

情報基盤システムおよび 運用支援業務 一式

仕様書

令和5年3月

目次

1	調達件名	6
2	目的	6
3	調達範囲	6
4	成果物	7
5	納品及び本調達の期間等	8
6	要求要件	8
7	留意事項	8
7.1	導入に関する留意事項	8
7.2	落札方式	9
7.3	著作権の帰属	9
7.4	本調達の更新(令和 11 年度以降)に関する留意事項	9
7.5	その他	10
8	提案書記載事項	10
8.1	提案書の作成	10
8.2	提案書記載項目	11
9	受注要件	12
9.1	実績に関する事項	12
9.2	実施体制及び要員に関する事項	12
9.3	品質管理能力に関する事項	13
9.4	個人情報保護及び情報セキュリティに関する事項	13
10	検査及び検収	13
11	賠償・復旧	13
12	情報セキュリティに関する遵守事項	13
12.1	機密情報	13
12.2	秘密保持	14
12.3	秘密情報の返却	15
12.4	損害賠償	15
12.5	本システムに格納されている情報の返却	15
13	外部委託等における情報セキュリティ上のサプライチェーン・リスク対応	15
13.1	外部委託	15
13.2	機器等の調達	16
14	システム方式要件	16
14.1	システム全体構成要件	16
14.2	信頼性要件	17
14.3	拡張性要件	17
15	システムセキュリティ要件	18
15.1	基本的な考え方	18
15.2	システムセキュリティ要件	18

16	機能要件	19
16.1	本部	19
16.1.1	外部接続L3 スイッチ	21
16.1.2	回線負荷分散装置	22
16.1.3	共通基盤 L2 スイッチ	23
16.1.4	共通基盤ファイアウォール	24
16.1.5	共通基盤 DMZ L2 スイッチ	25
16.1.6	共通基盤 DMZ 負荷分散装置	26
16.1.7	研究系 DMZ L2 スイッチ	27
16.1.8	基幹L3 スイッチ	28
16.1.9	事務 L3 スイッチ	29
16.1.10	事務負荷分散装置	30
16.1.11	事務クライアント L3 スイッチ	31
16.1.12	キャンパスネット L3 スイッチ	32
16.1.13	運用管理 L2 スイッチ	33
16.1.14	研究系内部 L2 スイッチ	34
16.1.15	本部 L2 エッジスイッチ	35
16.1.16	本部集約スイッチ	37
16.1.17	VPN 装置	38
16.1.18	本部用サーバ仮想化基盤	39
16.1.19	広報用 Web サーバ	42
16.1.20	外部DNSサーバ	43
16.1.21	SSO サーバ	44
16.1.22	学術認証連携 サーバ	46
16.1.23	グループウェアサーバ	47
16.1.24	教職員用メールサーバ	51
16.1.25	内部DNS プロキシサーバ	51
16.1.26	メールー斉送信・駅すぱあとサーバ	52
16.1.27	統合ID 管理サーバ	53
16.1.28	認証用LDAP サーバ	54
16.1.29	メタディレクトリLDAPサーバ	56
16.1.30	事務用ドメインコントローラサーバ	57
16.1.31	事務用クライアント管理サーバ	58
16.1.32	本部用共有ファイルサーバ	59
16.1.33	バックアップサーバ	61
16.1.34	ログ管理・監視サーバ	63
16.1.35	事務用 PC	64
16.1.36	ネットワークプリンタ(カラー)	65

16.1.37	外付けDVDドライブ.....	66
16.1.38	教員用メール・プロキシ・DNS(LSV)サーバ.....	67
16.1.39	検証用サーバ.....	67
16.1.40	情報公開用サーバ.....	68
16.1.41	西研究棟・東制作棟等ネットワーク基幹 L3 スイッチ.....	69
16.1.42	西研究棟・東制作棟等ネットワークフロア L2 スイッチ.....	70
16.1.43	西研究棟・東制作棟等ネットワークアクセススイッチ.....	71
16.1.44	インターネットVPN用ファイアウォール.....	72
16.1.45	SINET接続用外部L2スイッチ.....	73
16.1.46	RADIUS認証サーバ.....	74
16.2	学習センター及びサテライトスペース.....	76
16.2.1	学習センターファイアウォール.....	77
16.2.2	学習センタースイッチング HUB.....	78
16.2.3	無線LAN 用アクセスポイント.....	78
16.2.4	事務用 PC.....	79
16.2.5	学生用プリンタ(モノクロ).....	80
16.2.6	文京学習センター用 L2 スイッチ.....	81
16.3	ASP サービス.....	83
16.3.1	標的型攻撃メール対策兼スパム対策サービス.....	83
16.3.2	URLフィルタリングサービス.....	84
16.3.3	Web 会議システム.....	84
16.3.4	ASP メールサービス.....	86
16.3.5	ASP ファイルサービス.....	87
17	作業要件.....	88
17.1	システム構築.....	88
17.2	データ移行.....	90
17.3	テスト.....	91
17.4	運用環境.....	93
18	保守要件.....	96
18.1	ハードウェア製品保守.....	96
18.2	ソフトウェア製品保守.....	96
19	業務要件.....	97
19.1	システム運用支援業務全般.....	97
19.2	情報基盤システム.....	101
19.2.1	本部設置機器.....	103
19.2.2	学習センター及びサテライトスペース.....	109
19.2.3	ASP サービス.....	111
表1	PC 導入台数一覧.....	113

表2	PC 以外導入台数一覧.....	116
表3	事務用ソフトウェア一覧.....	119
表4	学習センター等所在地一覧.....	120
表5	運用支援業務対象機器一覧.....	124

1 調達件名

「情報基盤システムおよび運用支援業務 一式」

2 目的

放送大学学園(以下「本学園」という。)では、本部、全国 50 箇所の学習センター、及び 7 箇所のサテライトスペースにおいて、学習相談・研究指導などによる遠隔教育を行うこと及び、事務連絡の効率化・迅速化を図ることを目的としたネットワーク基盤として、情報基盤システムを構築している。

現在の情報基盤システムについては、令和 6年 3 月末を持って賃貸借の期限を迎える。今回、近年高度化する情報処理技術を利用し、現状における機器の処理能力不足やセキュリティレベルの向上等の諸問題を解決するため、システム更新を実施するものである。

あわせて、システム運用期間中のシステム運用支援業務の調達も実施する。

3 調達範囲

本調達の範囲は以下のとおりとし、中古品は不可とする。

(1) ハードウェア

本調達の要求要件を満たすハードウェアを調達し、ハードウェアに関する基本設計及び詳細設計を実施すること。基本設計及び詳細設計に基づき、ハードウェアの設定・導入を実施すること。

(2) ソフトウェア

本調達の要求要件を満たすソフトウェア(ASP サービスを含む)を調達し、ソフトウェアに関する基本設計及び詳細設計を実施すること。基本設計及び詳細設計に基づき、ソフトウェアの設定・導入を実施すること。

(3) テスト

導入機器についてシステム結合テスト、システム総合テストを実施すること。各テストにおいては、それぞれテスト計画書、テスト仕様書を作成し、本学園の承認を得ること。また、テスト実施後に、テスト結果報告書を作成し、本学園へ報告すること。

本学園が主体となって受入れテストを実施する。受託者はテスト計画及びテスト仕様の策定、テストの実施に関して本学園を支援すること。

(4) 導入教育

本システムの利用者や管理者に対して、教育訓練を実施すること。実施場所は原則利用者や管理者がいる現地(本部及び各学習センター)で各 1 回実施することとし、教育内容の詳細については、本学園と協議の上決定することとする。

(5) 本番移行・支援

本システムを稼働させるにあたり、次の作業を行うこと。

- 移行計画を策定すること。
- 本番稼働後の支援を行うこと。

- 本番稼働前にセキュリティ脆弱性試験を実施すること。
- 障害発生時には、本学園からの依頼により、対処を実施すること。

(6) システム運用設計

本調達の要求要件を満たすよう本システムに関する運用設計を行い、設計に基づき運用に関する仕組みを構築すること。また、運用に関するドキュメントを整備し、運用支援業務要員に引継ぎを行うこと。

(7) システム運用保守

本仕様書の各要件のとおり、運用業務を行なうこと。本学園の利用者からの問合せや障害発生時の原因切分け、障害復旧などを行い、問題の解決に当たること。定常的なバックアップ等も行なうこと。

報告資料を作成の上、毎月 1 回定例会を開催し、本学園に報告を行うこと。

(8) システム基盤監視

本仕様書の各要件のとおり、稼働状況、資源の利用状況、問題の発生などについて監視を行なうこと。機器の目視確認など必要な定常作業も行なうこと。また、監視対象機器に問題が発生した場合には障害復旧作業を行うこと。

(9) 機器撤去・データ消去

本システムがリース期間の満了を迎える際は、リース機器の撤去を行なうこと。リース機器の撤去費用は本調達に含めること。また、サーバ及び事務用 PC のハードディスク装置に対しては、データ消去等の処置を以下のとおり実施すること。

- ① 機器搬出途中での情報漏えいを防ぐために、撤去前に本学園担当職員立会いの上、各拠点内で本部、全国 50 箇所の学習センター及び 7 箇所のサテライトスペースを対象に全てのハードディスク内のデータを消去すること。
- ② ソフト的に実施する際には、フォーマットするだけでなく、専用ソフト等利用して完全にデータ消去すること。データを完全消去した報告書を提出すること。

4 成果物

本調達の納品成果物は以下のとおりとする。なお、(3)～(8)については、電子媒体(CD 等)でも1部納品すること。なお、電子媒体で提出する成果物については、市販のワープロソフト等のエディタで編集可能なファイル形式とすること。

- (1) ハードウェア 一式
- (2) ソフトウェア 一式
- (3) システム基本設計書 2 部
- (4) システム詳細設計書 2 部
- (5) システム運用設計書 2 部
- (6) システムテスト結果報告書 2 部

- (7) システム利用者向けマニュアル(教職員向け) 2 部
- (8) システム利用者向けマニュアル(学生向け) 50 部
- (9) システム保守運用者向けマニュアル 2 部
- (10) 定例会議資料
- (11) 「令和11年度情報基盤システム 一式」受託者向け引継ぎ書一式

5 納品及び本調達の期間等

- (1) 納入期限 令和 6 年 3 月 29 日
- (2) 履行期間 令和 6 年 4 月 1 日～令和 11 年 3 月 31 日
- (3) 納入場所、履行場所 本学園の指定する場所

6 要求要件

- (1) 本調達に係る性能・機能及び技術等(以下「性能等」という。)の要求要件は以下に示すとおりである。
 - ① 「16 機能要件」に記載のある要件を満たす機器及び業務要件を満足すること。
 - ② 「17 作業要件」に記載のある要件を満たす機器及び業務要件を満足すること。
- (2) 本仕様書が要求する要件は全て必須の要求要件である。
- (3) 必須の要求要件は本学園が必要とする最低要件を示しており、提案内容の性能等がこれらを満たしていないと判定された場合には、不合格となり、落札決定の対象から除外する。
- (4) 提案内容の性能等が技術的要件を満たしているか否かの判定は、本学園が設置する技術審査委員会において、提案システムに係る技術仕様書を含む入札説明書で求める提出資料の内容を審査して行う。
- (5) 入札仕様等の不知又は不明を理由として異議を申し立てることはできない。

7 留意事項

7.1 導入に関する留意事項

- (1) 導入・運用スケジュール等に関しては、本学園と協議し、その指示に従うこと。
- (2) 本仕様書に基づく作業を実施するにあたり、本学園経由あるいは同席の上で、既存システムの構築保守業者及び運用支援業者との協議等が必要な場合は、別途本学園と協議の上、その指示に従うこと。なお、協議に係る費用が発生する場合は、全て受託者が負担すること。
- (3) 本仕様書に基づくシステム構築作業のために必要となる機器等(開発・テスト環境のハードウェア、ソフトウェア及びネットワーク機器等を含む)及び消耗品等については、全て受託者が負担すること。
- (4) 本システムの構築に際し、他システムとの連携機能について問題なく稼動することを確認すること。なお、連携機能において問題が発生した場合には、該当システムの導入業者と協力し、対応を実施すること。本調達範囲のハードウェア及び基本ソフトウェア、ミドルウェアを含む全ての構成機器に対して稼動責任を負うこと。

- (5) 運用支援業務に関わるソフトウェアのパッチ適用に関しては、本学園と協議の上対応すること。
- (6) 本仕様書に基づく運用支援業務を実施するにあたり、本学園経由あるいは同席の上で、令和 6年 3 月末までに令和 5年度情報基盤システム運用支援業務受託者、情報基盤システム構築業者、クラウドシステム連携用サーバの構築業者から引継ぎを受けること。さらに協議等が必要な場合は、別途本学園と協議の上、その指示に従うこと。なお、引継ぎを受ける際に費用が発生する場合は、全て受託者が負担すること。
- (7) 本業務開始後に必要となる消耗品は本調達の範囲外とする。

7.2 落札方式

本調達は、総合評価落札方式にて行う。

7.3 著作権の帰属

受託者は、賃貸借する機器及びソフトウェア等を除く、システム設計書、マニュアル等納品物に係る著作権を対価の支払時点で本学園に無償で引き渡すものとする。ただし、受託者が本件特定役務の履行以前から有していたか又は汎用性のある著作物(他のソフトウェア等の著作物に共通に利用し得る汎用的なルーチン、モジュール、フォーマット等のコンポーネント著作物)(以下「受託者著作物」という。)に関する著作権は、受託者に留保される。ただし本件特定役務の履行のために作成した汎用性のある著作物についての著作権の扱いについては本学園と協議の上で決定するものとする。

本学園は、受託者著作物を本システムの開発、運用のために必要な範囲で使用できるが、受託者著作物に使用許諾条件が定められている場合は、その条件に従う。

また、第三者が著作権を有する著作物(以下「第三者著作物」という。)に関する著作権も、当該第三者に留保され、第三者著作物に使用許諾条件が定められている場合は、その条件に従う。

なお、受託者は本学園に著作権が帰属する納品物においても、本学園の承諾を得て、本件特定役務以外の目的に利用することができる。

7.4 本調達の更新(令和 11 年度以降)に関する留意事項

令和 11 年度以降、本調達内の全てについて更新を予定している。本調達の受託者は、次期情報基盤システム受託契約予定者に対し、本調達に関する情報提供等について誠意を持って対応すること。

特に運用支援業務に関しては、引継ぎをスムーズに行えるよう、以下の(1)~(5)の対応をすること。

- (1) 運用マニュアル、手順書等システム運用に関するドキュメントを令和 10 年 9 月 29 日までに本学園へ引き渡すこと。
- (2) 本学園が次期情報基盤運用に必要なと思われる情報に関して、随時本学園へ引き渡すこと。
- (3) 本調達期間を超えて行われる業務については、令和 11 年 3 月 31 日までに対応完了すべき業務と4 月 1 日以降に対応すべき業務を切り分け、次期情報基盤システム受託者に引継ぎを行うこと。
- (4) 受託期間における作業依頼・障害インシデント対応履歴、利用統計データを令和 11 年4 月 8 日までに本学園へ引き渡すこと。

- (5) 引継ぎ終了に際して不備があった場合、また引継ぎ後において受託者の責により運用支援業務に支障が生じる場合は、令和 11 年 4 月以降も随時対応すること。

7.5 その他

本調達仕様書に記載されていない事項又は仕様について疑義が生じた場合は、本学園、受託者双方が協議して決定するものとする。

8 提案書記載事項

応札者は、以下に示す事項を含む提案書を作成すること。

8.1 提案書の作成

(1) 全般事項

- ① 提案書の印刷用紙は A4 判縦置き又は横置きとする。ただし、図表等については A3 判も可とする。参考情報として添付する製品カタログがある場合にはこの限りではない。
- ② 提案書本文は日本語で記載し、10.5 ポイント程度の文字サイズとすること。また、分かりやすい構成を心がけ、目次及びページ番号を付与すること。
- ③ 提案書の提出部数は、印刷 1部とする。また、電子媒体(CD 等)で 1 式提出すること。なお、電子媒体で提出する提案書については、これをもとに審査資料を作成するため、市販のワープロソフト等のエディタで編集可能なファイル形式とすること。

(2) 留意事項

- ① 提案に際しては、提案するシステムが本仕様書の要求要件をどのように満たすのか、あるいはどのようにして実現するのかを要求要件毎に具体的かつ分かり易く、資料等を添付する等して説明すること。単に、「可能です」、「要求を満たします」等の表現ではなく、「可能にするための方法とその根拠」、「要求を満たす為の方法とその根拠」も具体的に明示すること。なお、提案の根拠が不明確の場合又は説明不十分で審査に重大な支障があると技術審査委員会が判断した場合は、要求要件を満たしていないものとする。
- ② 提案された内容等について、問合せやヒアリングを行うことがあるので、照会先を明記すること。
- ③ 提案を審査するものが特段の専門知識を持たなくとも評価が可能な提案書とすること。特に専門用語等を使用する必要がある場合には、注釈等による用語解説を付すこと。
- ④ 特定の製品を採用する場合は、当該製品を採用する理由を提案書本文中に記載するとともに、記載内容を証明する製品カタログ、製品紹介資料、製造者・販売者による機能証明等を添付すること。また、記載部分が分かり易いようにマーキングや見出しを付けること。
- ⑤ 提案書に不備があると判断した場合には、審査を行わないことがある。また、提案者による差し替えや再提出は認めない。
- ⑥ 入札金額、参考価格等は日本国通貨にて表示すること。参考価格は本体金額と保守金額を分けて提示すること。

- ⑦ 資格要件箇所については提案時に資格を証明することができる書類の写しを添付すること。

8.2 提案書記載項目

(1) 基礎事項

① 提案者の名称、所在地、代表者氏名等

提案者の名称、所在地、代表者氏名等を記載すること。なお、提案書に対する照会先(所属、連絡担当者、電話番号、FAX 番号、電子メールアドレス)を明記すること。

② 受託者の条件

「9.受注要件」に示す実績、実施体制及び要員、品質管理能力、個人情報保護及び情報セキュリティ等について記載すること。

(2) 基本方針

本仕様書の内容が理解できており、具体的かつ妥当性のある提案であることを評価するため、提案するシステムの基本方針及び概要について記載すること。

(3) 機能の実現について

「14 システム方式要件」「15 システムセキュリティ要件」「16. 機能要件」で求めている機能の実現方法について、下記内容に基づき具体的に記載すること。

① 提案するシステム構成を示すこと。その際、機器の構成及びシステム構成についてその妥当性や根拠について具体的に説明を記載すること。

② 具体的な移行方法(スケジュールや方式、利用者への影響、等)について記載すること。

(4) その他要件について

以下に示す事項について実現方法を記載すること。

① 「17 作業要件」に示される各要件に対して、具体的な実現方法を記載すること。

② 「18.1 ハードウェア製品保守」「18.2 ソフトウェア製品保守」に示される各要件に対して、保守内容、体制について具体的な実現方法を記載すること。

(5) 作業方針

本件の内容及び本システムの仕様内容を十分に理解し、提案者が本業務の遂行に当たっての作業方針を示すこと。想定する作業項目、手法について簡潔に記載すること。なお、システム構築作業のために必要となる機器等(開発・テスト環境のハードウェア、ソフトウェア及びネットワーク機器等を含む)及び消耗品等については、全て受託者が負担すること。

① 工程

想定する作業の全体工程について記述すること。なお、提案書に記載している項目との対応をつけて作成すること。

② 体制

下記に示す実行体制について記載すること。なお、主要な作業者については、実行体制上の役割を

明記した名簿を作成し、作業者毎の実績、主な保有資格を記載すること。また、作業中に変更が生じたときは、速やかに訂正版を提出すること。

- 業務実施体制図(責任者や作業者の役割を記載したもの)
- 作業要員一覧表(作業者の職名、氏名、所属、連絡先等を記載したもの)
- 作業スケジュール(詳細な作業項目を記載し、作業の進捗が確認できるもの)

なお、本業務に携わるプロジェクトマネージャが、過去 5 年以内に全国に 50 箇所以上の拠点を持つ組織で稼動するシステムの構築経験を有していると認められる場合には加点として評価する。

③ プロジェクト管理

確実かつ高品質な作業を遂行するために、適用するプロジェクト管理手法について具体的に示すこと。

④ 品質確保

品質確保に関する取組みについて記載すること。

⑤ 環境への配慮

省電力、グリーン購入等環境に配慮した製品を極力選定することとし、対応状況について記載すること。

9 受注要件

9.1 実績に関する事項

- (1) 公共機関(国、地方公共団体、国立大学法人等)、公共機関での実績がない場合は民間企業において、過去 5 年間に全国 30 以上の都道府県に拠点を有し、その拠点間をネットワークで結んだシステム基盤構築業務の実績を有し、これを証明すること。全国各都道府県に拠点を有する実績を有している場合は加点として評価する。
- (2) 公共機関(国、地方公共団体、国立大学法人等)、公共機関での実績がない場合は民間企業において、過去 5 年間にクライアント台数 1,000 台以上のネットワークシステムの設計、構築、移行及び運用保守を請け負った実績を有し、これを証明すること。また、3 件以上の実績を有している場合には加点として評価する。
- (3) 公共機関(国、地方公共団体、国立大学法人等)、公共機関での実績がない場合は民間企業において、過去 5 年間に仮想サーバ台数 30 台以上のサーバによる仮想化基盤環境の設計、構築、移行及び運用保守を請け負った実績を有し、これを証明すること。

9.2 実施体制及び要員に関する事項

- (1) 本業務は、受託者の従業員により実施することとし、原則、受注内容の再委託は禁止する。ただし、本業務の一部を第三者に再委託する場合は、再委託先の相手方(住所、氏名)、委託範囲と再委託の必要性を明記した上で、事前に本学園の了解を得ること。なお、主たる部分の業務の再委託、プロジェクトマネージャを再委託先の社員や契約社員とすることは認めない。また、再委託する第三者においても「12. 情報セキュリティに関する遵守事項」の全てを遵守すること。
- (2) 作業に当たっては、他の作業者の指揮・統括を行う主要な作業者(プロジェクトマネージャ)を設置するこ

と。なお、プロジェクトマネージャについては、以下1.~3.のいずれかに合格していること。

1. PMI(米国プロジェクトマネジメント協会)認定の「PMP(Project Management Professional)」
 2. IPA(情報処理推進機構)認定の「PM(プロジェクトマネージャ)」
 3. CompTIA(the Computing Technology Industry Association)認定の「Project +」
- (3) 本調達の運用支援業務を行うために、指定した人数の常駐 SE を本学園本部内に常駐させること。常駐 SE は本学園教職員の業務内容を踏まえた運用支援業務を行う関係上、学生・教職員からは学園構成員と同等に見られるため、本学園 Web サイトや資料等で公開されている本学園の制度や各種業務に関する情報を基礎知識として、理解していること。
- (4) 本業務を行うに当たっては本学園と協議の上、定期的な打ち合わせを持つこととする。

9.3 品質管理能力に関する事項

- (1) (財)日本適合性認定協会又は海外の認定機関により認定された審査登録機関による ISO9001:2015 の認証を有している組織・部門が、その品質システムに基づき作業品質の管理を実施すること。

9.4 個人情報保護及び情報セキュリティに関する事項

- (1) 受託者は、プライバシーマーク制度の認証により、現在有効なプライバシーマーク使用許諾を受けていることを証明できること。
- (2) 受託者において、システム構築を実施する担当部署は、現在有効な情報セキュリティマネジメントシステム(ISMS)認証を取得していることを証明できること。
- (3) リース提供者は、プライバシーマーク制度の認証により、現在有効なプライバシーマーク使用許諾を受けていることを証明できること。
- (4) リース提供者は、現在有効な JISQ27001 又は ISO/IEC27001 認証を取得していることを証明できること。

10 検査及び検収

本学園が実施する受入テスト合格及び納品物の納入をもって検収とする。

業務の完了については毎月業務完了報告書を提出し、本学園の承認を得ることをもって行うこと。

11 賠償・復旧

システム運用保守、システム運用支援業務によって発生した不具合が発見された場合には、受託者において無償で迅速に対応すること。また、必要な場合には、関係するドキュメントを修正して納入すること。

12 情報セキュリティに関する遵守事項

12.1 機密情報

- (1) 本契約において、機密情報とは本契約締結日以降、システム構築及び運用支援業務のために本学園が受託者に開示する一切の情報を指すものとする。

(2) 前項に関わらず機密情報が、受託者により以下に該当する情報である旨を証明する通知がなされ、本学園が当該通知の内容が適正であるものと判断した場合には、当該機密情報は機密保持義務を負わないものとする。

- 既に公知、公用の情報
- 開示後、受託者の責めによらず公知、公用となった情報
- 開示を受けたときに既に受託者が知得していた情報
- 開示を受けた後、正当な権限を有する第三者により守秘義務を負うことなしに受託者が入手した情報
- 受託者が開示された情報と無関係に開発、創作した情報
- 法令により開示することが義務付けられた情報

12.2 秘密保持

- (1) 受託者は、本調達業務に着手する以前に秘密情報管理者を選任し、本学園に書面にて通知すること。また、秘密情報管理者が変更された場合、速やかに変更事項を書面にて通知すること。
- (2) 受託者は、本調達業務に着手する以前に秘密情報にアクセスする作業者の名簿を作成し、本学園に提出すること。また、作業者の変更が生じた場合、速やかに変更事項を書面にて提出すること。
- (3) 受託者は、本学園から開示された秘密情報を秘密として保持すること。またいかなる場合も、秘密情報にアクセスする作業者の名簿に記載されていない第三者に秘密情報を開示、漏えい、公表してはならない。
- (4) 受託者は秘密情報を秘密にしておくために合理的な安全保証の予防措置を取らなければならない。
- (5) 全ての秘密情報は本学園の所有物であり、かつ本学園の所有物のまま残ることを確認する。受託者は秘密情報についていかなる権利も有さない。
- (6) 秘密情報の目的外利用については、全て禁止する。
- (7) 秘密情報の引渡し及び受領については、日時、種類、受取人等記録をつけること。
- (8) 秘密情報の複写については、原則禁止とする。ただし事前に本学園の許可を得た場合については、この限りではない。
- (9) 秘密情報の保管については、施錠管理等適切な対策を施すこと。
- (10) 秘密情報を電子メールにて送受信する際は、事前にパスワードを設定して行うこと。
- (11) 秘密情報の紛失等の事故が発生した場合に受託者は、速やかに本学園に報告すると共に、最善の策を講じなければならない。
- (12) 受託者は行政機関等個人情報保護法及び独立行政法人等個人情報保護法を厳守するとともに個人情報保護法等の関連法令を順守し、秘密情報を取り扱う業務を適正に履行すること。
- (13) 受託者は運用支援業務作業員に対し個人情報管理、情報セキュリティ教育に係る研修を受講させ、これを証明する押印付の書類を令和6年3月20日までに本学園に提出すること。また、本調達期間中は毎年研修を受講させ、これを証明する押印付の書類を本学園に提出すること。本調達期間内に作業員の交代がある場合は、着任前に研修受講を証明する押印付きの書類を本学園に提出すること。
- (14) 受託者は、本業務の実施にあたり本学園の情報セキュリティポリシーを厳守すること。情報セ

