

所内情報システムサーバ及び ネットワーク機器等賃貸借契約に係る仕様書

令和7年8月

地方独立行政法人大阪産業技術研究所 森之宮センター

目次

第 1	概要	1
1	目的	1
2	現在のネットワーク構成状況	1
3	導入機器一覧	1
(1)	サーバ	1
(2)	ネットワーク機器	2
4	納入・設置場所	2
5	借入期間	2
6	業務の概要	3
第 2	機器等の仕様	5
1	共通事項	5
2	機器構成仕様	5
(1)	全体構成	5
(2)	機器一覧表の作成	5
3	仮想化基盤サーバ、ハイパーコンバージドサーバ 仕様	5
(1)	ハードウェア	5
(2)	ハイパーバイザー	7
(3)	ハイパーコンバージド ソフトウェア	7
4	バックアップサーバ 仕様	7
(1)	ハードウェア	7
(2)	ソフトウェア	8
(3)	バックアップソフトウェア	8
5	公開 WWW サーバ 仕様	9
6	Mail/内部 DNS サーバ 仕様	9
7	DC サーバ 仕様	9
8	ファイルサーバ 仕様	9
9	ネットワーク監視サーバ 仕様	9
10	WSUS サーバ 仕様	10
11	資産管理サーバ 仕様	10
12	仮想化管理サーバ 仕様	14
13	メールフィルタリングサーバ 仕様	14
14	所内イントラ Web サーバ 仕様	14
15	ウイルス対策ソフト管理サーバ 仕様	14
16	ファイアウォール 仕様	15
17	センタースイッチ 仕様	15
18	サーバスイッチ 仕様	16
19	フロアスイッチ 仕様	17
20	エッジスイッチ 仕様	18
第 3	設置・保守・サポート	19
1	機器の設置・納品	19
(1)	機器の設置・搬入支援	19
(2)	借入期間満了時の取り扱い	20
2	保守案件	20
(1)	保守範囲	20
(2)	保守概要	20

(3) 保守の内容	20
(4) 保守対応	20
3 補足事項	20
(1) 機密保護	20
(2) その他	20
(別紙1)	21
 (参考資料)	22～30

第 1 概要

1 目的

本業務は、(地独)大阪産業技術研究所 森之宮センター(以下、「本研究所」という)で所内情報システム用として使用するハードウェア(サーバ、ネットワーク機器並びにそれらの付属品等)とソフトウェア(マニュアルを含む)を調達するものである。

なお、調達した機器の設定、納品(搬入・設置作業)、及び納品後の保守も本調達に含むものとする。

2 現在のネットワーク構成状況

本研究所所内情報システムにおける現状のネットワーク構成概略図を別紙1に示す。サーバ室内の機器、および各階のフロアスイッチ、各階居室内に設置するエッジスイッチが調達品の対象である。また、稼働サーバは以下の通りである。

名称	台数	用途
仮想化基盤サーバ	1式	
バックアップサーバ	1台	バックアップサーバ、DCサーバ
公開WWWサーバ	1台	公開WWWサーバ
Mail/内部DNSサーバ	1台	Mailサーバ、内部DNSサーバ
DCサーバ	1台	DCサーバ、ウイルス対策ソフト管理サーバ
ファイルサーバ	1台	ファイルサーバ
ネットワーク監視サーバ	1台	ネットワーク監視サーバ、WSUSサーバ
資産管理サーバ	1台	資産管理サーバ
仮想化管理サーバ	1台	仮想化管理サーバ
メールフィルタリングサーバ	1台	メールフィルタリングサーバ
所内イントラWebサーバ	1台	所内イントラWebサーバ
ハイパーコンバージド管理サーバ	2台	ハイパーコンバージド管理サーバ

3 導入機器一覧

(1) サーバ

ハードウェア関係

機器	台数	概要
仮想化基盤サーバ	1式	HCIクラスタ構成(複数台のノードで構成)
バックアップサーバ	1台	
無停電電源装置(UPS)	必要数	上記各サーバ用
サーバコンソール	1台	
KVMスイッチ	1台	上記各サーバ接続用
ハイパーコンバージド接続用スイッチ	必要数	HCI用

ソフトウェア関係

ソフトウェア	本数	インストール先等
Red Hat Enterprise Linux 9.0	3本	・ 公開WWW 1台 ・ Mail/内部DNSサーバ 1台 ・ メールフィルタリングサーバ 1台
Windows Server 2022 Datacenter	必要数	・ 仮想化クラスタノード台数分
Windows Server 2022 Standard	1本	・ バックアップサーバ
ハイパーバイザー	必要数	・ 仮想化クラスタノード台数分
ハイパーコンバージドソフトウェア	必要数	・ HCIクラスタ構成ノード台数分
バックアップソフトウェア	必要数	・ 全仮想サーバのバックアップを取得 ・ バックアップサーバのバックアップを取得
ネットワーク監視ソフトウェア	1本	・ ネットワーク監視サーバ
メールフィルタリングソフトウェア	1本	・ メールフィルタリングサーバ
ウイルス対策ソフトウェア	必要数	・ Windows系/Linux系サーバにインストール ・ 5年間分のライセンス
電源障害管理ソフトウェア	必要数	・ 仮想化クラスタノード台数分 ・ バックアップサーバ
資産管理ソフトウェア	1本	・ 資産管理サーバ 1台 ・ 監視対象クライアント 160台
Linux系OS (CentOS 後継製品)	1本	・ 所内イントラWebサーバ 1台

(2) ネットワーク機器

機器	個数	概要
ファイアウォール	2台	・ 冗長化構成
センタースイッチ	2台	・ スタック構成
サーバ用スイッチ	2台	・ スタック構成
フロアスイッチ	8台	・ 各フロア設置用
エッジスイッチ	60台	・ 各フロアのクライアント接続用

4 納入・設置場所

本研究so(所在地：大阪市城東区森之宮 1-6-50)における下記の場所に配置すること。

- (1) サーバ : 【研究棟】1階サーバ室
 (2) ネットワーク機器 : 【管理棟】1階事務室及び2階図書室
 【研究棟】1～6階指定箇所

※設置場所の詳細については後日指定することとする。

5 借入期間

2026年1月1日から2030年12月31日(60ヶ月)とする。

6 業務の概要

本業務は、本研究所端末・機器等賃貸借の内、調達機器の賃貸借、設定、設置及び保守を行うものであり、本業務に関わる必要な費用は全て本調達に含めるものとする。

業務内容は、以下の通り。

(ア) 機器などの賃貸借

サーバ、ネットワーク機器の賃貸借。

なお、借入れ物品その他すべての付属品は中古品であってはならない。

(イ) OS 及びソフトウェアのインストール及び設定、検証作業

OS 及びソフトウェアはライセンスの権利を行使したもので、本研究所に使用権があり適法に使用できること。

サーバについて、指定の OS 及びソフトウェアをインストールの上、検証を行うこと。既存のクライアント端末から本研究所業務用アプリケーションが正常に利用できること。

既存のクライアント端末からインターネット検索や外部との電子メール送受信が正常に行えること。

各種サーバ、及びネットワーク機器の設定に関しては、設計書を作成の上、事前に本研究所担当者と連絡調整、協議を行い、設定書に基づき設定作業を実施すること。詳細については本研究所側の意向を最大限適えるように努めること。

(ウ) セキュリティ設定、検証作業

システム全体を様々な脅威から保護するため、ファイアウォール、ネットワーク機器、サーバ等について、適切なセキュリティ設定を行うこと。

現在、本研究所内の各機器に定義されているセキュリティ設定（ファイアウォールルール、アクセスコントロールリスト、パスワード設定等）については、本調達に伴い、それぞれの必要性を本研究所と協議の上、移行又は適切な設定へ変更すること。

また、経済産業省「情報セキュリティサービス基準審査登録制度」に登録されているサービスを利用し、以下の脆弱性診断を行い、調査機関の報告書を提出すること。

1. UTM 装置

システム設定内容の監査を実施し、設定内容に問題がないことを確認すること。

外部に公開するグローバル IP アドレスに対し、脆弱性診断を実施すること。

2. Red Hat Enterprise Linux（公開 WWW サーバ、Mail/内部 DNS サーバ）

外部に公開するグローバル IP アドレスに対し、脆弱性診断を実施すること。

(エ) ネットワーク再構築作業

主として使用している VLAN の IP アドレス不足への対策を検討しネットワークの再構築を実施すること。（サブネットの拡張以外での対策を検討すること）

(オ) 設置作業

機器設置作業については、本研究所担当者と連絡調整のうえ、円滑に進めること。

物品の納入・運搬に係る費用は受託者の負担とすること。

(カ) 保守・技術サポート

システムが常に完全な機能を保つように、機器障害時に必要な部品や代替機等を用意し、対象ハードウェア、ソフトウェア等の保守作業を行うこと。

OS ソフトウェアの脆弱性、バージョンアップに関する情報等を主体的に提供すること。

また、起動・シャットダウン・操作・設定・機能などに関して調査、技術支援及びレクチャーを行うこと。また、これらに必要となるマニュアルの提供も行うこと。

(キ) 運用支援

サーバ・ネットワーク機器の設定変更、OS アップデート（脆弱性対応等により必要となるアップデートを含む）、セキュリティ対策、障害対応、各種調査、技術指導等の運用支援を、参考資料「所内情報システム運用支援業務委託仕様書」の通り実施できること。

