

会津大学情報ネットワークシステム運用管理
及び

教育研究環境整備業務仕様書

Contents

1	前提	4
1.1	AINS について	4
1.2	委託者の業務	4
1.3	システムの更新予定	4
2	委託業務の概要	5
3	委託業務の内容	5
3.1	AINS の環境整備及び運用に係る管理作業	5
3.2	障害、セキュリティインシデントに係る管理作業	7
3.3	システム更新に係る作業	7
3.4	法令電気設備定期点検に係る全停電時の作業	7
3.5	AINS の資産管理に係る作業	8
3.6	教育研究活動、大学行事等の利用支援に係る作業	8
3.7	AINS の運用管理業務改善に係る提案	8
3.8	その他	8
4	業務の計画、報告、記録	8
5	業務日、業務時間及び体制	8
6	後方支援体制	9
7	技術員	9
7.1	技術員の定義	9
7.2	技術員チーム全体	10
7.3	遠隔での業務対応	11
7.4	技術員交代	12
8	協業について	12
9	相互協力	12
10	委託業務引継ぎ	12
10.1	委託業務開始時の引継ぎに関する注意	12
10.2	委託業務終了時の引継ぎに関する注意	12
10.2.1	契約満了時の提出資料	13
11	その他留意事項	13
11.1	個人情報等	13
11.2	守秘義務等	13
11.3	著作権等	13
11.4	疑義	13
12	個別要求仕様	14
12.1	ヘルプデスク	14
12.1.1	対応の開始	14
12.1.2	対応内容	14
12.1.3	情報センターと協議の上で決定する内容	14
12.2	ユーザ管理	14
12.2.1	対応の開始	14
12.2.2	対応内容	14
12.2.3	情報センターと協議の上で決定する内容	15
12.3	バックアップ	15
12.3.1	対応の開始	15
12.3.2	対応内容	15
12.3.3	情報センターと協議の上で決定する内容	16
12.4	運転監視	16
12.4.1	対応の開始	16
12.4.2	対応内容	16
12.4.3	情報センターと協議の上で決定する内容	17
12.5	ソフトウェアおよびユーザ環境管理	17
12.5.1	対応の開始	17
12.5.2	対応内容	17

12.5.3	情報センターと協議の上で決定する内容	18
12.6	障害対応	18
12.6.1	対応の開始	18
12.6.2	対応内容	18
12.7	セキュリティ対策および対応	19
12.7.1	対応の開始	19
12.7.2	対応内容	19
12.8	AINS のシステムの更新/変更作業	19
12.8.1	対応の開始	20
12.8.2	対応内容	20
12.8.3	情報センターと協議の上で決定する内容	20
12.9	資産管理等の支援	20
12.9.1	対応の開始	20
12.9.2	対応内容	20
12.10	利用支援	20
12.10.1	対応の開始	20
12.10.2	対応内容	21
13	主な申請書一覧	22
14	主な運用管理対象機器一覧	22
14.1	主な教育用端末、サーバ	22
14.2	教育用計算機システム 1	23
14.3	教育用計算機システム 2	24
14.4	教育用計算機システム 3	25
14.5	ネットワークシステム	25
14.6	その他システム	26

会津大学情報ネットワークシステム運用管理及び教育研究環境整備業務は、会津大学に設置された会津大学情報ネットワークシステム (University of Aizu Information Network System 以下 AINS) のシステム運用管理及び教育研究のための環境整備に関する業務を本仕様書に従って実施する。

1 前提

1.1 AINS について

会津大学では、内部動作に関する情報の透明性、ネットワークも含めた総合性能が高く、安定した教育研究環境の実現に適した UNIX 系プラットフォームを全面的に採用しており、その性能を生かした高度・高品質なマルチメディア情報システムを実装したコンピュータシステムをネットワーク上に構築している。また、教育研究環境の運用維持を分担している事務組織において利用される計算機資源のうち、AINS に関連する (メールシステムなどの) 計算機システムの維持管理および、AINS に関する要望、質問などへの対応を行っている。

情報センターが管理しているコンピュータとネットワークは、一部を除き、以下が実現されている。

- 24 時間利用可能
- 共通の認証、認可の提供
- 様々なシステム上に共通して構築された環境の提供

また、会津大学のシステムは、以下の基本理念に基づき運営されている。

- (1) コンピュータのハードウェア及びソフトウェア並びにその要素及び付加機構の技術的發展に対応して、常時機能向上可能なオープン・アーキテクチャ (開かれた基本設計) のシステムであること。
- (2) 国際的かつ膨大なソフトウェア資源の蓄積をそのまま、あるいはわずかな労力で、教育、研究及び管理に、直ちに有償あるいは無償で活用可能にするために、長期的視点からスタンダードに準拠したものであること。
- (3) コンピュータにアクセスするまでの時間を短縮し、かつ、全てのコンピュータ上の資源をどこからでも利用できるよう、ネットワーク・グローバル・アーキテクチャを採用すること。

1.2 委託者の業務

委託者 (以下、情報センター) は、主に下記の業務を行っている。

- ネットワークおよび計算機に関するセキュリティ情報、及び、Security Operation Center (以下、SOC) からの情報を収集分析し、システム運用におけるセキュリティを確保するための技術的な判断を行い、管理運用すること。
- ネットワークシステム、教育用計算機システム、その他業務システム等の納入業者との連絡調整をすること。
- 全学的コンピュータ・ネットワークシステムの運用、利用全般に関する技術的管理運用をすること。
- システム運用等に関する作業を実施する上での技術的、総合的な判断をすること。
- Free/Libre and Open Source Software (FLOSS) の導入調査および導入手順書 (運用管理委託業者は、この手順に従って作業する) の作成
- 利用者からの教育及び研究のためのシステムへの要求を具体化し、運用管理業務受託業者 (以下、受託業者) へ指示すること。
- 会津大学の行事等の利用の支援への対応を技術的に検討し、受託業者へ指示すること。
- 受託業者からの現場の具体的な報告を整理して、必要に応じて情報センター内で対応すること。