セキュリティポリシーについては契約後に本学園より提供する。

12.3 秘密情報の返却

- (1) 受託者は、本学園の要求があったときは、速やかに秘密情報の現物、複写、要約及び各業務につき直接発生した二次的資料を本学園に返却又は破棄し、一切のこれらの資料を保管しないものとする。本学園から提出された秘密情報等の資料については、シュレッダー等で判読できないようにしてから全て廃棄すること。
- (2) 受託者は、秘密情報を本システムの構築・運用業務にのみ使用するものとし、その他の目的及び用途で使用してはならない。
- (3) 受託者は、契約任期満了後、速やかに秘密情報の現物、複写、要約及び各業務につき直接発生した二次的資料を本学園に返却又は破棄し、一切のこれらの資料を保管しないものとする。本学園から提出された秘密情報等の資料については、シュレッダー等で判読できないようにしてから全て廃棄しこれを証明する書類を提出すること。

12.4 損害賠償

受託者が、本契約に違反して秘密情報及び秘密資料を外部に漏えいしたり、持ち出したりしたことを起因として、本学園又は関係機関が損害を被った場合には、本学園は受託者に対して損害賠償を請求し、かつ本学園が適当と考える必要な措置を取る権利を有する。

12.5 本システムに格納されている情報の返却

- (1) 受託者は、本学園の要求があったときは、速やかに本システムに格納されている本学園が作成した情報を取り出すことに協力するものとする。
- (2) 受託者は、契約期間満了後、速やかに本システムに格納されている本学園が作成した情報を破棄するものとする。

13 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応

13.1 外部委託

(1) 外部委託に係る契約事項

1. 本システム調達における各工程において、本学園の意図しない変更や機密情報の窃取等が行われなことを保証する管理が、一貫した品質保証体制の下でなされていること。
2. 本システムに本学園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、追跡調査や立入検査等、本学園と連携して原因を調査し、排除するための手順及び体制(例えば、運用・保守業務におけるシステムの操作ログや作業履歴等を記録し、発注先から要求された場合には提出させるようにするなど)を整備していること。
3. 委託事業において取り扱う情報について、再委託先が閲覧することがないよう、受託者は情報を厳重に管理すること。止むを得ず、再委託先において委託事業に係る情報を閲覧する必要がある場合には、受託者は、事前に本学園と調整し、指示に従うこと。

(2) 委託先の資本関係・役員の情報等に関する事項

1. 受託者は、資本関係・役員の情報、委託事業の実施場所、委託事業従事者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報を提示すること。

2. 委託事業の運用に係る要員を限定すること。また、全ての要員の所属、専門性(資格等)、実績及び国籍について掲示すること。委託事業の実施期間中に要員を変更する場合は、事前に本学園へ連絡し、許可(又は確認)を得ること。
3. 運用に係る者の所属(契約社員、派遣社員等の雇用形態は問わず、委託事業に従事する全ての要員)、実績(経験年数、資格等)及び国籍について、本学園にあらかじめ提出し、許可(又は確認)を得ること。
4. 再委託を行う場合には、受託者は、再委託先の事業者名、住所、再委託対象とする業務の範囲、再委託する必要性について、委託元である本学園へ提示し、許可(又は確認)を得ること。
5. 前号に掲げる情報の提供に加えて、再委託先において本委託事業に関わる要員の所属、専門性(資格等)、実績及び国籍についての情報を委託元である本学園へ提示すること。

(3) 監査に関する事項

本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、本学園が情報セキュリティ監査の実施を必要と判断した場合は、本学園が定めた実施内容(監査内容、対象範囲、実施者等)に基づく情報セキュリティ監査を受託者は受け入れること。(本学園が別途選定した事業者による監査を含む)。

13.2 機器等の調達

- (1) 当該機器等の製造工程において意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。
- (2) 機器等に対して不正な変更が加えられないように製造者等が定めたセキュリティ確保のための基準等が整備されており、その基準等が当該機器等に適用されていること。
- (3) 情報システムを構成する要素(ソフトウェア、ハードウェア)に対して不正な変更があった場合に識別できる構成管理体制が確立していること。
- (4) 受託者が情報システムを構成する要素(ソフトウェア、ハードウェア)として採用した機器等について、不正な変更が加えられていないことを検査する体制が受託者において確立していること。

14 システム方式要件

14.1 システム全体構成要件

(1) システム化方針

- システムを構成するハードウェア及びソフトウェア全般について、最新の技術や製品群の採用が可能となるよう、オープン性を有する技術を採用すること。
- システムやシステムで取り扱われるデータの安全性・機密性・信頼性等を十分に確保するため、システム全体やデータに対する脅威への対策を十分に実施すること。

(2) システム化構成要件

- 情報基盤システムは、複数の利用者類型(学生、教員、職員 他)が利用するため、運用面やセキュリティ面を考慮して、ネットワークセグメントを分割構成し、それぞれに関連するサーバ機器、ネットワーク機器及びクライアント機器を配置することとする。
- ネットワークセグメントは、大きく基幹ネットワーク、学習系(キャンパスセグメント)、事務系(事務セグメ

ント)、研究系(研究系セグメント)、図書系(図書系セグメント)の4系統からなり、その他、外部公開サーバの配置を目的とした共通基盤 DMZ セグメント及び研究系 DMZ セグメント、構成機器の監視・バックアップを目的とした運用管理セグメントで全体を構成する。

- 学習系(キャンパスセグメント)は、本部に設置するキャンパスセグメントの各サーバ、各学習センター及びサテライトスペースにおける学生の接続機器等が接続されるセグメントから構成される。
- 事務系(事務セグメント)は、本部に設置する事務セグメントの各サーバ、本部の事務用 PC が接続されるセグメント、各学習センター及びサテライトスペースにおける事務用 PC が接続されるセグメントから構成される。
- 研究系(研究系セグメント)は、本部内の教員用 PC が接続されるセグメントから構成される。
- システム全体の機密性を確保するため、各構成機器及びデータを一元管理する機器を、各々論理的あるいは物理的に分離した構成とし、ネットワークセグメントを別にするとともに、それぞれのセグメント間には適切にファイアウォールを設置する等セキュリティ対策を実施すること。

14.2 信頼性要件

- 情報基盤システムは、学生及び教職員等が全体で利用するインフラシステムであり、本システムが提供する様々な重要サービスの停止は、業務に影響を与えることとなる。従って、システムの信頼性は十分考慮すること。
- システムを構成するハードウェア、ソフトウェア、ネットワーク等は、製品として動作が十分に保証・確認されたものを用い、システム全体として安定して動作すること。
- システム構成要素の冗長化方式として、負荷分散装置による複数台構成、クラスタ構成など適切な方式を選択し、具体的に提案すること。
- 障害の局所化を図るため、機器のクラスタ構成、ハードディスクの RAID 構成等による冗長化方式を採用すること。これにより、障害発生時には障害要因を発生した機器を切り離して運用できる縮退運転や自動継続運転を実現できること。
- 機器の状態を監視し、CPU、メモリ、HDD 等の状態が設定した安全な値の範囲を超えた際に、システム管理者へ通知する機能を導入すること。

14.3 拡張性要件

- 将来の業務機能の拡張、対象事業及び利用者数等の増加による処理量の増加に備えて、十分なスケーラビリティを確保した構成とし、その旨を提案書に記載すること。
- 負荷分散装置配下の機器は、負荷分散装置の設定のみで増設が可能な構成とすること。
- データを保存するサーバは、データ量増加に伴う機器増設等が可能な構成とすること。
- 将来的な機器増設に伴うネットワーク見直しも考慮し、ネットワーク機器の予備ポートやサーバ機器の予備スロットを十分に備えた構成とすること。

15 システムセキュリティ要件

15.1 基本的な考え方

情報基盤システムの構築に当たっては、学生及び教職員の個人情報保護に配慮し、データの完全性・機密性・信頼性の維持、利用者アクセス権限の厳密な管理、システムの可用性とセキュリティ確保が重要となる。

そのため、本学園の情報セキュリティポリシー基本方針及び同対策基準に準拠し、かつ必要な対策を講じること。

15.2 システムセキュリティ要件

(1) 情報基盤システムのセキュリティ要件

以降に示す情報基盤システムの情報セキュリティ要件を満たす機器等の導入を行い、情報セキュリティへの脅威についての対策を講じること。

(2) 利用者の識別と認証

情報基盤システムを構成する機器へは、ログイン ID/パスワードによる利用者の識別及び認証ができること。

(3) データの保護

情報基盤システムで取り扱う学生及び教職員に関する重要なデータについて、セキュアな通信経路の確保又は通信経路の暗号化によりセキュリティを確保すること。

(4) セキュリティホール対策

機器及びネットワーク装置に対して、当該機器上で利用する OS 及びソフトウェアに関連する公開されたセキュリティホールの対策を実施すること。対策のタイミングや実施方法については、運用設計にて提案すること。

(5) 不正プログラム対策

商用ウイルス対策ソフトウェアを導入し、想定される不正プログラムの感染経路の全てにおいて商用ウイルス対策ソフトウェアによる不正プログラム対策を実施すること。

商用ウイルス対策ソフトウェアについては、バージョン、検索エンジン及びパターンファイルを含め、常に最新の状態に維持できる機能を導入すること。

(6) サービス不能攻撃(DoS,DDoS 攻撃)対策

サービス不能攻撃を受ける可能性のある機器、ネットワーク装置を監視し、それらに対するサービス不能攻撃の影響を排除又は低減する対策機能を導入すること。

(7) セキュリティ障害等への対策

情報セキュリティに関する障害(アカウントの不正利用によるサービスダウンや情報漏えい)等が発生した場合に備えて、何らかの異常が発生したことを知らせる、セキュリティアラートを可視化できるようにすること。また、本学園からの連絡を受け障害復旧するために必要となる体制を整備し、本学園へ提示し承認を得ること。

16 機能要件

16.1 本部

本部には、ネットワーク基盤及び学生・教員が利用するシステムと事務職員が利用するシステムが稼動しており、本学園の運営にとって重要な機能を提供するシステムが配置されている。各機器は以下の要件を満たすこと。

- (1) 本部、50 箇所の学習センター及び 7 箇所のサテライトスペースからの利用を想定し、最適な機器構成、台数を提案すること。
- (2) 今回調達する機器は、機器の障害によるサービス停止時間を低減するため、可能な限りアクティブ/アクティブ方式とするなど、最適かつ効果的な冗長構成の設定をすること。
- (3) 主要ネットワーク機器はサーバ機器に対して、1Gbps 以上で接続すること。
- (4) 各機器間を接続するケーブルについて、RJ45 のツイストペアケーブルで接続する場合にはCAT5E 以上のツイストペアケーブルを用いること。
- (5) セキュリティ脅威分散のため用途別にセグメントを分離し、セグメント間のルーティングを行うこと。
- (6) SSO サーバなど負荷が集中するセグメントでは、負荷分散装置等の設置により最適な手法で負荷分散を行うとともに、可用性を確保すること。
- (7) 以下に主要機器の役割を記載する。
 - 広報用 Web サーバは、本学園から情報を発信するためのサーバであり共通基盤 DMZ セグメントに配置する。
 - スпам対策サービスは、本学園のメール送受信に対するスパムメールの排除を提供するサービスである。
 - 外部 DNS サーバは、本学園の DNS サービスを提供するサーバであり共通基盤 DMZ セグメントに配置する。
 - SSO サーバは、本学園のシングルサインオンによる各種システム認証、学生メールサービスとして利用する ASP サービス(Gmail)へのメールリレーを行うサーバであり共通基盤 DMZ セグメントに配置する。
 - グループウェアサーバは、教職員に対して、グループウェアサービスを提供するサーバであり事務セグメントに配置する。
 - 教職員用メールサーバは、教職員へのメールサービスを提供するサーバであり事務セグメントに配置する。
 - 標的型攻撃メール対策サービスは、本学園のメール受信に対する標的型攻撃メールの排除を提供するサービスである。
 - 内部 DNS サーバは、教職員に対して、学内の DNS サービスを提供するサーバであり事務セグメントに配置する。
 - プロキシサーバは、教職員に対して、プロキシサービスを提供するサーバであり事務セグメントに配

置する。

- URL フィルタリングサービスは、教職員に対して、Web アクセス時におけるフィルタリングを提供するサービスである。
- 統合 ID 管理サーバは、本学園のアカウント情報を管理するサーバであり事務セグメントに配置する。
- LDAP サーバは、本学園のアカウント情報を保持するサーバであり事務セグメントに配置する。
- 事務用ドメインコントローラサーバは、事務職員に対し Windows ドメインサービスを提供するサーバであり事務セグメントに配置する。
- クライアント管理サーバは、事務用 PCの管理を行い、WSUS サービスを提供するサーバであり、職員が利用する PC(事務用 PC 等)のクライアント管理サーバを事務セグメントに配置する。
- 本部用共有ファイルサーバは、事務職員に対しファイル共有サービスを提供するサーバであり事務セグメントに配置する。
- 情報公開用サーバは、本学園から情報を公開するためのサーバであり、研究系外部セグメントに配置する。

16.1.1 外部接続L3 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

2台

② 仕様

項目	仕様など
インターフェース	<p>a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。</p> <p>b 1G SFP 光ファイバーポートを 4 ポート以上搭載可能なこと。</p>
スイッチング容量	スタック接続機能を用いて650Gbps 以上であること。
転送レート	スタック接続機能を用いて500Mpps 以上であること。
ネットワーク機能	<p>a OSPF、BGP、PIM及び IPv6 ルーティング (OSPFv3)をサポートすること。</p> <p>b 全スイッチポートで、ダイナミックリンクを設定できること。</p> <p>c IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。</p> <p>d Internet Group Management Protocol (IGMP) v1、v2、v3 スヌーピングに対応していること。</p> <p>e 各スイッチ ポートにセキュリティポリシーを適用できること。</p> <p>f ブリッジ プロトコル データ ユニット (BPDU)ガードをサポートすること。</p> <p>g スパニングツリー ルート ガード (STRG)をサポートすること。</p> <p>h Secure Shell (SSH) Protocol、Kerberos及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3)をサポートすること。</p> <p>i CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。</p>
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	110W 以下であること。
その他	<p>a 本部基幹ネットワークに設置し、SINET 用 ONU (調達範囲外) に接続された SINET 接続用外部 L2 スイッチと 1000Base-T で接続すること。</p> <p>b 本部基幹ネットワークに設置し、KDDI 用 ONU (調達範囲外) に接続すること。</p>

16.1.2 回線負荷分散装置

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 1000BASE-T インターフェースを 6 ポート以上有すること。 b SFP 光ファイバーポートを 2 ポート以上搭載可能なこと
ネットワーク機能	<ul style="list-style-type: none"> a VRRP などの Active-Standby 構成、リンクアグリゲーション構成が可能であること。 b 送信先、送信元の IP アドレスや Port 番号毎に、負荷分散手法、接続回線、セッション維持時間を指定したマルチホーミングを実現することができること。 c セッション情報を 12,000,000 以上保持することができること。 d アドレス変換機能として、DynamicNAT機能、StaticNAT 機能、NoNAT 機能を有すること。 e ヘルスチェック機能として、ICMP と HTTP の利用が可能であること。 f NTP, SYSLOG に対応していること。
プロセッサ	Intel quad-core 同等以上の機能を有すること。
メモリ	16GB 以上有すること。
スループット	スループット最大値が 6Gbps 以上であること。
管理	Web ベースの GUI及び CLI による管理機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	標準消費電力が 160W 以下であること。
その他	<ul style="list-style-type: none"> a 外部接続回線(SINET 及びISP(KDDI))の冗長化を行ない、マルチホーミング環境を提供すること。 b 本部基幹ネットワークに 2 台設置し、冗長構成をとること。 c 本学園で公開しているサーバの A レコードについて、SINET 用、KDDI 用を保持すること。 <p>SINET サービスである ICMP サーバ(2サーバ)に対し、ICMP による通信確認を行い、両方のサーバが応答無しの場合に、KDDI 回線に切り替えること。また、ICMP サーバの通信確認に対する応答が復旧した際は、自動で SINET 回線を利用する構成に戻るよう設定を実施すること。</p>

16.1.3 共通基盤 L2 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。 b アップリンクインターフェースとして、4SFP 以上搭載可能なこと。
スイッチ帯域幅	スタック接続機能を用いて130Gbps 以上であること。
転送パフォーマンス	スタック接続機能を用いて100Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a IEEE 802.1s/w 高速スパニングツリープロトコル (RSTP) をサポートすること。 b Per-VLAN Rapid Spanning Tree (PVRST+) をサポートすること。もしくは PVST+ をサポートすること。 c 全スイッチポートで、ダイナミックリンクを設定できること。 d IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。 e Internet Group Management Protocol (IGMP) スヌーピングに対応していること。 f 個々のスイッチ ポートにセキュリティポリシーを適用できること。 g ブリッジ プロトコル データ ユニット (BPDU) ガードをサポートすること。 h スパニングツリー ルート ガード (STRG) をサポートすること。 i Secure Shell (SSH) Protocol、Kerberos 及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3) をサポートすること。 j CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMP トラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	37.1W 以下であること。
その他	<ul style="list-style-type: none"> a 回線負荷分散装置と共通基盤セグメント用ファイアウォールを接続すること。 b 本部基幹ネットワークに 2 台設置し、冗長構成をとること。

16.1.4 共通基盤ファイアウォール

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 8 ポート以上有すること。 b 1GbE SFP インターフェースを 8 ポート以上有すること。
スループット	<ul style="list-style-type: none"> a ファイアウォールスループットは、25Gbps 以上の性能を有すること。 b 不正侵入防御機能 (IPS 機能)のスループットは、3.5Gbps 以上の性能を有すること。
同時接続数	ファイアウォール同時セッション数が 8,000,000 以上の性能を有すること。
機能	<ul style="list-style-type: none"> a ファイアウォール機能と IPS 機能を 1 台で提供すること。なお、ファイアウォール、IPS それぞれの機能において ICSCA Labs の認定を受けている場合は加点とする。 b UTM(統合脅威管理)として実装可能であり、ライセンスを追加することで、アンチウイルス機能、アンチスパム機能、WEB フィルタリング機能、アプリケーション制御機能が利用可能であること。 c 10 個以上の独立した仮想 UTM を作成可能なこと。 d ファイアウォールポリシー数を 10,000 以上設定できること。 e VLAN 及び IEEE802.1Q VLAN トランク機能をサポートすること。 f ネットワークアドレス変換 (NAT) 機能、ポートアドレス変換 (PAT) 機能を有すること。 g ファイアウォール機能及び各 UTM 機能の負荷を軽減するために ASIC を搭載していること。 h Active-Active, Active-Standby いずれの冗長構成も可能なこと。
管理	Web ベースの GUI、及び CLI による管理機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMP トラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
その他	インターネットから内部ネットワークへのアクセス制限及び IPS 機能を提供すること。

16.1.5 共通基盤 DMZ L2 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。 b アップリンクインターフェースとして、4SFP 以上搭載可能なこと。
スイッチ帯域幅	スタック接続機能を用いて130Gbps 以上であること。
転送パフォーマンス	スタック接続機能を用いて100Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a IEEE 802.1s/w 高速スパニングツリープロトコル (RSTP) をサポートすること。 b Per-VLAN Rapid Spanning Tree (PVRST+) をサポートすること。もしくは PVST+ をサポートすること。 c 全スイッチポートで、ダイナミックリンクを設定できること。 d IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。 e Internet Group Management Protocol (IGMP) スヌーピングに対応していること。 f 個々のスイッチ ポートにセキュリティポリシーを適用できること。 g ブリッジ プロトコル データ ユニット (BPDU) ガードをサポートすること。 h スパニングツリー ルート ガード (STRG) をサポートすること。 i Secure Shell (SSH) Protocol、Kerberos 及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3) をサポートすること。 j CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMP トラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	37.1W 以下であること。
その他	<ul style="list-style-type: none"> a 共通基盤 DMZ 負荷分散装置と共通基盤ファイアウォールを接続すること。また、VPN 装置を接続すること。 b 本部共通基盤 DMZ に 2 台設置し、スタック接続による冗長構成をとること。

16.1.6 共通基盤 DMZ 負荷分散装置

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	1000BASE-T インターフェースを 4 ポート以上有すること。
スループット	<ul style="list-style-type: none"> a 負荷分散装置のスループットとして、1Gbps 以上のパフォーマンスを有すること。 b SSL 暗号化処理速度として、1Gbps 又は 2,000tps 以上のパフォーマンスを有すること。 c HTTP リクエストとして、L7ベースで75,000req/sec 又は同時セッション数L4ベースで1,000,000 以上をサポートすること。
ネットワーク機能	<ul style="list-style-type: none"> a レイヤ 4 における負荷分散において、ラウンドロビン、最小コネクション、最小パケット、最小応答時間のバランシングポリシーによる負荷分散が可能であること。 b アクセラレーション機能を有すること。 c レイヤ 7 における負荷分散が可能であること。 d SSL アクセラレータにより、HTTP を SSL 化し、HTTPS としてサービス提供できること。 e IPv6 に対応していること。 f 標準でL4ファイアウォール機能を有すること。
管理	<p>Web ブラウザによって各種機能設定を行う事が可能なこと。</p> <p>GUIが日本語に対応していること。</p> <p>CLIでの設定が可能なこと。</p>
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 2U 以下の大きさであること。
消費電力	300w 以下であること。
その他	<ul style="list-style-type: none"> a 冗長化されたサーバ(外部 DNS サーバ、スパム対策サーバ、SSO サーバ)に対して負荷分散機能を提供すること。 b 共通基盤 DMZ L2 スイッチに接続し、共通基盤 DMZ セグメントを提供すること。 c 本部共通基盤 DMZ に 2 台設置し、アクティブ/スタンバイの冗長構成をとること。

16.1.7 研究系 DMZ L2 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。 b アップリンクインターフェースとして、4SFP 以上搭載可能なこと。
スイッチ帯域幅	スタック接続機能を用いて130Gbps 以上であること。
転送パフォーマンス	スタック接続機能を用いて100Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a IEEE 802.1s/w 高速スパニングツリープロトコル (RSTP) をサポートすること。 b Per-VLAN Rapid Spanning Tree (PVRST+) をサポートすること。 c 全スイッチポートで、ダイナミックトランクを設定できること。 d IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。 e Internet Group Management Protocol (IGMP) スヌーピングに対応していること。 f 個々のスイッチ ポートにセキュリティポリシーを適用できること。 g ブリッジ プロトコル データ ユニット (BPDU) ガードをサポートすること。 h スパニングツリー ルート ガード (STRG) をサポートすること。 i Secure Shell (SSH) Protocol、Kerberos 及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3) をサポートすること。 j CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMP トラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	37.1W 以下であること。
その他	<ul style="list-style-type: none"> a 本部研究系 DMZ に 2 台設置し、スタック接続による冗長構成をとること。 b 共通基盤ファイアウォールに接続すること。 c 本学園で用意するサーバ (Weblog サーバ、ストリーミングサーバ等) に接続すること。 d 本学園が指定する本部 L2 エッジスイッチ及び本学園が所有する既存スイッチと接続すること。

16.1.8 基幹L3 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 48 ポート以上有すること。 b 1G SFP 光ファイバーポートを 4 ポート以上搭載可能なこと。
スイッチング容量	スタック接続機能を用いて700Gbps 以上であること。
転送レート	スタック接続機能を用いて500Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a OSPF、BGP、PIM及び IPv6 ルーティング (OSPFv3)をサポートすること。 b 全スイッチポートで、ダイナミックリンクを設定できること。 c IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。 d Internet Group Management Protocol (IGMP) v1、v2、v3 スヌーピングに対応していること。 e 各スイッチ ポートにセキュリティポリシーを適用できること。 f ブリッジ プロトコル データ ユニット (BPDU)ガードをサポートすること。 g スパニングツリー ルート ガード (STRG)をサポートすること。 h Secure Shell (SSH) Protocol、Kerberos及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3)をサポートすること。 i CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	本体 (NWモジュールなどを含まない) 消費電力が120W 以下であること。
その他	本部基幹ネットワークに 2 台設置し、スタック接続による冗長構成をとること。

16.1.9 事務L3 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 48 ポート以上有すること。 b 1G SFP 光ファイバーポートを 4 ポート以上搭載可能なこと。
スイッチング容量	スタック接続機能を用いて700 Gbps 以上であること。
転送レート	スタック接続機能を用いて500Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a OSPF、BGP、PIM及び IPv6 ルーティング (OSPFv3)をサポートすること。 b 全スイッチポートで、ダイナミックリンクを設定できること。 c IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。 d Internet Group Management Protocol (IGMP) v1、v2、v3 スヌーピングに対応していること。 e 各スイッチ ポートにセキュリティポリシーを適用できること。 f ブリッジ プロトコル データ ユニット (BPDU)ガードをサポートすること。 g スパニングツリー ルート ガード (STRG)をサポートすること。 h Secure Shell (SSH) Protocol、Kerberos及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3)をサポートすること。 i CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	本体 (NWモジュールなどを含まない) 消費電力が120W 以下であること。
その他	<ul style="list-style-type: none"> a 共通基盤ファイアウォール、事務クライアント用 L3 スイッチと接続すること。事務用負荷分散装置を接続すること。事務セグメントに設置する各サーバと接続すること。 b 本部事務セグメントに 2 台設置し、スタック接続による冗長構成をとること。 c 教務情報システムにアクセスする配線 (RJ-45) を接続すること。