当該運用支援については、本調達には含まず別途契約を行うものとし、受託者は本調達業務の構築業者（再委託先も含む）に限るものとする。

第2 機器等の仕様

1 共通事項

- (ア) 機器は、製品カタログ等に掲載されており、未使用のものであること。
- (イ) 数量が2以上のものについては、すべて同一機種(製品)であること。
- (ウ) 調達するソフトウェア等は全て問題なく動作可能なこと。
- (エ) OS 及びソフトウェアはライセンスの権利を行使したもので、本研究所に使用权があり適法に使用できること。
- (オ) 調達した機器の利用に伴って必要となる物品(接続部品、ケーブル等)については、本仕様書の記載の有無に関わらず提供すること。
- (カ) 大阪府グリーン調達方針に基づく、令和7年度の「判断基準」に適合したものであること。
(<https://www.pref.osaka.lg.jp/o120020/chikyukankyo/jigyotoppage/greenchotatsu.html>)

2 機器構成仕様

(1) 全体構成

調達機器等の構成は、【第1『概要』の3『導入機器一覧』】のとおり。

(2) 機器一覧表の作成

機器等の仕様適合を確認するため、仕様適合証明書の添付書類として、以下の資料を提出すること。

- ・ 導入機器等の数量が確認できるもの。
- ・ 搭載する CPU、メモリの性能及び数量が確認できるもの。
- ・ ネットワークインターフェースの種類及びポート数が確認できるもの。

3 仮想化基盤サーバ、ハイパーコンバージドサーバ 仕様

以下に示す条件を満たすサーバを納入すること。

(1) ハードウェア

(ア) 仮想化基盤サーバ

以下 仮想化基盤サーバ1台当たりのスペック

項目	内容
形状	ラックマウント可能でありかつ、1U以下であること。
CPU	Xeon Gold 5515+ プロセッサ(3.20GHz、8コア、22.5MB)同等品以上を2基以上搭載すること。
メモリ	256GB以上搭載すること。 又、メモリモジュールを最大32枚搭載可能であること。
OSブートモジュール	M.2 Flashモジュール 240GB以上をRAID1構成で2基搭載すること。 Drive Writes Per Day : 1.0以上とする。

ハードディスク	HDD+SSDのハイブリッドで構成し、SSDはキャッシュとして動作させること。HDD：9.6TB（SAS、10krpm以上）以上、SSD：1.9TB（Drive Writes Per Day：3以上）以上、SASコントローラカードを搭載すること。
光学ドライブ装置	DVDドライブを有すること。
ネットワークインターフェース	25GBASE ×2ポート以上有すること。（HCI用） 10GBASE-T ×4ポート以上有すること。（仮想化用） 1000BASE-T ×1ポート以上有すること。
電源ユニット	電源ユニットは冗長構成であること。 80PLUS® Platinum認証電源であること。 ホットプラグ対応電源であること。
外部インターフェース	外部接続可能なUSB3.0対応のインターフェースを標準で1ポート以上、ディスプレイ接続インターフェースを標準で1ポート以上、管理用LANポート（1000BASE-T）を標準で1ポート以上搭載していること。
無停電電源装置（UPS）	停電時にシステムが安全にシャットダウンを行うために必要なバックアップ時間を有すること。 停電時切り替え時間は10ms以下であること。 UPS管理ソフトをインストールし、停電時に安全にシステムがシャットダウンされるように設定すること。 ラックマウントが可能であること。 借入期間中にバッテリー寿命が尽きた場合のバッテリー交換に要する費用は本調達に含まれること。
監視機能	モジュールやコンポーネントの異常・故障を通知するLEDがあること。 又、電力監視、消費電力上限値設定が可能なこと。 リモート監視機能としてiRMCと同等機能を有すること。 OSの稼働状況に関わらず、サーバの各部品（CPU、メモリ、電源、HDD/RAID）が監視できること。 サーバ・OSの状態に関わらず、メール等による障害通知が可能であること。 遠隔地等からサーバの電源投入・切断・ハードリセット操作が行えること。
保守サポートパック	サーバ機器、無停電電源装置 5年間分の保守サポートパック ・ 当日訪問修理 平日8時30分～19時00分 又は、24時間対応

(イ) サーバコンソール、KVM スイッチ、ハイパーコンバージド接続用スイッチ

項目	内容
サーバコンソール	サーバ機器用のコンソールを1台納入すること。 ・ ラックマウント可能でありかつ、1U以下であること。 ・ 17 インチ以上の液晶ディスプレイを搭載していること。 ・ 日本語配列キーボード（OADG準拠）を搭載していること。 ・ ポインティングデバイスを搭載していること。 ・ サーバ機器本体と同一メーカーの製品であること。 ・ 5年間のオンサイト保守サポートを実施すること。
KVMスイッチ	サーバ機器用のKVMスイッチを1台納入すること。 ・ 仮想化基盤サーバ、バックアップサーバが接続出来ること。 ・ サーバ機器本体と同一メーカーの製品であること。 ・ 5年間のオンサイト保守サポートを実施すること。
ハイパーコンバージド接続用スイッチ	ハイパーコンバージドインフラストラクチャを構成するにあたり必要となるスイッチを必要台数納入すること。 ・ 5年間のオンサイト保守サポートを実施すること。

(2) ハイパーバイザー

- (ア) 仮想化ハイパーバイザーは、ノード障害発生時に自動的に仮想マシンを再起動する HA 機能を有していること。
- (イ) ライブマイグレーション機能を有していること。
- (ウ) ハイパーコンバージドインフラストラクチャに適した製品であること。
- (エ) ゲスト OS として、Windows 系、Linux 系の OS が搭載可能であること。
- (オ) 管理機能を有していること。
- (カ) 5 年間の使用権とソフトウェア保守サポートに加入すること。

(3) ハイパーコンバージド ソフトウェア

- (ア) ノードを跨いで冗長構成が可能なこと。
- (イ) ノード単位での増設が可能であり、CPU／メモリ／内蔵ストレージ単位の拡張も可能であること。
- (ウ) アプライアンスの形態ではなく、汎用的な x86 サーバとソフトウェアでストレージ機能を実装すること。
- (エ) 管理機能を有していること。
- (オ) 5 年間の使用権とソフトウェア保守サポートに加入すること。

4 バックアップサーバ 仕様

以下に示す条件を満たすサーバを納入すること。

(1) ハードウェア

項目	内容
形状	ラックマウント可能でありかつ、2U以下であること。
CPU	Xeon プロセッサ Silver 4509Y (2.60GHz、8コア、22.5MB) 同等品以上を搭載すること。
メモリ	32GB以上搭載すること。 又、メモリモジュールを最大24枚搭載可能であること。
RAIDカード	SASコントローラカードを搭載し、以下の機能を有すること。 データ転送速度：SAS 12Gbps RAID 0 / 1 / 5 / 10 をサポート
ハードディスク	OS用として、SSD：240GB (Drive Writes Per Day：1.5以上) 以上を2本以上搭載しRAID構成とすること。 バックアップ用として、HDD：4TB (7,200rpm以上) 以上を6本以上搭載しRAID構成とすること。
光学ドライブ装置	DVDドライブを有すること。
ネットワーク インターフェース	10GBASE-T ×2ポート以上有すること。 1000BASE-T ×1ポート以上有すること。
電源ユニット	電源ユニットは冗長構成であること。 80PLUS® Platinum認証電源であること。 ホットプラグ対応電源であること。
外部インターフェース	外部接続可能なUSB3.0対応のインターフェースを標準で3ポート以上、ディスプレイ接続インターフェースを標準で1ポート以上、管理用LANポート (1000BASE-T) を標準で1ポート以上搭載していること。

無停電電源装置 (UPS)	<p>停電時にシステムが安全にシャットダウンを行うために必要なバックアップ時間を有すること。</p> <p>停電時切り替え時間は10ms以下であること。</p> <p>UPS管理ソフトをインストールし、停電時に安全にシステムがシャットダウンされるように設定すること。</p> <p>ラックマウントが可能であること。</p> <p>借入期間中にバッテリー寿命が尽きた場合のバッテリー交換に要する費用は本調達に含まれること。</p>
監視機能	<p>モジュールやコンポーネントの異常・故障を通知するLEDがあること。</p> <p>又、電力監視、消費電力上限値設定が可能なこと。</p> <p>リモート監視機能としてiRMCと同等機能を有すること。</p> <p>OSの稼働状況に関わらず、サーバの各部品（CPU、メモリ、電源、HDD/RAID）が監視できること。</p> <p>サーバ・OSの状態に関わらず、メール等による障害通知が可能であること。</p> <p>遠隔地等からサーバの電源投入・切断・ハードリセット操作が行えること。</p>
バックアップ用HDD	<p>本サーバのバックアップデータを格納する外部接続用ハードディスク装置（NAS等）</p> <ul style="list-style-type: none"> ・電源内蔵の装置であること。 ・RAID構成であること。 ・使用可能容量が16TB以上であること。 ・無償保証期間が5年間以上の製品であること。
保守サポートパック	<p>サーバ機器、無停電電源装置 5年間分の保守サポートパック</p> <ul style="list-style-type: none"> ・当日訪問修理 平日8時30分～19時00分又は、24時間対応