本委託業務では、情報センターの指示、監督の下に本運用管理業務仕様書に基づき業務を行うものとする。

1.3 システムの更新予定

会津大学では 2021 年度から 2022 年度にかけて以下のシステムが更新される予定である。

時 期	更新予定のシステム
2021 年 4 月	教育用計算機システム 1
2021 年 10 月	教育用計算機システム 2
2021 年 10 月	教育用計算機システム 3
2022 年 4 月	ネットワークシステム

2 委託業務の概要

- (1) 名称 …… AINS 運用管理及び教育研究用環境整備業務
- (2) 場所 …… 会津大学 (会津若松市一箕町大字鶴賀)
- (3) 期間 …… 2021 年 4 月 1 日から 2022 年 3 月 31 日
- (4) 業務対象
 - (a) 情報センターが管理する機器 (14 主な運用管理対象機器一覧 (22 頁参照の事))、ソフトウェア、サービス、ネットワークおよびデータの運用管理
 - (b) 情報センターが業務で利用する機器およびソフトウェア、サービス、ネットワーク、セキュリティおよびデータの運用管理
 - (c) (a) と (b) に付随する業務

3 委託業務の内容

3.1 AINS の環境整備及び運用に係る管理作業

教育研究、特に教育における講義・演習が円滑に滞りなく行われるよう定期的にシステムを維持管理するため、AINS の運用管理に関して以下の作業を行うこと。受託業者は、下記作業について実施計画書を作成し、事前に情報センターに提出し、承認を受けること。

- (1) ヘルプデスク (12.1 ヘルプデスク (14 頁) 参照の事)
 - (a) 教職員及び学生 (以下ユーザ) からの問い合わせへの対応、障害切り分け、障害通知、ユーザのシステム誤用への対応、応急措置の検討と実施、障害記録作成等。
 - (b) 口頭での問い合わせ、指示、依頼についての問い合わせ記録を情報センターが指定するメーリングリストへ報告。
- (2) ユーザ管理 (12.2 ユーザ管理 (14 頁) 参照の事)
ユーザからの AINS 利用のための申請書等に基づく各種システム設定と管理、利用のルールに基づく措置とユーザ指導等。
- (3) バックアップ (12.3 バックアップ (15 頁) 参照の事)
システムバックアップ、バックアップメディアの整理保管及びリストア等。
- (4) AINS の基盤部分の運用管理
 - (a) ネットワークに関する運用管理
 - i. 運転監視 (12.4 運転監視 (16 頁) 参照の事)。ネットワーク及びネットワークへ接続される計算機の運転状況監視、異常時の措置、利用ルール違反の監視等。
 - (b) 認証に関する運用管理
 - i. OpenLDAP, Unicorn ID Manager, Infoblox などの設定と管理
 - ii. 各種 OS の LDAP の設定と管理
 - iii. 研究室向け LDAP 認証サービスの設定と管理
 - iv. ネットワーク機器の LDAP に関する設定と管理
 - v. LDAP に関するソフトウェアの設定と管理
 - vi. Active Directory の設定と管理
 - (c) メールに関する運用管理
 - i. Postfix, Dovecot, Active!Mail, Secure Matrix の設定と管理
 - ii. IMAP(IMAP4S など), POP(POP3S など), SMTP(SMTP-AUTH 等を含む) の設定と管理
 - iii. GetMail, Maildrop の設定と管理
 - (d) Firewall に関する運用管理
 - i. Palo Alto Networks PA の設定と管理
 - ii. Cisco ASA の設定の設定と管理
 - iii. ポート番号の利用制限、利用許可の設定と管理
 - (e) DNS/DHCP 及び BIND に関する運用管理
 - (f) 情報センター管理下の各種サーバに関する運用管理
 - i. Web サーバ, FTP サーバの設定と管理
 - ii. ライセンスサーバ、WSUS/KMS サーバ、ログサーバ、アンチウイルスサーバ等の設定と管理
 - (g) 情報センター管理下の仮想環境の構築、チューニング、運用管理