16.1.10 事務負荷分散装置

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	1000BASE-T インターフェースを 4 ポート以上有すること。
スループット	<ul style="list-style-type: none"> a 負荷分散装置のスループットとして、1Gbps 以上のパフォーマンスを有すること。 b SSL 暗号化処理速度として、1Gbps又は 2,000tps 以上のパフォーマンスを有すること。 c HTTP リクエストとして、L7ベースで75,000req/sec又は同時セッション数L4ベースで1,000,000 以上をサポートすること。
ネットワーク機能	<ul style="list-style-type: none"> a レイヤ 4 における負荷分散において、ラウンドロビン、最小コネクション、最小パケット、最小応答時間のバランシングポリシーによる負荷分散が可能であること。 b アクセラレーション機能を有すること。 c レイヤ 7 における負荷分散が可能であること。 d SSL アクセラレータにより、HTTP を SSL 化し、HTTPS としてサービス提供できること。 e IPv6 に対応していること。 f 標準でL4ファイアウォール機能を有すること。
管理	<p>Web ブラウザによって各種機能設定を行う事が可能なこと。</p> <p>GUIが日本語に対応していること。</p> <p>CLIでの設定が可能なこと。</p>
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 2U 以下の大きさであること。
消費電力	300w 以下であること。
その他	<ul style="list-style-type: none"> a 本部事務セグメントに 2 台設置し、アクティブ・スタンバイの冗長構成をとること。 b 冗長化された事務セグメント設置の各サーバに対して負荷分散機能を提供すること。 c 事務 L3 スイッチに接続すること。

16.1.11 事務クライアント L3 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。 b 1G SFP 光ファイバーポートを 4 ポート以上搭載すること。
スイッチング容量	スタック接続機能を用いて650Gbps 以上であること。
転送レート	スタック接続機能を用いて500Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a OSPF、BGP、PIM及び IPv6 ルーティング (OSPFv3)をサポートすること。 b 全スイッチポートで、ダイナミックリンクを設定できること。 c IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。 d Internet Group Management Protocol (IGMP) v1、v2、v3 スヌーピングに対応していること。 e 各スイッチ ポートにセキュリティポリシーを適用できること。 f ブリッジ プロトコル データ ユニット (BPDU)ガードをサポートすること。 g スパニングツリー ルート ガード (STRG)をサポートすること。 h Secure Shell (SSH) Protocol、Kerberos及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3)をサポートすること。 i CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	100W 以下であること。
その他	<ul style="list-style-type: none"> a 本部事務セグメントに 2 台設置し、スタック接続による冗長構成をとること。 b 事務 L3 スイッチと接続すること。 c 本学園が指定する本部 L2 エッジスイッチ及び本学園が保有する既存スイッチと接続すること。 d マルチモードの 1000BASE-SX SFP を 4 個用意すること。

16.1.12 キャンパスネット L3 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。 b 1G SFP 光ファイバーポートを 4 ポート以上搭載可能なこと。
スイッチング容量	スタック接続機能を用いて650Gbps 以上であること。
転送レート	スタック接続機能を用いて500Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a OSPF、BGP、PIM及び IPv6 ルーティング (OSPFv3)をサポートすること。 b 全スイッチポートで、ダイナミックリンクを設定できること。 c IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。 d Internet Group Management Protocol (IGMP) v1、v2、v3 スヌーピングに対応していること。 e 各スイッチ ポートにセキュリティポリシーを適用できること。 f ブリッジ プロトコル データ ユニット (BPDU)ガードをサポートすること。 g スパニングツリー ルート ガード (STRG)をサポートすること。 h Secure Shell (SSH) Protocol、Kerberos及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3)をサポートすること。 i CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	100W 以下であること。
その他	<ul style="list-style-type: none"> a 共通基盤ファイアウォールと接続すること。 b 本部キャンパスセグメントに 2 台設置し、スタック接続による冗長構成をとること。 c 千葉学習センターにおける学外接続のためのルーティングを実施すること。

16.1.13 運用管理 L2 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (必要な台数を用意すること)

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 48 ポート以上有すること。 b アップリンクインターフェースとして、4SFP 以上搭載可能なこと。
スイッチ帯域幅	スタック接続機能を用いて180Gbps 以上であること。
転送パフォーマンス	スタック接続機能を用いて130Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a IEEE 802.1s/w 高速スパニングツリープロトコル (RSTP) をサポートすること。 b Per-VLAN Rapid Spanning Tree (PVRST+) をサポートすること。もしくは PVST+ をサポートすること。 c 全スイッチポートで、ダイナミックリンクを設定できること。 d IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。 e Internet Group Management Protocol (IGMP) スヌーピングに対応していること。 f 個々のスイッチ ポートにセキュリティポリシーを適用できること。 g ブリッジ プロトコル データ ユニット (BPDU) ガードをサポートすること。 h スパニングツリー ルート ガード (STRG) をサポートすること。 i Secure Shell (SSH) Protocol, Kerberos 及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3) をサポートすること。 j CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMP トラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	50W 以下であること。
その他	全てのサーバ、ネットワーク機器を接続し、運用管理用のネットワークを設定すること。そのために必要となる台数のスイッチを用意すること。

16.1.14 研究系内部 L2 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。 b アップリンクインターフェースとして、4SFP 以上搭載可能なこと。
スイッチ帯域幅	スタック接続機能を用いて130Gbps 以上であること。
転送パフォーマンス	スタック接続機能を用いて100Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a IEEE 802.1s/w 高速スパニングツリープロトコル(RSTP)をサポートすること。 b Per-VLAN Rapid Spanning Tree(PVRST+)をサポートすること。もしくはPVST+をサポートすること。 c 全スイッチポートで、ダイナミックリンクを設定できること。 d IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。 e Internet Group Management Protocol (IGMP) スヌーピングに対応していること。 f 個々のスイッチ ポートにセキュリティポリシーを適用できること。 g ブリッジ プロトコル データ ユニット (BPDU) ガードをサポートすること。 h スパニングツリー ルート ガード (STRG) をサポートすること。 i Secure Shell (SSH) Protocol、Kerberos 及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3) をサポートすること。 j CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMP トラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	37.1W 以下であること。
その他	<ul style="list-style-type: none"> a 本部研究系内部セグメントに 2 台設置し、スタック接続による冗長構成をとること。 b 共通基盤ファイアウォールと接続すること。 c 本学園が指定する本部 L2 エッジスイッチと接続すること。

16.1.15 本部 L2 エッジスイッチ

(1) 本部 L2 エッジスイッチ A(48 ポート以上)

ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

12 台

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 48 ポート以上有すること。 b SFP 光ファイバーポートを 4 ポート以上搭載可能なこと。
スイッチファブリック	100Gbps 以上であること。
パケット処理能力	77Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a IEEE 802.1s/w 高速スパンニングツリープロトコル(RSTP)をサポートすること。 b Per-VLAN Rapid Spanning Tree(PVRST+)をサポートすること。もしくは PVST+をサポートすること。 c IEEE802.1Q VLAN トランク機能をサポートすること。 d 64 個以上の VLAN をサポートすること。 e ネットワーク管理機能として、Web UI及び CLI を利用できること。 f VLAN トランキング・プロトコル機能を有すること。 g スタック専用ポートを必要とせずに単一の IP を用いて最大 8 台のスイッチを管理できること。
障害検知	ハードウェアの障害や異常を検知し、SNMP トラップで通知する機能を有すること。
筐体	a 19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	60W 以下であること。
その他	<p>以下の場所に設置すること。なお、SFP(1000BASE-SX)を 2 個以上用意すること。2 台を予備機として保管すること。</p> <ul style="list-style-type: none"> a 東管理棟 1 階 学生課作業室 EPS:1 台 b 東管理棟 2 階 財務部長室 EPS:2 台 SFP:1 個 c 放送研究棟 6 階 EPS:3 台 d 東制作棟 3 階 制作部内:1 台 SFP:1 個 e 図書館 1 階 事務室内:1 台 f 放送研究棟 1 階 計算機室:2 台

(2) 本部 L2 エッジスイッチB(24 ポート以上)

ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

8 台

② 仕様

項目	仕様など
インターフェース	a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。 b SFP 光ファイバーポートを 4 ポート以上搭載可能なこと。
スイッチファブリック	56Gbps 以上であること。
パケット処理能力	41Mpps 以上であること。
ネットワーク機能	a IEEE 802.1s/w 高速スパンニングツリープロトコル(RSTP)をサポートすること。 b Per-VLAN Rapid Spanning Tree(PVRST+)をサポートすること。もしくはPVST+をサポートすること。 c IEEE802.1Q VLAN トランク機能をサポートすること。 d 64 個以上の VLAN をサポートすること。 e ネットワーク管理機能として、Web UI及び CLI を利用できること。 f VLAN トランキング・プロトコル機能を有すること。 g スタック専用ポートを必要とせずに単一のIPを用いて最大8台のスイッチを管理できること。
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	30W 以下であること。
その他	以下の場所に設置すること。なお、SFP(1000BASE-SX)を 2 個以上用意すること。2 台を予備機として保管すること。 a. 東管理棟 1 階 学生課作業室 EPS: 1 台 b. 東管理棟 3 階 事務局長室 EPS: 1 台 c. 西管理棟 1 階 印刷室: 1 台 SFP: 1 個 d. 図書館 1 階 物品倉庫内 EPS 室: 1 台 SFP: 1 個 e. 放送研究棟 1 階 計算機室: 2 台

16.1.16 本部集約スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

2 台

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。 b アップリンクインターフェースとして、4SFP 以上搭載可能なこと。
スイッチ帯域幅	スタック接続機能を用いて130Gbps 以上であること。
転送パフォーマンス	スタック接続機能を用いて100Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a IEEE 802.1s/w 高速スパニングツリープロトコル(RSTP)をサポートすること。 b Per-VLAN Rapid Spanning Tree(PVRST+)をサポートすること。もしくはPVST+をサポートすること。 c 全スイッチポートで、ダイナミックトランクを設定できること。 d IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。 e Internet Group Management Protocol (IGMP) スヌーピングに対応していること。 f 個々のスイッチ ポートにセキュリティポリシーを適用できること。 g ブリッジ プロトコル データ ユニット (BPDU) ガードをサポートすること。 h スパニングツリー ルート ガード (STRG) をサポートすること。 i Secure Shell (SSH) Protocol、Kerberos 及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3) をサポートすること。 j CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	37.1W 以下であること。
その他	<p>以下の場所に設置すること。なお、SFP(1000BASE-SX)を 2 個以上用意すること。</p> <ul style="list-style-type: none"> a 西研究棟 1 階 計算機室:1 台 SFP:1 個 b 放送研究棟 1 階 計算機室:1 台 SFP:1 個

16.1.17 VPN 装置

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1台

② 仕様

項目	仕様など
インターフェース	10BASE-T/100BASE-TX/1000BASE-T インターフェースを6ポート以上有し、そのうち WAN ポートとして 2 ポート以上指定できること。
メモリ	メインメモリ 4 GB 以上、フラッシュメモリ 4GB 以上を有すること。
セキュリティ・ネットワーク機能	<ul style="list-style-type: none"> a IPsec/IKEv1、IKEv2、IPsec over IPV6、VRF-aware Ipsec をサポートすること。 b トンネルレス Group Encrypted Transport VPN をサポートすること。 c ハードウェア アクセラレーションによる DES、3DES、AES 128、AES 192及び AES 256 の暗号化が行えること。 d ステートフルファイアウォール機能を有すること。 e ネットワーク管理機能として、Web UI及び CLI を利用できること。 f ルーティング機能としてRIP、RIPv2、OSPF、BGP、BGP ルータリフレクタ及びIS-ISに対応していること。
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
その他	本学園と協議の上学外拠点との VPN 接続ができるようにすること。

16.1.18 本部用サーバ仮想化基盤

本部に設置するサーバは本部用共有ファイルサーバ、バックアップサーバを除き、仮想化ソフトウェアを用いたサーバ仮想化基盤を構築し、仮想サーバにより構成すること。

(1) サーバ仮想化基盤のハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (3 台以上の構成とすること。)

② 仕様

項目	仕様など
CPU	Intel Xeon プロセッサ 6342(クロック速度 2.8GHz/24 コア/48スレッド)相当以上の処理能力を有すると判断される CPU を 2基以上搭載していること。
メモリ	256GB 以上を搭載すること。
ハードディスク	SATA SSD 480GB以上 ×3基(RAID1+ホットスペア1基相当)を搭載すること。)
LAN	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T に対応したポートを 4 ポート以上有すること。 b リモート管理用LAN ポートを有すること。 c 仮想サーバ用ストレージとの接続を 10G 以上とするためのモジュールを2ポート以上有すること。なお、FC接続で16Gbps以上の接続の場合は加点とする。
光学ドライブ装置	仮想メディア機能を有し、リモートからパソコンもしくはネットワーク上にある CD/DVDドライブやISOイメージにアクセスしてOSのインストール等が可能なこと。なお、SANブートの場合は、ディスク装置の搭載は不要とする。
電源、ファン	ホットスワップに対応した 2 つ以上の電源ユニット、ファンにより冗長化構成とすること。
監視	<ul style="list-style-type: none"> a CPU、メモリ、電源ユニット、ファン、システムの温度のステータス(正常又は障害)を機器外面から目視で又はサーバ監視ソフトで確認できる場合は加点とする。 b サーバ管理ツールはメインサーバCPUから独立している専用のプロセッサを使用することでサーバ本体や OS の 障害の影響を受けることなく管理が可能なこと。 c 監視で取得したサーバ情報の過去のデータとの比較が可能であること。またグラフ表示が可能なこと。ただし、機能を別のサーバで実現してもよい。ただし、データをエクスポートする事で、機能を別のサーバやPC等で実現してもよい。 d 電力監視、消費電力上限値設定が可能なこと。 e ネットワークやRAID構成における故障をボード上で LED 通知又はサーバ監視ソフトで確認することが可能であること。 f システムエラー発生時、障害対応連絡がツール上から発行できること。ログ情報はメーカーの保守技術者が取得することでシステム障害

	<p>対応時間の短縮化・管理者作業の省力化を図ること。</p> <p>g 管理コンソールはグラフィカルもしくはツリー構造を用いた異常箇所の表示が可能なこと。</p> <p>h SNMP 機能を有すること。また、電源ユニットやハードディスクなどのハードウェアに故障が生じた時は、SNMP トラップにより通知する機能を有すること。</p>
スケジュール	<p>あらかじめ設定した時間にサーバの電源オン/オフができる機能(スケジュール運転機能)を、サーバ単体もしくはリモート端末から制御できる機能を有すること。</p>
インターフェース	<p>a USB ポートを 2ポート以上有すること。</p> <p>b サーバの状態及びオペレーティングシステムの状態に依存しない Ethernet ネットワーク経由で使用可能な専用のリモートコンソールポートを有すること。</p>
筐体	<p>19 インチラックに搭載可能であること。</p>
その他	<p>全ての物理サーバについて同一構成とすること。また、物理サーバが 1 台故障した場合は、残りの物理サーバに機能分散できること。</p>
仮想サーバ用ストレージ	<p>a ラックマウント可能なストレージを導入すること。</p> <p>b ストレージ領域として RAID6相当の構成で、実効容量を 28TB 以上搭載すること。</p> <p>c ディスクドライブとして SSDのみを搭載すること。</p> <p>d インラインでの重複排除機能を有し、可変長による重複判定が可能であること</p> <p>e コントローラー及びコントローラー内の各ポート、電源、ファンは冗長化されていること。</p> <p>f 仮想サーバホストとなる物理サーバとは 10Gb以上 で接続すること。なお、FC接続で16Gbps以上の接続の場合は加点とする。</p> <p>g 仮想サーバ単位でのスナップショット機能を有し、世代管理(最大 50,000世代)が可能であること。スナップショット取得の際に性能影響がないこと。</p> <p>h 毎時・日次・週次のスケジュール及び採取したスナップショット毎に保持期間を設定できること。</p> <p>i 仮想化ソフトウェアと連携し、仮想マシン単位でのクローン機能を有すること。</p> <p>j ストレージ管理にあたり、GUIベースの管理ツールを無償で提供すること。また、各種情報(容量、IOPS、遅延、スループット)がリアルタイムで可視化できること。</p>

	<p>k 重複排除及び圧縮処理を実行し、SSD の容量空間を効率的に使用できること。スナップショット に含まれるデータも重複排除及び圧縮処理の対象になること。</p> <p>l SNMP 機能を有すること。また、電源ユニットやハードディスクなどのハードウェアに故障が生じた時は、SNMP トラップにより通知する機能を有すること。</p> <p>m システムの稼働ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。</p> <p>n NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。</p>
集約スイッチ	16.1.16 本部集約スイッチと同等仕様の機器を2台スタック構成で導入し、仮想化基盤の各物理サーバと1G以上で接続すること。

(2) 仮想化ソフトウェアに関し、以下の仕様を満たすこと。

- ① 仮想化ソフトウェアは、VMware vSphere 7 essentials plus 又はこれと同等以上の性能・機能を有すること。
- ② 導入時点で最新版のパッチを適用すること。

(3) 仮想管理サーバは仮想サーバとし、以下の仕様を満たすこと。

- ① 調達台数
1式(1台)
- ② 仕様

項目	仕様など
CPU	4vCPU 以上割り当てること。
メモリ	21GB 以上割り当てること。
ハードディスク	694GB 以上割り当てること。

(4) 仮想管理ソフトウェアに関し、以下の仕様を満たすこと。

- ① 仮想管理用ソフトウェアとして、VMware vCenter Server Applianceを導入し、仮想ホストと仮想マシンを対象とした統合管理環境を構築すること。
- ② 導入時点で最新版のパッチを適用すること。
- ③ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。

16.1.19 広報用 Web サーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

2 式（複数台での構成でも構わない）

② 仕様

項目	仕様など
CPU	2vCPU 以上割り当てること。
メモリ	4GB 以上割り当てること。
ハードディスク	300GB 以上割り当てること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Red Hat Enterprise Linux 8 又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ apache2 と同等以上の機能を有するソフトウェアの最も安定した最新版を導入すること。
- ④ インターネット向けに WWW サービスを提供すること。なお、同時アクセス数が 1024 以上あった場合でも利用が可能であること。
- ⑤ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。なお、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。
- ⑥ 本学園が提供する広報用 Web サイトのコンテンツを移行し、稼働させること。
- ⑦ 本学園が提供する科目ナビ(Web サービス)の DB及びコンテンツを移行し、稼働させること。
- ⑧ 本学園が提供する番組表(Web サービス)の DB及びコンテンツを移行し、稼働させること。
- ⑨ アプリケーションの移行については、範囲外とする。
- ⑩ 本学園が提供する授業科目案内のコンテンツを移行し、稼働させること。
- ⑪ FTP にてコンテンツのアップロードが可能であること。
- ⑫ CUI によるリモート操作が行えること。リモートアクセス時は、SSHv2 による暗号化が行えること。
- ⑬ システムの稼働ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑭ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。
- ⑮ アプリケーションの可用性を確保するためのソフトウェアを導入し、ハードウェア障害に加えてアプリケーション障害の際も自動復旧する仕組みを有すること。
- ⑯ SSL サーバ証明書(5 年間以上)を実装すること。

16.1.20 外部DNSサーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

1式(2台の冗長構成とすること)

② 仕様

項目	仕様など
CPU	2vCPU 以上割り当てること。
メモリ	4GB 以上割り当てること。
ハードディスク	300GB 以上割り当てること。
その他	2 台が異なる物理サーバで稼動するように調整すること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Red Hat Enterprise Linux 8 又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ bind9 と同等以上の機能を有するソフトウェアの最も安定した最新版を導入すること。
- ④ インターネット向けにプライマリ DNS サービスを提供すること。
- ⑤ 本学園内向けに再帰検索用のプライマリ・セカンダリ DNS サービスを提供すること。
- ⑥ セカンダリDNS として、SINET 提供の「分散セカンダリ DNS サービス」を利用するため、提供機関への申請処理における支援を実施するとともに、必要な設定を行うこと。
- ⑦ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。なお、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。
- ⑧ CUI によるリモート操作が行えること。リモートアクセス時は、SSHv2 による暗号化が行えること。
- ⑨ システムの稼動ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑩ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。

16.1.21 SSO サーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
CPU	2vCPU 以上割り当てること。
メモリ	4GB 以上割り当てること。
ハードディスク	300GB 以上割り当てること。
その他	2 台が異なる物理サーバで稼働するように調整した上、アクティブ/スタンバイの冗長構成をとること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

① OS は、Red Hat Enterprise Linux 8 又はこれと同等以上の性能・機能を有すること。

② OS については、導入時点で最新版のセキュリティパッチを適用すること。

③ apache2 と同等以上の機能を有するソフトウェアの最も安定した最新版を導入すること。

④ インターネット向けに WWW サービスを提供すること。

⑤ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。なお、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。

⑥ CUI よりリモート操作が行えること。リモートアクセス時は、SSHv2 による暗号化が行えること。

⑦ CAS(Central Authentication Service)によるシングルサインオン(以降 SSO を記載)を実現すること。SSO 対象システムについては、本学園内外に設置した約 30 システムが存在しており、認証方法について現行システムから変更することなく継続して SSO 環境を実現すること。SSO 対象システム側の設定変更無しに CAS による SSO 環境を提供すること。なお、教務情報システムも SSO 対象システムである。

⑧ SSO に参加するシステムを設定可能な、Web サービスを提供すること。

⑨ 本学園の認証は LDAP を中心とした認証を行っているが、SSO 連携するシステムにおいては、LDAP 内に保持するユーザ情報と異なるログイン ID、パスワードが必要となるシステムが存在する。このため、利用者が入力したログイン ID を連携先のシステム用 ID に振替、連携先システムへ ID 情報を引き渡す事ができる機能を実現すること。また、実現方法について、具体的な提案を行うこと。

⑩ 本学園 SSO 連携システムを利用するアカウントごとに、SSO 連携システムに対するアクセス制御を実現すること、また、実現方法について、具体的な提案を行うこと。

⑪ 稼働ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。

- ⑫ NTP(¹RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。
- ⑬ SSL サーバ証明書(5年間以上)を SSO サービス用に実装すること。
- ⑭ SSO を実現する際、対象システムに対するログインの順番を問わないこと。
- ⑮ SSO 対象システムに対して、SSO を実現するため受託者の責任の上で設定作業を実施し、現行機能の動作を保証すること。実施に当たっては各対象システムの開発業者と連携の上実施すること。なお、費用が発生する場合は全て受託者が負担するものとする。
- ⑯ SSO 対象システムとして、学生用メール(ASP メールサービス)のユーザ認証を可能にすること。ただし、パスワードは ASP 側に保有しないこと。
- ⑰ Gmail アカウントの申請画面を用意し、申請があった際、運用管理者宛にメールで通知すること。
- ⑱ WEB 会議システムの利用申請画面を用意し、申請があった際、運用管理者宛にメールで通知すること。
- ⑲ WEB 会議システムのアカウント申請画面を用意し、申請があった際、運用管理者宛にメールで通知すること。
- ⑳ ASP メールサービスに対するメールリレー機能を提供すること。また、送受信ログを記録すること。記録したログについて、過去 1 年間のメール送受信の確認ができること。

¹ Juchuusha

16.1.22 学術認証連携 サーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
CPU	4vCPU 以上割り当てること。
メモリ	8GB 以上割り当てること。
ハードディスク	300GB 以上割り当てること。
その他	2 台が異なる物理サーバで稼動するように調整した上、アクティブ/スタンバイの冗長構成をとること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Red Hat Enterprise Linux 8又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。なお、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。
- ④ CUI によるリモート操作が行えること。リモートアクセス時は、SSHv2 による暗号化が行えること。
- ⑤ Shibboleth4.0又はそれと同等以上の性能・機能を有すること。
- ⑥ Shibboleth認証を行うためにIdP(IDプロバイダ)機能を提供できること。
- ⑦ 学術認証フェデレーションと連携可能であること。
- ⑧ Google Workspaceに対してShibbolethを使った認証情報を提供できること。
- ⑨ 稼動ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑩ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。

16.1.23 グループウェアサーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

1 式(複数台での構成でも構わない)

② 仕様

項目	仕様など
CPU	20vCPU 以上割り当てること。スタンバイ機を導入する場合は 10vCPU 以上割り当てること。
メモリ	64GB 以上割り当てること。スタンバイ機を導入する場合は 32GB 以上割り当てること。
ハードディスク	4.8TB 以上割り当てること。スタンバイ機を導入する場合はグループウェアのデータ領域をアクティブ機と共有できるようにすること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Red Hat Enterprise Linux 8 又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ アプリケーションの可用性を確保するためのソフトウェアを導入し、ハードウェア障害に加えてアプリケーション障害の際も自動復旧する仕組みを有すること。
- ④ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。尚、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。
- ⑤ CUI によるリモート操作が行えること。リモートアクセス時は、SSHv2 による暗号化が行えること。
- ⑥ システムの稼動ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑦ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。
- ⑧ SSL サーバ証明書(5 年間以上)をグループウェアサービス用に実装すること。

グループウェア製品については、以下の仕様を満たすこと。

<全体要件>

- ① 1 システムで 2 万ユーザ以上で正常利用した動作実績を持つ製品であること。
- ② ユーザのアクセスは全て Web 経由で行えること。また、グループウェアシステムは利用者及び管理者機能が Web で利用できること。
- ③ 利用者が Web ブラウザ(Microsoft Edge、Firefox、Safari、Google Chrome)でアクセスできること。
- ④ ポータル機能を標準機能もしくは追加機能で実現できること。追加機能で実現する場合は本サーバ納入時点で本機能を搭載していること。
- ⑤ 部署別ポータル及び個人別ポータル機能を標準機能もしくは追加機能で実現できること。追加機能で実現す

る場合は本サーバ納入時点で本機能を持っていること。

- ⑥ 共通、グループ、個人と3つのポータルを作成できること。
- ⑦ グループ(組織)として最大10段階の管理ができること。
- ⑧ グループウェアに1度ログインした後はグループウェア内で実現する各機能を利用する際に再度認証を必要としないこと。
例)グループウェアへログインしたアカウントにてWebメール機能を利用するために、Webメール機能用に手動でpopアカウント設定を必要とするような仕組みは不可。
- ⑨ ユーザ情報、組織階層、ユーザの組織所属情報は、CSVファイルから一括して追加・変更・削除を行うことができること。
- ⑩ 統合ID管理サーバと連携し、LDAPサーバにアカウント登録時、自動でグループウェアサーバにもアカウントが作成されること。
- ⑪ グループウェア製品自体のセキュリティパッチ適用について、9時間以内に作業を完了できる製品であること。

<利用者数>

- ① 1500人以上が同時利用可能であること。
- ② 1500人分以上のアカウントライセンスを用意すること。

<メール機能>

- ① Webメール機能を有すること。
- ② グループウェアの機能として内包していても、異なるメールクライアントとの組み合わせで実現してもよいが、他のメールクライアント側でのフォルダ分け状態等はWebメール利用時にも反映されていること。
- ③ 各利用者は自身のメールフォルダに任意にメール保存用のフォルダを追加・編集・削除可能なこと。
- ④ 各利用者はメールフィルタを設定可能で、フィルタの機能により受信メールを自動的に各フォルダへ振り分け可能であること。
- ⑤ メール1件単位、フォルダ単位にてメールをeml形式にてエクスポートが可能であること。
- ⑥ 既存システムから今回導入するシステムにメールデータを移行する際、他のメールクライアントでエクスポートしたeml形式のメールを複数同時にインポート可能であること。インポートする際に制限がある場合はその旨を提案資料に明記すること。(件数、容量、既存システムでのフォルダ分け状態がインポート先で維持できない、など)
- ⑦ 利用者側・管理者側でメール転送設定が可能であること。ただし、本機能はグループウェア以外で実現してもよい。
- ⑧ メールのスプール領域として、全体で最大5TBを利用可能であること。クォータ機能により、管理者が利用者毎に利用可能な容量の制限をかけられること。