（２） ソフトウェア

- （ア）OS に Windows Server 2022 Standard 相当以上をインストールすること。
- （イ）ウイルス対策ソフトとしてトレンドマイクロ製サーバ対応品をインストールすること。
- （ウ）既存の Active Directory からオブジェクトを移行し、既存ドメインのドメインコントローラとして構成すること。
- （エ）移行に伴い、既存クライアント端末で設定変更が必要な場合は、既存保守業者に依頼を行うこと、又、設定変更費用を本調達に含めるものとする。
- （オ）電源管理ソフトウェアをインストールし、電源障害時に自動でシャットダウンが可能であること。
- （カ）既存のプリントサーバ設定を移行すること。

（３） バックアップソフトウェア

以下の機能を有するバックアップソフトウェアを導入し、本調達のサーバ群よりバックアップを取得すること。また、バックアップサーバ自身のバックアップもバックアップ用 HDD に取得すること。

- （ア）仮想マシンをエージェントレスでバックアップする機能を有していること。
- （イ）仮想化クラスターノード単位でバックアップする機能を有していること。
- （ウ）重複排除バックアップ機能を有していること。
- （エ）復旧は、仮想マシン単位、および、ファイル単位で復旧が可能であること。
- （オ）5年間のソフトウェア保守サポート

5 公開 WWW サーバ 仕様

以下に示す条件を満たすサーバを仮想環境上に構築すること。

- (ア) OS に Red Hat Enterprise Linux 9.0 をインストールすること。
- (イ) ウイルス対策ソフトとしてトレンドマイクロ製サーバ対応品をインストールすること。
- (ウ) 公開 WWW サーバでは現行システムにおいて提供している下記のネットワークサービスを現行環境のサービスを維持しつつ構築すること。
 - 1) 公開 Web サーバ
 - 2) 外向け DNS
 - 3) メール中継 HUB
 - 4) 所内向け NTP サーバ
- (エ) DNS データの移行を行うこと。
- (オ) 経済産業省「情報セキュリティサービス基準審査登録制度」に登録されているサービスを利用し、脆弱性診断を行い、調査機関の報告書を提出すること。

6 Mail/内部 DNS サーバ 仕様

以下に示す条件を満たすサーバを仮想環境上に構築すること。

- (ア) OS に Red Hat Enterprise Linux 9.0 をインストールすること。
- (イ) ウイルス対策ソフトとしてトレンドマイクロ製サーバ対応品をインストールすること。
- (ウ) Mail サーバでは現行システムにおいて提供している下記のネットワークサービスを現行環境のサービスを維持しつつ構築すること。
 - 1) メール受信サーバ
 - 2) メール送信サーバ
 - 3) 所内向け DNS マスタサーバ
- (エ) 既存メールデータ・ユーザデータ・DNS データの移行を行うこと。
- (オ) 経済産業省「情報セキュリティサービス基準審査登録制度」に登録されているサービスを利用し、脆弱性診断を行い、調査機関の報告書を提出すること。

7 DC サーバ 仕様

以下に示す条件を満たすサーバを仮想環境上に構築すること。

- (ア) OS に Windows Server 2022 Standard 相当以上をインストールすること。
- (イ) ウイルス対策ソフトとしてトレンドマイクロ製サーバ対応品をインストールすること。
- (ウ) 既存の Active Directory からオブジェクトを移行し、既存ドメインのドメインコントローラとして構成すること。
- (エ) 既存のクライアント端末用トレンドマイクロ社製ウイルスバスターの管理サーバの移行を実施すること。
- (オ) 移行にあたっては、既存のクライアント端末に影響を与えないように既存保守業者と十分協議を行うこと。
- (カ) 既存クライアント端末で設定変更が必要な場合は、既存保守業者に依頼を行うこと、又、設定変更費用を本調達に含めるものとする。

8 ファイルサーバ 仕様

以下に示す条件を満たすサーバを仮想環境上に構築すること。

- (ア) OS に Windows Server 2022 Standard 相当以上をインストールすること。
- (イ) ウイルス対策ソフトとしてトレンドマイクロ製サーバ対応品をインストールすること。
- (ウ) 既存のファイルサーバからアクセス権を含めデータの移行を行うこと。

9 ネットワーク監視サーバ 仕様

以下に示す条件を満たすサーバを仮想環境上に構築すること。

(ア) OS に Windows Server 2022 Standard 相当以上をインストールすること。

(イ) ウイルス対策ソフトとしてトレンドマイクロ製サーバ対応品をインストールすること。

(ウ) 以下の機能を有するネットワーク監視ソフトウェアを導入すること。

1. 監視対象機器をグループで階層的に管理ができること。
2. 監視対象機器台数は 3000 台、5 年間の使用が可能なこと。
3. マルチベンダーに対応した製品であること。
4. すべての装置に対し、ping による ICMP パケットでの死活監視を定期的に行う機能を有すること。
5. SNMP による監視機能を有すること。
6. 外部システムとの連携用インターフェースとして REST API を搭載していること。
7. サーバのリソース監視（CPU、メモリー、ディスク）が可能であること。
8. 重要アラーム発生時は、パトランプを鳴動させる機能を有していること。
9. アラーム発生時、E-Mail によるエスカレーションが可能であること。
10. 計画停止時に装置の監視を止める機能を有すること。
11. 本調達で導入する全装置を含め既設機器（別途打合せ）を監視対象として設定すること。
12. 作成したレポートを HTML 形式、Excel 形式、PDF 形式のいずれかのファイルへ出力できること。
13. 5 年間の使用権とソフトウェア保守サポートに加入すること。
14. 監視対象機器は、「ファイアウォール」「センタースイッチ」「サーバスイッチ」「フロアスイッチ」「エッジスイッチ」「サーバ機器」とすること。

1 OWSUS サーバ 仕様

Windows Server Update Service サーバを仮想環境上に構築すること。

(ア) OS に Windows Server 2022 Standard 相当以上をインストールすること。

(イ) ウイルス対策ソフトとしてトレンドマイクロ製サーバ対応品をインストールすること。

1.1 資産管理サーバ 仕様

以下に示す条件を満たすサーバを仮想環境上に構築すること。

(ア) OS に Windows Server 2022 Standard 相当以上をインストールすること。

(イ) ウイルス対策ソフトとしてトレンドマイクロ製サーバ対応品をインストールすること。

(ウ) 既設資産管理サーバより管理データの移行を行うこと。

(エ) 以下の資産管理機能を有すること。

1. 各クライアントコンピュータに関する各種ハードウェア情報を、資産情報として自動的に収集できること。

メモリ増設等資産情報が変化した際には変更された資産内容を変更した期間や変更内容を限定して抽出することができること。

収集したハードウェアおよびソフトウェア情報を、一覧で表示できること。

クライアントコンピュータが通信している、本ソフトウェアのマスタサーバを一覧で確認できること。

資産情報の検索の際は、インベントリ情報や WindowsOS のバージョン、サービスパックなどから、同時に複数項目、複数キーワードおよび数値の範囲を指定して検索が可能であること。

検索の際には、本ソフトウェアから削除されたクライアントコンピュータも、検索対象として指定できること。

2. クライアントコンピュータ上のソフトウェアに関するインストール状況を収集する機能を有すること。収集できる内容としては、以下の通りとする。また、クライアントコンピュータごとにアプリケーション状況を把握できること。(収集対象：アプリケーションインストール状況・OS ライセンス状況・Office インストール状況・ウイルス対策ソフトウェアインストール状況・Windows 更新プログラム適用状況・Windows ストアアプリインストール状況・Office アプリケーション (MicrosoftOffice) の GUID、バージョン、インストール日付、不許可ファイル検出状況)
3. 収集した資産情報を検索できること。検索条件には、インベントリ情報や OS のバージョン、空き容量、死活監視状態など複数項目を指定した AND, OR, NOT 検索が可能で、キーワードを指定する際は、空白を挟むことで複数のキーワードを指定できること。
検索条件ごとに表示項目の順序・表示非表示を定義・保存でき、呼び出せること。
セグメント内で最後に電源を切るクライアントコンピュータに対して、セグメント内で電源が入っているプリンタなどネットワーク機器情報をポップアップで通知する機能を有すること。
4. 指定したクライアントコンピュータに対して、Windows 更新プログラムを配布し、自動的に更新プログラムの実行を行う等のセキュリティパッチを適用する機能を有すること。
配布した Windows 更新プログラムが適用されていないクライアントコンピュータを検出し、一覧化できること。
クライアントコンピュータ毎の更新プログラムの適用状況が管理コンソールで確認できること。
5. クライアントコンピュータに対して、Windows 更新プログラムを配布し、自動的に更新プログラムの実行を行う等のセキュリティパッチを適用する際、WSUS (Microsoft Windows Server Update Services) と連携し、更新日や更新時間を設定して適用できること。
電源 ON/OFF を制御できる環境下にある場合、適用時に、クライアントコンピュータの電源 ON/OFF が自動で行える設定ができること。
6. IP アドレスの管理台帳と、資産情報 (不許可端末検知情報も含む) を照合し、競合や不正使用、使用期限切れの表示を行えること。また表示方法は、一覧表示およびマップ表示を行えること。