- (h) ロードバランサの運用管理
- (5) ソフトウェア管理 (12.5 ソフトウェア管理 (17 頁) 参照の事)
 - (a) 教育研究及び管理用として利用する各種ソフトウェアのインストールおよび安定的な維持管理
 - i. 情報センターで作成したインストール指示書または製品マニュアルに従ったソフトウェアの導入、削除、動作検証。(平均で月間 10 本。年間 150 時間を予定)
 - ii. 有償ソフトウェアの事前調査と動作検証
 - iii. 月 1 回の installer working report の提出
- (6) ソフトウェアに関する下記の業務
 - (a) Red Hat Enterprise Linux および CentOS(以降、Linux), Oracle Solaris(以降、Solaris), macOS, Windows 等のベンダ、メーカ、ディストリビュータ提供のセキュリティ更新プログラムの事前調査、適用、動作検証。
 - (b) 主要サーバソフトウェアの更新チェック (SSH, SSL, OpenLDAP, Postfix, Dovecot, Active!Mail, BIND, Apache, CUPS 等) および導入調査
 - (c) 定期的または不定期に更新されるソフトウェアの更新チェックおよび前回指示書に基づいた導入調査 (Google Chrome, Firefox, OpenSSL, Java, PHP, Thunderbird, Adobe Reader, DOSBox, AndroidStudio 等)
 - (d) Linux のパッケージ管理システムで導入するソフトウェアの定期更新、動作検証
 - (e) Google Chrome, Firefox, Netbeans 等のプラグインの定期更新
- (7) 無線 LAN に関する下記の業務
 - (a) 無線 LAN 機器 (AP, WCS など) の管理
 - (b) 動作状況の管理
 - (c) 設定の変更
 - (d) CISCO Wireless Control System(WCS) を使った管理
 - (e) 固定アドレス払い出し作業とそのアドレスの管理
 - (f) CISCO clean air を使った電波管理
 - (g) EAP-TTLS, EAP-PEAP のためのユーザ認証に関する管理
 - (h) eduroam のためのユーザ管理
 - (i) eduroam 用 RADIUS Proxy の設定と管理
- (8) 無線 LAN ユーザ証明書システムの運用管理
 - (a) 証明書発行管理
 - (b) アカウント管理
 - (c) EAP-TLS の認証サーバの管理
 - (d) プライベート認証局の管理
 - (e) クライアント証明書発行管理
- (9) CentOS を利用した演習室に関する業務
 - (a) ブートイメージの作成
 - (b) イメージ更新、再起動のスケジューリング
 - (c) 定期再起動後の動作確認作業
- (10) macOS を利用した演習室に関する業務
 - (a) ブートイメージの作成
 - (b) イメージ更新、再起動のスケジューリング
 - (c) 定期再起動後の動作確認作業
- (11) Windows を利用した演習室に関する業務
 - (a) ブートイメージの作成
 - (b) ブートイメージ更新、再起動のスケジューリング
 - (c) 定期再起動後の動作確認作業
- (12) 以下のソフトウェア、サービスに関する運用管理、アカウント登録削除等のユーザ管理
 - (a) iOS Developer(University)Program
 - (b) MATLAB

- (c) Mathematica
 - (d) Office365
 - (e) SPAM フィルタ
- (13) 授業別メーリングリスト (以下、ML) に関する業務
授業別 ML をメールサーバでサービスするための環境整備・管理で利用する、以下のスクリプトの作成・設定変更・保守・動作検証を行うこと。
- (a) 日次処理
学務システムから出力される授業別 ML メンバー用データを、ML として展開する処理
 - (b) 期末処理 [前期末・後期末 年 2 回]
ML 展開時に、直前期間の ML を併合するための設定変更
- (14) 業務の為の会議
- (a) 情報センター、システムの納入業者等との連絡調整会議に出席し、議事録を作成すること。
 - (b) システムの更新時期には、システムの更新や導入についての会議に参加すること。
- (15) その他の業務
- (a) AINS を正常に動かすために必要な設定 (システム更新による機器設定及び環境設定を含む)
 - (b) ユーザが AINS を利用するために必要な標準環境の作成、検証、管理

3.2 障害、セキュリティインシデントに係る管理作業

障害、セキュリティインシデントが発生した場合に原因究明、対処、回復が可能になるように作業を行うこと。

- (1) 障害対応 (12.6 障害対応 (18 頁) 参照の事)。情報センターおよび各システムの納入業者と連携した復旧措置。
- (2) セキュリティ対策 (12.7 セキュリティ対策 (19 頁) 参照の事)。システム全体の堅牢性の確保、ユーザによる不正・不適切な利用への対処と調査、学外からの不正アクセスへの対応を行うこと。

3.3 システム更新に係る作業

AINS のシステムの更新において、必要とされる機能・性能が確実に実現できるよう、情報センターの指示の下、以下の作業を行うこと。(12.8 AINS のシステムの更新/変更作業 (19 頁) 参照の事)

- (1) 評価機の構築および設定調査、検証
- (2) 各計算機のシステム設定作業及びテスト
- (3) 管理マニュアルの加筆・修正
- (4) 更新のために必要な情報の収集の補助作業
- (5) 運用管理の検討と体制の見直し
- (6) ソフトウェアの導入作業
- (7) ユーザの標準環境移行支援、導入業者提供のスクリプトの保守等
- (8) その他、更新に付随する作業

3.4 法令電気設備定期点検に係る全停電時の作業

年に一度、法令に基づき実施される会津大学の受電設備点検に伴う全停電時に以下の作業を行うこと。

- (1) 停電前作業
 - (a) システム・バックアップを取得すること。バックアップの対象は、事前に情報センターと協議し決定すること。
 - (b) システムのパッチ適用を行うこと。作業量等の理由で平常時に適用が困難なパッチを集中して適用する。
 - (c) 必要と認めたシステムについて、パッチ適用後、バックアップを取得すること。対象システム及び具体的な作業内容は、事前に情報センターと協議の上、決定すること。
 - (d) システムのシャットダウン
- (2) 復電後作業
 - (a) 教育・研究への影響を最小限にするため、復電後速やかにシステムを再起動すること。
 - (b) 再起動時に発生した障害を回復し、納入業者、メーカー、ベンダ、情報センターへの報告を行うこと。
- (3) その他作業
 - (a) 停電中に稼働させるいくつかのシステムについて、停電体制開始および終了時の設定変更および点検を行うこと。停電中に稼働させるシステムについては、事前に情報センターと協議の上、決定すること。
 - (b) 停電時にサーバールーム内のシステムの設定、配置変更を行う場合は、事前に情報センターと協議の上、対応すること。

3.5 AINS の資産管理に係る作業

会津大学の教育・研究活動において、AINS が支障なく機能するための資産管理等の作業を行うこと。(12.9 資産管理等の支援 (20 頁) 参照の事)