- ⑨ クライアントにメール着信をポップアップ等で通知する機能を提供すること。グループウェア製品以外のソフトウェアとの組み合わせや、クライアントへの機能実装により実現してもよい。
- ⑩ 利用者はログインアカウントとは別にマルチアカウントでの利用も可能であること。

<メール検索機能>

- ① グループウェアのメールを検索する機能を有すること。
- ② メール の 件名、本文、添付ファイル内容、差出人での検索が可能であること。
- ③ メールに添付されたファイルのタイトルや作成者だけでなく、次のファイルの中身も検索できること。
 - Word(doc,docx,docm)
 - Excel(xls,xlsx,xlsm)
 - PowerPoint(ppt,pptx,pptm)
 - PDF(pdf)
 - HTML(html,htm)
 - XML(xml)
 - テキスト(txt)
- ④ 検索結果の画面では、アプリケーションの種類や検索内容を表示できること。

<アドレス帳>

- ① 組織毎に3階層以上の階層を設けられること。
- ② 各階層の部課室係名、人名の並び順は管理者側で特別な記号を付与することなく任意に変更可能であること。

<スケジュール>

- ① 閲覧権限を利用者側で任意に設定可能であること。
- ② 個人1日・個人週間・個人月間、所属グループ週間・所属グループ1日、の単位で一覧表示が可能であること。
- ③ 他ユーザのスケジュール登録の際、グループからユーザ選択できること。

<幹部スケジュール閲覧>

- ① 役員スケジュール一覧ページ、部課長スケジュール一覧ページを設けること。
- ② それぞれのページへはポータル画面から1クリックでアクセス可能なこと。
- ③ それぞれのページの閲覧権限を職員毎に設定可能なこと。

- ④ 役員、部課長を 1 画面で一覧表示できること。
- ⑤ 個人 1 日・個人週間・個人月間、所属グループ週間・所属グループ 1 日、の単位で一覧表示が可能であること。
- ⑥ 各人の並び順は任意に変更可能なこと。
- ⑦ 本人だけでなく、秘書等がスケジュールの編集・削除・追加を行えること。

<お知らせ掲示板>

- ① 新規投稿記事があった際、利用者に新着投稿記事がある旨を通知するマークが表示されること。
- ② 各記事にはファイルの添付が可能であること。
- ③ グループ単位でアクセス権(参照可、不可)の設定が可能であること。
- ④ アクセス権は、閲覧権限・書き込み権限・フォローの書き込み権限の 3 パターンで設定が可能であること。

<アラーム機能>

- ① スケジュール機能で設定した時刻にて、画面上にアラームを表示する機能を有すること。

<設備予約>

- ① 幕張本部内会議室等の予約及び予約状況の閲覧が可能であること。
- ② 20 箇所以上の設備を管理可能なこと。

<ポータル画面>

- ① 共通ポータル画面には初期状態として次の機能を表示すること。
 - 機能へのアイコン
 - 個人スケジュール(週間)
 - 掲示板
 - 共通ブックマーク
- ② その他各種機能についても共通ポータル画面への表示・非表示が選択可能であること
- ③ 個人ポータル画面も設定可能であること。

16.1.24 教職員用メールサーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 調達台数

1 式（複数台での構成でも構わない）

② 仕様

項目	仕様など
CPU	2vCPU 以上割り当てること。
メモリ	12GB 以上割り当てること。
ハードディスク	2.4TB 以上割り当てること。スタンバイ機を導入する場合はメールのデータ領域をアクティブ機と共有できるようにすること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Red Hat Enterprise Linux 8 又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ アプリケーションの可用性を確保するためのソフトウェアを導入し、ハードウェア障害に加えてアプリケーション障害の際も自動復旧する仕組みを有すること。
- ④ Postfix と同等以上の機能を有するソフトウェアの最も安定した最新版を導入すること。
- ⑤ Dovecot と同等以上の機能を有するソフトウェアの最も安定した最新版を導入すること。
- ⑥ POPs、IMAPs によるアクセスが可能であり、学外からメール利用が可能であること。
- ⑦ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。なお、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。
- ⑧ CUI によるリモート操作が行えること。リモートアクセス時は、SSHv2 による暗号化が行えること。
- ⑨ メーリングリストの作成、変更、削除が可能なこと。
- ⑩ システムの稼動ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑪ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。
- ⑫ SSL サーバ証明書(5 年間以上)を教職員用メールサービス用の実装すること。

16.1.25 内部DNS プロキシサーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

1 式（2 台の冗長構成とすること）

② 仕様

項目	仕様など
CPU	2vCPU 以上割り当てること。
メモリ	8GB 以上割り当てること。
ハードディスク	300GB 以上割り当てること。

その他	2台が異なる物理サーバで稼動するように調整すること。
-----	----------------------------

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Red Hat Enterprise Linux 8 又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ bind9 と同等以上の機能を有するソフトウェアの最も安定した最新版を導入すること。
- ④ プロキシサーバ機能を提供すること。
- ⑤ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。なお、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。
- ⑥ CUI によるリモート操作が行えること。リモートアクセス時は、SSHv2 による暗号化が行えること。
- ⑦ システムの稼動ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑧ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。

16.1.26 メールー斉送信・駅すぱあとサーバ

(1) ASPサービス又は仮想サーバで機能を提供すること。仮想サーバで提供する場合、仮想サーバは以下の仕様を満たすこと。

- ① 構成
1台
- ② 仕様

項目	仕様など
CPU	2vCPU 以上割り当てること。
メモリ	8GB 以上割り当てること。
ハードディスク	300GB 以上割り当てること。
その他	ソフトウェアの要件を満たすよう、適切な台数で構成すること。

(2) ソフトウェア、サービスに関し、以下の仕様を満たすこと。なお、ASPサービスで提供する場合、

- ①、②は満たさなくてよい。
- ① OS は、Red Hat Enterprise Linux 8 又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ メールー斉送信機能として、以下を実現すること。
 - One to One で配信するメール配信システムを提供すること。
 - GUI 操作で送信先メールアドレスを csv ファイルで登録ができ、複数の csv ファイルを保存可能であること。また、メールー斉送信時、保存した csv ファイルより選択ができ、かつ、選択した csv ファイル内のメールアドレスより、送信するメールアドレスを選択可能であること。
 - メール配信システムに、メール本文をGUI で登録でき、複数のメール本文を保存できる

こと。また、一斉メール送信時、保存したメール本文より送信するメール本文を選択ができること。

- 保存する csv ファイル及びメール本文は、部署ごとに保存が可能であること。
- 1 度に配信するアドレス数として、最大で 100,000 アドレスへの一斉送信が可能であること。
- 学生アドレス(ASP メールサービス上の単一メールアドレス)10 万件へひとつの送信元メールアドレスから一斉配信しても ASP メールサービス側に迷惑メールと判定されない仕組みとすること。

16.1.27 統合ID 管理サーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

1 式(1台)

② 仕様

項目	仕様など
CPU	4vCPU 以上割り当てること。
メモリ	8GB 以上割り当てること。
ハードディスク	500GB 以上割り当てること。
その他	ソフトウェアの要件を満たすよう、適切な台数で構成すること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Microsoft Windows Server 2019/2022 Standard 又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ LDAP とActive Directory のアカウント同期機能を有すること。
- ④ アカウント管理用の GUI 画面を提供し、アカウント情報の追加、更新、削除が可能であること。なお、パスワードについては、画面上に表示しないこと。
- ⑤ PDF ファイルによるパスワード通知書を発行できること。
- ⑥ パスワードの初期化及び設定機能を有すること。
- ⑦ 学生用パスワードの初期化については、職員で実施でき GUI 画面を用意すること。
- ⑧ 利用者自身で、パスワードを変更できる画面を用意すること。
- ⑨ アカウント管理者の GUI 画面からの変更や、利用者からの変更においては、LDAP サーバ、ActiveDirectory 連携(事務用ドメインコントローラ)及び ASP メールサービス、ASP ファイルサービス、教職員用メールサーバ、グループウェアサーバへアカウント情報がリアルタイムに同期変更されること。
- ⑩ バッチ実行による LDAP サーバへの更新ならびに連携先のディレクトリシステム等への反映については、管理者の手動実行、外部コマンドからの実行が可能であること。
- ⑪ ユーザエントリの一括登録、更新、削除の方法として、CSV ファイルでの投入が可能であること。
- ⑫ CSV ファイルを用いた入出力を行なう場合の文字コードとして、Shift-JIS 及び、UNICODE が使用できる

こと。

- ⑬ パスワードの連携においては、業界にて保証のある暗号方式を用いて、安全な連携が実行できること。
- ⑭ 動作証跡を残すためにログ出力機能を有すること、ログを絞り込む機能を有し、Windows のイベントログへの出力も可能であること。
- ⑮ 検索結果の一覧画面に表示できる項目は上記設定 GUI で変更ができ、また設定されたリスト項目によってソートが可能でかつ検索結果を外部 CSV ファイルとして出力できること。またMicrosoft Office を導入し編集・加工ができること。
- ⑯ 操作管理者に対する操作 ACL が設定でき、同一の画面を利用しても管理者の ACL によって、生成、更新、削除、参照の各操作の制限ができること。
- ⑰ Active Directory 連携に関して、ユーザアカウントの新規作成の場合には、ユーザのホームディレクトリを指定してフォルダ作成が実行できること。
- ⑱ 連携によって Active Directory 側のユーザを削除(論理、物理)する場合は、Home Directory の削除が行えること。
- ⑲ LDAP サーバのユーザエントリの情報をもとにして、Active Directory 側にグループ作成を行いメンバーの更新ができること。
- ⑳ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。なお、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行い、本学園が指示するアドレスにメールで通知すること。
- ㉑ 本学園より提示する教務情報システムから抽出されたユーザデータ(CSV ファイル)を、LDAP サーバと、各ドメインコントローラに対して同期して登録・変更・削除が可能なこと。
- ㉒ システムの稼動ログやアプリケーションログを集約し、監視サーバへ転送する機能を有すること。
- ㉓ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。

16.1.28 認証用LDAP サーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
CPU	6vCPU 以上割り当てること。
メモリ	64GB 以上割り当てること。
ハードディスク	600GB 以上割り当てること。

その他	<ul style="list-style-type: none"> a 本部事務セグメントに2台1式として設置すること。 b 事務負荷分散装置配下で、マルチマスタ構成とすること。
-----	--

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Red Hat Enterprise Linux 8又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ LDAP によるユーザ認証サービスを提供すること。
- ④ LDAP サーバは、2 台でマルチマスタ構成とすること。
- ⑤ 2 台の LDAP マルチマスタを設定したサーバにおける LDAP サービスの提供は、事務負荷分散装置に設定された LDAP マルチマスタ用 VIP を介して行い、認証用の LDAP サービスを提供すること。
- ⑥ LDAP 認証システムについては、本学園内外に設置した約 10 システムが存在しており、継続してLDAP 環境を実現すること。
- ⑦ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。尚、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。
- ⑧ SNMP 機能を有すること。
- ⑨ システムの稼動ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑩ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。
- ⑪ LDAP 対象システムに対して、LDAP を実現するため受託者の責任の上で設定作業を実施し、現行機能の動作を保証すること。実施に当たっては各対象システムの開発業者と連携の上実施すること。なお、費用が発生する場合は全て受託者が負担するものとする。

16.1.29 メタディレクトリLDAPサーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
CPU	4vCPU 以上割り当てること。
メモリ	32GB 以上割り当てること。
ハードディスク	600GB 以上割り当てること。
その他	本部事務セグメントに 2 台 1 式として設置すること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

① OS は、Red Hat Enterprise Linux 8又はこれと同等以上の性能・機能を有すること。

② OS については、導入時点で最新版のセキュリティパッチを適用すること。

③ LDAP によるメタディレクトリサービスを提供すること。

④ LDAP サーバは、2 台でマルチマスタ構成とすること。

⑤ 2 台の LDAP マルチマスタを設定したサーバにおける LDAP サービスの提供は、事務負荷分散装置に設定された LDAP マルチマスタ用 VIP を介して行い、更新用の LDAP サービスを提供すること。

⑥ LDAP の属性は、既設 LDAP サーバより移行するものとするが、一部属性情報の追加を想定している。本学園が指示する LDAP の属性情報について変更を実施すること。

⑦ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。尚、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。

⑧ SNMP 機能を有すること。

⑨ システムの稼動ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。

⑩ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。

⑪ LDAP 対象システムに対して、LDAP を実現するため受託者の責任の上で設定作業を実施し、現行機能の動作を保証すること。実施に当たっては各対象システムの開発業者と連携の上実施すること。なお、費用が発生する場合は全て受託者が負担するものとする。

16.1.30 事務用ドメインコントローラサーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

1 式 (2 台の冗長構成とすること)

② 仕様

項目	仕様など
CPU	2vCPU 以上割り当てること。
メモリ	8GB 以上割り当てること。
ハードディスク	300GB 以上割り当てること。
その他	2 台が異なる物理サーバで稼動するように調整すること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Microsoft Windows Server 2019/2022 Standard 又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ 統合ID 管理サーバと連携し、Active Directory ドメイン管理できること。
- ④ 本部職員がクライアント PC にログインした際、「16.1.32 本部用共有ファイルサーバ」内の指定の領域に対するドライブ割り当てを行うこと。なお、職員個人ごとに割り当てる領域については、別途本学園と打合せの上決定する。
- ⑤ 本部、学習センター及びサテライトスペースの教職員(約 1500 人)のユーザアカウント情報を一元管理し、クライアント PC を使用する際に認証機能を提供すること。なお、ドメインコントローラはマルチマスタによる 2 台構成とし、1 台サーバが停止しても提供機能に影響を与えないこと。
- ⑥ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。尚、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。
- ⑦ システムの稼動ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑧ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。
- ⑨ 本ドメインに必要となるクライアントアクセスライセンス(CAL)を納入すること。

16.1.31 事務用クライアント管理サーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

1 式（複数台の構成でも構わない）

② 仕様

項目	仕様など
CPU	2vCPU 以上割り当てること。
メモリ	8GB 以上割り当てること。
ハードディスク	300GB 以上割り当てること。
その他	ソフトウェアの要件を満たすよう、適切な台数で構成すること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Microsoft Windows Server 2019/2022 Standard 又はこれと同等以上の性能・機能を有すること。
 - ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
 - ③ 事務用 PC にインストールするブラウザについて、バージョンアップが可能な構成を用意すること。
 - ④ 事務用 PC(管理用を含む)を管理するためのクライアント管理ソフトウェアを導入すること。
なお、クライアント管理ソフトウェアは、以下の機能を有すること。
 - a 「プログラムの追加と削除」の使用禁止や、Windows に関する全端末及び特定の端末群に対して一括設定変更が可能であること。なお、本要件はグループポリシーでの制御でもよい。
 - b 不正ソフトウェアやインストール exe の起動抑止が可能であること。
 - c OS 種別/SP 種別/特定アプリケーションなど、PC の状況を自動識別しての配布設定が可能であること。
 - d Windows ログオン時の強制配信、任意のタイミングでの選択配信などの設定が可能であること。
 - e Office、Adobe など 1,200 種類以上の配布用スクリプトを提供されていること。
 - f 電源オプションの設定変更や、指定時刻でのシャットダウン設定が可能であること。
 - g 管理者PC から、利用者 PC をリモートで操作できること。
 - h クライアント PC のハードウェア情報、ソフトウェア情報を自動的に取得し、一元管理できること。
 - i ライセンス購入情報を登録することで、ライセンスの過不足管理が可能であること。
 - j PC 資産情報を台帳形式で参照できること。
 - k ドライブ、ファイル、メディアを暗号化することで、盗難や紛失の緊急時でも第三者への情報漏えいを防止できること。
 - クライアント PC のドライブ暗号化
 - USB メモリなどのメディア暗号化
 - 持ち出しファイルの自己復号型暗号化
- なお、本学園より承認が得られた場合、同等のセキュリティレベルを確保できる別の方法で実現してもよい。

- I WSUS サービスを提供し、事務用 PC の Update が可能であること。
- ⑤ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。尚、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行い、本学園が指示するアドレスにメールで通知すること。
- ⑥ システムの稼動ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑦ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。

16.1.32 本部用共有ファイルサーバ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1台

② 仕様

仕様項目	仕様など
全般	a ファイルサーバ専用のアプライアンス(NAS)であること。 b CIFS プロトコルによるファイル共有を提供するファイルサーバとすること。
コントローラ	2 台以上搭載し、冗長構成とすること。サービス停止することなく、コントローラの増設・取り外しができること。
メモリ	48GB 以上有すること。また、不揮発メモリ(NVRAM)はバッテリーバックアップされており、停電発生時にライトデータを保持する機能を有すること。
ハードディスク	ニアライン SAS もしくは SAS もしくは SSD 2TB 以上のものを内蔵し、障害時でもデータ消失が起きないように構成したうえ、実効容量 12TB 以上とすること。また、ホットプラグ対応であること。
インターフェース	1 つの物理ポートで 10GbE 又は 16Gb FC に使用可能なポートを 4 ポート以上有すること。
電源、ファン	それぞれ冗長構成とすること。障害時はサービス停止することなく復旧交換が可能なこと。
監視	a ディスクの障害予兆を検出した場合、そのディスクドライブから、冗長性を維持した状態でホットスペアディスクドライブへデータを自動コピーし、コピー完了後にホットスペアディスクドライブを自動的に RAID グループに組み込み、障害予兆が検出されたディスクドライブを RAID グループから切り離す機能を有すること。 b ハードウェアの異常・障害予兆が発生した場合に、指定したメールアドレスに検出した内容を通知するリモート通報機能を有すること。
筐体	ラックマウントできるものであること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① 専用OS を搭載すること。
- ② ネットワーク処理とファイルシステム処理を一体化することにより高速処理が可能であること。
- ③ RAID 上の全データブロックを管理するとともに、書込み要求毎に一時的にメモリに保存したデータを、近傍となる空きブロックへ一括して書込み処理を実施することでシーク時間を短縮し、高速処理が可能なディスクアクセス方式であること。
- ④ 未使用領域をストレージプールにまとめ、記憶容量を効率的に利用すること。
- ⑤ 必要に応じてボリューム容量を動的に増減可能なこと。
- ⑥ 重複しているブロックを排除する機能を有すること。
- ⑦ あらかじめ設定したスケジュールにより、バックアップ実行時点におけるボリューム内データブロックのマッピングテーブルを作成する(データブロックのコピーは行わない) Snapshot 機能を有すること。またマッピングテーブルにおいては 255 世代まで維持管理が可能なこと。
- ⑧ CUI、GUI それぞれによるリモート操作が行えること。リモートアクセス時は、SSHv2 による暗号化が行えること。
- ⑨ SNMP 機能を有すること。また、電源ユニットやハードディスクなどのハードウェアに故障が生じた時は、SNMP トラップにより通知する機能を有すること。
- ⑩ システムの稼動ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑪ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。

(3) ファイルサーバにおけるフォルダ構成・アクセス権・容量については、以下の仕様を満たすこと。

- ① 役員専用、幹部直員専用のフォルダを用意すること。
- ② 各部及び室・課(既存数 17)のフォルダを作成し権限設定を行うこと。また、共通で利用可能となる公開用フォルダを作成すること。なお、フォルダの構成については、本学園との打合せにより決定するものこととする。
- ③ 部長、役員等一部のアカウントを除き、各部・課・室用のフォルダについて、各課・室に所属している本部職員のアカウントから読み書きを可能とする。公開用フォルダについては、各部・室・課に所属する本部職員全てが利用できること。事務用ドメインコントローラサーバの Active Directory で管理されているアカウントを利用すること。
- ④ 部長、役員等一部のアカウントを除き、公開用フォルダ内に、各部・室・課用のフォルダを作成し、当該部・室・課の本部職員のみ読み書きを可能とし、以外の本部職員からは参照のみが可能であること。
- ⑤ 部長、役員等一部のアカウントにおけるアクセス可権限については、別途本学園との打合せにより決定するものとする。
- ⑥ 各フォルダは事務用端末からネットワークドライブとしてマウントすること。
- ⑦ 各フォルダにはクォータをかけること。サイズについては本学園と協議の上決定すること。
- ⑧ クォータ容量はサービス提供後も管理者側で任意に調整可能なこと。
- ⑨ 組織改編の際には部・室・課の名称変更やフォルダ数の増減を行うことが可能であること。
- ⑩ クォータ容量の調整や各部・室・課のフォルダ作成、変更の際、サービスの停止を伴わないこと。また、保存されているファイルを削除することなく上記操作を行えること。
- ⑪ クォータ容量の調整や各部・室・課のフォルダ削除の際、サービスの停止を伴わないこと。
- ⑫ 既存システムファイルサーバ上のデータを本部用共有ファイルサーバの各部署のフォルダ

へ移行すること。移行に当たっては、事前に本学園の承認を得た上で作業を実施すること。

16.1.33 バックアップサーバ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1 式 (2 台以上の構成とすること)

② 仕様

仕様項目	仕様など
CPU	クロック速度 2.0GHz/キャッシュ10MB/8コア)相当以上の処理能力を有すると判断される CPU を 1 個以上でソフトウェアを安定稼働させるための CPU 数を搭載すること。
メモリ	64GB 以上でソフトウェアを安定稼働させるための容量を搭載すること。
ハードディスク	バックアップデータ領域として、実効容量47TB以上の容量を搭載すること。
LAN	a 10BASE-T/100BASE-TX/1000BASE-T に対応したポートを 4 ポート以上有すること。 b リモート管理用LAN ポートを有すること。 c 仮想サーバ用ストレージとの接続を 10G以上 とするためのモジュールを 2ポート以上有すること。
光学ドライブ装置	内蔵 DVD-ROM ユニットが望ましいが、外付けで共有する形でも構わない。
電源、ファン	ホットスワップに対応した 2 つ以上の電源ユニット、ファンにより冗長化構成とすること。
筐体	19 インチラックに搭載可能であること。
その他	a 本部運用管理セグメントに必要な数設置すること。 b 本部が被災した場合にも、システムがリストア可能なバックアップデータを保存する、遠隔地バックアップ機器を提供すること。遠隔地バックアップ機器は、本学園が指定する学習センターか、受託者が提案する、関東地方を除く日本国内のデータセンターに必要な数設置すること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Microsoft Windows Server 2019/2022 Standard 又はこれと同等以上の性能・機能を有すること。あるいは、バックアップアプライアンスとして提供し、独自のOSをバンドルすること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ 今回導入するすべてのサーバについて、サポートを受けることが可能な商用バックアップソフトウェアを導入すること。また自動運転により取得したバックアップデータを接続されている遠隔地バックアップ機器

へ保存すること。

- ④ 初回のフルバックアップ取得以降は日次で増分バックアップを実施し、永久増分バックアップを取得すること。バックアップの保持期間は1週間以上とすること。
- ⑤ バックアップジョブの実行優先順位を、ジョブ毎に指定することが可能であること。
- ⑥ ジョブが失敗した場合、自動的にそのジョブをリトライさせることが可能であること。
- ⑦ バックアップ取得時は、システム全体を停止せずサービスを提供している状態でのバックアップができ、システム障害が発生した場合でもバックアップしたデータからリストアすることにより迅速に復旧が出来ること。
- ⑧ フルバックアップは 24 時間以内に完了すること。24 時間以内に完了させるために必要なハードウェアを導入すること。
- ⑨ 全データのリストアは翌営業日中には完了可能であること。なお、遠隔バックアップ機器からのリストアは、この限りでは無い。
- ⑩ 利用者からの要望に従い、フォルダ毎、ファイル毎のリストアが可能であること。
- ⑪ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。尚、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行い、本学園が指示するアドレスにメールで通知すること。
- ⑫ SNMP 機能を有すること。また、電源ユニットやハードディスクなどのハードウェアに故障が生じた場合は、SNMP トラップにより通知する機能を有すること。
- ⑬ システムの稼動ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑭ NTP (RFC 1305) 機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。

16.1.34 ログ管理・監視サーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

1 式（複数台の構成でも構わない）

② 仕様

項目	仕様など
CPU	2vCPU 以上割り当てること。
メモリ	8GB 以上割り当てること。
ハードディスク	300GB 以上割り当てること。
その他	a ソフトウェアの要件を満たすよう、適切な台数で構成すること。 b 外部データ保管用の NAS サーバを用意すること。なお、サイズは 10TB 以上保存が可能であること。 c 本部運用管理セグメントに必要数設置すること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Red Hat Enterprise Linux 8 又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ 導入サーバ機器及び導入ネットワーク機器のシステムログを収容し、保存する機能を有すること。
- ④ 導入サーバ機器の CPU、メモリ、トラフィック、HDD 等を監視する機能を有すること。
- ⑤ 監視対象の稼働状況をレポート化して表示できること。
- ⑥ Web ブラウザよりホストや監視に関する追加や変更などの設定ができること。
- ⑦ 監視対象のトラフィック状態や、CPU、メモリなどの使用状況などをグラフにより視覚的に確認できること。運用業務における定例会議資料に必要となる情報を取得できること。
- ⑧ 収集したログに異常を検知した際、管理者へのメール通知機能を有していること。
- ⑨ ログを収集する対象機器、ログを保管する期間については、本学園との打合せの上決定すること。
- ⑩ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。尚、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。
- ⑪ CUI によるリモート操作が行えること。リモートアクセス時は、SSHv2 による暗号化が行えること。
- ⑫ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。

16.1.35 事務用 PC

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

本学園より、420台のノートPCを提供する。ソフトウェアについては本調達に含め、インストールするものとする。

端末タイプA 400台

端末タイプB 20台

(導入場所については、「表 1 PC 導入台数一覧」を参照のこと)

② 仕様

端末タイプA(400台)

