各システムに対して以下の項目を監視する設定を行うこと。
 - (1) PING 監視(死活監視)
 - (2) CPU 監視
 - (3) メモリ監視
 - (4) ファイルシステム監視
2. ネットワーク機器に対して以下の項目を監視する設定を行うこと。
 - (1) PING 監視(死活監視)
 - (2) SNMP ポーリング監視
3. ハイパーバイザーに対して以下の項目を監視する設定を行うこと。
 - (1) PING 監視(死活監視)
 - (2) CPU 監視

- (3) メモリ監視
- 4. 異常を検知したらアラートメールを送信する設定を行うこと。設定内容については、機構担当者と協議の上決定すること。

2. 3. 7 ネットワーク機器

- 1. 機構担当者の指示に従い、VLAN 設定や IP アドレス等の設定を行うこと。
- 2. 障害が発生しても継続して使用できるよう冗長構成とすること。
- 3. ファイアウォールにおいて、機構担当者と協議の上アクセス制限等の設定を行うこと。
- 4. ロードバランサーにおいて、ルーティング、SSL 変換処理、負荷分散、負荷分散先の死活監視等の設定を行うこと。また、負荷分散先のサービス停止が発生した場合はメールで管理者に通知する構成にすること。なお、通知に必要なメールサーバは、本調達物品にある仮想基盤システムの中で構築する SMTP サーバと連携させること。
- 5. 障害が発生した場合、メールで管理者に通知すること。

2. 4 保守・運用サポート

2. 4. 1 全体

- 1. 保守・運用サポートの対象は、本調達物品全てとすること。
- 2. 契約期間中における本調達物品のハードウェア保守は、下記のとおりとすること。月曜日～金曜日（祝祭日と年末年始 12/29～1/3 を除く）9 時～17 時対応のオンサイト保守とすること。
- 3. 契約期間中における本調達物品のソフトウェア保守は、下記のとおりとすること。また、下記に関し、脆弱性が発見された際は速やかに対応すること。システム停止しなければならない場合は機構担当者と日程等協議の上実施すること。
 - (A) Red Hat Enterprise Linux Server 7 相当以上
全台に対してサブスクリプション及びテクニカルサポートサービスを提供すること。
 - (B) 仮想基盤ソフトウェアおよびサービス
導入するすべてに対してサブスクリプション及びテクニカルサポートサービスを提供すること。
 - (C) バックアップサーバ用ソフトウェア
全台に対してサブスクリプション及びテクニカルサポートサービスを提供すること。
 - (D) その他納品する OS に対してサブスクリプション及びテクニカルサポートサービスを提供すること。
- 4. 本調達物品に障害が発生した場合、アプリケーション保守業者と原因の切り分けを行い、本調達物品のハードウェア及びソフトウェアに起因する障害については復旧作業を行うこと。なお、復旧作業の対応時間については、保守条件や運用サポート条件に従い行うものとする。
- 5. 本調達物品の監視システム等を使用し、ハードウェア、OS およびミドルウェアの 24 時間 365 日の自動監視を行うこと。
- 6. サーバについて、OS の再インストールが必要となった場合は、バックアップデータを元にリストア作業を行うこと。