(オ) 以下のログ管理機能を有すること。

1. クライアントコンピュータに対して行われた操作、ログオン・ログオフの日時、実行されたソフトウェアについての起動時刻・操作時間、ファイル操作、共有フォルダへのアクセス・ファイル操作、Web へのアクセス・書き込み・アップロード、クリップボード (テキスト・画像)、USB メモリなどの記憶媒体を利用した内容、記憶媒体のシリアル情報、接続した通信デバイス、および外部との通信状況等を記録する機能を有すること。
2. クライアントコンピュータからサーバ上の共有ファイルや、他のコンピュータからクライアントコンピュータ上に作成された共有フォルダへのアクセスおよびファイル操作 (作成、コピー、ファイル名変更、移動、上書き、削除) をログとして記録する機能を有すること。
3. 操作したファイルのフルパスを、フォルダオプション設定を変更することなく、ログとして表示すること。
4. 指定した範囲の IP アドレス以外に対する TCP 通信をログとして記録する機能を有すること。なお、http プロトコル以外の通信を行った場合、およびブラウザ以外のアプリケーションが外部と通信を行ったログも記録すること。
5. 指定した IP アドレス範囲内であっても、特定の IP アドレスについては記録対象から除外する設定が行えること。また、指定したデータ送受信量の閾値、ファイルおよびフォ

- ルダについても、記録対象から除外する設定が行えること。
6. クライアントコンピュータ上でクリップボードが利用された際に、クリップボードにコピーされたテキストや画像を記録する機能を有すること。
 7. 収集したクライアントコンピュータのログを管理画面で複数条件で検索できること。
 8. 検索条件はそれぞれ名前をつけて複数の条件を保存できること。
 9. 検索結果に対して、任意のログを選び、マーキングできること。
 10. 検索結果に表示されたクライアントコンピュータをグループ化し、検索グループとして登録できること。
 11. クライアントコンピュータの操作ログの検索を行う場合に、検索対象として複数のデータサーバが存在している場合でも、データサーバを一度にまとめて選択できる機能を有すること。なお、複数のバックアップログに対しても、現在のログと同様に検索が行えること。
 12. クライアントコンピュータから収集したログデータをバックアップし、またバックアップデータを管理コンソール上で閲覧できること。収集したログを一定期間ごとに自動でバックアップする機能を有すること。圧縮してバックアップした複数のログデータに対して、同時に検索できること。データサーバのハードウェアの障害等に備えてバックアップ後から障害発生までのログを保全するため、指定した期間は端末側でもログを保持し、データサーバへの再回収が行えること。端末側で保存するログデータは改変されないように難読化されていること。
 13. クライアントコンピュータから Web サイトにアクセスした内容を表示できるとともに、表示する集計期間や集計を除外する URL の設定も可能であること。また、クライアントコンピュータごとおよび部署ごとの表示においては、ネットワーク全体でのアクセスが少ない URL に対するアクセスを自動的に判定し、強調すること。表示できる内容は、次の通りとする。(グループ内のクライアントコンピュータごとの Web アクセス利用期間・各クライアントコンピュータの URL ごとのアクセス期間・選択したクライアントコンピュータの Web 閲覧状況・ネットワーク全体の Web アクセスランキング)

(カ) 以下のセキュリティ管理機能を有すること。

1. 収集したログに基づいて、事前定義されたルールに反した際に、その操作ログはアラートログとして、ログ閲覧画面および検索画面にて、アラート項目の優先順位に応じて 3 段階以上に色分けして表示できること。
2. 端末一覧画面では、発生している一番優先順位の高いアラート項目の色で、クライアントコンピュータを色付けして表示できること。
3. アラート優先順位を用いて、クライアントコンピュータやログを絞り込んで表示できること。
4. アラートの優先順位は、アラート項目ごとに設定できること。
5. アラート項目ごとにメールでの通知先の設定ができ、アラートの発生時には、設定された通知先にメールを自動送信できること。通知先の設定では、複数のメールアドレスをまとめたグループを使用することができること。
6. 端末の操作画面を管理端末で表示し、アラート発生端末の操作画面を拡大して強調することで、ネットワーク管理者の作業負担を軽減する機能を有すること。
7. 端末の操作画面を管理端末で表示する際に、アラート未発生端末の操作画面は非表示とする、プライバシー保護に配慮した機能を有すること。
8. アラート発生時における端末操作画面を、マウスカーソルの位置が強調された形式で表示し、不正操作及び誤操作発生時に早期の問題把握ができる機能を有すること。
9. 事前定義されたルールに反した際に、通知する機能、もしくは操作を禁止する機能について、設定したグループごと、クライアントコンピュータごとおよび利用者ごとに設定

できること。ルール の定義の際には、操作ログのログ種別を基準に、特定の曜日や時間帯、および特定時間内の操作回数などの複数条件を組み合わせて定義することもできること。

10. 端末に対して出力指令される音情報及びその回数を検出・解析することで、ゲームや動画等の業務外アプリケーションの使用判定を行う機能を有すること。
11. 指定したアプリケーションの起動中は、印刷やクリップボードへのコピー、Print Screen キー、アプリケーションによる画面キャプチャーなどの特定の操作を検知および禁止できること。指定したアプリケーションの起動中に印刷を禁止している場合も、指定したプリンタのみ印刷可能と設定できること。
12. 任意のアプリケーション実行について、ハッシュ値やバージョンリソースから実行ファイルを特定し、実行の検知および禁止できる機能を有すること。
13. 印刷操作した端末に対し、印刷物に付与されたコード（印刷物識別番号）によってのみ解除可能な操作制限を自動実行し、印刷物の取忘れ事故を防止する機能を有すること。
14. 本ソフトウェアの通信を行うため、Windows ファイアウォールの通信許可設定について、部署ごとに許可するプロファイルの範囲を指定できること。
15. クライアントコンピュータのネットワークカードごとのネットワークカテゴリ情報を、一覧で確認できること。

(キ) 以下のデバイス管理機能を有すること。

1. USB デバイスをクライアントコンピュータもしくは管理者のクライアントコンピュータに挿入した際、利用した USB デバイスのメーカー名、シリアルナンバー、ベンダ ID を自動で収集し、管理台帳を作成できること。利用者や所属部署、管理番号などを任意で入力できること。収集した情報をもとに、指定した USB デバイスまたは、ネットワーク全体及び指定した部署のみを使用許可/不許可を設定できること。
2. USB デバイスの管理台帳に登録されている USB メモリについて、その有無はシステムを利用して確認できること。USB メモリの有無は、各 USB メモリの利用者もしくは管理責任者が USB メモリをクライアントコンピュータに挿入することでその有無を一括管理でき、管理台帳に反映できること。棚卸を調査する期間は任意で設定でき、期間を超過しても棚卸が確認できていない USB メモリや利用者を表示できること。
3. USB メモリが端末に装着された日時を利用して、所定時間以上使用実績のない USB メモリを、紛失の可能性があるとして自動判定し、棚卸通知する機能を有すること。
4. USB メモリ等の端末への着脱日時と記録されたファイル情報とを利用して、外部漏洩の危険性があるファイルを自動判定する機能を有すること。
5. USB デバイスが端末に装着された日時とログオンユーザ名とを利用し、USB デバイスを現在所持している可能性が高いユーザを自動的に特定して表示する機能を有すること。
6. シリアル番号やベンダ ID、およびプロダクト ID が取得できず、個体識別が行えない USB デバイスについては、台帳への登録を制限できること。
7. USB デバイス内ファイルの日時情報を比較し、システム外で作成・編集された外部ファイルの持ち込みを自動判定し、その USB デバイスを使用禁止にする機能を有すること。

(ク) 以下のメンテナンス機能を有すること。

1. 特定のクライアントコンピュータに対して、ネットワーク経由で、リモート操作が行える機能を有すること。なお、管理機操作の際のログオンパスワードは、変更できること。
2. 管理機は、クライアントコンピュータ 1 台もしくは複数台の画面を静止画で同時に確認することができ、その静止画は順次更新できること。
3. 管理機から複数のクライアントコンピュータを同時に画面に表示させ、切り替えてリ

モート操作できること。

4. リモート操作されているクライアントコンピュータのデスクトップに、操作中であることを通知するポップアップを表示する設定ができること。
5. リモート操作を円滑に行うため、ミラードライバー設定が可能であること。
6. パスワード入力など、セキュリティの観点からクライアントコンピュータに表示したくない遠隔操作を行う場合は、クライアントコンピュータに対して操作画面を隠しながら遠隔操作を行えること。Windows8 以降でも可能であること。
7. 操作画面を隠しながらの遠隔操作中は、操作側の画面に隠しながら操作中である旨を通知すること。
8. リモート操作の範囲は、管理機が登録されているグループ内に限定されること。
9. リモート操作時に、通信帯域を制限できること。また、リモート操作で画面を受信する際、画質等を落として通信データ量を抑制できること。