項目	仕様など
CPU	CPU は、インテル Core i5 プロセッサ 同等以上の機能を有するものを搭載する。
メモリ	8GB 以上有する。
記憶装置	SSD 256GB 以上を有する。
ネットワーク	10BASE-T/100BASE-TX/1000BASE-T、WakeUp-On-LAN 対応。変換アダプタでの拡張である。
無線 LAN	内蔵し、IEEE802.11a/b/g/n/ac に対応している。
ディスプレイ解像度	1,920 × 1080 ドット以上、1,600 万色以上の 13.3 インチ以上のワイド液晶ディスプレイである。
インターフェース	<ul style="list-style-type: none"> a USB ポートは、Type-A USB3.0 以上を 2 ポート以上、Type-C(ディスプレイ出力対応)を1ポート以上有する。 b Bluetooth(5.1以上)の機能を有する。 c HDMI 端子を 1 ポート以上有する。 d ヘッドフォン/マイクコンボポート、ヘッドフォン/スピーカージャック又はユニバーサルジャックを有する。
マウス	有線接続の光学式ホイールマウスを付属している。
カメラ	内蔵している。
スピーカ	内蔵している。

端末タイプB(20台)

項目	仕様など
CPU	CPU は、インテル Core i5 プロセッサ 同等以上の機能を有するものを搭載する。
メモリ	8GB 以上有する。
記憶装置	SSD 256GB 以上を有する。
ネットワーク	10BASE-T/100BASE-TX/1000BASE-T、WakeUp-On-LAN 対応である。インターフェースは内蔵している。

無線 LAN	内蔵し、IEEE802.11a/b/g/n/ac に対応している。
ディスプレイ解像度	1,366×768ドット以上、1,600 万色以上の 15.6 インチ以上の液晶ディスプレイである。
インターフェース	a USB ポートは、Type-A USB3.0 以上を 2 ポート以上、Type-C(ディスプレイ出力対応)を1ポート以上有する。 b Bluetooth(5.1以上)の機能を有する。 c HDMI 端子を 1 ポート以上有する。 d ヘッドフォン/マイクコンボポート、ヘッドフォン/スピーカージャック又はユニバーサルジャックを有する。
マウス	有線接続の光学式ホイールマウスを付属して。
カメラ	内蔵している。
スピーカ	内蔵している。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS 及びインストールするソフトウェアは、「表 3 事務用ソフトウェア一覧」に示す。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。なお、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。
- ④ 「16.1.31 事務用クライアント管理サーバ」に示したソフトウェア仕様を満たすため、必要に応じてエージェントソフトウェアをインストールすること。
- ⑤ 管理者権限のアカウント及びパスワードを職員に公開することなく、管理者権限を必要とするソフトウェアのインストールができること。
- ⑥ 教務情報システム(システム WAKABA)を利用するために必要な設定を、Web ブラウザに施すこと。設定内容は本学園より提供する。

16.1.36 ネットワークプリンタ(カラー)

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

16 台(導入場所については、「表 2 PC 以外導入台数一覧」を参照のこと)

② 仕様

項目	仕様など
印刷方式	LED アレイ+乾式 1 成分電子写真方式又はレーザーゼログラフィ(半導体レーザー+乾式電子方式)であること。

印刷速度	(フルカラー)30枚/分(A4横送り)、18枚/分(A3)、両面印刷時:22ページ/分(A4横送り)以上の性能であること。 (モノクロ)30枚/分(A4横送り)、18枚/分(A3)、両面印刷時:22ページ/分(A4横送り)以上の性能であること。
解像度	1,200×1,200dpi/600×600dpiに対応していること。
用紙サイズ	A3、A4、B4サイズが利用可能であること。
給紙量	標準トレイが250枚以上、手差しトレイが100枚以上給紙できること。
製品寿命	最大60万ページ又は5年のいずれか早い方以上であること。
インターフェース	1000BASE-T/100BASE-TX/10BASE-Tのインターフェースを有すること。
メモリ	1GB以上であること。
両面印刷機能	両面印刷が可能であること。
消費電力	1,500W以下であること。
筐体サイズ	本体サイズが600(W)×600(D)×430(H)mm以下であること。
その他	a 本部に導入すること。 b 設置場所については、本学園の指示に従うこと。

16.1.37 外付けDVDドライブ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

136台(導入場所については、「表2 PC以外導入台数一覧」を参照のこと)

16.2.4 事務用PCにDVDに書き込みが可能な内蔵ドライブを搭載した場合は16.1.37 外付けDVDドライブは不要とする。

② 仕様

項目	仕様など
対応メディア	DVD±RWに対応すること。
インターフェース	①で挙げたすべてのPCについて、USB2.0で接続してDVD±RWドライブとして利用できること。
筐体サイズ	150mm×150mm×20mm以下であること。
その他	VRモード・CPRM再生に対応していること

16.1.38 教員用メール・プロキシ・DNS(LSV)サーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

1 式 (1 台)

② 仕様

項目	仕様など
CPU	2vCPU 以上割り当てること。
メモリ	4GB 以上割り当てること。
ハードディスク	100GB 以上割り当てること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Red Hat Enterprise Linux 8 又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ 16.1.25 内部DNS プロキシサーバ、16.1.24 教職員用メールサーバ、16.3.2 URLフィルタリングサービスと連携して、教員向けにメール・プロキシ・DNS サービスを提供すること。
- ④ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。なお、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行い、本学園が指示するアドレスにメールで通知すること。
- ⑤ システムの稼動ログやアプリケーション動作ログを集約し、ログ管理サーバへ転送する機能を有すること。
- ⑥ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。

16.1.39 検証用サーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

① 構成

1 式 (1 台)

② 仕様

項目	仕様など
CPU	2vCPU 以上割り当てること。
メモリ	4GB 以上割り当てること。
ハードディスク	100GB 以上割り当てること。
その他	検証用として、上記リソースを確保しておくこと。システム構築の際に本サーバを構築する必要はないが、運用時に本サーバを構築できるように利用マニュアルを作成すること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Red Hat Enterprise Linux 8 又は Microsoft Windows Server 2019/2022 Standardを検証する際に導入できるようにすること。

16.1.40 情報公開用サーバ

(1) 仮想サーバに関し、以下の仕様を満たすこと。

- ① 構成

1 式 (1 台)

- ② 仕様

項目	仕様など
CPU	4vCPU 以上割り当てること。
メモリ	4GB 以上割り当てること。
ハードディスク	100GB 以上割り当てること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

- ① OS は、Red Hat Enterprise Linux 8 又はこれと同等以上の性能・機能を有すること。
- ② OS については、導入時点で最新版のセキュリティパッチを適用すること。
- ③ apache2 と同等以上の機能を有するソフトウェアの最も安定した最新版を導入すること。
- ④ 本学園が提供する単位認定試験問題、印刷教材等のコンテンツを移行し公開すること。
- ⑤ 本学園が提供する、教員が作成したサイトのコンテンツを移行し公開すること。
- ⑥ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。なお、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行い、本学園が指示するアドレスにメールで通知すること。
- ⑦ システムの稼動ログやアプリケーション動作ログを集約し、ログ管理サーバへ転送する機能を有すること。
- ⑧ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期をする設定を行うこと。
- ⑨ SSL サーバ証明書(5 年間以上)を実装すること。

16.1.41 西研究棟・東制作棟等ネットワーク基幹 L3 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

2台

② 仕様

項目	仕様など
インターフェース	a 1G SFP 光ファイバーポートを 24 ポート以上有すること。
スイッチング容量	スタック接続機能を用いて650Gbps 以上であること。
転送レート	スタック接続機能を用いて500Mpps 以上であること。
ネットワーク機能	<p>a OSPF、BGP、PIM及び IPv6 ルーティング (OSPFv3)をサポートすること。</p> <p>b 全スイッチポートで、ダイナミックリンクを設定できること。</p> <p>c IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。</p> <p>d Internet Group Management Protocol (IGMP) v1、v2、v3 スヌーピングに対応していること。</p> <p>e 各スイッチ ポートにセキュリティポリシーを適用できること。</p> <p>f ブリッジ プロトコル データ ユニット (BPDU)ガードをサポートすること。</p> <p>g スパニングツリー ルート ガード (STRG)をサポートすること。</p> <p>h Secure Shell (SSH) Protocol、Kerberos 及び簡易ネットワーク管理 プロトコル バージョン 3 (SNMPv3)をサポートすること。</p> <p>i CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。</p>
障害検知	ハードウェアの障害や異常を検知し、SNMP トラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	130W 以下であること。
その他	<p>a 西研究棟 1 階サーバ室に 2 台設置し、スタック接続による冗長構成をとること。</p> <p>b 西研究棟 1 階に設置する本部集約スイッチと接続すること。LAN ケーブル配線は既設のものを流用すること。</p> <p>c 付属するマルチモードの1000BASE-SX SFP を各フロアスイッチ(7 台)に接続すること。また、付属する 1000BASE-T SFP を西研究棟 1 階に設置する本部集約スイッチと接続すること。</p>

16.1.42 西研究棟・東制作棟等ネットワークフロア L2 スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

7台

② 仕様

項目	仕様など
インターフェース	<p>a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。</p> <p>b アップリンクインターフェースとして、4SFP 以上搭載可能なこと。</p>
スイッチ帯域幅	スタック接続機能を用いて130Gbps 以上であること。
転送パフォーマンス	スタック接続機能を用いて100Mpps 以上であること。
ネットワーク機能	<p>a IEEE 802.1s/w 高速スパニングツリープロトコル(RSTP)をサポートすること。</p> <p>b Per-VLAN Rapid Spanning Tree(PVRST+)をサポートすること。もしくはPVST+をサポートすること。</p> <p>c 全スイッチポートで、ダイナミックトランクを設定できること。</p> <p>d IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。</p> <p>e Internet Group Management Protocol (IGMP) スヌーピングに対応していること。</p> <p>f 個々のスイッチ ポートにセキュリティポリシーを適用できること。</p> <p>g ブリッジ プロトコル データ ユニット (BPDU) ガードをサポートすること。</p> <p>h スパニングツリー ルート ガード (STRG) をサポートすること。</p> <p>i Secure Shell (SSH) Protocol、Kerberos 及び簡易ネットワーク管理プロトコル バージョン 3 (SNMPv3) をサポートすること。</p> <p>j CPU (コントロールプレーン) への通信のレート・リミッタ機能を有すること。</p>
障害検知	ハードウェアの障害や異常を検知し、SNMP トラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	37.1W 以下であること。
その他	<p>a. マルチモードの 1000BASE-SX SFP を 20 個用意すること。</p> <p>b. 以下の場所に設置し、西研究棟・東制作棟等ネットワーク基幹 L3 スイッチと接続すること。配線は既設のものを流用すること。 (ア) 西研究棟 1 階、2 階、4 階、5 階、6 階、7 階:各 1 台 (イ) 東制作棟 1 階:1 台</p>

16.1.43 西研究棟・東制作棟等ネットワークアクセススイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

33台

② 仕様

項目	仕様など
インターフェース	a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。 b SFP 光ファイバーポートを 4 ポート以上搭載可能なこと。
スイッチファブリック	56Gbps 以上であること。
パケット処理能力	41Mpps 以上であること。
ネットワーク機能	a IEEE 802.1s/w 高速スパンニングツリープロトコル(RSTP)をサポートすること。 b Per-VLAN Rapid Spanning Tree(PVRST+)をサポートすること。もしくはPVST+をサポートすること。 c IEEE802.1Q VLAN トランク機能をサポートすること。 d 64 個以上の VLAN をサポートすること。 e ネットワーク管理機能として、Web UI及び CLI を利用できること。
障害検知	ハードウェアの障害や異常を検知し、SNMP トラップで通知する機能を有すること。
筐体	a 19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	30W 以下であること。
その他	a. マルチモードの 1000BASE-SX SFP を 6 個用意すること。 b. 以下の場所に設置すること。LAN ケーブル配線は既設のものを流用すること。2 台を予備機として保管すること。 (ア) 西研究棟 2 階、3 階、4 階、5 階、6 階、7 階、8 階:計 26 台 (イ) 東制作棟 2 階、PRIME セミナールーム:計 2 台 (ウ) 学生課:1 台 (エ) エネルギーセンター:1 台 (オ) 仮想環境研究施設:1 台

16.1.44 インターネットVPN用ファイアウォール

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

2台

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 8 ポート以上有すること。 b 1GbE SFP インターフェースを 8 ポート以上有すること。 c 10GbE SFP+インターフェースを2ポート以上有すること。
スループット	<ul style="list-style-type: none"> a ファイアウォールスループットは、10Gbps 以上の性能を有すること。 b IPSec VPN スループットは10Gbps以上の性能を有すること。
同時接続数	ファイアウォール同時セッション数が 3,000,000 以上の性能を有すること。
機能	<ul style="list-style-type: none"> a ゲートウェイ間 IPSec VPNTunnelは2000以上の接続を有すること。 b ファイアウォール機能及び各 UTM 機能の負荷を軽減するために ASIC を搭載していること。 c Active-Active, Active-Standby いずれの冗長構成も可能なこと。
管理	Web ベースの GUI及び CLI による管理機能を有すること。
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	19 インチラックに搭載可能な 1U 以下の大きさであること。
その他	<ul style="list-style-type: none"> a 本部側は固定グローバルIPアドレス、各学習センター及びサテライトスペース側は動的IPアドレスにて拠点間VPNが確立できること。 b 回線側の選定によりマルチモードの 10000BASE-SX SFP+もしくは 1000BASE-SX を 2 個以上用意可能なこと。

16.1.45 SINET接続用外部L2スイッチ

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1台

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a. 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。 b. SFP 光ファイバーポートを 4 ポート以上搭載可能なこと。
スイッチファブリック	50Gbps 以上であること。
パケット処理能力	40Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a. IEEE 802.1s/w 高速スパニングツリープロトコル(RSTP)をサポートすること。 b. Per-VLAN Rapid Spanning Tree(PVRST+)をサポートすること。 c. 全スイッチポートで、ダイナミックトランクを設定できること。 d. IEEE 802.3ad 準拠のデバイスでイーサネット チャネリングを作成できること。 e. Internet Group Management Protocol(IGMP)スヌーピングに対応していること。 f. 個々のスイッチ ポートにセキュリティポリシーを適用できること。 g. ブリッジ プロトコル データ ユニット(BPDU)ガードをサポートすること。 h. スパニングツリー ルート ガード(STRG)をサポートすること。 i. Secure Shell(SSH)Protocol、Kerberos及び簡易ネットワーク管理 j. プロトコル バージョン 3(SNMPv3)をサポートすること。
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	a. 19 インチラックに搭載可能な 1U 以下の大きさであること。
消費電力	40W 以下であること。

16.1.46 RADIUS認証サーバ

- (1) ハードウェア又は仮想サーバに関し、以下の仕様を満たすこと。
 - ① 調達台数
2台
 - ② 管理・運用の観点から、アプライアンス製品であること。
- (2) ソフトウェアに関し、以下の仕様を満たすこと。
 - ① RADIUS機能を有し、本調達におけるネットワークシステムと連携したネットワーク認証を提供すること。
 - ② 外部のActive Directory、LDAPサーバにあるアカウント情報を参照し、認証情報として利用することができる機能を有すること。
 - ③ 管理画面はWebブラウザかつ日本語で表示できる機能を有すること。
 - ④ マスタ、スレーブの冗長構成とし、マスタからスレーブに対して設定情報の同期ができる機能を有すること。
 - ⑤ 認証プロトコルとして、以下に対応していること。
 - PAP
 - CHAP
 - MSCHAPv1
 - MSCHAPv2
 - EAP-TLS
 - PEAP(EAP-MSCHAPv2/EAP-TLS)
 - EAP-TTLS(PAP/CHAP/MSCHAPv2/EAP-MSCHAPv2/EAP-TLS)
 - EAP-MD5
 - EAP-MSCHAPv2
 - ⑥ MAC認証の際、MACアドレスの区切り文字やパスワードに関わらず認証を成功する機能があること。
 - ⑦ RADIUSクライアントをグルーピングできる機能を有すること。
 - ⑧ 標準及び任意の追加されたRADIUS属性の応答に対応していること。
 - ⑨ ライセンス数に関わらずRADIUSクライアントを最大10,000台登録できる機能を有すること。
 - ⑩ 標準及び任意の追加されたRADIUS属性の応答に対応していること。
 - ⑪ RADIUSプロキシサーバとして動作できる機能を有すること。
 - ⑫ realmごとに転送先RADIUSサーバを指定できる機能を有すること。
 - ⑬ システムの稼動ログやアプリケーション動作ログを集約し、ログ管理サーバへ転送する機能を有すること。
 - ⑭ NTP(RFC 1305)機能を有すること。本学園より指示されたネットワークタイムサーバと定期的に時刻同期

をする設定を行うこと。

16.2 学習センター及びサテライトスペース

学習センター及びサテライトスペースには、面接授業の実施や学生証発行など学生に対するサービスの提供を行うために必要な機能を実現するため、ネットワーク環境、パソコン環境が配置されている。各機器は以下の要件を満たすこと。

- (1) 学習センター及びサテライトスペースには、学習系セグメント及び事務系セグメント、教員系セグメント、図書系セグメントを用意すること。
- (2) 学習センター及びサテライトスペースの学習系セグメント、教員系セグメントにおいて DHCP サービスを提供すること。
- (3) DHCP サービスにおいて、許可された MAC アドレス以外への IP アドレス割当をしない仕組みを用意すること。各学習センター及びサテライトスペースの DHCP サービスにおいて、許可する MAC アドレスの登録数は 100個以上とすること。
- (4) 本部に設置されるサーバが提供するサービスと、セキュアな通信を行うために IP-SecVPN接続環境と、インターネット接続環境(回線は本調達外)を提供すること。
- (5) 全国 50 箇所の学習センター及び 7 箇所のサテライトスペースからの利用を想定し、最適な機器構成を提案すること。

16.2.1 学習センターファイアウォール

(1) 本項目の物品については以下①、②を満たす数量、機種を調達すること。下記(2)の要件に従い、調達及び作業を行うこと。

① 調達台数

60 台（導入場所については、「表 2 PC 以外導入台数一覧」を参照のこと。）

② 機種

Fortinet 社製 FG-40F

(2) 要件

- ① 製品メーカーのセンドバック保守を、本システムの契約終了日(令和 11 年 3 月 31 日)までとすること。
- ② 本学園が提供する学習センターファイアウォールを、全国50ヶ所の学習センター及び7ヶ所のサテライトスペースに設置し、利用者(教員、学生、職員)への各種サービス(認証サービス、インターネットサービス、本部各種サーバへのアクセス等)に必要な最適な設定を実施すること。
- ③ 設定実施については、学習センター、サテライトスペースのネットワーク環境、利用機器を十分に調査、検討を行い、本学園の承認の下、利用者への影響を極力与えないように設定を実施すること。

16.2.2 学習センタースイッチング HUB

(1) 本項目の物品については本学園から提供することとする。下記(2)作業要件に従い、設定を行うこと。

① 提供台数

218 式（導入場所については、「表 2 PC 以外導入台数一覧」を参照のこと。）

② 機種

Netgear社製 JGS524-300JPS 等

(2) 作業要件

① 本学園が提供するスイッチング HUBを、全国50ヶ所の学習センター及び7ヶ所のサテライトスペースに設置し、利用者（教員、学生、職員）への各種サービス（認証サービス、インターネットサービス、本部各種サーバへのアクセス等）に必要となる最適な設定を実施すること。

② 設定実施については、学習センター、サテライトスペースのネットワーク環境、利用機器を十分に調査、検討を行い、本学園の承認の下、利用者への影響を極力与えないように設定を実施すること。

16.2.3 無線LAN 用アクセスポイント

(1) 本項目の物品については本学園から提供することとする。下記(2)作業要件に従い、設定を行うこと。

① 提供台数

101 式（導入場所については、「表 2 PC 以外導入台数一覧」を参照のこと）

② 機種

BUFFALO 社製 WAPM-AG1266R+ 等

(2) 作業要件

① 本学園が提供する無線 LAN 用アクセスポイントを、「表 2 PC以外導入台数一覧」記載の無線 LAN 用アクセスポイント導入学習センター、サテライトスペースに設置し、利用者（教員、学生、職員）への各種サービス（認証サービス、インターネットサービス、本部各種サーバへのアクセス等）に必要となる最適な設定を実施すること。

② 設定実施については、学習センター、サテライトスペースのネットワーク環境、利用機器を十分に調査、検討を行い、本学園の承認の下、セキュリティを十分に考慮し、設定を実施すること。

16.2.4 事務用 PC

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

471 台（導入場所については、「表 1 PC 導入台数一覧」を参照のこと）

② 仕様

ノート PC とする。

項目	仕様など
CPU	CPU は、インテル Core i5 プロセッサ 同等以上の機能を有するものを搭載すること。
メモリ	8GB 以上有すること。
記憶装置	SSD 256GB 以上を有すること。
ネットワーク	10BASE-T/100BASE-TX/1000BASE-T、WakeUp-On-LAN 対応であること。
無線 LAN	内蔵し、IEEE802.11a/b/g/n/ac に対応していること。
ディスプレイ解像度	1,920× 1080 ドット以上、1,600 万色以上の 13.3 インチ以上のワイド液晶ディスプレイであること。
インターフェース	<ul style="list-style-type: none"> a USB ポートは、Type-A USB3.0 以上を 2 ポート以上、Type-C（ディスプレイ出力対応）を1ポート以上有すること。 b Bluetooth(5.1以上)の機能を有すること。 c HDMI 端子を 1 ポート以上有すること。 d ヘッドフォン/マイクコンボポート、ヘッドフォン/スピーカージャック又はユニバーサルジャックを有すること。
マウス	有線接続の光学式ホイールマウスであること。
カメラ	内蔵していること。
スピーカ	内蔵していること。

(2) ソフトウェアに関し、以下の仕様を満たすこと。

① OS 及びインストールするソフトウェアは、「表 3 事務用ソフトウェア一覧」に示す。

② OS については、導入時点で最新版のセキュリティパッチを適用すること。

③ 商用ウイルス対策ソフトウェアを導入しリアルタイム検索によりウイルスの検出が実施できること。また、定期的に全てのファイルをチェックするように設定すること。なお、ウイルスを検知した場合は自動的にウイルスを駆除する処理を行うこと。

④ 「16.1.31 事務用クライアント管理サーバ」に示したソフトウェア仕様を満たすため、必要に応じてエージェントソフトウェアをインストールすること。

⑤ 管理者権限のアカウント及びパスワードを職員に公開することなく、管理者権限を必要とするソフトウェアのインストールができること。

⑥ 教務情報システム(システム WAKABA)を利用するために必要な設定を、Web ブラウザに施すこと。設定内容は本学園より提供する。

16.2.5 学生用プリンタ（モノクロ）

(1) ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

学生用プリンタ 102 式

(導入場所については、「表 2 PC 以外導入台数一覧」を参照のこと。)

② 仕様

項目	仕様など
種類	モノクロレーザプリンタかモノクロ LED プリンタであること。
印刷速度	30 枚/分(A4 縦送り)以上の印刷速度を有すること。
給紙サイズ	a. A4 用紙に対応可能であること。 b. ラベル用紙に対応していること。
印刷解像度	1200×1200dpi に対応すること。
インターフェース	a. 10BASE-T と 100BASE-TX を自動認識可能なネットワーク接続インターフェースを有すること。 b. TCP/IP に対応可能であること。
両面印刷機能	両面印刷が可能であること。
給紙トレイ	不定型用紙のセットが可能であること。

16.2.6 文京学習センター用 L2 スイッチ

(1) 文京学習センター用 L2 スイッチA

ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

1台

② 仕様

項目	仕様など
インターフェース	<ul style="list-style-type: none"> a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 24 ポート以上有すること。 b SFP 光ファイバーポートを 4 ポート以上搭載可能なこと。
スイッチファブリック	56Gbps 以上であること。
パケット処理能力	41Mpps 以上であること。
ネットワーク機能	<ul style="list-style-type: none"> a IEEE 802.1s/w 高速スパンニングツリープロトコル(RSTP)をサポートすること。 b Per-VLAN Rapid Spanning Tree(PVRST+)をサポートすること。もしくはPVST+をサポートすること。 c IEEE802.1Q VLAN トランク機能をサポートすること。 d 64 個以上の VLAN をサポートすること。 e ネットワーク管理機能として、Web UI及び CLI を利用できること。 f VLAN トランキング・プロトコル機能を有すること。 g スタック専用ポートを必要とせずに単一のIPを用いて最大8台のスイッチを管理できること。
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	<ul style="list-style-type: none"> a 19 インチラックに搭載可能な 1U 以下の大きさであること。 b ファンレスであること。
消費電力	30W 以下であること。
その他	1000BASE-LX/LH のSFP を 2 個用意すること。

(2) 文京学習センター用 L2 スイッチ B

ハードウェアに関し、以下の仕様を満たすこと。

① 調達台数

2台

② 仕様

項目	仕様など
インターフェース	a 10BASE-T/100BASE-TX/1000BASE-T インターフェースを 8 ポート以上有すること。 b SFP 光ファイバーポートを 2 ポート以上搭載可能なこと。
スイッチファブリック	20Gbps 以上であること。
パケット処理能力	14Mpps 以上であること。
ネットワーク機能	a IEEE 802.1s/w 高速スパンニングツリープロトコル(RSTP)をサポートすること。 b Per-VLAN Rapid Spanning Tree(PVRST+)をサポートすること。もしくはPVST+をサポートすること。 c IEEE802.1Q VLAN トランク機能をサポートすること。 d 64 個以上の VLAN をサポートすること。 e ネットワーク管理機能として、Web UI及び CLI を利用できること。 f VLANトランキング・プロトコル機能を有すること。 g スタック専用ポートを必要とせずに単一のIPを用いて最大8台のスイッチを管理できること。
障害検知	ハードウェアの障害や異常を検知し、SNMPトラップで通知する機能を有すること。
筐体	a 1U 以下の大きさであること。 b ファンレスであること。
消費電力	15W 以下であること。
その他	1000BASE-LX/LH のSFP を 2 台で合計 2 個用意すること。

16.3 ASP サービス

本学園では、学生メールサービスと Web 会議システムについて、ASP サービスを利用している。今回の調達でも継続して、学生メールサービスと Web 会議システムは ASP サービスを利用することとする。最適な ASP サービス及びライセンス数を提案すること。