- (1) 利用状況の管理、計算機関連消耗品管理 (バックアップテープやプリンタのトナー等)。消耗品の利用状況に基づいた需要概算等の作業を行うこと。

3.6 教育研究活動、大学行事等の利用支援に係る作業

会津大学の教育・研究活動や行事等を行う上で必要な設定等の作業を行うこと。(12.10 利用支援 (20 頁) 参照の事)

3.7 AINS の運用管理業務改善に係る提案

- (1) AINS 運用管理業務を行う上で、運用業務に支障をきたす恐れやユーザがより活用しやすい環境改善等がある場合や、情報センターからの改善計画 (日常的な改善と長期的な移行計画) が提示された場合は、情報センターに対して改善の提案を行うこと。
- (2) 作業の実施や方法については効果や優先度を考慮し、情報センターと協議の上、柔軟に対応すること。

3.8 その他

AINS 運用管理に必要と認められる立会い、連絡調整及び報告を行うこと。

4 業務の計画、報告、記録

- (1) 情報センターの承認を必要とする業務については、実施計画書を作成し、情報センターに事前に承認を受けること。計画書の提出が必要な業務については、情報センターと協議すること。
- (2) 実施作業の報告及び記録の様式を作成し、これを事前に提出し、情報センターの承認を受けること。各業務で様式を定義している場合はこれに従うこと。
- (3) 実施作業の報告及び記録は、業務終了後 2 営業日以内に提出し、情報センターの承認を受け、必要な期間保存すること。保存期間は、予め情報センターと相談すること。
- (4) 一日の業務終了時に、技術員毎に実施した業務の業務日誌を提出すること。
- (5) 要約した月次報告書及び月次業務実績書 (会津大学に常駐し作業した技術員 (以降、技術員) の業務開始・終了時間、業務区分 (12 個別要求仕様 (14 頁) 参照の事)、業務内容等を確認できるもの) を翌月 7 営業日までに提出すること。作業報告の仕方について、必要に応じて別途協議すること。
- (6) その他委託業務に関し、情報センターの指示に基づき、情報センターが必要と認める文書を情報センターが指定した期日までに提出すること。これらは電子データで提出することとし、その形式は予め情報センターと相談すること。
- (7) 上記作業に必要な情報の積極的な収集とその整理及び報告を行うこと。
- (8) 上記 (1)-(7) の作業に関して、業務の引継ぎが可能なドキュメント類の整備を行うこと。

5 業務日、業務時間及び体制

- (1) 業務日は土曜日、日曜日、2021 年 12 月 29 日から 2022 年 1 月 3 日、国民の祝日に関する法律に規定されている祝日及び休日を除く日とする。
- (2) 休業期間は学部が休業となる以下の期間が見込まれるが、祝日等の変更により変更となる場合がある。
 - (a) 夏季休業：2021 年 8 月 7 日 (土) から 2021 年 9 月 30 日 (木)
 - (b) 冬季休業：2021 年 12 月 25 日 (土) から 2022 年 1 月 3 日 (月)
 - (c) 春季休業：2022 年 3 月 1 日 (火) から 2022 年 3 月 31 日 (木)
- (3) 業務時間は、7 時 00 分から 20 時 00 分とする。
- (4) 常駐する技術員 (7.2 技術員チームの条件 (10 頁) 参照の事) の体制は原則以下の通りとする。
 - (a) 7 時 00 分から 8 時 30 分は、技術員を 2 人以上 (休業期間は 1 人以上) とすること。
 - (b) 8 時 30 分から 17 時 30 分は、上級技術員 1 人を含む、2 人以上 (12 時 00 分から 13 時 00 分は 1 人以上) とすること。
 - (c) 17 時 30 分から 20 時 00 分は、技術員を 1 人以上とすること。
 - (d) 初級技術員のみとなる時間帯が無いようにすること。

- (e) 会津大学の行事対応や繁忙期などに於ては、その期間に限定して、情報センターと協議の上、個別に業務時間、配置する人員を定めるものとする。

・通常期間 技術員は原則、7:00から8:30は2人以上、8:30から17:30は上級技術員1人を含む2人以上(12:00-13:00は1人以上)、17:30から20:00は1人以上

	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00
技術員1名以上														
技術員2名以上														
上級技術員1名を含む2人以上														

・休業期間 技術員は原則、7:00から8:30は1人以上、8:30から17:30は上級技術員1人を含む2人以上(12:00-13:00は1人以上)、17:30から20:00は1人以上

	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00
技術員1名以上														
上級技術員1名を含む2人以上														

- (5) 受託業者は、以下の条件により業務を遂行するものとする。
- 一般的に想定される、会津大学規模の情報系大学の計算機システムの障害回復に必要な体制と障害初動対応に十分な人員を確保すること。
 - 8時30分から17時30分は、システム障害に即時対応できるとともに、ハードウェア障害・ユーザによる誤用等が通常の頻度で発生している環境下においても、少なくとも1人は、ユーザからの障害通知・問い合わせに対して技術的な判断・回答ができるよう必要な人員を確保すること。
 - 日本語及び英語による対応が可能な体制をとること。主な対応は、直接の会話、電話対応、電子メール対応、アナウンスや技術情報の作成・更新、その他情報センター業務に関する資料の英訳などとなる。(英語対応が必要なユーザは、100人以上在籍している)
 - 情報センターがシステム運用上必要と認めるときは、業務日及び業務時間の変更に応ずるものとし、この場合の経費は、別途合意のない限り契約額に含むものとする。
- (6) 常駐する技術員の作業場所は、管理棟情報センター員室B(以下作業室)もしくはSystem Support Base(研究棟207-E)(以下SSB)等、情報センターが指定した場所とする。なお、委託業務を遂行するために必要な範囲内において、当該場所及びその付帯設備(水道、電気等)を無償で貸与、提供するものとする。但し、作業場所に設置されている電話の利用は学内連絡に限定するものとする。
- (7) 人員体制に関して、年間を通しての人員スケジュールを業務開始時に、当月勤務表を前月1週間前までに提出すること。
- (8) 業務体制について実施計画書を作成し、これを事前に提出し、情報センターの承認を受けること。