1 2 仮想化管理サーバ 仕様

導入するハイパーバイザーの要件に合う仮想化管理サーバを構築すること。

1 3 メールフィルタリングサーバ 仕様

以下に示す条件を満たすスパム対策サーバを仮想環境上に構築すること。

(ア) OS に Red Hat Enterprise Linux 9.0 をインストールすること。(仮想アプライアンス製品でも可とする)

(イ) ウイルス対策ソフトとしてトレンドマイクロ製サーバ対応品をインストールすること。

(ウ) スпамメールの検出とブロックが可能なメールフィルタリングシステムであること。

(エ) 以下のフィルタリング機能を有すること。

1. ブラックリストでのメールチェック機能
2. メール本文の正規表現によるフィルタリング機能
3. DCC を参照し大量送信メールを検知する機能
4. 送信元アドレスの MX レコードを確認する機能
5. グレイリスティング機能

以下のメールなりすまし防止機能に対応していること。

1. SPF (Sender Policy Framework)
2. DKIM (DomainKeys Identified Mail)
3. DMARC (Domain-based Message Authentication, Reporting, and Conformance)
4. ARC (Authenticated Received Chain)

管理機能を有しユーザライセンスが不要であること。

管理機能は Web インターフェースでアクセス可能であり、「統計情報の表示」「設定確認・変更」「スパムパターンの学習」が可能であること。

1 4 所内イントラ Web サーバ 仕様

以下に示す条件を満たすサーバを仮想環境上に構築すること。

(ア) CentOS の後継 OS をインストールすること。

(イ) 既存サーバの Web コンテンツ及び設定を移行すること。(サーバ機器の設定変更が必要な場合は作業を行うこと)

(ウ) 設定変更内容は IP アドレスの変更、不要なサービスの停止等を行うこと。

(エ) 移行後の動作確認を行うこと。

1 5 ウイルス対策ソフト管理サーバ 仕様

以下に示す条件を満たすサーバを仮想環境上に構築すること。

- (ア) OS に Windows Server 2022 Standard 相当以上をインストールすること。
- (イ) ウイルス対策ソフトとしてトレンドマイクロ製サーバ対応品をインストールすること。
- (ウ) 既設ウイルス対策ソフトウェア管理サーバ（クライアント用）から管理機能を本サーバに移行すること。

16 ファイアウォール 仕様

以下に示す条件を満たすファイアウォールを2台納入し冗長化構成とすること。

以下1台あたりのスペック

- (ア) 19 インチラックにマウントが可能なこと。
- (イ) ファイアウォールのスループットは、20Gbps 以上の性能を有すること。
- (ウ) IPS のスループットは、2.6 Gbps 以上の性能を有すること。
- (エ) 設定画面が日本語対応していること。
- (オ) VPN 機能（IPSec, SSL）を有すること。
- (カ) NAT 機能を有すること。
- (キ) IEEE 802.1Q VLAN タギング機能を有すること。
- (ク) リンクアグリゲーション機能として、IEEE802.3ad 又はこれと同等の機能を有すること。
- (ケ) IPS 機能のシグネチャ定義ファイルを自動更新可能なこと。
- (コ) Syslog、SNMP、NTP または SNTP に対応すること。
- (サ) 10/100/1000BASE-T インターフェースを12ポート以上、WAN 用インターフェース（10/100/1000BASE-T）を2ポート以上、DMZ 用インターフェース（10/100/1000BASE-T）を1ポート以上、SFP インターフェースを4ポート以上有すること。
- (シ) センタースイッチと 10GBASE（LinkAggregation）、サーバスイッチと 1 GBASE（LinkAggregation）で接続すること。
- (ス) コンソール接続専用ポートを有すること。
- (セ) 高可用性（HA）構成が可能であること。
- (ソ) 5 年間のファイアウォール・保守ライセンスを含めること。
- (タ) 5 年間の先出しセンドバック対応を行うこと。（オプション製品含む）

17 センタースイッチ 仕様

以下に示す条件を満たすセンタースイッチを2台納入しスタック構成とすること。

1000BASE-SX のトランシーバを合計5個以上備え、フロアスイッチ5台と 1000BASE（光ケーブル）で接続を行うこと。

以下1台あたりのスペック

- (ア) 10/100/1000BASE-T ポートを24ポート以上有していること。
- (イ) SFP/SFP+ポートを8ポート以上（内 SFP28 ポートを4ポート以上）搭載していること。（オプション対応可）
- (ウ) サーバスイッチと 10GBASE（LinkAggregation）、ファイアウォールと 10GBASE（LinkAggregation）で接続すること。
- (エ) コンソール接続専用ポートを有すること。
- (オ) 400Gbps 以上のスイッチング容量を有すること。
- (カ) 300Mpps 以上のパケット転送能力を有すること。
- (キ) 32,000 個以上の MAC アドレスを自動学習可能であること。
- (ク) 25GB 以上でスタック接続を行うこと。
- (ケ) Jumbo Frame 転送が可能であること。

- (コ) ループ検知機能を有していること。
- (サ) 4094 個以上の VLAN が登録可能であること。
- (シ) ポートベース、802.1Q ベース、プロトコルベース、プライベートの VLAN をサポートしていること。
- (ス) IP アドレスの設定が可能なインターフェースを 192 以上有すること。
- (セ) IEEE802.3ad に準拠した LACP による LinkAggregation をサポートしていること。
- (ソ) IEEE802.1p に準拠した QoS 機能を有すること。
- (タ) IPv4 ルーティング・プロトコルとして、RIPv1/v2 をサポートすること。
- (チ) IPv6 ルーティング・プロトコルとして、RIPng をサポートすること。
- (ツ) DHCP リレー機能を有すること。
- (テ) IGMP Snooping v1, v2, v3 をサポートすること。
- (ト) MLD Snooping v1, v2 をサポートすること。
- (ナ) IEEE802.1x 認証機能を有すること。
- (ニ) MAC アドレスベースでの認証機能を有すること。
- (ヌ) Web ブラウザを使用した認証 (SSL 対応) 機能を有すること。
- (ネ) DHCP Snooping 機能を有すること。
- (ノ) SNMPv1, SNMPv2c, SNMPv3 エージェント機能を有すること。
- (ハ) Secure Shell (SSH) にてリモートログイン可能であること。
- (ヒ) ポートベース、リモート ミラーリング機能を有すること。
- (フ) LLDP をサポートしていること。
- (ヘ) sFlow をサポートしていること。
- (ホ) 機器のサイズは 1U 以内であること。
- (マ) 動作保障温度は 0~50℃以上をサポートすること。
- (ミ) 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。
- (ム) USB メモリ等の外部メディアが接続可能であること。
- (メ) 設定情報が格納された外部メディアから装置のブートが可能であること。
- (モ) 5 年間のオンサイト保守を行うこと。(平日 9 時~17 時、オプション製品含む)

18 サーバスイッチ 仕様

以下に示す条件を満たすセンタースイッチを 2 台納入しスタック構成とすること。

以下 1 台あたりのスペック

- (ア) 100BASE-TX/1000/10GBASE-T ポートを 20 ポート以上有していること。
- (イ) SFP/SFP+ポートを 4 ポート以上有していること。
- (ウ) センタースイッチと 10GBASE (LinkAggregation)、ファイアウォールと 10GBASE (LinkAggregation)、各サーバ機器と 10GBASE (チーミング) で接続すること。
- (エ) コンソール接続専用ポートを有すること。
- (オ) 480Gbps 以上のスイッチング容量を有すること。
- (カ) 350Mpps 以上のパケット転送能力を有すること。
- (キ) 32,000 個以上の MAC アドレスを自動学習可能であること。
- (ク) 10GB 以上でスタック接続を行うこと。
- (ケ) Jumbo Frame 転送が可能であること。
- (コ) ループ検知機能を有していること。
- (サ) 4094 個以上の VLAN が登録可能であること。
- (シ) ポートベース、802.1Q ベース、プロトコルベース、プライベートの VLAN をサポートしていること。
- (ス) IEEE802.3ad に準拠した LACP による LinkAggregation をサポートしていること。
- (セ) IEEE802.1p に準拠した QoS 機能を有すること。

- (ソ)IGMP Snooping v2, v3 をサポートすること。
- (タ)MLD Snooping v1, v2 をサポートすること。
- (チ)IEEE802.1x 認証機能を有すること。
- (ツ)MAC アドレスベースでの認証機能を有すること。
- (テ)Web ブラウザを使用した認証 (SSL 対応) 機能を有すること。
- (ト)DHCP Snooping 機能を有すること。
- (ナ)SNMPv1, SNMPv2c, SNMPv3 エージェント機能を有すること。
- (ニ)Secure Shell (SSH)にてリモートログイン可能であること。
- (ヌ)ポートベース、リモート ミラーリング機能を有すること。
- (ネ)LLDP をサポートしていること。
- (ノ)sFlow をサポートしていること。
- (ハ)機器のサイズは 1U 以内であること。
- (ヒ)動作保障温度は 0~50℃以上をサポートすること。
- (フ)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。
- (ヘ)USB メモリ等の外部メディアが接続可能であること。
- (ホ)設定情報が格納された外部メディアから装置のブートが可能であること。
- (マ)5 年間のオンサイト保守を行うこと。(平日 9 時~17 時、オプション製品含む)