16.3.1 標的型攻撃メール対策兼スパム対策サービス

標的型攻撃メール対策及びスパム対策機能を TREND MICRO 社製 Email Securityの機能で提供すること。

機能に関し、以下の仕様を満たすこと。

- ① 本システムの契約終了日まで有効なライセンスを提供すること。そのために必要な費用は本調達に含めること。
- ② ウイルス対策として、サンドボックスによる未知の脅威への動的解析機能を有していること。
- ③ メール の 件 名、本 文 及 び 添 付 ファイル 内 に 含 ま れ る URL が 不正 な も の か 検 査 で き る こと。検 査 の 結 果、未 知 の 脅 威 を 検 知 し た 場 合 は サ ン ド ボ ッ ク ス に て 解 析 を 行 う こと。
- ④ システムの稼働ログやアプリケーション動作ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。
- ⑤ IP レベルでのスパムフィルタリング機能を有していること。
- ⑥ 同じ接続元からの連続した接続を一定時間遮断する機能を有していること。
- ⑦ オンライン経由でのアップデート機能を有していること。
- ⑧ 管理者がメールのサイズや添付ファイル数でスパムとして扱う機能を有していること。
- ⑨ スパム判定したメールをそのまま配送・隔離・件名にスパムマーキングを挿入・ヘッダにスパムマーキングを挿入が可能なこと
- ⑩ スパムと判定されたメールは、サーバ内に隔離され、利用者による Web 画面からの指定により、再送が可能なこと。
- ⑪ 隔離したメールの一覧を知らせるレポート送信機能を有すること。
- ⑫ 各利用者が個人毎の管理画面からホホワイトリスト・ブラックリストの登録が可能なこと。
- ⑬ 利用者管理に LDAP と連携が可能なこと。
- ⑭ 運用業務における定例会議資料に必要となるスパム統計情報を取得できること。

16.3.2 URLフィルタリングサービス

URLフィルタリング機能を TREND MICRO 社製 Web Securityの機能で提供すること。

機能に関し、以下の仕様を満たすこと。

- ① 本システムの契約終了日まで有効なライセンスを提供すること。そのために必要な費用は本調達に含めること。
- ② 事務端末からのインターネットアクセスの際のフィルタリング機能として導入すること。
- ③ フィルタリングの設定内容は本学園と協議すること。
- ④ 監査ログを集約し、監視、解析できるようにログ管理サーバへ転送する機能を有すること。

16.3.3 Web 会議システム

本学園の学生と教員が遠隔ゼミを実施できる Web 会議システムを ASP 方式で提供すること。

同時 50 人が利用でき、会議室数を同時利用者数まで自由に増減できること。なお、1会議室あたりの最大入室人数は 50 人とする。

(1) 映像品質

- ① 映像は最大解像度 Full HD(1920×1080)で表示が可能であること。
- ② 映像の表示サイズにあわせて解像度の自動調整機能があること。
- ③ 回線の帯域にあわせて自動でフレームレートを調整する機能があること。

(2) レイアウト機能

- ① 映像の表示レイアウトを変えられること。
- ② 講師や発表者など特定参加者を大画面で、それ以外の参加者を小画面で表示ができること。
- ③ 映像を別ウィンドウ表示にして複数モニタで表示が可能なこと。

(3) 資料共有機能

<アプリケーション共有>

- ① 参加者が起動したアプリケーション画面を共有で閲覧ができること。
- ② 遠隔から他拠点で起動しているアプリケーションの操作が可能なこと。
- ③ 共有時にデスクトップ全体を見せることなく、特定アプリケーションの画面のみを共有閲覧できること。

<デスクトップ共有>

- ① 会議参加者のデスクトップを共有して遠隔から操作可能なこと。
- ② 会議参加者のデスクトップを共有する際、遠隔操作の要求に対して承諾や拒否ができること。

<ホワイトボード>

- ① パソコンのキーボード、マウス、タッチパッド、ペンタブレットを使って、相互に文字や絵の書込みができるホワイトボードの機能があること。

<ファイル転送>

- ① Web 会議システム内で、参加者に対してファイルを配布できること。

<チャット機能>

- ① 会議中に全員とテキストチャットができること。
- ② 会議中に特定の人とだけテキストチャットができること。
- ③ テキストチャットの会話ログの印刷や保存ができること。
- ④ チャット画面にクリック可能な URL リンクを貼り付けられること。

(4) 周辺機器操作機能

- ① 全ての参加者は、ワンクリックで自らのカメラ・マイク・スピーカーのオンオフを変更できること。
- ② カメラ・マイク・スピーカーの設定は、会議中に Web 会議システム内で変更ができること。

(5) その他の会議機能

- ① Web 会議用アカウントを持っていないユーザに対しては、URL 付の招待メールを送るだけで Web 会議に無料で参加させることができること。
- ② 参加者全員がマイクオフの会議であっても、参加者がアイコンなどをクリックするだけで、議長や講師の画面上に発言の意思を表示できること。その際、どこの拠点からリクエストがあったのか議長や講師が容易に把握できること。
- ③ 会議参加者のリスト一覧の表示・非表示が可能なこと。
- ④ 会議中に参加者の権限や機能制限を変更できること。
- ⑤ 会議・講義の録画をローカルストレージとクラウドストレージに選択的に保存することができること。
- ⑥ 録画データは汎用的な動画再生アプリケーションで再生できること。
- ⑦ 会議の録画データを保存できるクラウドストレージがあること。

- ⑧ 会議開始時に自動で録画を開始する設定ができること。
- ⑨ iOS、Android に対応したモバイル端末で会議・講義に参加できること。

(6) 管理者機能

<会議設定機能>

- ① 会議予約時に会議招待の URL を生成できること。

(7) セキュリティ機能

- ① TLS, AES など暗号化された通信を行っていること。
- ② 会議室をロックして新規の入室を禁止する機能があること。
- ③ 不適切な会議参加者を強制的に退室させる機能があること。

(8) その他

- ① 大学本部において、教員及び職員向けに Web 会議システムの利用に関する説明会を毎年度1回以上開催すること。
- ② 利用に関わる内容について簡易オンラインマニュアルを準備すること。

16.3.4 ASP メールサービス

(1) ASP メールサービスに関し、以下の仕様を満たすこと。

- ① Google 社提供 Google Workspace のGmail サービスを継続利用できるようにすること。利用可能アカウント数は、学生用として、300,000 アカウント、教職員用として、60,000 アカウントである。
- ② 学校ドメイン(本学園ドメイン)でメールアドレスが発行できること。
- ③ 利用者は、本学園の学生・教職員(申請者のみ)とする。
- ④ 利用者は、本部・学習センター及びサテライトスペースからだけでなく、自宅等のインターネット接続環境からも ASP メールサービスが利用できること。
- ⑤ 利用者はブラウザを用いてメールサービスが利用できること。
- ⑥ POP を使用して、メッセージをダウンロードできること。接続は SSL を利用すること。
- ⑦ ウイルス、迷惑メール、フィッシング対策を有していること。
- ⑧ ASP メールサービス上の学生の氏名を学生自身に変更できること。ASP メールサービス上の学生の氏名を変更した際に、LDAP サーバ上の当該学生の氏名は変更されないこと。

16.3.5 ASP ファイルサービス

(1) ASP ファイルサービスに関し、以下の仕様を満たすこと。

- ① 利用者は、本学園の学生・教職員（申請者のみ）とする。
- ② 利用者は、本部・学習センター及びサテライトスペースからだけでなく、自宅等のインターネット接続環境からも ASP ファイルサービスが利用できること。
- ③ 利用者はブラウザを用いてファイルサービスが利用できること。

17 作業要件

17.1 システム構築

- (1) システム構築作業を行なうにあたり、作業体制図、作業スケジュール等を作成し、本学園の承認を受けること。
- (2) 受託者は、対象機器を指定した場所(本部、学習センター、サテライトスペース)に対して搬入、据付、配線、調整作業を行なうこと。
- (3) 本部のネットワーク機器、サーバ機器は本学園が指定するラックに搭載すること。指定ラックはシュナイダーエレクトリック社製19 インチラック AR3100である。
- (4) 分電盤からラックまでの間で必要な電源工事を実施すること。なお、分電盤の工事は含めないものとする。
- (5) 幹線ネットワーク
 - ① 現在、サーバ室のネットワーク機器にて構成されている幹線ネットワークを、本調達機器(外部接続L3スイッチ、回線負荷分散装置、共通基盤L2スイッチ、共通基盤ファイアウォール等)にて構成すること。設置場所は放送研究棟1階サーバ室とする。
 - ② 外部接続用ネットワークは、SINET回線(10Gbps)、KDDI(100Mbps)の2回線を有しており、回線冗長構成をとること。
 - ③ 幹線ネットワークと共通基盤DMZ、研究系ネットワーク等、本調達機器によって構成する各支線ネットワークを接続すること。
 - ④ 作業に関し、具体的な各移行計画、ラック収容計画を提案すること。
- (6) 本学園指定の事務用 PC に対して、教務情報システム(システム WAKABA)で使用する、証明書発行用プリンタ、学生証印刷用プリンタ、出欠管理用バーコードリーダ、磁気カードリーダの接続設定、学生証・エキスパート認証の定義データの設定及び学生証印刷カードプリンタ用ソフト(CardPAS)のインストール作業を手順書に従って、本部、各学習センター及びサテライトスペースにおいて実施すること。必要なドライバソフト、定義データ及び手順書は本学園から支給する。なお、問題が発生した場合には、システム WAKABA 導入業者と協力して解決すること。
- (7) その他ソフトウェア及びドライバ等について、本学園より指示のあった際に協議の上、事務用 PC に対して稼動確認を行い、稼動を保証できる場合はインストール及び設定を行うこと。
- (8) ネットワーク機器、サーバ機器の設置にあたり納品物以外で必要となる配線ケーブル類、及びその他物品等は、受託者で用意し、費用も受託者が負担すること。
- (9) 導入機器に対して、リース物品管理シールとは別に管理上識別が可能なラベルを貼り付けること。端末のラベルについてはラベルケースを張り付けた上ラベルを挿入すること。色・記載内容については本学園より別途指示する。
- (10) 本学園にて稼動中の既存システム(オンライン授業システム、財務会計システム、人事給与システム、教務情報システム等)に影響を与えることがないようにデータ転送等の容量を考慮し、本学園と協議の上、システム構築を行うこと。

- (11) 既存システムの調査及び確認を実施する際は、本学園と協議の上承認を得ること。
- (12) 機器納入又は設置時等に発生した空箱、廃材は受託者にて廃棄・処分すること。
- (13) 本システムの各種運用に関する設計書(サーバ構成、ネットワーク構成、ハードウェア・ソフトウェア台帳、保守情報、導入機器における設定情報)を作成し、本調達範囲の運用要員に対する教育を実施すること。
- (14) サーバ室に設置するネットワーク機器、サーバ機器を対象とした稼動監視環境を構築すること。主たる稼動監視項目については、死活監視、プロセス監視、ログ監視、リソース監視を細分化して実施することとし、本学園の承認を得ること。
- (15) 運用における定常業務(本部サーバ室内機器の目視確認、各システムの動作確認、導入する機器に対するリソース利用状況確認、ユーザ登録/変更/削除、クライアント PC のパッチ適用手順、システム統計情報の集計等)、及び非定常業務(障害発生時の対応方法等)に関するマニュアルを作成し、本調達範囲の運用要員に対する教育を実施すること。
- (16) サーバ室に設置するネットワーク機器又はサーバ機器に障害が発生した場合、障害の発生時に電話又は電子メールにより本学園に通知を行う監視環境を構築すること。
- (17) 環境設定等に必要なケーブル等消耗品は、受託者で用意すること。
- (18) 本システムの構築で作成されるシステムアカウントに関して、パスワード設定の必要が無いものにはパスワードを設定せずログイン不可とし、パスワードの設定が必要なものには脆弱性の無いパスワードを設定して適切に管理すること。
- (19) 本システム構築時に作成する作業用アカウントは本学園の承認の上必要最小限とし、脆弱性の無いパスワードを設定して適切に管理すること。構築終了後、不必要な作業用アカウントは速やかに削除すること。やむを得ず残すアカウントに関しては、本学園と本調達範囲の運用支援業務要員に、情報を確実に引き継ぐこと。
- (20) 本システム構築後の運用が円滑に実施できるように運用設計を行い、本調達範囲の運用支援業務要員に引継ぎを行うこと。なお、引継ぎに必要な環境及び機材については受託者にて準備すること。
- (21) 運用支援業務を行う際に必要となるパソコン等の機器を準備及び環境を構築し、本調達範囲の運用支援業務要員に引き渡すこと。
- (22) 運用開始後、構築の不備に起因する問題が発生し、運用支援業務要員から問題解決への協力の要請があった場合は、直ちに本調達範囲の運用支援業務要員と協力して解決を図ること。
- (23) 納品時点の全てのサーバ機器のシステムバックアップ、及び全ての機器の設定情報のバックアップを取得し、いつでもリストア可能な状態とすること。

17.2 データ移行

データ移行については、移行計画書、及び移行設計書を作成し、本学園の承認を得ること。移行作業実施については、利用者への影響を極力少なくなるよう調整し実施すること。

- (1) 既存の広報用 Web サイトのコンテンツを広報用 Web サーバへ移行し、正常に動作させること。移行対象については、本学園と協議の上決定する。
- (2) 科目ナビ、番組表、授業科目案内のコンテンツを広報用 Web サーバへ移行し正常に動作させること。また、同ホームページにおいて稼動しているアクセシビリティサポート機能(日立公共システムエンジニアリング社製アクセシビリティサポートソフトウェア「ZoomSight」)に関して、全ての機能を移行し設定すること。「ZoomSight」は本学園より提供する。
- (3) 現在利用しているグループウェアに関して、システム移行時点で保存されている全利用者の受信及び送信済みメールデータを移行すること。
- (4) 現在利用している教職員メールに関して、システム移行時点で保存されている全利用者のメールデータを移行すること。
- (5) 現在利用しているグループウェア上で稼動している掲示板機能に関して、本学園と協議の上システム移行時点で保存されている投稿文書(添付ファイルも含む)を移行すること。
- (6) 現在利用している本部用共有ファイルサーバに関して、システム移行時点で保存されている全利用者のデータを移行すること。その際、アクセス権等も保持した状態で移行すること。
- (7) 事務用 PC について、PALLET CONTROL with 秘文を用いて秘文フォーマットされた外部媒体を継続的に利用できること。もしくは、同等以上の機能を有するソフトウェアにおいて、秘文フォーマットされた外部媒体を支障なく円滑、簡便に利用可能な手段を提供すること。また、本学園と協議の上、承認を得られた場合のみ、別の運用方法としてよい。
- (8) 現在利用している LDAP サーバに登録されているアカウント情報を、本システムの LDAP サーバに移行すること。この際、利用者によるパスワードの再設定を実施することなく移行すること。また、今回必要となる属性については、本学園と協議の上決定すること。なお、LDAP サーバを参照している本調達外のシステムについて、LDAP サーバが更新されることに伴い設定変更が必要となった場合その作業は本調達には含まないものとするが、本学園、及び本調達外のシステムの運用保守業者と協力して正常動作を確認すること。
- (9) 現在利用している事務用ドメインコントローラに登録されているユーザ情報を、本システムの事務用ドメインコントローラに移行すること。なお、事務用ドメインコントローラと財務会計システム内ドメインコントローラは信頼関係を設定しているため、信頼関係の再設定が必要であるが、財務会計システム側の設定作業は本調達には含まないものとする。
- (10) データ移行において、配線ケーブル類、ハブやメディアコンバータ等の部材や機器が必要となる場合は、受託者で用意し、費用も受託者が負担すること。

17.3 テスト

(1) システム結合テスト

システム結合テストは、本部、学習センター及びサテライトスペースに設置する、本調達内の導入機器やソフトウェア、サービスについて、問題なく動作することを確認するテストである。

テスト計画書、テスト仕様書を作成し、本学園の承認の下、以下についてテストを実施すること。なお本部、学習センター及びサテライトスペースに機器を設置する際は、本学園、及び既設情報基盤システム保守業者、情報基盤システム運用支援業者と十分に協議し、極力本学園業務に影響を与えないようにすること。また、発生した費用については受託者が全て負担すること。

- ① ネットワーク構成について、本システム設計の妥当性を確認すること。また、システム内及び本部、学習センター及びサテライトスペースとのネットワーク疎通の確認、及びアプリケーションの動作との整合性を確認すること。
- ② 利用者サービス(Web サービス、DNS サービス、プロキシサービス、認証サービス、グループウェア、メールサービス等)、及び運用管理(バックアップ、ログ収集等)について、本システム設計の妥当性を確認すること。
- ③ 本調達範囲内の全ての PC について、本学園の指示に従って設置し、各 PC におけるソフトウェアの動作、及びプリンタ出力等を確認すること。なお、各 PC について電源オンから利用できるようになるまでの時間が短くなるよう調整を行い、利用に支障をきたさないこと。
- ④ ASP サービスである Web 会議システム、及び ASP メールサービス、ASP ファイルサービスについて、本部、学習センター及びサテライトスペースで事務用 PCを用い正常に動作することを確認すること。
- ⑤ 本調達内の各機器について、異常が発生又は発生する予兆を検知し、本学園に通知する仕組みを構築し、問題なく動作することを確認すること。
- ⑥ ネットワーク機器に対するパラメータ調整を実施し、システム内及び本部、学習センター及びサテライトスペースとのネットワーク疎通の確認、及びアプリケーションの動作との整合性を確認すること。

(2) システム総合テスト

システム総合テストは、本学園にて稼動中である、本調達外のシステム(教務情報システム、財務会計システム、人事給与システム等の本学園基幹システムや、オンライン授業システム、Web 通信指導支援システム、ネット配信システム、自己学習サイト、放送授業インターネット配信システム、Web通信指導システム等)と正しく連携できることを確認するテストである。

テスト計画書、テスト仕様書を作成し、本学園の承認の下以下についてテストを実施すること。テストの実施については、本学園と協議を行い、各システムの動作を確認すること。なお、問題が発生した場合は、本学園と協議の上、問題解決にあたること。

- ① 教務情報システムについて、Web サービス、業務サービスが正常に動作する事を確認すること。
- ② 財務会計システムについて、Web サービス、業務サービスが正常に動作する事を確認すること。
- ③ 人事給与システムについて、業務サービスが正常に動作することを確認すること。

- ④ その他、本学園で稼働中のシステムについて、サービスが正常に動作する事を確認すること。
- ⑤ 本調達内で導入する学外に公開するサーバについて、脆弱性診断を実施し、脆弱性が発見された場合は対処を実施すること。

(3) 受入れテスト

受入れテストは、本調達範囲である機能全般について仕様のとおりであるかどうかを確認し、検収可能であるかどうかを判断する事を目的として、本学園が主体となって実施するテストである。受入れテスト実施にあたり、本学園で作成するテスト計画書、テスト仕様書の作成に協力すること。また実施場所は本学園と協議の上、本学園が指定する場所で行うこと。

17.4 運用環境

受託者は、運用支援業者が円滑に運用を行えるよう運用環境を構築すること。

(1) 運用設計

- ① 各種運用管理業務における方針を示した運用設計を行い、本学園の承認を得ること。管理項目としては以下を含めること。
 - 構成管理
管理対象とするHWやSW等の各種情報における管理方針を示したもの。
 - 性能管理
管理対象とするHWの各種リソース情報における管理方針を示したもの。定常業務として行う機器の管理(本部サーバ室内機器の目視確認、各システムの動作確認、導入する機器に対するリソース利用状況確認等)を含めること。
 - 変更管理
構成変更の実施に関する管理方針を示したもの。
 - リリース管理
変更のリリース作業実施に関する管理方針を示したもの。
 - バックアップ管理
バックアップとリストアに関する管理方針を示したもの。テープにおける外部保管に関する内容も含めること。定常業務として行うバックアップ管理を含めること。
 - セキュリティ管理
セキュリティに関する管理方針を示したもの。セキュリティホールに関する対応方針も含めること。
 - ユーザ管理
システム利用者である教職員や学生に関するユーザ管理及びシステム機器管理者のユーザ管理における管理方針を示したもの。
 - 問合せ／作業依頼インシデント管理
利用者からの問合せや各種作業の依頼があった際の対応方針を示したもの。現在の運用業務における作業一覧は本学園より別途提示する。
 - 障害インシデント管理
障害が発生した際における復旧対応方針を示したもの。障害監視の項目についても含めること。
- ② 本調達範囲の運用要員が、運用設計に基づいて運用業務が実施できるよう、各種ドキュメントを整備すること。ドキュメントには以下の内容を含むこと。
 - 運用要件定義書

- 運用設計書
- 運用手順書(運用手順書には、以下の項目が網羅されていること)
 - ・ 運用管理
 - ・ 構成管理
 - ・ 資源管理
 - ・ 性能管理
 - ・ バックアップ管理(リストア手順を含む)
 - ・ セキュリティ
 - ・ ユーザ管理
 - ・ ベンダ管理
 - ・ マニュアル管理
- 障害対応手順書

なお、運用開始後の各種インシデント対応や運用改善に伴うドキュメント更新は運用要員にて行うものとする。

ベンダ管理とは、本調達範囲で導入する製品(ハードウェア及びソフトウェア)に対する保守問合せに必要となる情報を「保守契約一覧表」として整備するものである。

- ③ 既存システムの調査及び確認を実施する際は、本学園と協議の上承認を得ること。

(2) 運用システム構築

- ① 本システムのハードウェア、ソフトウェアを対象とした稼働監視環境を構築すること。主たる稼働監視項目については、死活監視、プロセス監視、ログ監視、リソース監視を細分化して実施することとし、本学園の承認を得ること。
- ② 稼働監視にて障害が発生した場合、電子メール等により本学園に通知を行うこと。
- ③ 納品時点の全てのサーバ機器のシステムバックアップ、及び全ての機器の設定情報のバックアップを取得し、いつでもリストア可能な状態とすること。
- ④ 運用業務において以下の月次報告書を作成できるよう、システムを構築すること。また、報告書の作成方法を示したドキュメントを整備すること。
 - 課題管理一覧
 - インシデント管理台帳

(課題発生・処理件数・残件数の月ごとのグラフ、該当月の課題発生・処理件数の日単位グラフ、該当月の区分(作業・障害・質問・その他)ごとの日単位グラフ、及び詳細一覧)
 - ハードウェア障害発生件数

- Windows Update 更新一覧
 - セキュリティ脆弱性情報
 - ウイルス検知状況
(該当月でのウイルス検知・対処一覧、日付別ウイルス検知件数グラフ、拠点別ウイルス検知
数グラフ、検知したウイルスの内訳グラフ、月別ウイルス検知数グラフ)
 - Web 会議システム利用状況
 - トラフィック状況
(各ネットワーク機器の月毎のInbound/Outbound トラフィックの平均と最大、及び該当月で
のInbound/Outboundトラフィックの平均と最大)
 - サーバリソース状況
(全てのサーバのCPU 使用率、メモリ使用率、ディスク使用率)
(月毎のメール受信・送信件数、該当月での日毎のメール受信・送信・スパムメール件数)
 - Webサイトアクセス解析
 - 広報用Webサイトのサイト毎のページビュー
(日本語サイト、英語サイト、全体)、アクセス機種毎のページビュー(PC, スマートフォン、モ
バイル)、月毎のページビュー推移
 - SSO 利用数(各システム毎延べ数、ユニーク利用者数)
- ⑤ 本学園が支給する運用業務に用いるパソコン等の機器に必要となる設定・環境構築を受託者が
実施し、本調達範囲の運用要員に引き渡すこと。

18 保守要件

本調達に含まれるハードウェア製品、ソフトウェア製品に関する保守期間は令和 11 年 3 月 31 日まで(運用開始より 60 ヶ月)とする。リース機器の保守を行うこと。

18.1 ハードウェア製品保守

- (1) サーバ機器の保守は、24 時間 365 日オンサイトで対応であること。
- (2) ネットワーク機器の保守は、24 時間 365 日オンサイトであること。ただし、以下の機器の保守は記載のとおりとする。
 - 本部 L2 エッジスイッチ:センドバック保守
 - 西研究棟・東制作棟等ネットワークアクセススイッチ:センドバック保守
 - 学習センターファイアウォール:センドバック保守
 - 文京学習センター用 L2 スイッチ:センドバック保守
- (3) クライアント PC の保守は、センドバック保守又はオンサイト保守とする。ただし、本学園より提供する PC は下記の(4)を除き、保守に含めないものとする。
- (4) 本学園より提供する本部事務用PC 端末タイプB 20 台(DELL社製 Latitude 3510)の保守は、製品メーカーのセンドバック保守を、本システムの契約終了日(令和11 年 3 月 31 日)まで延長すること。令和3年3月より4年間のセンドバック保守を持つ。
- (5) プリンタの保守は、月曜～土曜 9:00～17:00 オンサイト対応(年末年始及び日祭日を除く)であること。消耗品は保守に含めないが、定期交換部品の交換対応は保守に含めること。

18.2 ソフトウェア製品保守

- (1) 各サーバに搭載するソフトウェアに関して、パッチの適用、障害分析などの技術的問合せが可能なこと。パッチの適用にあたり、メーカーより修正パッチの提供を受けとれること。
- (2) 各クライアントに搭載するソフトウェア(フリーソフトウェアを除く)に関して、パッチの適用、技術的問合せが可能なこと。

19 業務要件

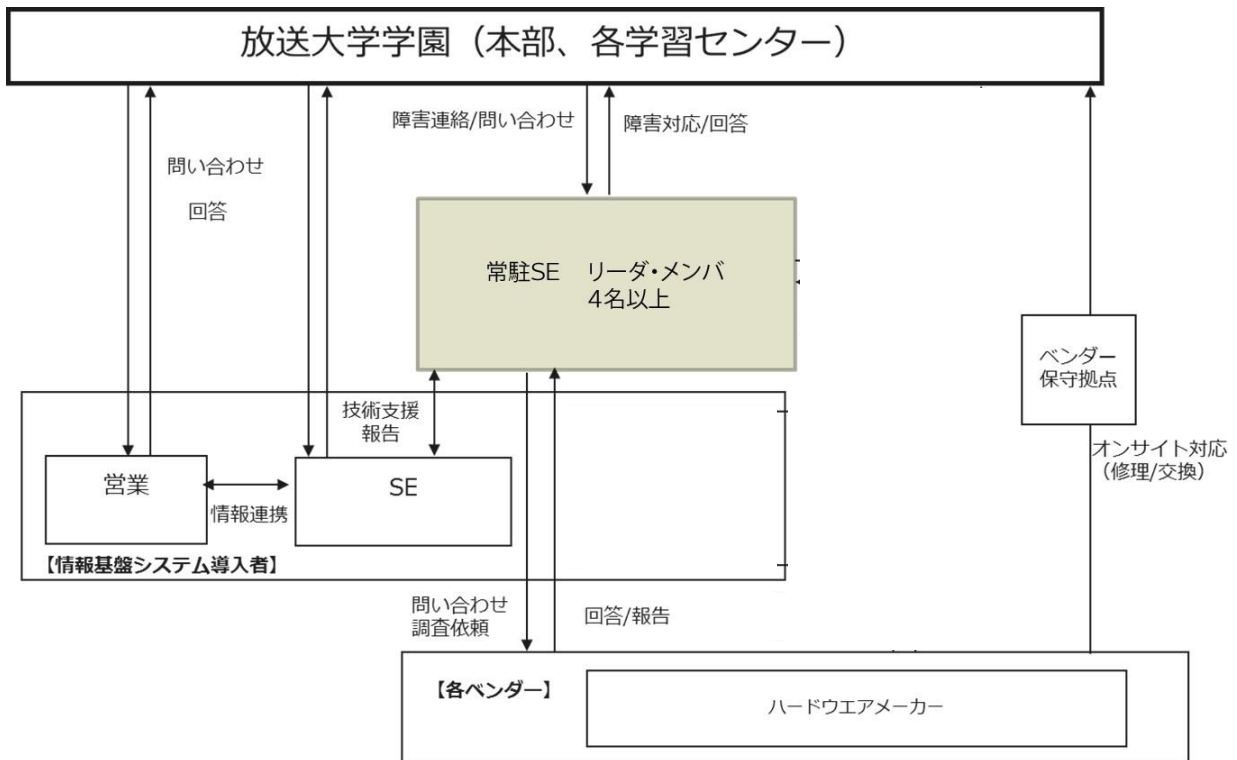


図1 システム運用支援業務体制図

19.1 システム運用支援業務全般

システム運用支援業務の対象は、「表5 運用支援業務対象機器一覧」のとおりとする。

- (1) システム運用支援業務は、本学園本部、千葉学習センターでの現地作業、あるいは保守用回線を介して遠隔で実施することとする。
- (2) 運用支援業務担当者を次のように定義する。それぞれ担当者を置くこと。