6 後方支援体制

受託業者は常駐する技術員で対応できない場合に備えて、あらかじめ後方支援体制を構築すること。また、各実施計画書を作成する際には後方支援との連携を明らかにすること。

7 技術員

- 受託業者は、大学等の教育研究機関でのUNIXシステム管理・環境構築の委託業務を直近で3年以上または、複数の一般企業でのUNIXシステム管理・環境構築の委託業務を直近で5年以上受託した実績があること。
- 会津大学におけるコンピュータ・ネットワークを用いた教育研究の可用性、完全性、機密性を確保できるようにするために、以下の条件を満たした技術員を配置すること。なお、一部の技術員については、遠隔による作業も可能とする。(7.3 遠隔での業務対応(11頁)参照のこと)

7.1 技術員の定義

プロジェクト・リーダー、上級技術員、標準技術員、初級技術員の要件は以下の通りとする。

- プロジェクト・リーダー:
 - 1年以上継続する4人以上のプロジェクトのプロジェクト・リーダーの経験を5年以上有すること。
 - 直近の3年間は、受託業者に在籍していること。
 - ITスキル標準(ITSSv3)キャリアフレームワークのITサービスマネジメント職種について、ハイレベルと同程度の技術レベルを有すること。
 - UNIX環境での計算機システム管理・環境構築としての実務経験を5年以上有すること。
 - 大学等の教育研究機関でのシステム管理・環境構築の実務経験を5年以上または、複数の一般企業でのシステム管理・環境構築の実務経験を8年以上有すること。システム管理・環境構築が主たる業務のもののみ計上すること。
 - ユーザ数300人以上・300台以上の計算機の管理・運用の経験を3年以上有していること。システム管理・環境構築が主たる業務のみ計上すること。

- 上級技術員:
 - (1) IT スキル標準 (ITSSv3) キャリアフレームワークの IT サービススマネジメント職種について、ハイレベルと同程度の技術レベルを有すること。
 - (2) 直近の 1 年間は、受託業者に在籍していること。
 - (3) UNIX 環境での計算機システム管理・環境構築としての実務経験を直近 5 年のうち 3 年以上有すること。
 - (4) 大学等の教育研究機関でのシステム管理・環境構築の実務経験を 7 年以上または、複数の一般企業でのシステム管理・環境構築の実務経験を 7 年以上有すること。システム管理・環境構築が主たる業務のもののみ計上すること。
 - (5) ユーザ数 300 人以上・300 台以上の計算機の管理・運用の実務経験を直近 5 年のうち 3 年以上有していること。ユーザとしての管理・運用は含まないこと。
 - (6) UNIX のシステム管理、環境構築を他者のサポートなしで独立して行うことができること。
 - (7) 標準技術員、初級技術員の指導をできること。
- 標準技術員:
 - (1) 直近の 3ヶ月間は、受託業者に在籍していること。
 - (2) UNIX 環境での計算機システム管理・環境構築としての実務経験を直近 4 年のうち 2 年以上有すること。
 - (3) 大学等の教育研究機関でのシステム管理・環境構築の実務経験を 3 年以上または、複数の一般企業でのシステム管理・環境構築の実務経験を 5 年以上有すること。システム管理・環境構築が主たる業務のみ計上すること。
 - (4) ユーザ数 100 人以上・100 台以上の計算機の管理・運用の経験を直近 4 年のうち 2 年以上有していること。システム管理・環境構築が主たる業務のみ計上すること。
- 初級技術員:
 - (1) UNIX 環境での計算機システム管理・運用の実務経験を 2 年以上有すること。システム管理・運用が主たる業務のもののみ計上すること。

7.2 技術員チーム全体

技術員は、チーム全体として、以下の条件を満たしていること。

- (1) チームは、以下 (a) もしくは (b) の構成とし、契約期間途中でのチーム構成の変更は、情報センターと協議の上、可とする。
 - (a) 常駐する技術員及び常駐しない技術員でチームを編成する場合
 - 常駐する技術員はプロジェクト・リーダー 1 人、上級技術員 2 人を含む 5 人以上とすること。
 - 6 人以上常駐する技術員を配置する場合は、初級技術員でも可とする。
 - 常駐しない技術員については、標準技術員以上とすること。
 - (b) 常駐する技術員のみでチームを編成する場合
 - 常駐する技術員はプロジェクト・リーダー 1 人、上級技術員 2 人を含む 6 人以上とすること
 - 7 人以上技術員を配置する場合は、初級技術員でも可とする。