19 フロアスイッチ 仕様

以下に示す条件を満たすフロアスイッチを 8 台納入すること。

但し、内 1 台は予備機とする。

フロアスイッチ 5 台に 1000BASE-SX のトランシーバ 1 個以上備え、センタースwitchと接続すること。

以下 1 台あたりのスペック

- (ア)10/100/1000BASE-T ポートを 24 ポート以上有していること。
- (イ)SFP ポートを 4 ポート以上搭載 10/100/1000BASE-T ポートと全ポート同時利用可能なこと。
- (ウ)56Gbps 以上のスイッチング容量を有すること。
- (エ)41.6Mpps 以上のパケット転送能力を有すること。
- (オ)16,000 個以上の MAC アドレスを自動学習可能であること。
- (カ)Jumbo Frame 転送が可能であること。
- (キ)ループ検知機能を有していること。
- (ク)4094 個以上の VLAN が登録可能であること。
- (ケ)ポートベース、802.1Q ベース、プロトコルベースの VLAN をサポートしていること。
- (コ)IEEE802.3ad に準拠した LACP による LinkAggregation をサポートしていること。
- (サ)IEEE802.1p に準拠した QoS 機能を有すること。
- (シ)IGMP Snooping v1, v2, v3 をサポートすること。
- (ス)MLD Snooping v1, v2 をサポートすること。
- (セ)IEEE802.1x 認証機能を有すること。
- (ソ)MAC アドレスベースでの認証機能を有すること。
- (タ)Web ブラウザを使用した認証 (SSL 対応) 機能を有すること。
- (チ)SNMPv1, SNMPv2c, SNMPv3 エージェント機能を有すること。
- (ツ)Secure Shell (SSH)にてリモートログイン可能であること。
- (テ)ポートベースミラーリング機能を有すること。
- (ト)LLDP をサポートしていること。
- (ナ)機器のサイズは 1U 以内であること。

- (ニ)動作保障温度は-5～50℃以上をサポートすること。
- (ヌ)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。
- (ネ)USB メモリ等の外部メディアが接続可能であること。
- (ノ)設定情報が格納された外部メディアから装置のブートが可能であること。
- (ハ)5 年間の先出しセンドバック対応を行うこと。(オプション製品含む)

20 エッジスイッチ 仕様

以下に示す条件を満たすエッジスイッチを 60 台納入すること。
但し、内 1 台は予備機とする。

- (ア)1000BASE-T/100BASE-TX/10BASE-T ポートを 8 ポート以上有すること。
- (イ)20Gbps 以上のスイッチング容量を有すること。
- (ウ)14.8Mpps 以上のパケット転送能力を有すること。
- (エ)ループ検知機能を有していること。
- (オ)ポートベース、802.1Q ベース、プロトコルベースの VLAN をサポートしていること。
- (カ)IEEE802.3ad に準拠した LACP による LinkAggregation をサポートしていること。
- (キ)SNMPv1, SNMPv2c, SNMPv3 エージェント機能を有すること。
- (ク)電源を内蔵していること。
- (ケ)金属製筐体であること。
- (コ)質量 1.6kg 程度以下であること。
- (サ)電源抜け防止対策がなされた製品であること。
- (シ)固定用マグネットを添付すること。
- (ス)5 年間無償保証の製品であること。

第3 設置・保守・サポート

1 機器の設置・納品

(1) 機器の設置・搬入支援

- (ア) 本業務の受託者は、本研究所と打ち合わせを行い、作業内容等について十分な調整を図り、作業計画書を作成し提出すること。作業の途中段階で計画の修正・見直しが必要となる場合は速やかに本研究所の担当者と協議すること。
- (イ) 搬入日の1週間程度前に本研究所と調整し、搬入すること。
- (ウ) 物品の納入・運搬に係る経費は受託者の負担とすること。
- (エ) アカウントは、必要なものを除いて削除すること。また、不要なサービス、プログラム等は停止・削除等を行い動作させないこと。
- (オ) 納品までの間に機器・OS及びソフトウェア等に不具合が生じた場合は、直ちに原因調査を行い、対応方法を協議した上で対処すること。
- (カ) コンセントの形状が設置済みのものと異なる場合は、機器に見合ったアダプタ等を用意すること。なお、アダプタ等の利用については、本研究所と調整を行うこと。
- (キ) 本調達機器の設置作業及びアップグレード作業等は、平日の9時から17時に行うことを原則とするが、本研究所の指示により休日（土曜日・日曜日及び国民の祝日に関する法律に規定する休日）に作業を行う場合もあることとする。
- (ク) 機器を梱包している箱等は、受託者が処分すること。また、本研究所が不要と判断する付属品、マニュアル等を撤去すること。
- (ケ) 本件借入れ品の全て（他社製のハードウェアやソフトウェアも含め）を対象とし、一つの窓口で対応すること。
- (コ) 設置した機器が、正常に動作することを確認すること。
- (サ) 機器の正常稼働に必要なOSやソフトウェア等のQ&A、技術支援について、確実に実施すること。
- (シ) 機器の構成、機器毎の設定やルール定義、OS及びアプリケーションの設定、仮想サーバの構成、ネットワーク全体図、アカウント等についての詳細設計書を作成し、文書及び電子媒体にて本研究所へ提出を行うとともに、内容について説明を行うこと。
- (ス) 機器の操作・設定について問い合わせることがある。問い合わせ内容及びその操作・設定方法の内容に応じて、口頭若しくは書面で応対すること。
- (セ) 機器の設定や組立に係る作業場所については、受託者側にて用意すること。ただし機器納入時の一時搬入場所や簡易な作業場所については、打合せの上、可能な範囲内は本研究所側で用意することとする。

(ソ)借入物品その他全ての付属品は中古品であってはならない。

(2) 借入期間満了時の取り扱い

(ア)納入機器の借入期間満了時には、対象機器の撤去を行うこと。また、ハードディスクのデータ内容を完全に消去し、その作業が完了した旨の証明書を発行すること。

(イ)本研究所が指定した機器・付属品・OS・ソフトウェアの買取に対応すること。買取を指定したものについては、撤去やデータ消去は不要とする。

2 保守案件

(1) 保守範囲

保守の範囲は、本業務により調達する機器及びOS・ソフトウェアであり、借入期間前に発生した障害・不具合等であっても保守の対象とすること。

(2) 保守概要

システムが常に完全な機能を保つように、機器の障害時に必要な部品や代替機等を用意し、対象ハードウェア、ソフトウェア等の保守作業を行うこと。

保守作業にあたっては、本研究所の運用支援業者との円滑な協力体制を実現すること。

なお、保守作業に関し、保守の範囲を超えるものを除き、本研究所に対して別途費用を請求することはできない。

(3) 保守の内容

以下の作業を受託者の責任において確実に実施すること。なお、下記に示す内容は必須条件であり、これ以外の内容についても本研究所業務に影響を与えないよう必要に応じて実施すること。

(ア)障害時の連絡対応、問診

障害切り分け作業、障害時のオンサイト対応、必要に応じた部品交換

ネットワークを含む不良部位の切り分けを行うとともに、ハードウェアの交換

(メモリ、ハードディスク等を含む)が必要な場合は、交換を行うこと。また必要に応じて、OS やソフトウェアの回復およびネットワークの疎通確認を行うこと。他のシステム構築関係業者側に障害が起因する場合には、必要に応じ当該業者への連絡を行うこと。

(4) 保守対応

サーバについては、5年間平日（土曜日・日曜日及び国民の祝日に関する法律に規定する休日以外の日。以下同じ。）9時から17時のオンサイト保守であること。

ネットワーク機器については予備機を用意するものについてはセンドバック修理、その他の機器は、5年間平日（土曜日・日曜日及び国民の祝日に関する法律に規定する休日以外の日。以下同じ。）9時から17時のオンサイト保守であること。