7. その他設定変更等の依頼があった場合は対応すること。なお、システム全体にかかる大幅な設定変更については、機構担当者と協議の上決定すること。
8. 機構担当者からの技術的相談にも応じること。
9. 障害発生時の調査及び対応や設定変更作業などは、本調達物品に対してリモートアクセスし行うこと。なお、リモートアクセス方法については、機構担当者と協議の上決定するが、リモートアクセスに必要な通信回線費用（工事費、回線費、ISP 接続費など）等が発生する場合は、受注者の負担とすること。
10. リモートアクセスからの対応が難しい場合は、機構担当者と日程調整の上、オンサイトでを行うこと。なお、オンサイトでの対応時間については、平日（国民の祝日に関する法律第3条に規定する休日及び12月29日～1月3日の年末年始を除く月曜日～金曜日）の「9時～17時」とする。
11. 本調達物品について、システムの重大な不具合に対する修正や重大なセキュリティホール等の情報が公表された際は、3営業日以内に機構担当者に情報を提供し、機構担当者と協議の上、対策を実施すること。
12. 機構担当者からの問い合わせについて、総合受付窓口（FAX または電話、およびメール）を設け一本化し無制限受付とすること。なお、受付時間は24時間365日とすること。
13. オンサイト保守物品の障害発生等について、24時間365日対応の受付窓口（FAX または電話、およびメール）を設け受け付けること。この受付窓口は上記12.の総合受付窓口と同じでも構わない。なお、オンサイト保守の時間帯以外に受け付けた場合は、翌オンサイト保守時間帯に至急対応すること。
14. オンサイト保守についての要員配置等の体制を明示すること。
15. 機構担当者との定例会議を、導入段階では2週間に1回、運用段階では3か月ごとに1回以上又は適宜行い、また、その議事録を作成し機構担当者の承認を得ること。なお、定例会議の出席者は、営業担当者及び技術担当者とする。
16. 契約期間内におけるバージョンアップ等の対応については、機構担当者と協議の上適宜実施すること。

2. 4. 2 データセンターの保守運用サポート

以下の24時間365日対応でサービスを行うこと。

1. 異常を検知したときは機構指定の場所へ連絡を行うこと。なお、異常の内容については、月次に報告を行うこと。
2. 機構の職員から指示があった場合、機器の電源オフ、オンを行うこと。
3. 機構及びアプリケーション保守業者からの依頼に応じて、機器のランプ状況、画面状況を確認（目視）し報告すること。
4. 作業報告書を、毎月機構に提出すること。尚、作業報告書は作業が発生しなかった月でも提出すること。

2. 5 提出物及び提出期限

1. 故障発生時の保守手順マニュアルを日本語で提供すること。
2. 運用手順マニュアル（サーバのバックアップ管理、サーバのハードウェアステータス確認、仮想基盤システムの管理、ネットワーク機器の管理、その他機構およびソフトウェアベンダーがシステムを管理維持するのに必要な手順）を日本語で提供すること。
3. 独自マニュアルを作成した際、製本された紙媒体及び改変できる電子データで提供

すること。

4. 独自マニュアルは必要に応じて改訂し、変更した際はその都度提供すること。
5. 受注者が独自作成したマニュアルの著作権及び所有権は、機構に帰属すること。
6. 下記の完成図書（冊子3部）と下記全ての電子データ（CDまたはDVD格納）を契約開始日まで納品すること。
 - (A) 機器の仕様書
 - (B) プロジェクト計画書及び完了報告書
 - (C) 設計書（詳細設計、運用設計等、本調達業務に係るもの等）
 - (D) 設定書（パラメータシート等）
 - (E) テスト報告書（テスト計画書、テスト結果報告書等）
 - (F) ラック搭載一覧及び施工写真
 - (G) 説明書、マニュアル（改訂版も含む）
 - (H) 議事録（定例会、個別打合せ等）

2. 6 操作教育

1. 機構担当者に対して、本調達物品の管理・運用に関する説明・教育を実施すること。なお、説明・教育の内容については、機構担当者と協議の上決定すること。
2. データセンター担当者に対して、本調達物品のハードウェアステータス確認に関する説明・教育を現地で実施すること。なお、説明・教育の内容については、機構担当者と協議の上決定すること。

2. 7 機密保持

1. 受注により知り得た全ての情報について守秘義務を負うものとし、これを第三者に漏らし、又は他の目的に使用しないこと。
2. 受注により知り得た情報については、契約期間はもとより、契約終了後においても第三者に漏らしてはならない。
3. 正当な理由があつてやむを得ず第三者に開示する場合、書面によって事前に承諾を得ること。また、情報の厳重な管理を実施すること。
4. 機構が提供した資料は、原則として全て複製禁止とすること。但し、業務上やむを得ず複製する場合であつて、事前に書面にて機構の許可を得た場合はこの限りではない。なお、この場合にあつても使用終了後はその複製を機構に返納又は焼却・消去する等適切な措置をとり、機密を保持すること。