常駐する技術員について、事前に情報センターと協議し承認された場合、一時的に自宅や会社等、遠隔からの作業を行うことを可する。
- (2) 情報センターからの通知内容にしたがって、AINS に接続されている各システムの納入業者と協力し、適切な運用・管理、障害等の対応が出来ること。
- (3) 会津大学における教育・研究がセキュアに行えるようにするために、技術員チームは下記についての 運用管理経験があること。
 - (a) 会津大学が教育・研究に用いる主なプラットフォームは、Linux, macOS, Solaris, Windows である。これらのプラットフォームについて、以下のクライアントサーバシステムの運用管理経験があること。
 - i. ユーザ数 200 人以上の Linux のシステム
 - ii. ユーザ数 200 人以上、端末 200 台以上の macOS の集中管理および Managed Client for OS X(MCX) による設定および管理
 - iii. ユーザ数 200 人以上、端末 100 台以上の Windows のネットブート
 - (b) 会津大学が利用する機器 (14 主な運用管理対象機器一覧 (22 頁) 参照の事) に相当する機器の設定、運用管理経験があること。
 - (c) 会津大学では学生・教職員のホームディレクトリを NFS で複数のプラットフォームに提供管理している。教育環境の維持管理、運用において非常に重要な NFS の運用管理について以下の実績があること。

- i. Linux, macOS, Solaris 等の複数種類の UNIX クライアント 300 台以上 (但し、同一 OS の複数バージョンは除く) について、ユーザのホームディレクトリを NFS で利用するシステムの運用管理経験
 - ii. Netapp を含む主要な NFS サーバについての運用管理経験
 - iii. ユーザ数 300 人以上のシステムについて、Netbackup を用いたユーザファイルのバックアップとリストアの運用管理経験
- (d) 会津大学で利用している以下の仮想化環境について、十分な知識・経験があること。
 - i. VMware
 - ii. VirtualBox
- (e) 無線 LAN について、以下の運用管理経験があること。
 - i. ユーザ数 300 人以上で EAP-TLS,EAP-TTLS, EAP-PEAP の運用管理実績
 - ii. eduroam の運用実績。(Idp, Radius Proxy の設定、運用管理を含む)
- (f) コンピュータ・ネットワークのセキュリティ(可用性、完全性、機密性)を保持するために必要な知識、DNS、NFS(am-utils など含む)、LDAP および LDAPS、DHCP、ActiveDirectory、LDAP および LDAPS と ActiveDirectory の連携、Zabbix、News、Web、FTP、LPR、CUPS、パスワード管理ツール、Network Time Protocol(NTP) の知識、経験、技術を有すること。
- (g) メールサービスに関連して、以下についての十分な経験・知識を有すること。
 - i. Postfix
 - ii. IMAP4, IMAP4S
 - iii. POP3, POP3S
 - iv. SMTP-AUTH
 - v. STARTTLS
 - vi. Active!Mail
 - vii. FML
- (h) 会津大学のコンピュータやネットワークを効率的に管理運用するための以下の知識を有すること。
 - i. sh, bash, csh, awk, sed, perl, ruby, javascript, Python などのスクリプト言語
 - ii. ThinClient
 - iii. Gnome(Gnome3) Desktop
 - iv. VNC, RDP, VHD
 - v. Redmine
- (i) ソフトウェアの開発・導入・運用について、以下の要件を満たすこと。
 - i. UNIX 等において、bash, perl を含むスクリプト言語を用いて、スクリプトの作成を業務として行うことができること。
 - ii. 会津大学で利用する無償ソフトに関する導入・管理・運用ができるだけの知識・経験・技術を有すること。ソースコードが提供されているものについては、ソースコードからの構築ができること。代替ソフトやソフト運用に関する豊富な知識を有し、ユーザからの問い合わせに対して適切な対応が出来ること。
 - 大学等の教育研究機関で、UNIX の環境において、50 本以上の無償ソフトを環境に即した方法により、ソースから構築し、環境を整えて運用した経験があること。
 - 会津大学でライセンス契約しているソフトウェアの導入、管理、運用について適切な対応ができること。
- (j) 会津大学で導入しているアプライアンス機器やネットワーク管理ソフトウェア、もしくはその同等品に関して、豊富な知識を有するとともに適切な対応ができること。同等品の場合は、詳細な資料を提出すること。
- (k) 上記各項目について、本契約後新たに導入されるハードウェア・ソフトウェアに対しても導入、管理、運用について上記項目と同様に適切な対応を行うこと。

7.3 遠隔での業務対応

- (1) 技術員が作業を行う場所は、事前に情報センターと協議し承認された場所及び環境から行うものとする。
- (2) 遠隔作業での通信はセキュアな通信回線を利用すること。回線障害等で遠隔作業が行えない場合は、学内で作業する技術員に引き継ぐこと。
- (3) 業務に関する連絡等は、常駐する上級技術員から行なうものとする。
- (4) 常駐する上級技術員は実施する遠隔作業を把握し、責任を負うこと。
- (5) 以下に示す作業の一部に於て、遠隔作業も対応可能とするものとする。
 - ユーザー管理 12.2 ユーザ管理 (14 頁)
 - バックアップ 12.3 バックアップ (15 頁)

- 運転監視 12.4 運転監視 (16 頁)
- ソフトウェア管理 12.5 ソフトウェア管理 (17 頁)
- AINS の更新/変更作業 12.8 AINS の更新/変更作業 (19 頁)
- 業務に関する文書の英訳対応 5 営業日、業務時間及び体制 (8 頁)
- 上記以外の作業についても、情報センターと協議の上、遠隔による作業対応も可能とする。

7.4 技術員交代

受託業者は、技術員が事故等によりその業務遂行が不可能な事態になった場合には、何らかの方法で業務に支障が出ないように対策を講じること。その後、速やかに同等の技術を持つ業務従事者を業務に従事させるものとし、業務従事者変更の計画と業務従事者の技術者経歴書、チーム全体のスキルマップを情報センターに提出し、承認を得ること。