3 補足事項

(1) 機密保護

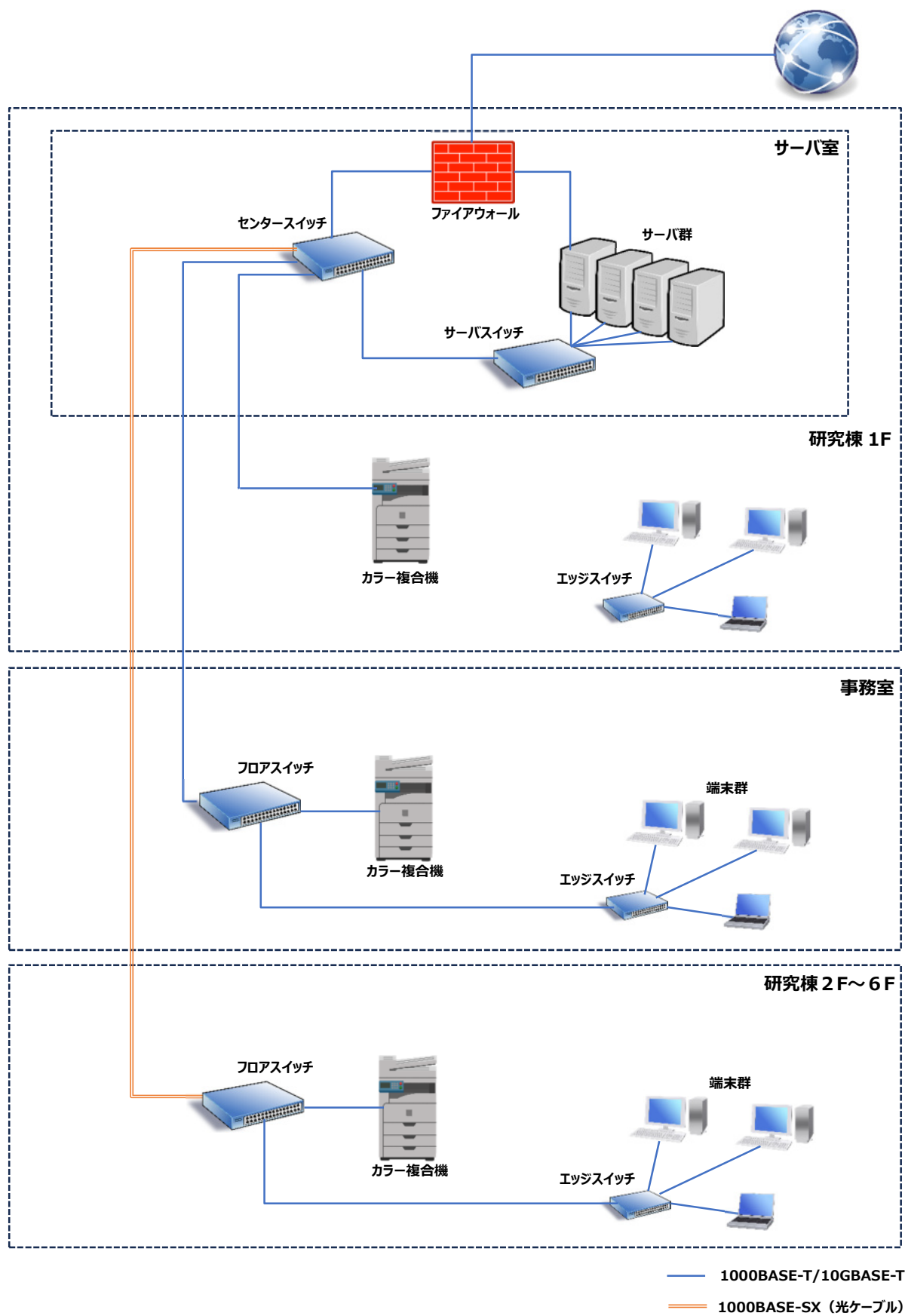
本契約内で得た情報に関して機密を保持すること。

(2) その他

(ア)本仕様書に疑義がある場合は、本研究所に質問しその指示を受けること。

(イ)契約後の本仕様書の解釈は本研究所側によるものとする。

(別紙 1)



(参考資料)

所内情報システム 運用支援業務委託仕様書

地方独立行政法人大阪産業技術研究所
森之宮センター

1. 委託名

所内情報システム運用支援業務委託

2. 委託期間

年度毎とする。

3. 作業時間

原則9時から17時30分までとする。ただし、年末年始（12月29日～1月3日）、土日、祝日を除く。

4. 委託対象

下記の（1）サーバ、（2）ネットワーク機器、（3）端末（PC）、プリンタ、およびネットワーク全体の設定運用を本委託対象とする。

5. 設置場所

- （1）サーバ : 大阪産業技術研究所森之宮センター内1階サーバ室
- （2）ネットワーク機器 : 大阪産業技術研究所森之宮センター内1階サーバ室、各階EPS及び1階事務室内ラック
- （3）端末（PC）、プリンタ : 大阪産業技術研究所森之宮センター内1階・2階事務室及び1階～6階研究室

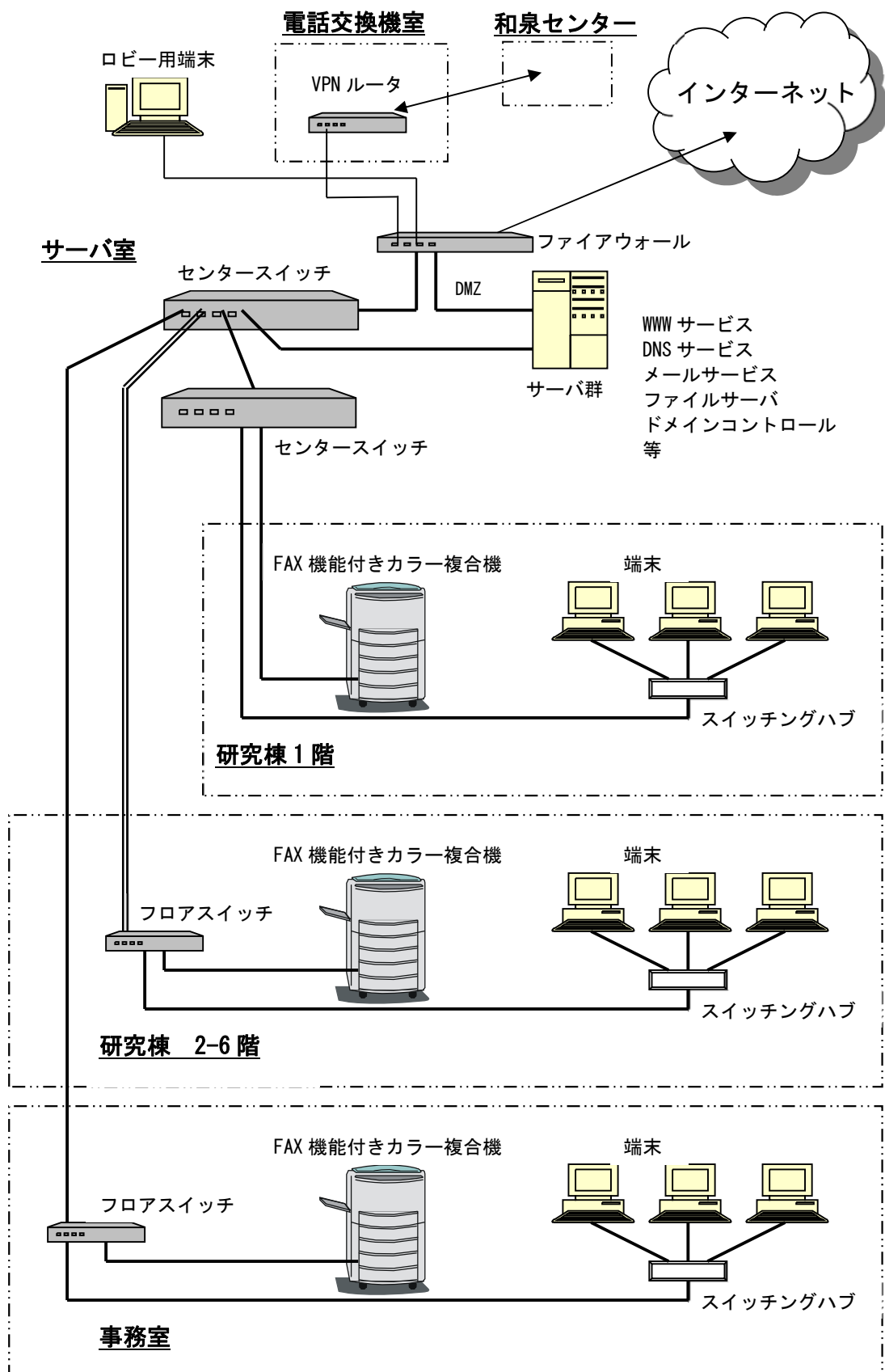
6. 情報資産保護、および秘密保持

本委託対象に係わる情報資産の保護及び、本契約内で得た情報に関して秘密保持ができること。

7. その他

- （1）本仕様書に疑義がある場合は、本研究所に質問しその指示を受けること。
- （2）契約後の本仕様書の解釈は本研究所側によるものとする。

(参考) 所内情報システム構成図



———光ケーブル 1000BASE-SX

———1000BASE-TX

運用支援委託内容

- 1. サーバ概要 -

1 機器一覧

名称	台数	概要
「所内情報システムサーバ及びネットワーク機器等賃貸借契約」における導入機器		

2 業務用サーバ群

2.1 公開WWWサーバ

○公開 WWW サーバでは下記のネットワークサービスを構築している。

- 1) 公開 Web サーバ
- 2) 外向け DNS
- 3) メール中継 HUB
- 4) 所内向け NTP サーバ
- 5) Web 訪問者集計

○公開 WWW サーバには別途外部委託による CMS（コンテンツマネジメントシステム）アプリケーションを導入しているが、本アプリケーションの運用に際して設定内容の変更等の必要事項が生じた場合については十分に協議の上、他に支障がなきようにサポートを行なうこと。