2. 8 検査及び検収

高専機構担当職員の立ち会いのもと行われる現場での動作確認及び納品成果物の納入をもって検収とする。

2. 9 損害賠償

受注者が本契約に違反して、高専機構が損害を被った場合には、高専機構は受注者に対して損害賠償を請求し、かつ、高専機構が適当と考える必要な措置をとることを請求できる権利を有するものとする。

2. 10 サプライチェーンリスクマネジメントについて

1. 受注者は、サプライチェーン・リスクの要因となる脆弱性を発生させない又は増大させないための管理体制を構築すること。また、応札時に管理体制図を機構に提示すること。
2. 受注者は、機構がサプライチェーン・リスクに係る情報セキュリティインシデントを認知した場合又はその疑いが生じた場合に、必要に応じて業務内容、作業プロセス又は成果物を立ち入り検査等で機構が確認することを了承すること。
3. 本業務において使用する機器等については予め機構に機器等リストを提出し、機構がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、機構と迅速かつ密接に連携し提案の見直しを図ること。
4. その他、サプライチェーン・リスクに関し、以下の資料を提出し、対策を講じていることを証明した場合は加点する。
 - (1) 当該システムに関して、想定されるサプライチェーン・リスク及びそれに対する軽減策についての説明資料
 - (2) 想定されるサプライチェーン・リスクに鑑み、当該システムで使用される機器を選定した理由に関する説明資料
 - (3) 調達機関の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や品質保証体制を証明する書類
 - (4) 当該システムに調達機関の意図しない変更が行われるなどの不正が見つかったときに、追跡調査等を実施する手順及び体制を示す資料
 - (5) 各種認証取得に関する資料
 - (6) 我が国政府機関における類似のシステム構築・運用実績

2. 11 ワーク・ライフ・バランス等の推進に関する評価について

女性の職業生活における活躍の推進に関する法律に基づく認定企業（えるぼし認定企業）、次世代育成支援対策推進法に基づく認定企業（くるみん認定企業等）及び、青少年の雇用の促進等に関する法律に基づく認定企業（ユースエール認定企業）については加点するので、認定されていることが確認できる書面の写しを提出すること。なお、配点は別紙評価基準により、複数の認定が該当する場合は、最も配点が高い区分により加点することとする。

2. 12 その他

1. 導入する機器及びソフトウェアについて、型番変更、バージョンアップ、製造中止が発生した場合、技術的要件及び価格が同等である場合は、最新版を導入すること。なお、その最新版の導入にあたっては、機構と協議の上決定すること。
2. 本調達の履行について疑義が生じたとき、又は本調達に伴い高専機構と交わす契約書に定めない事項については、機構及び受注者の双方で協議の上決定すること。それにより追加業務等が発生する場合は、機構本部事務局財務課契約係を通して発注するので、受注者はそれ以外の者からの発注や依頼を受け付けないこと。
3. 本調達における保守・運用サポート条件以外の対応については、別途適正な価格による有償契約によって対応が可能なこと。
4. 受注者の故意又は過失により損害が発生した場合は、受注者の責により原状復帰すること。

5. 本調達物品を導入するに当たっては、機構から「国立高専機構情報セキュリティポリシー」に基づき、情報セキュリティに係る事項等の説明を受け遵守すること。
6. 本調達を導入事例としてパンフレット発行等の各種メディアへの掲載やプレス発表を行う場合は、必ず機構と調整の上とり行うこと。
7. 受注者は本業務を自ら履行するものとし、本業務の全部を第三者に委託、又は請け負わせてはならない。ただし、本業務の一部を第三者に委託する場合であり、かつ、機構に書面によって外部委託の詳細を提出し許可された場合は、この限りではない。なお第三者委託を許可された場合であっても、受注者は契約による責任を免れることはできない。