8 協業について

常駐する技術員は、全て受託業者に在籍する社員で対応することを原則とするが、初級技術員は最大 2 人まで、他社に協力を求めることも可能とする。その場合は、以下の具体的かつ詳細な内容を明記した書面を提出すること。

- (1) 責任の所在
- (2) 管理体制
- (3) 役割分担
- (4) 協力会社と行うことによる相乗効果を示すもの
- (5) 協力会社に於けるバックエンド (後方支援) 体制を部署単位で記したもの
- (6) 同様の業務での協業の実績を示すもの

9 相互協力

各システム納入業者、機器製造業者、備品納入業者、関連する他の委託業者及び会津大学の建築設備保守業者との連絡を密にし、建物、機器等の使用、取扱いに留意し、会津大学の施設および設備管理に必要な事項について、相互に協力し、適切な管理を行うこと。

10 委託業務引継ぎ

10.1 委託業務開始時の引継ぎに関する注意

現在の受託業者からの引継ぎは、2021 年 3 月 1 日以降、速やかに行うものとする。業務引継ぎの際は、情報センターの担当者と密に連絡を取り合い、2021 年 4 月 1 日からの委託業務に支障が出ないようにすること。なお、業務引継ぎに関わる費用は委託契約の中に含むものとする。また、現行受託業者が 2021 年 3 月 31 日までに要する業務引継ぎに関わる費用は、現行契約に含めている。委託業務の引継ぎは、会津大学、現行受託業者、今回受託する業者の三者の合意を以て完了とする。少なくともプロジェクトリーダーと上級技術員は、業務従事者が引継ぎを行うこと。以下の項目に関して、作業内容について具体的かつ詳細に記述した計画書を提出すること。

- (1) ソフトウェアのインストール及びテスト
- (2) OS(Linux, macOS, Solaris, Windows) の環境設定、管理、運用
- (3) 各種ファイルサーバおよびアプライアンスの環境設定、管理、運用
- (4) ネットワークの設定、管理、運用
- (5) データのバックアップ及びリストア
- (6) セキュリティ体制
- (7) その他、個別要求仕様に記載されている作業

10.2 委託業務終了時の引継ぎに関する注意

受託業者は、委託期間満了時に、下記作業について、引継ぎ作業を行うこと。なお、業務引継ぎに関わる費用は委託契約の中に含むものとする。

- (1) 今回受託する業者と次期受託業者が異なる場合
 - (a) 日常的な運用作業内容の確認および作業手順の作成
 - (b) 委託に関わる業務報告方法の確認
 - (c) 現行業者および過去の運用業者が残した作業報告の確認

- (d) 現行業者および過去の運用業者への情報センターからの指示、依頼などの内容その対応記録の確認
 - (e) 現行委託内容と次期委託内容の差異の確認とそれに伴う作業の計画策定
 - (f) 次期委託作業量の確認と報告
 - (g) 遠隔で実施した業務に関する作業
- (2) 今回受託する業者と次期受託業者が同一の場合
- (a) 日常的な運用作業内容についての年次報告書 (概要報告及び詳細報告) の作成
 - (b) 委託に関わる業務報告方法の整理、まとめの作成
 - (c) 現行業者および過去の運用業者が残した作業報告についての業務内容、作業方法についての分析と総括
 - (d) 現行業者および過去の運用業者への情報センターからの指示、依頼などの内容とその対応記録の確認とそれに関する分析と総括
 - (e) 現行委託内容と次期委託内容の差異の確認とそれに伴う作業の計画策定
 - (f) 次期委託作業量の確認
 - (g) 遠隔で実施した業務に関する作業

10.2.1 契約満了時の提出資料

契約満了時には、以下の資料を提出すること。報告の様式については情報センターと協議すること。

- (1) 年間作業報告
- (2) 継続して行った作業について、線表等を用い 1 年間の作業の流れが分かるような一覧表を作成すること。各作業については、詳細を記述すること。
- (3) 詳細作業のまとめ (分析と総括を含む)
- (4) インストールソフトウェアの一覧表
 - (a) バージョン
 - (b) 種別 (ソースまたはバイナリ)
 - (c) 依存関係
 - (d) 作業量 (時間等)
- (5) 各 OS についてパッチ等の記録
- (6) 未完了作業の報告
- (7) システムの問題点、改善した方がよい点の提案

11 その他留意事項

11.1 個人情報等

- (1) 受託業者は、業務上知り得た個人情報について第三者に漏らし他の目的に利用してはならない。なお、このことは契約解除後及び契約期間終了後も同様とする。
- (2) 受託業者は、個人情報を複製、転記等を行ってはならない。ただし、業務履行上やむなく複製転記等を行う場合は、大学に使用目的、期間終了時の破棄状況の形態を申請し許可を得るものとする。

11.2 守秘義務等

受託業者はいかなる場合においても、本契約の履行中に大学から提供された資料・情報や知り得た業務に関する事項及びそれに付随する事項を第三者に開示及び漏洩せず、また本契約の履行に係る目的以外に転用及び流用してはならないものとし、本契約終了後も同様とする。

11.3 著作権等

受託業者が本契約の業務で開発・作成したツール、スクリプトおよび計画書、手順書、報告書、マニュアル等各種文書に係る権利については、すべて情報センターに帰属するものとする。

11.4 疑義

この仕様書に定めのない事項、この仕様書に定める業務の実施に当たって必要な詳細事項及び疑義が生じた場合は、遅滞なく情報センターと協議するものとする。

12 個別要求仕様

12.1 ヘルプデスク

ユーザからの問い合わせへの対応、障害切りわけ、障害通知、ユーザのシステム誤用への対応、応急措置の検討と実施、障害記録作成等を行うこと。

- (1) ユーザ対応は、平日の 9 時 00 分から 18 時 00 分とする。
- (2) 問い合わせ内容は記録して、2 営業日以内に報告すること。回答または解決できない場合、情報センターに速やかに報告すること。