2.2 Mailサーバ

○Mail サーバでは下記のネットワークサービスを構築している。

- 1) メール受信サーバ
- 2) メール送信サーバ
- 3) 所内向け DNS マスタサーバ

2.3 ドメインコントローラサーバ

○ドメインコントローラサーバでは下記のネットワークサービスを構築している。

- 1) Active Directory サーバ
- 2) ネットワーク監視機能
- 3) ウイルス対策ソフトウェア管理サーバ
- 4) Windows Server Update Services
- 5) 所内向け DNS スレーブサーバ
- 6) DHCP サーバ

2.4 ファイルサーバ

○ファイルサーバでは下記のネットワークサービスを構築している。

- 1) 全所員向けファイルサーバ
- 2) 事務部門向けファイルサーバ

他の部門からは不可視にし、事務部門からはネットワークドライブとしてアクセスできるよう設定。

3 バックアップサーバ

○下記のサービスを構築している。

- 1) バックアップサーバ（バックアップ対象は業務用サーバ群）
- 2) Active Directory サーバ（スレーブ）
- 3) サーバ監視ソフトウェア
- 4) クライアント管理サーバ

- 2. ネットワーク機器概要 -

1 機器一覧

名称	台数	概要
「所内情報システムサーバ及びネットワーク機器等賃貸借契約」における導入機器		

- 3. 端末 (PC) 、プリンタ概要 -

1. 機器一覧

名称	台 数	概 要
デスクトップ型端末	130台	HP製 ProOne 440 G9 All-in-One Windows11 64bit
カラー複合機	6 台	OKI製 MC 863 d n w v
モノクロプリンタ	3 台	エプソン製 LP-S 3290Z
モノクロプリンタ	35台	京セラ製 P 2040 d w
ポスター印刷用 プリンタ	1 台	エプソン製 SC-P 8050

- 初期導入時の HDD のイメージをバックアップし、障害発生時等にはその HDD イメージを使用し復元できる。
- 各端末に本研究所が指示する名称 (マシン名) が付与されているので、ドメインコントローラサーバの管理のもとに Windows ドメインに参加しドメインユーザでログオン出来る。
- 各端末の IP アドレスは DHCP サーバから払い出しを受けるように設定済みである。
- 上記機器の更新が発生した場合の初期作業は含まない。

- 4. 委託内容 -

本委託対象機器であるサーバ、ネットワーク機器及び端末 (PC) 、プリンタに関して、下記の 1～13 の作業を行う。ただし、作業を行うときは、その内容を事前に本研究所と協議の上、作業を行うこととする。また、作業内容についての報告書を提出することとする。

1. 障害管理 (随時)

- 委託対象機器の稼動状況を管理すること。

2. 障害原因調査及び障害切り分け (随時)

- 委託対象機器の障害に関して、障害の発生部分を特定すること。(リモート又はオンサイトによる障害原因調査、障害切り分け等を行うこと。)

3. 障害復旧 (随時)

- 委託対象機器の障害に関して、電話、電子メール及びファクシミリによる質疑応答、メーカーや修理業者への連絡を行うこと。
- サーバに関して、リモートによるプログラムの修正及びバックアップデータからのデータの復旧を行うこと。
- サーバに関して、オンサイトによるプログラムの修正、OS やアプリケーションソフトの再インストール、システムの初期設定状態への復旧、バックアップデータからデータの復旧を行うこと。
- 端末 (PC) に関して、初期導入時の HDD イメージの復元作業を必要に応じて行うこと。

4. サーバ運用管理 (随時)

- サーバに関して、ハードディスク容量の確認、不要データの削除、データのバックアップ

を行うこと。

- サーバに関して、OS やアプリケーションソフトへのパッチの適用及びバージョンアップを行うこと。ただし、パッチの適用及びバージョンアップを行うときは、その内容について事前に本研究所と協議の上、システム運用に支障がないことを十分に確認できた後に行うこと。

5. 不正アクセスの監視及びセキュリティの改善（随時）

- 外部からの不正アクセスの監視及び発見を行うとともに、セキュリティの改善を行うこと。公知のセキュリティホールや最新のセキュリティ情報を調査するとともに、セキュリティの改善のための設定等を行うこと。ただし、設定変更等を行うときは、その内容を事前に本研究所と協議の上、着手すること。

6. 電子メールアカウントの管理について（必要に応じて）

- 本研究所の指示により、電子メールアカウントの登録、削除及び変更を行うこと。

7. ファイアウォールのルール設定について（必要に応じて）

- セキュリティ上の必要性に応じて、または本研究所の求める内容に応じ、ファイアウォールのルールを変更すること。ルールの変更については、本研究所との協議の上、着手すること。変更後は config ファイルの出力を保存すること。

8. アクティブディレクトリの管理について（必要に応じて）

- 所内の組織に合わせてセキュリティグループ・OU を作成しユーザを所属させている。本研究所の指示により、セキュリティグループ・OU の新設・変更およびユーザの登録・所属グループ変更等を行うこと。

9. 端末等の管理について（随時）

- 導入してあるクライアント管理サーバ用ソフトウェアにより、クライアント管理ソフトウェアを導入した端末を以下により管理すること。

(1) リモート管理機能

- ・リモート端末からクライアントの各種情報（コンピュータ名、IPアドレス、MACアドレス、OS名、電源状態、ログインユーザ名、ディスク使用量）を参照するよう設定してあるので、問題が生じた場合は正しく参照するよう運用すること。
- ・リモート端末からグループ指定または任意クライアント指定で、電源のON/OFF/再起動操作やユーザのログオン/ログオフ操作、メッセージ送信機能、また、タイマー機能を有する電源OFF/再起動を行える機能を有するが、この運用については本研究所の指示により行うこと。

(2) 資源配付機能

- ・即時、およびスケジューリングによるクライアントへのファイル配付機能を有し、複数の配付処理を連続実行させる機能を有するが、この運用については本研究所の指示により行うこと。

- ・任意のフォルダを配付用資源として登録することにより、当該フォルダで変更のあった差分ファイルのみを抽出し配付する機能を有するが、この運用については本研究所の指示により行うこと。

(3) ディスクイメージ取得／配信（クローニング）機能

- ・雛形パソコンからディスクイメージを取得し、取得したディスクイメージを複数クライアントに一斉配信（マルチキャスト配信）または特定クライアントに指定配信（ユニキャスト配信）する機能を有するが、この運用については本研究所の指示により行うこと。
- ・ディスク全体（プライマリ・セカンダリ）もしくは各ディスクのパーティション単位にディスクイメージを取得／配信する機能を有するが、この運用については本研究所の指示により行うこと。
- ・ディスクイメージ配信後あるいは任意のタイミングで、クライアント毎の個別設定情報（コンピュータ名、IPアドレス、ゲートウェイアドレス、DNSアドレス、OSのプロダクトID、ドメイン参加等）を自動設定する機能を有するが、この運用については本研究所の指示により行うこと。

(4) データ保全機能

- ・クライアントのローカルハードディスク上のユーザファイル保全のため、利用者がユーザファイルを変更（作成保存／更新／削除）すると同時に、ローカルハードディスク上の隠し領域に変更前のファイルを自動で取得する機能を有するが、この運用については本研究所の指示により行うこと。
 - ・同じくユーザファイルをスケジュール指定（曜日、日時など）によりサーバに自動取得（複製）する機能を有するが、この運用については本研究所の指示により行うこと。
- 各端末の設定を一元管理できるよう、グループポリシーの運用を行うこと。また、本研究所の指示により、随時新規ポリシーの作成や変更を行うこと。
- WSUS サーバ(Microsoft Windows Server Update Services)により Windows Update が行われるように運用すること。
- Windows11 の機能アップデート時における WSUS サーバ、アクティブディレクトリ等の設定を行うこと。
- 各端末に導入されるウイルス対策ソフトウェアはウイルス対策ソフトウェア管理サーバで統合管理されるよう運用すること。
- Adobe Acrobat Reader 等について、常に最新バージョンが利用できるように設定を行うこと。
- 端末それぞれについて本研究所が指定するプリンタに対して印刷が行えるように、設定を行うこと。
- その他、端末等の管理及びその設定に当たっては本研究所と協議の上行うこと。また、必要に応じて端末導入業者と協議を行うこと。

10. ネットワーク（必要に応じて）

- Fortigate 社製 Fortigate60D を介してのコンピュータ室からの接続、およびポリコム社製テレビ会議システムの接続に対応したネットワークシステムの運用を行うこと。
- ネットワーク構成についてアドバイスをを行うこと。新規機器の導入に際しては、ネットワ

ーク接続を支援すること。

1 1. 質疑応答（随時）

○OS やソフトウェア、機器の起動・シャットダウン・操作・設定方法、システム・ネットワークに関する質疑応答や、改善提案、最新の技術情報の提供を随時行うこと。

1 2. ドキュメント管理（随時）

○サーバ等に関して、各種の設定変更にもなうドキュメントの差分の更新及び管理を行うこと。

1 3. 定期訪問及び作業報告（1 回/月）

○稼働状況・障害内容や各種作業等の本委託に関する作業内容を報告すること。

1 4. その他

○本委託の実施に必要なソフトウェアの費用は、本研究所が負担する。

○本委託の実施に必要なフリーソフトウェアについては、受託者が用意し、委託内容に基づく作業を行うこととする。