- 業務統括 SE

常駐 SE の運用支援業務を統括・監督する SE を置くこと。業務統括 SE は本学園に常駐する必要はないが、常駐 SE とともに、お互いに協力してシステムをサポートすること。

業務統括 SE は、本学園の情報基盤システムの全体像を把握する能力を有すること。サーバ（仮想基盤を含む）・ネットワーク・PC 運用の幅広いスキルを持ち、常駐 SE では判断が難しい事象（特に障害対応等）に対して助言・サポートを行うこと。また、毎月1回の定例会に参加し、運用支援業務全般に関する内容について必要に応じて報告すること。

- 常駐SE

情報基盤システムの運用支援を行う運用支援員を置くこと。常駐SE は本学園本部に常駐すること。

常駐SEは年末年始(12/29-1/3)、祝日を除き、チームの中から以下の時間に記載の人数を常駐させること。ただし、公共交通機関の遅延、自然災害時等による止むを得ない事由の場合はこの限りではない。

平日(月曜を除く)	9時～18時:3名以上
月曜、土曜、日曜	9時～18時:2名以上
繁忙期 (4月上旬5日間程度、7月下旬10日間程度、9月下旬～10月上旬5日間程度、1月下旬10日間程度、3月下旬5日間程度)	8時～9時:1名以上、9時～13時:2名以上、13時～17時:3名以上、17時～18時:2名以上、18時～21時:1名以上

なお、パッチ適用など就業時間(18時)後に処理を行う必要がある場合は、本学園と協議の上決定すること。繁忙期の日程は前年度3月上旬頃に決定する。

常駐SEは、リーダー、メンバ計4名以上でチームを組み業務を行うこと。

リーダーは、以下の要件を満たすこと。

- チーム内の業務を監視し、円滑に運用を行うよう調整できること。また、メンバに対して明確な手順書、指示書を作成することができること。
- 一人で通常業務を任せられる業務スキルを有していること。
- メンバに不足しているスキルがある場合は指導・教育を行うことができること。

メンバは、以下の要件を満たすこと。

- メール、電話対応にてPC初心者に対して専門用語を使わずにわかりやすい説明ができること。
- リーダーの指示に従い、手順書・指示書に従い円滑に業務を実施できること。
- 業務遂行に不足しているスキルがある場合は、身に付ける向上心があること。

また、毎月28日(土日祝日の場合は前営業日)までに、翌月1ヵ月分の常駐SE勤務予定を本学園に提示すること。

- (3) 各運用支援担当者の要員交代がある場合は、交代する2週間前までに本学園に連絡すること。常駐SEの交代の場合は、新しい要員に対する業務の教育計画を事前に提示すること。
- (4) 業務統括SEは、毎年度、運用保守計画を作成し、本学園に提出すること。
- (5) 業務統括SEは、本学園の情報基盤システムに問題点や課題が無いかわかりやすく検証し、問題点や課題がある場合は解決策を提案すること。
- (6) 常駐SEは、障害発生時の原因一次切り分けと原因の特定を行い、問題の解決に当たること。問題

の解決ができない場合は、業務統括 SE が指導し、問題解決に当たること。

- (7) 常駐SE 間で作業依頼・障害インシデント内容等を共有し、利用者からの問い合わせに対しどの常駐 SE でも同じ対応が可能ないように体制を整えること。
- (8) 常駐SE は、障害・不具合については軽微なものであっても必ず本学園へ報告すること。
- (9) 常駐 SE は、日々の業務内容について日報を作成の上、すみやかに本学園へ提出し確認を受けること。
- (10) 常駐 SE は、作業依頼・障害インシデント、問い合わせ対応などについては都度一覧表に記載し、本学園とネットワーク共有できる場所に一覧表を設置すること。共有場所は本学園が提供する。
- (11) 常駐 SE が用いるアカウントは各人個別に作成し、セキュリティに留意したパスワード管理を行うこと。
- (12) 常駐 SE は、出勤日の毎日午前 9:00 に本学園の各種業務システムや、職員・学生・一般向けサービスが正常稼働しているかを確認し、異常が確認された場合はすみやかに本学園へ報告すること。確認対象のサービス一覧は別途本学園から提示する。
- (13) 常駐時間帯に本学園教職員からの障害及び各種問い合わせについて、電話又はメールによる受付窓口を設置すること。電話及びメールは本学園より提供する。障害の際は連絡を受けてから原則として 30 分以内に初期対応を行うこと。また障害解析を開始し、障害解析状況について随時本学園に報告すること。障害復旧作業を行う際は、原則として 2 人作業とし 2 次障害が発生しないよう留意すること。
- (14) システムの保守として以下に対応すること。
 - ① システム操作上の不明点や運用に関する問い合わせ対応
 - ② システムの操作ミスに起因するトラブルへの対応、データ復旧サポート
 - ③ ハードウェア障害の復旧及び原因調査
 - ④ 情報基盤システム導入業者と連携し、障害防止策の策定及び実施
 - ⑤ ソフトウェア障害の復旧及び原因調査
 - ⑥ ネットワーク障害の復旧及び原因調査
 - ⑦ その他何らかの原因でシステムが使用できなくなった場合の復旧対応及び原因調査
 - ⑧ メーカーによる保守を行う場合の各種作業手配
 - ⑨ システム機能追加・改善時の技術サポート
 - ⑩ システム運用や構成変更に対する技術サポート
- (15) 本学園が毎月 1 回開催する定例会議(情報基盤システム)に参加すること。その際、以下の資料を必要に応じて作成し提出すること。作成した資料は報告資料提供サーバ上に保存し、本学園が閲覧できるようにすること。令和 5 年度情報基盤システム運用支援業務の受注業者の資料フォーマットに関しては契約締結後開示を行うので同等のフォーマットで作成すること。

情報基盤システムにおける資料は以下のとおり。

- 課題管理一覧
 - インシデント管理台帳
(課題発生・処理件数・残件数の月ごとのグラフ、該当月の課題発生・処理件数の日単位
 - グラフ、該当月の区分(作業・障害・質問・その他)ごとの日単位グラフ、及び詳細一覧)
 - ハードウェア障害発生件数
 - Windows Update 更新一覧
 - セキュリティ脆弱性情報
 - ウイルス検知状況
(該当月でのウイルス検知・対処一覧、日付別ウイルス検知件数グラフ、拠点別ウイルス
 - 検知数グラフ、検知したウイルスの内訳グラフ、月別ウイルス検知数グラフ)
 - Web 会議システム利用状況
 - トラフィック状況
(各ネットワーク機器の月毎の Inbound/Outbound トラフィックの平均と最大、及び該当月での Inbound/Outbound トラフィックの平均と最大)
 - サーバリソース状況
(「表5 運用支援業務対象機器一覧」の全てのサーバの CPU 使用率、メモリ使用率、ディスク使用率)
(月毎のメール受信・送信件数、該当月での日毎のメール受信・送信・スパムメール件数)
 - Webサイトアクセス解析
 - 広報用Webサイトのサイト毎のページビュー(日本語サイト、英語サイト、全体)、アクセス機種毎のページビュー(PC, スマートフォン、モバイル)、月毎のページビュー推移
 - SSO 利用数(各システム毎延べ数、ユニーク利用者数)
 - その他 特記事項
- (16) 本学園幕張本部外から本学園幕張本部内のサーバへリモート操作を実施する場合は、本学園が提供する VPN 装置等セキュアな接続を利用すること。接続に必要な VPN ソフトウェアは本学園より提供を行う。ただし、利用する PC については、受託者で用意すること。接続方法の詳細については、打ち合わせで調整すること。
- (17) 設定の変更を実施する際は、本学園に許可を得たのち実施すること。設定の変更が他システムへ影響を及ぼす可能性がある場合は、業務統括 SE が行うこと。なお、土日等で本学園へ連絡が取れない場合はリーダーの判断で対応し、翌営業日に本学園へ報告すること。なお、事後報告の際に本学園が不許可と判断した場合は元の設定へ戻すこと。
- (18) 本学園で新たなシステムを追加する際に、情報基盤システムの機器に設定変更を行う必要がある場合は、本学園及び設定変更を行う必要がある機器の導入業者と協議の上、作業実施方針を決定する

- こと。常駐 SE で作業を実施する場合は、本学園が提示する作業手順書に従い作業を実施すること。
- (19) 本学園で新たなシステムを追加する際に、それらのシステムに関する運用業務を依頼する場合があります。本学園から提示する新システムの運用マニュアルに従って運用業務が実施可能か判断し、本学園と協議すること。
 - (20) 保守運用業務を遂行するにあたり、定常業務及び非定常業務に関するマニュアルを作成し、最新化して利用すること。
 - (21) 保守運用業務を遂行するにあたり、構成管理や性能管理等の各運用管理業務における管理方針を順守すること。管理方針の詳細は「17.4.(1) 運用設計」で示している。
 - (22) 業務統括 SE は、保守運用業務全般の問題点や課題を把握し、報告や対策の提案をすること。また、保守運用業務の改善活動を実施すること。

19.2 情報基盤システム

- (1) 調達期間中、「表5 運用支援業務対象機器一覧」の全てのサーバ・ネットワーク機器について、稼働しているソフトウェアに対する脆弱性情報及び不具合情報の収集及び本学園への情報提供を行うこと。脆弱性及び不具合対応については、本学園と必要に応じて情報基盤システム導入業者を含めて協議の上、対応方針を決定すること。作業を実施する場合は、本学園による許可の下脆弱性対応・修正パッチ適用を行うこと。
- (2) 「表5 運用支援業務対象機器一覧」全てのサーバのバックアップ及びバックアップ状況を管理し、必要に応じてテープ媒体を交換すること。また、バックアップテープの遠隔地保管の支援(テープの引き渡し、受け取り)を行うこと。システム障害時は必要に応じて手順書に従いバックアップからリストアを行うこと。バックアップにおいて障害が発生した場合は情報基盤システム導入業者と協力の上、障害解消作業を実施すること。

人事給与システム・財務会計システムについては、本学園から提示する手順書に従いバックアップテープの交換と遠隔地保管の支援を行うこと。
- (3) 計画停電時及び本学園からの要請に応じて、手順書に従いシステムを構成する機器の停止・起動、バックアップ等の作業を行なうこと。
- (4) 対象となるシステムに対して、本学園が指定する期日までに本学園が依頼するユーザ登録・変更・削除を行なうこと。登録するユーザには情報基盤システム利用者や管理者も含まれる。作業後は、適切に作業が完了したかどうかを、ログオン試行等により確認し、本学園に報告すること。
- (5) 本学園からの依頼やネットワークの脆弱性対応等ネットワーク機器、サーバ機器、クライアント機器に関する設定の変更が必要な場合、本学園と情報基盤システム構築業者と協議の上対応方針を決定すること。サーバについては、必要に応じて検証サーバにて検証作業を実施すること。設定変更を行う場合は、状況に応じて情報基盤システム構築業者と協力して作業を行うとともに、作業後は適切に作業が完了したことを確認し、本学園に報告すること。
- (6) サーバ構成、ネットワーク構成、各種機器設定情報、各種バージョン情報を管理すること。また、保守情報を管理すること。

- (7) システムに関する資産を管理すること、内容に変更が生じた場合は本学園に更新版を提出・報告すること。管理する資産としては、DNS 情報、ネットワーク機器及びサーバ機器(設置場所、ホスト名、IP アドレス等)、クライアント機器(設置場所、設置台数、ホスト名、IP アドレス、独自に導入したソフトウェア、利用者名簿等)とする。なお、クライアント機器は「表5 運用支援業務対象機器一覧」の全PCとする。
- (8) 「表5 運用支援業務対象機器一覧」の全ての PC に対する修正パッチ(Windows Update、Java 修正パッチ、Adobe 関連ソフトウェア修正パッチなど)について、動作の検証を実施し、本学園の依頼の下適用すること。パッチの適用に際しては各業務システムへの影響を検証するため、PC のグループを作成し、本学園の各業務システム担当者が検証した後で全 PC へ展開すること。
- (9) 「表5 運用支援業務対象機器一覧」の全ての PC に導入されているソフトウェアについて、導入されているソフトウェア名称と、必要に応じてバージョンを定期的(月1回)に取得し、管理すること。
- (10) ソフトウェア修正プログラムの適用、ソフトウェアの追加については、原則、クライアント PC 管理用ソフトウェアを用いてリモートで実施すること。
- (11) 情報基盤システムで調達した PC とは別に本学園が所有する PC について、本学園からの依頼に従い管理の対象とすること。障害対応・パッチ適用等の運用作業も情報基盤システムで調達した PC と同様に実施すること。同様に実施するために必要な、情報基盤システムで導入予定の管理ソフトウェアは用意する。
- (12) 本部用共有ファイルサーバの運用支援業務を行うこと。(職員からの操作上の不明点や運用に関する問い合わせへの対応、フォルダ作成、権限設定、アカウント設定、ファイル復元等)
- (13) 学習センターASP ファイルサービス(事務職員用)の運用支援業務を行うこと。(職員からの操作上の不明点や運用に関する問い合わせへの対応、フォルダ作成、権限設定、アカウント設定、ファイル復元等)
- (14) 学生用 ASP ファイルサービスの運用支援業務を行うこと。(学生サポートセンター職員からの操作上の不明点や運用に関する問い合わせへの対応等)
- (15) 本学園からの依頼に従い、LDAP サーバへのアカウントの登録/変更作業を実施すること。学生アカウントの登録/変更作業の場合は、本学園から提供する教務情報システム(システム WAKABA)のアカウントデータを、LDAP サーバに登録/変更を行うこと。実施後は確実にデータの登録・変更が行われたことを確認すること。
- (16) 本学園からの依頼に従い、グループウェアへのアカウント登録/変更作業を実施すること。実施後は、確実にデータの登録・変更が行われたことを確認すること。
- (17) サーバ、PC、プリンタ、その他保守対象製品についてメーカーの対応が必要になった場合、本学園の了解を得てメーカー保守作業の手配を行うこと、また、作業完了後動作に問題がないことを確認すること。
- (18) 常駐 SE の作業報告を個人ごとに毎日作成し、リーダーが管理を行うこと。なお、本学園が作業報告書の開示請求を行った場合にはリーダーは速やかに提示すること。
- (19) 「表5 運用支援業務対象機器一覧」記載の全 PC に対するプリンタドライバやユーティリティの管理を

行うこと。

- (20) 各事務 PC へ次期人事給与システム起動のために必要な設定がある場合は、そのソフトのインストールやアップグレード等の作業について担当ベンダに協力し対応すること。
- (21) 令和 6 年 4 月以降に各課室、学習センター及びサテライトスペースの判断で独自購入した PC について、PC 管理台帳により管理すること。管理する PC 情報は本学園より提供する。
- (22) Web 会議システムについて、利用者からの会議室予約受付・調整、会議録画希望者のサポート、Web 会議利用方法についての問い合わせ対応等の運用支援を行うこと。
- (23) 本学園からの依頼に従い、各種メーリングリストの追加、削除、変更等管理を行うこと。
- (24) 本学園からの依頼に従い、URL フィルタリングサーバへの URL 追加作業を実施すること。
- (25) 本学園からの依頼に従い、無線 LAN アクセスポイントに対し、PC の MAC アドレスを登録すること。
- (26) 本学園から、本部及び千葉学習センター内への PC の臨時設置依頼があった場合は、PC のセットアップ作業、設置作業、設置場所のネットワーク敷設作業、利用終了後の撤去作業を行うこと。
- (27) その他、本学園から運用支援業務を依頼する場合は、本学園から提示する運用マニュアルに従って運用支援業務が実施可能か判断し、本学園と協議すること。

19.2.1 本部設置機器

19.2.1.1 本部設置ネットワーク機器

本部設置のネットワーク機器(1-22)について、(1)-(2)のハードウェアのサポートを行うこと。

1. 外部接続L3 スイッチ
2. 回線負荷分散装置
3. 共通基盤 L2 スイッチ
4. 共通基盤ファイアウォール
5. 共通基盤 DMZ L2 スイッチ
6. 共通基盤 DMZ 負荷分散装置
7. 研究系 DMZ L2 スイッチ
8. 基幹L3 スイッチ
9. 事務 L3 スイッチ
10. 事務負荷分散装置
11. 事務クライアント L3 スイッチ
12. キャンパスネット L3 スイッチ
13. 運用管理 L2 スイッチ
14. 研究系内部 L2 スイッチ
15. 本部 L2 エッジスイッチ
16. 本部集約スイッチ
17. VPN 装置
18. 西研究棟・東制作棟等ネットワーク基幹 L3 スイッチ
19. 西研究棟・東制作棟等ネットワークフロア L2 スイッチ

20. 西研究棟・東制作棟等ネットワークアクセススイッチ
21. SINET接続用外部L2スイッチ
22. インターネットVPN用ファイアウォール

(1) 構成変更

- 機器に対する設定変更等が必要になった場合は、本学園と必要に応じて情報基盤システム構築業者との協議の上で対応方針を決定すること。設定変更を行う場合は、状況に応じて情報基盤システム構築業者と協力して作業を行うこと。

(2) 異常時の対応

- ハードウェア、ネットワーク負荷の監視を行い、異常を検知した場合、サービスの影響範囲を確認し、速やかに本学園に連絡し判断を仰ぐこと。なお土日で本学園に連絡が付かない場合はリーダの判断で対応し、翌営業日に本学園へ報告すること。
- 監視する項目の変更や追加が発生した場合は、本学園と内容について協議の上で対応すること。
- ハードウェアについて、異常が発生した場合、復旧対応を実施すること。ただし、使用上の誤り又は、改造、誤接続による故障及び損傷は除く。

19.2.1.2 本部設置サーバ

本部設置の各サーバ(1～21)について、(1)～(5)の対応を行うこと。

1. 本部用サーバ仮想化基盤
2. 広報用 Web サーバ
3. 外部DNS サーバ
4. SSO サーバ
5. 学術認証連携サーバ
6. グループウェアサーバ
7. 教職員用メールサーバ
8. 内部DNS プロキシサーバ
9. 統合ID 管理サーバ
10. 認証用LDAP サーバ
11. メタディレクトリLDAPサーバ
12. 事務用ドメインコントローラサーバ
13. 事務用クライアント管理サーバ
14. 本部用共有ファイルサーバ
15. バックアップサーバ
16. ログ管理・監視サーバ

17. 教員用メール・プロキシ・DNS(LSV)サーバ
18. 検証用サーバ
19. 情報公開用サーバ
20. RADIUS認証サーバ
21. クラウドシステム連携用サーバ

(1) ハードウェアのサポート

1) 異常時の対応

- ハードウェアについて、異常が発生した場合、復旧対応を実施すること。ただし、使用上の誤り又は、改造・誤接続による故障及び損傷は除く。
- ハードウェアの修理後、手順書をもとに動作確認を実施すること。

(2) OS・搭載ソフトウェアサポート

1) パッチ適用の実施

- セキュリティ上問題となる脆弱性や不具合が発表された場合、本学園と情報基盤システム構築業者と協議の上、パッチの適用を実施すること。ただし、適用は運用中のソフトウェア及びコンテンツに問題がないことが確認できた場合に限る。
- インストールされているコンテンツに影響がないかどうか、予めコンテンツ構築業者へ確認すること。

2) 設定の追加／変更

- 設定の追加／変更が必要になった場合、本学園と必要に応じて情報基盤システム構築業者と協議の上、対応方針を決定すること。設定の追加／変更を行う場合は、状況に応じて情報基盤システム構築業者と協力して作業を行うこと。

(3) 監視

- ハードウェアやソフトウェア、セキュリティアラートの監視で、異常を検知した場合、情報基盤システムで提供しているユーザサービスの影響範囲を確認し、本学園へ報告すること。なお土日で本学園に連絡が付かない場合はリーダーの判断で対応し、翌営業日に本学園へ報告すること。
- ハードウェアの異常を検知した場合、本学園の指示の下復旧作業を実施すること。
- ソフトウェアの異常を検知した場合、本学園の指示の下復旧作業を実施すること。なお、検知した異常の内容に応じて、本学園の指示の下、情報基盤システム構築業者、およびコンテンツ構築業者と協議の上、協力して復旧作業を支援すること。
- セキュリティアラート監視にて異常を検知した場合、本学園にすぐに報告し、本学園の指示の下復旧作業を実施すること。
- 監視する項目の変更や追加が発生した場合は、本学園と内容について協議の上で対応すること。
- 一日一回各サーバの LED ランプやファン音の異常が無いか、目視確認を行い異常が検出されていない

いか確認を行うこと。

(4) バックアップ

- バックアップ対象又はバックアップ時間の変更が必要になった場合対応すること。
- バックアップからリストアが必要な場合、手順書をもとに常駐 SE にて実施すること。リストアを実施後、動作確認を行うこと。

(5) リソース状況

- CPU、メモリ、ディスク、ネットワークのリソース状況について監視すること。
- CPU、メモリ、ディスク、ネットワークのリソース状況を定期的に報告すること。
- CPU、メモリ、ディスク、ネットワークのリソース状況について異常な値を示している場合、速やかに本学園に連絡し判断を仰ぐこと。なお土日で本学園に連絡が付かない場合はリーダーの判断で対応し、翌営業日に本学園へ報告すること。

19.2.1.3 本部設置 PC

本部設置の PC(1～2)について、(1)–(4)の対応を行うこと。

1. 事務用 PC
2. 事務用 PC(管理用)

(1) ハードウェアのサポート

1) 構成変更

- PC に対する接続機器の追加など、構成変更が発生した場合、本学園と内容を協議の上、対応すること。

2) 異常時の対応

- 異常であると連絡が来た場合、速やかに現地確認に行き状況を確認すること。
- ハード(PC の構成部品)について、異常が発生した場合、復旧対応を実施すること。ただし、使用上の誤り又は、改造・誤接続による故障及び損傷は除く。
- 本学園からの提供 PC が故障した場合は、本学園が提供する代替 PC と交換すること。その際、本学園の指示に従ってソフトウェアのインストール作業を行うこと。
- ハードウェアの修理又は交換後、リカバリー作業が必要な場合は、復旧対応を行うこと。
- OS 障害の場合は代替機を手配し代替機への交換を行うこと、なお、代替機交換時の個人データの移行は対応しなくてもよい。

(2) OS サポート

1) パッチ適用の実施

a. Windows Update

- 「1.事務用 PC」、「2.事務用 PC(管理用)」の Windows Update は、本学園の指示の下、毎月1回実施すること。
- 情報基盤システムへの影響が大きい問題(脆弱性、不具合等)に対する緊急パッチが発行された場合は、本学園と協議の上、随時パッチの適

用を実施すること。

- なお、Windows Update によるパッチの適用は、搭載ソフトウェアや各種本学園業務システム、各種ホームページなどの利用に問題がないことが確認できた場合に限るものとする。
 - b. ウイルス対策ソフト
 - ウイルス対策ソフトで最新のパッチ(エンジンやウイルス定義)がリリースされた場合、適用作業を実施すること。
 - 2) プログラムの追加／削除
 - プログラムの追加／削除について、本学園と協議の上実施すること。
 - 3) 利用者の追加削除(ドメインへの参加を含む)
 - 利用者の追加・削除・更新を実施すること。
- (3) プログラムのサポート
- 1) Java
 - a. アップデートの実施
 - Java(JRE)の最新版がリリースされた場合、Windows Update のタイミングに合わせ、アップデート作業を実施すること。ただし、緊急修正が必要な場合はこの限りではない。
 - b. 設定の変更
 - Java(JRE)の設定変更について対応すること。
 - 2) Adobe Reader
 - a. アップデートの実施
 - Adobe Reader の最新版がリリースされた場合、Windows Update のタイミングに合わせ、アップデート作業を実施すること。ただし、緊急修正が必要な場合はこの限りではない。
 - 3) その他のプログラム
 - 本学園と協議の上、必要に応じてプログラムの追加及び搭載されているソフトウェアのアップデート作業を実施すること。アップデートは Windows Update のタイミングに合わせ実施すること。ただし、緊急修正が必要な場合はこの限りではない。

上記いずれについても適用は搭載ソフトウェアや各種本学園業務システム、各種ホームページなどの利用に問題がないことが確認できた場合に限る。

(4) トラブル時の対応

- 1) ウイルス検知
 - ウイルスを検知した場合、本学園にメール通知を行い、感染した PC のウイルス除去作業などの対応を行うこと。
- 2) ネットワークトラブル対応
 - 本部設置 PC が起動しているにも関わらず本学園のネットワークに接続できない場合、速やかに現地確認を行い、LAN ケーブル変更や HUB 交換などの対応を行うこと。ただし、居室間のネットワーク敷設等工事が必要となる場合は、別途協議とする。なお、各事務室内での交換に必要な部材は別途本学園より提供する。

19.2.1.4 ネットワークプリンタ(カラー)

本部設置のネットワークプリンタ(カラー)について、(1)の対応を行うこと。

(1) ハードウェアのサポート

1) 構成変更

- 機器に対する設定変更等が必要になった場合は、本学園と協議の上で実施すること。

2) 異常時の対応

- ハードウェアについて異常が発生した場合、復旧対応を実施すること。ただし、使用上の誤り又は、改造・誤接続による故障及び損傷は除く。

19.2.1.5 情報推進課保有仮想サーバ基盤システム用共有ストレージ

本部設置の情報推進課保有仮想サーバ基盤システム用共有ストレージについて、(1)の対応を行うこと。

(1) 監視

- 一日一回本体の LED ランプやファン音の異常が無いかを目視で確認し、異常がみられる場合は本学園へ報告すること。LED ランプ点灯状態の違い(正常時、異常時)が不明な場合は本学園へ確認すること。

19.2.2 学習センター及びサテライトスペース

本部以外に全国 57 箇所の学習センターとサテライトスペースがある。全国の学習センター及びサテライトスペース設置機器に関して本部からリモート操作でサポートを行うこと。現地への出張が伴う作業は実施しない。ただし、本部と同敷地内にある千葉学習センターに関しては、現地作業を依頼する場合がある。

19.2.2.1 学習センター設置ネットワーク機器

学習センター及びサテライトスペース設置のネットワーク機器(1~3)について、(1)-(2)のハードウェアのサポートを行うこと。

1. 学習センターファイアウォール
2. 学習センタースイッチング HUB
3. 無線LAN 用アクセスポイント

(1) 構成変更

- 機器に対する設定変更等が必要になった場合は、本学園と必要に応じて情報基盤システム構築業者との協議の上で対応方針を決定すること。設定変更を行う場合は、状況に応じて情報基盤システム構築業者と協力して作業を行うこと。

(2) 異常時の対応

- 異常を検知した場合、サービスの影響範囲を確認し、速やかに本学園に連絡し判断を仰ぐこと。なお土日で本学園に連絡が付かない場合はリーダの判断で対応し、翌営業日に本学園へ報告すること。
- 監視する項目の変更や追加が発生した場合は、本学園と内容について協議の上で対応すること。
- 学習センターファイアウォール、無線 LAN アクセスポイントの機器交換が必要な場合は、予備機への設定変更等を実施すること。機器交換に伴い、学習センター及びサテライトスペース職員と各種調整を行うこと。

19.2.2.2 学習センターPC

学習センター及びサテライトスペース設置の事務用PCについて、(1)-(4)の対応を行うこと。

(1) ハードウェアのサポート

1) 構成変更

- PC に対する接続機器の追加など、構成変更が発生した場合、本学園と内容を協議の上、対応すること。

2) 異常時の対応

- 異常であると連絡が来た場合、サービスの影響範囲を確認し、速やかに本学園に連絡し判断を仰ぐこと、なお土日で本学園に連絡が付かない場合はリーダの判断で対応し、翌営業

日に本学園へ報告すること。

- ハード(PCの構成部品)について、異常が発生した場合、復旧対応を実施すること。ただし、使用上の誤り又は、改造・誤接続による故障及び損傷は除く。
- 本学園からの提供PCが故障した場合は、本学園が提供する代替PCと交換すること。その際、本学園の指示に従ってソフトウェアのインストール作業を行うこと。
- ハードウェアの修理又は交換後、リカバリー作業が必要な場合は、復旧対応を行うこと。

(2) OSサポート

1) パッチ適用の実施

a. Windows Update

- 「事務用PC」のWindows Updateは、本学園の指示の下、毎月1回実施すること。
- 情報基盤システムへの影響が大きい問題(脆弱性、不具合等)に対する緊急パッチが発行された場合は、本学園と協議の上、随時パッチの適用を実施すること。
- なお、Windows Updateによるパッチの適用は、搭載ソフトウェアや各種本学園業務システム各種ホームページなどの利用に問題がないことが確認できた場合に限るものとする。

b. ウイルス対策ソフト

- ウイルス対策ソフトで最新のパッチ(エンジンやウイルス定義)がリリースされた場合、適用作業を実施すること。

2) プログラムの追加／削除

- プログラムの追加／削除について、本学園と協議の上実施すること。

3) 利用者の追加削除(ドメインへの参加を含む)

- 利用者の追加、削除、更新を実施すること。

(3) プログラムのサポート

1) Java

a. アップデートの実施

- Java(JRE)の最新版がリリースされた場合、Windows Updateのタイミングに合わせ、アップデート作業を実施すること。ただし、緊急修正が必要な場合はこの限りではない。

b. 設定の変更

- Java(JRE)の設定変更について対応すること。

2) Adobe Reader

a. アップデートの実施

- Adobe Reader の最新版がリリースされた場合、Windows Update のタイミングに合わせて、アップデート作業を実施すること。ただし、緊急修正が必要な場合はこの限りではない。

3) その他のプログラム

- 本学園と協議の上、必要に応じてプログラムの追加及び搭載されているソフトウェアのアップデート作業を実施すること。アップデートは Windows Update のタイミングに合わせて実施すること。ただし、緊急修正が必要な場合はこの限りではない。

上記いずれについても適用は搭載ソフトウェアや各種本学園業務システム、各種ホームページなどの利用に問題がないことが確認できた場合に限る。

(4) トラブル時の対応

1) ウイルス検知

- 業務中ウイルスを検知した場合、対応についてサポートすること。

19.2.2.3 学生用プリンタ（モノクロ）

学習センター及びサテライトスペース設置の学生用プリンタ(モノクロ)について、(1)の対応を行うこと。

(1) ハードウェアのサポート

1) 構成変更

- 機器に対する設定変更等が必要になった場合は、本学園と協議の上で実施すること。

2) 異常時の対応

- ハードウェアについて異常が発生した場合、本学園へ報告し復旧対応を実施すること。ただし、使用上の誤り又は、改造・誤接続による故障及び損傷は除く。

19.2.3 ASP サービス

19.2.3.1 標的型攻撃メール対策兼スパム対策サービス

- 標的型攻撃メール対策兼スパム対策サービスについて、教職員からの問い合わせ対応等を行うこと。
- システムトラブルが発生した場合は利用者に周知すること。

19.2.3.2 URLフィルタリングサービス

- URLフィルタリングサービスについて、教職員からの問い合わせ対応等を行うこと。
- システムトラブルが発生した場合は利用者に周知すること。

19.2.3.3 Web 会議システム

- Web 会議システムについて、利用者からの会議室予約受付・調整、会議録画希望者のサポート、利用方法についての問い合わせ対応等の運用支援を行うこと。
- Web 会議録画データ提供の要望があった教員に対して録画データを提供すること。
- システムトラブルが発生した場合は利用者に周知すること。

19.2.3.4 ASP メールサービス

- ASP メールサービスについて、教職員からの問い合わせ対応等を行うこと。
- システムトラブルが発生した場合は利用者に周知すること。

19.2.3.5 ASP ファイルサービス

- ASP ファイルサービスについて、教職員からの問い合わせ対応等を行うこと。
- システムトラブルが発生した場合は利用者に周知すること。

以上

表1 PC 導入台数一覧

(※既存機器台数を含む。詳細は各機器の項目を確認のこと)

No.	場所	事務用PC
1	北海道 SC	10
2	青森 SC	8
3	岩手 SC	9
4	宮城 SC	10
5	秋田 SC	6
6	山形 SC	7
7	福島 SC	6
8	茨城 SC	8
9	栃木 SC	9
10	群馬 SC	8
11	埼玉 SC	12
12	千葉 SC	12
13	東京渋谷 SC	15
14	東京文京 SC	20
15	東京足立 SC	10
16	東京多摩 SC	10
17	神奈川 SC	13
18	新潟 SC	10
19	富山 SC	7
20	石川 SC	9
21	福井 SC	8
22	山梨 SC	8
23	長野 SC	8

No.	場所	事務用PC
24	岐阜 SC	9
25	静岡 SC	8
26	愛知 SC	10
27	三重 SC	8
28	滋賀 SC	6
29	京都 SC	10
30	大阪 SC	13
31	兵庫 SC	9
32	奈良 SC	6
33	和歌山 SC	8
34	鳥取 SC	9
35	島根 SC	8
36	岡山 SC	10
37	広島 SC	9
38	山口 SC	7
39	徳島 SC	8
40	香川 SC	8
41	愛媛 SC	9
42	高知 SC	6
43	福岡 SC	10
44	佐賀 SC	8
45	長崎 SC	8
46	熊本 SC	7
47	大分 SC	8
48	宮崎 SC	7

No.	場所	事務用PC
49	鹿児島 SC	9
50	沖縄 SC	8
51	旭川 SS	2
52	八戸 SS	3
53	いわき SS	2
54	浜松 SS	1
55	姫路 SS	1
56	福山 SS	3
57	北九州 SS	4
58	奄美大島	0
59	東京オフィス	6
60	本部	0 (420)
合計		471 (420)

※注 1: SC は「学習センター」、SS は「サテライトスペース」の略。

※注 2: 各SC 等への配置台数は現時点での予定であるため、配置する際に本学園に再確認すること。

※注 3: 各 SC 等の所在地は、「表 4 学習センター等所在地一覧」を参照すること。

※注 4: 括弧付きの数字は、本学園からの提供台数を示している。本調達で新規に導入するPC と同様に各 SC 等に設置すること。

表2 PC 以外導入台数一覧

(※既存機器台数を含む。詳細は各機器の項目を確認のこと)

No.	場所	外付けDVDドライブ	無線LAN用アクセスポイント	学習センターファイアウォール	学習センタースイッチングHUB	ネットワークプリンタ(カラー)	学生用プリンタ(モノクロ)
1	北海道 SC	2	(2)	(1)	(5)	0	1
2	青森 SC	2	(2)	(1)	(4)	0	1
3	岩手 SC	2	(2)	(1)	(5)	0	2
4	宮城 SC	2	(2)	(1)	(5)	0	2
5	秋田 SC	2	(2)	(1)	(5)	0	2
6	山形 SC	2	(2)	(1)	(2)	0	2
7	福島 SC	2	(2)	(1)	(5)	0	1
8	茨城 SC	2	(2)	(1)	(3)	0	2
9	栃木 SC	2	(3)	(1)	(4)	0	2
10	群馬 SC	2	0	(1)	(1)	0	2
11	埼玉 SC	2	0	(1)	(5)	0	2
12	千葉 SC	2	0	(1)	(5)	0	2
13	東京渋谷 SC	2	(2)	(1)	(6)	0	2
14	東京文京 SC	2	(2)	(1)	(5)	0	3
15	東京足立 SC	2	(2)	(1)	(6)	0	2
16	東京多摩 SC	2	0	(1)	(5)	0	3
17	神奈川 SC	2	0	(1)	(5)	0	2
18	新潟 SC	2	(2)	(1)	(3)	0	2
19	富山 SC	2	(2)	(1)	(3)	0	2
20	石川 SC	2	(3)	(1)	(3)	0	2
21	福井 SC	2	(2)	(1)	(3)	0	2
22	山梨 SC	2	(2)	(1)	(3)	0	1
23	長野 SC	2	(2)	(1)	(4)	0	2

No.	場所	外付けDVDドライブ	無線LAN用アクセスポイント	学習センターファイアウォール	学習センタースイッチングEIB	ネットワークプリンタ(カラー)	学生用プリンタ(モノクロ)
24	岐阜 SC	2	(2)	(1)	(4)	0	2
25	静岡 SC	2	(2)	(1)	(5)	0	2
26	愛知 SC	2	(3)	(1)	(5)	0	2
27	三重 SC	2	(2)	(1)	(4)	0	2
28	滋賀 SC	2	(2)	(1)	(3)	0	2
29	京都 SC	2	(3)	(1)	(1)	0	2
30	大阪 SC	2	(3)	(1)	(4)	0	2
31	兵庫 SC	2	(2)	(1)	(4)	0	2
32	奈良 SC	2	(2)	(1)	(3)	0	2
33	和歌山 SC	2	(2)	(1)	(4)	0	1
34	鳥取 SC	2	(2)	(1)	(4)	0	2
35	島根 SC	2	(2)	(1)	(4)	0	2
36	岡山 SC	2	(2)	(1)	(4)	0	2
37	広島 SC	2	(2)	(1)	(2)	0	2
38	山口 SC	2	(2)	(1)	(5)	0	3
39	徳島 SC	2	(2)	(1)	(4)	0	1
40	香川 SC	2	(2)	(1)	(5)	0	2
41	愛媛 SC	2	(2)	(1)	(3)	0	2
42	高知 SC	2	(2)	(1)	(5)	0	2
43	福岡 SC	2	(3)	(1)	(4)	0	1
44	佐賀 SC	2	(4)	(1)	(2)	0	2
45	長崎 SC	2	(2)	(1)	(5)	0	2
46	熊本 SC	2	(2)	(1)	(5)	0	2
47	大分 SC	2	(2)	(1)	(3)	0	1
48	宮崎 SC	2	(3)	(1)	(3)	0	2

No.	場所	外付けHDDドライブ	無線LAN用アクセスポイント	学習センターファイアウォール	学習センタースイッチング機	ネットワークプリンタ(カラー)	学生用プリンタ(モノクロ)
49	鹿児島 SC	2	(2)	(1)	(5)	0	2
50	沖縄 SC	2	(2)	(1)	(5)	0	2
51	旭川 SS	1	0	(1)	(3)	0	1
52	八戸 SS	1	0	(1)	(2)	0	1
53	いわき SS	1	0	(1)	(2)	0	1
54	浜松 SS	1	0	(1)	(2)	0	1
55	姫路 SS	1	0	(1)	(2)	0	1
56	福山 SS	1	(2)	(1)	(2)	0	1
57	北九州 SS	1	0	(1)	(2)	0	1
58	奄美大島	0	0	0	0	0	0
59	東京オフィス	1	0	0	0	0	0
60	本部	26	0	(3)	(3)	16	0
合計		134	(101)	(60)	(218)	16	102

※注 1: SC は「学習センター」、SS は「サテライトスペース」の略。

※注 2: 各SC 等への配置台数は現時点での予定であるため、配置する際に本学園に再確認すること。

※注 3: 各 SC 等の所在地は、「表 4 学習センター等所在地一覧」を参照すること。

※注 4: 括弧付きの数字は、本学園からの提供台数を示している。

表3 事務用ソフトウェア一覧

(表中に特記がある物を除き、以下のソフトウェアを 891 台分導入すること)

No.	ソフトウェア
1	OS マイクロソフト社製「Microsoft Windows11 Professional (64bit 版)」 ※本学園より提供する本部事務用 PC420 台を除いた、数量 471 を導入すること。
2	マイクロソフト社製「Microsoft Office Professional Plus 2019 アカデミック版」 又はその後継製品
3	ウイルス対策ソフト(ウイルスバスターCorp又は同等以上の機能を有する製品)
4	マイクロソフト社製「Microsoft Edge」
5	Google Chrome もしくは Mozilla Firefox
6	Windows Media Player(導入時の最新バージョン)
7	アドビシステムズ社製「Adobe Reader」(導入時の最新バージョン)
8	ヴァル研究所社製「駅すばあと イン트라ネット」 ※数量 10 を導入すること。
9	ジャストシステム社製「一太郎ビューア」
10	秘文 Advanced Edition Information Cypher又は同等以上の機能を有する製品
11	Lhaplus(最新版) 又は同等以上の機能を有する製品(パスワード付き zip ファイルの作成、展開が可能なもの)
12	テキストエディタ(TeraPad又は同等以上の機能を有する製品)
13	画像加工ソフト(PictBear又は同等以上の機能を有する製品)
14	スクリーンショット取得ソフト(WinShot又は同等以上の機能を有する製品)
15	CD/DVD 再生ソフトウェア(VR モード・CPRM 再生に対応していること)
16	CD/DVD 書き込みソフトウェア
17	リモート操作用ソフトウェア
18	学生証印刷カードプリンタ用ソフト(Card PAS) ※ソフトウェアは、本学園より支給する。
19	富士ゼロックス社製「DocuWorks アカデミック版」
20	マイクロソフト社製「.NET Framework 4.5」

表4 学習センター等所在地一覧

No.	場所	郵便番号	所在地
1	北海道 SC	〒060-0817	札幌市北区北 17 条西 8 丁目 (北海道大学札幌キャンパス 情報教育館 5・6 階)
2	旭川 SS	〒070-0044	旭川市常磐公園 (旭川市常磐館内)
3	青森 SC	〒036-8561	弘前市文京町 3 (弘前大学文京町地区 コラボ弘大 7 階)
4	八戸 SS	〒039-1102	八戸市一番町 1-9-22 (八戸地域地場産業振興センター [ユートリー]4 階)
5	岩手 SC	〒020-8550	盛岡市上田 3-18-8 (岩手大学図書館 3・4 階)
6	宮城 SC	〒980-8577	仙台市青葉区片平 2-1-1 (東北大学片平キャンパス 金属材料研究所内)
7	秋田 SC	〒010-8502	秋田市手形学園町 1-1 (秋田大学手形キャンパス 地方創生センター2 号館 4 階)
8	山形 SC	〒990-8580	山形市城南町 1-1-1 (霞城セントラル 10 階)
9	福島 SC	〒963-8025	郡山市桑野 1-22-21 (郡山女子大学 もみじ館内)
10	いわき SS	〒970-8023	いわき市平菱川町1-1-3 (いわき市社会福祉センター)
11	茨城 SC	〒310-0056	水戸市文京 2-1-1 (茨城大学水戸キャンパス 環境リサーチラボラトリー2・3 階)
12	栃木 SC	〒321-0943	宇都宮市峰町 350 (宇都宮大学峰キャンパス 附属図書館 1・2 階)
13	群馬 SC	〒371-0032	前橋市若宮町 1-13-2 (群馬県立図書館北隣)
14	埼玉 SC	〒330-0853	さいたま市大宮区錦町 682-2 (大宮情報文化センター8・9・10 階)
15	千葉 SC	〒261-8586	千葉市美浜区若葉 2-11 (放送大学本部敷地内)
16	東京渋谷 SC	〒150-0043	渋谷区道玄坂 1-10-7 (五島育英会ビル 1 階)

No.	場所	郵便番号	所在地
17	東京文京SC	〒112-0012	文京区大塚 3-29-1 (筑波大学東京キャンパス文京校舎内)
18	東京足立SC	〒120-0034	足立区千住 5-13-5 (学びピア 21 6階)
19	東京多摩SC	〒187-0045	小平市学園西町 1-29-1 (一橋大学小平国際キャンパス 国際共同研究センター3・4階)
20	神奈川SC	〒232-0061	横浜市南区大岡 2-31-1
21	新潟SC	〒951-8122	新潟市中央区旭町通 1 番町 754 (新潟大学旭町キャンパス 医歯学図書館 4～6階)
22	富山SC	〒939-0311	射水市黒河 5180 (富山県立大学 計算機センター3階)
23	石川SC	〒921-8812	野々市市扇が丘 7-1 (金沢工業大学扇が丘キャンパス 9号館)
24	福井SC	〒910-0858	福井市手寄 1 丁目 4-1 (AOSSA7階)
25	山梨SC	〒400-0016	甲府市武田 4-4-37 (山梨大学甲府キャンパス 総合研究棟Y号館隣接建物内)
26	長野SC	〒392-0027	諏訪市諏訪1-6-1 (アーク諏訪3階)
27	岐阜SC	〒500-8384	岐阜市藪田南 5-14-53 (OKB ふれあい会館第 2 棟 2階)
28	静岡SC	〒411-0033	三島市文教町 1-3-93 (静岡県立三島長陵高等学校 2階)
29	浜松SS	〒430-0916	浜松市中区早馬町 2-1 (クリエート浜松 2階)
30	愛知SC	〒466-0825	名古屋市西区則武新町三丁目1番17号 (イオンモール Nagoya Noritake Garden 内)
31	三重SC	〒514-0061	津市一身田上津部田 1234 (三重県総合文化センター 生涯学習棟 4階)
32	滋賀SC	〒520-2123	大津市瀬田大江町横谷 1-5 (龍谷大学瀬田キャンパス 4号館 1階)

No.	場所	郵便番号	所在地
33	京都 SC	〒600-8216	京都市下京区西洞院通塩小路下る東塩小路町 939 (キャンパスプラザ京都 3 階)
34	大阪 SC	〒543-0054	大阪市天王寺区南河堀町 4-88 (大阪教育大学天王寺キャンパス 中央館 6・7 階)
35	兵庫 SC	〒657-8501	神戸市灘区六甲台町 2-1 (神戸大学六甲台第 1 キャンパス アカデミア館 6・7 階)
36	姫路 SS	〒670-0012	姫路市本町 68-290 (イーグレひめじ地下 2 階)
37	奈良 SC	〒630-8589	奈良市北魚屋東町 (奈良女子大学コラボレーションセンター3 階)
38	和歌山 SC	〒641-0051	和歌山市西高松 1-7-20 (和歌山大学松下会館内)
39	鳥取 SC	〒680-0845	鳥取市富安 2-138-4 (鳥取市役所駅南庁舎 5 階)
40	島根 SC	〒690-0061	松江市白湊本町 43 (スティックビル 4 階)
41	岡山 SC	〒700-0082	岡山市北区津島中 3-1-1 (岡山大学津島北キャンパス 文化科学系総合研究棟 5・6 階)
42	広島 SC	〒730-0053	広島市中区東千田町 1-1-89 (広島大学東千田キャンパス 東千田総合校舎 3・4 階)
43	福山 SS	〒720-0812	福山市霞町 1-10-1 (まなびの館ローズコム 3 階)
44	山口 SC	〒753-0841	山口市吉田 1677-1 (山口大学吉田キャンパス 大学会館内)
45	徳島 SC	〒770-0855	徳島市新蔵町 2-24 (徳島大学新蔵キャンパス 日垂会館 3 階)
46	香川 SC	〒760-0016	高松市幸町 1-1 (香川大学幸町北キャンパス 研究交流棟 7・8 階)
47	愛媛 SC	〒790-0826	松山市文京町 3 (愛媛大学城北キャンパス 総合情報メディアセンター棟 3・4 階)
48	高知 SC	〒780-8072	高知市曙町 2-5-1 (高知大学朝倉キャンパス メディアの森内)

No.	場所	郵便番号	所在地
49	福岡 SC	〒816-0811	春日市春日公園 6-1 (九州大学筑紫キャンパスE棟 4,5階)
50	北九州 SS	〒806-0021	北九州市八幡西区黒崎 3-15-3 (コムシティ 3階)
51	佐賀 SC	〒840-0815	佐賀市天神 3-2-11 (アバンセ 4階)
52	長崎 SC	〒852-8521	長崎市文教町 1-14 (長崎大学文教キャンパス 附属図書館南隣)
53	熊本 SC	〒860-8555	熊本市中央区黒髪 2-40-1 (熊本大学黒髪北キャンパス 附属図書館南棟 2・3階)
54	大分 SC	〒874-8501	別府市北石垣 82 (別府大学別府キャンパス 39号館 2階)
55	宮崎 SC	〒883-8510	日向市本町 11-11 (日向市役所北隣)
56	鹿児島 SC	〒892-8790	鹿児島市山下町 14-50 (かごしま県民交流センター西棟 4階)
57	沖縄 SC	〒903-0129	沖縄県中頭郡西原町字千原 1 (琉球大学千原キャンパス 地域国際学習センター棟 4・5階)
58	本部	〒261-8586	千葉市美浜区若葉 2-11

※注: SC は「学習センター」、SS は「サテライトスペース」の略

表5 運用支援業務対象機器一覧

名称	台数(予定)	本学園既存機器
本部(サーバ/ネットワーク/PC/周辺機器)		
本部用サーバ仮想化基盤	1 式	
広報用 Web サーバ	2 式(仮想)	
外部DNS サーバ	2 台(仮想)	
SSO サーバ	2 台(仮想)	
学術認証連携サーバ	1 式(仮想)	
グループウェアサーバ	1 式(仮想)	
教職員用メールサーバ	1 式(仮想)	
内部DNS プロキシサーバ	2 台(仮想)	
統合ID 管理サーバ	1 台(仮想)	
認証用LDAP サーバ	2 台(仮想)	
メタディレクトリLDAPサーバ	2 台(仮想)	
事務用ドメインコントローラサーバ	2 台(仮想)	
事務用クライアント管理サーバ	1 式(仮想)	
本部用共有ファイルサーバ	1 台	
バックアップサーバ	2 台以上	
遠隔地バックアップ機器	1式	
ログ管理・監視サーバ	1 式(仮想)	
教員用メール・プロキシ・DNS(LSV)サーバ	1 台(仮想)	
検証用サーバ	1 台(仮想)	
情報公開用サーバ	1 台(仮想)	
クラウドシステム連携用サーバ	1 台	○
情報推進課保有仮想サーバ基盤用共有ストレージ	1 台	○

名称	台数(予定)	本学園既存機器
外部接続L3 スイッチ	2 台	
回線負荷分散装置	2 台	
共通基盤 L2 スイッチ	2 台	
共通基盤ファイアウォール	2 台	
共通基盤 DMZ L2 スイッチ	2 台	
共通基盤 DMZ 負荷分散装置	2 台	
研究系 DMZ L2 スイッチ	2 台	
基幹L3 スイッチ	2 台	
事務 L3 スイッチ	2 台	
事務負荷分散装置	2 台	
事務クライアント L3 スイッチ	2 台	
キャンパスネット L3 スイッチ	2 台	
運用管理 L2 スイッチ	1 式	
研究系内部 L2 スイッチ	2 台	
本部 L2 エッジスイッチ	20 台	
本部集約スイッチ	2 台	
VPN 装置	1 台	
西研究棟・東制作棟等ネットワーク基幹 L3 スイッチ	2 台	
西研究棟・東制作棟等ネットワークフロア L2 スイッチ	7 台	
西研究棟・東制作棟等ネットワークアクセススイッチ	33 台	
SINET 接続用外部L2 スイッチ	1 台	
インターネットVPN用ファイアウォール	2 台	
RADIUS認証サーバ	2 台	
その他居室内エッジスイッチ	数十台	○
事務用 PC	420台	うち 420 台(全台学園提供)

名称	台数(予定)	本学園既存機器
外付けDVDドライブ	26台	
ネットワークプリンタ(カラー)	16台	
事務用プリンタ(本学園既存所有)	3台	○
課金式代替プリンタ(本学園既存所有)	8台	○
学習センター(サーバ/ネットワーク/PC/周辺機器)		
学習センターファイアウォール	60台	○
学習センタースイッチング HUB	218台	○
無線LAN用アクセスポイント	101台	○
事務用PC	471台	
外付けDVDドライブ	110台	
学生用プリンタ	102台	
ASP サービス		
標的型攻撃メール対策兼スパム対策サービス	1式	
URLフィルタリングサービス	1式	
Web 会議システム	1式	
ASP メールサービス(Gmail)	1式	
ASP ファイルサービス(Google ドライブ)	1式	