12.1.1 対応の開始

ヘルプデスクは、以下により随時受け付ける。緊急時を除き、対応は翌営業日とする。

- (1) ユーザからの指定したメールアドレス (別に定める) 宛のメール
- (2) ユーザからの指定した電話番号 (別に定める) の電話
- (3) SSB を訪れたユーザの要求

12.1.2 対応内容

- (1) 問い合わせの受付と回答
 - (a) 必要に応じて、演習室、教室、研究室などに行って対応する。
 - (b) 内容を検討した結果、機器やシステムに不具合があると考えられる場合、障害対応を行う。
 - (c) 内容を検討した結果、セキュリティインシデントが疑われる場合は適切なセキュリティインシデント対応を行う。
 - (d) 類似の問い合わせが繰り返し発生した場合には、情報センターにそのことを速やかに報告する。
 - (e) 管理対象となっていない機器 (研究室で用いている計算機など) に関する問い合わせがあった場合は、適切なアドバイスを行う。
 - (f) 問い合わせ記録は 2 営業日以内に報告する。また、報告内容は情報センターと協議の上決定する。
 - (g) 情報センター業務では無い事柄の問い合わせがあった場合、本来の担当部署への問い合わせを促す。担当部署が不明の場合は、情報センターへ引き継ぐ。
- (2) 機器貸し出しに関すること

12.1.3 情報センターと協議の上で決定する内容

- (1) 本来情報センター業務では無い事柄の質問についてのリダイレクト先
- (2) 貸し出し用機器

12.2 ユーザ管理

ユーザからの AINS 利用のための申請書等に基づく各種システム設定と管理、利用のルールに基づく措置とユーザ対応等を行うこと。情報センターと協議の上、一部の作業について遠隔操作での作業も可とする。

12.2.1 対応の開始

- (1) 電子申請システムで受け付けたユーザからの申請書
- (2) 情報センターからの依頼
- (3) 運転監視によるルール違反の発見

12.2.2 対応内容

- (1) 申請書の処理と集計
受理した申請書は翌営業日の 9 時までに、情報センターに引き渡すこと。申請の内容が具体的で無い場合や特殊な要求の場合は、情報センターと相談すること。作業終了後は、2 営業日以内に情報センターに報告すること。
 - (a) 申請書受け付け後、原則として 3 営業日以内に必要な作業を行い、申請者に報告すること。
 - (b) ユーザアカウントの作成は情報センターと協議し、作業すること。
新年度の新入生アカウント (約 300) は概ね 1 日程度で作成すること。
 - (c) 情報センターが提供するツール以外を業務に用いる場合は、事前に動作概要、ソースコードおよび入力出力インターフェースの情報を文書化し、情報センターの承諾を得ること。
 - (d) 作業手順を文書化し、情報センターに提出すること。

- (e) 統計情報を集計し、情報センターに報告すること。
- (2) 利用ルール違反に対する対応
 - (a) 利用ルール違反があった場合、情報センターに報告し、情報センターが指示する方法によりユーザーに注意を促すこと。その後、所定の期間内に状況が改善されない場合、情報センターに報告し、予め定められた利用制限を行うこと。
 - (b) 他のユーザーに影響するルール違反の場合は、情報センターからの指示に基づいて直ちに利用制限を行うこと。
 - (c) 直接のルール違反ではないが、利用ルール違反に結びつくような利用を見つけた場合は、情報センターに報告すること。
- (3) 情報センターが提供するツールについては、動作を正しく理解した上で使用すること。

12.2.3 情報センターと協議の上で決定する内容

- (1) 各申請書の記載不備等
- (2) 利用ルール
- (3) 利用ルール違反ユーザーへの注意の手順と方法
- (4) 利用ルール違反ユーザーへの利用制限の手順と方法
- (5) 情報センターが提供するユーザー管理ツール
- (6) ユーザーへの注意を促す方法
- (7) 遠隔操作での対応について、実施方法、作業時間等

12.3 バックアップ

システムバックアップ、バックアップメディアの整理保管及びリストア等を行うこと。情報センターと協議の上、一部の作業について遠隔操作での作業も可とする。

12.3.1 対応の開始

- (1) 情報センターからのリストア依頼
- (2) バックアップルールによる対応

12.3.2 対応内容

- (1) 会津大学で使用しているバックアップツールによる最適な運用方法を提案・実行すること。必要に応じて、ツールを作成すること。
- (2) バックアップ対象およびバックアップルールは、概ね以下の通りであるが、詳細は情報センターと相談し運用すること。
 - (a) サーバ上のユーザーデータ (各ユーザーの home directory, system mail spool, IMAP メールデータとそれらに関連するデータ、共有ディレクトリなどに保存されているデータ等) のバックアップを情報センターの指定したツールで管理を行うこと。
 - (b) 情報センターが指定したサーバや機器の log 等のバックアップを情報センターの指定したツールで管理を行うこと。
 - (c) SUP を動かすサーバ (3.1 AINS の可用性・完全性を維持するために必要な管理作業 (5 頁) 参照の事) で SUP を使って同期させるファイルやディレクトリのバックアップをセンターの指定したツールで管理を行うこと。
 - (d) CentOS のブートイメージのバックアップを行うこと。
 - (e) macOS のブートイメージのバックアップを行うこと。
 - (f) Windows のブートイメージのバックアップを行うこと。
 - (g) 会津大学では新規導入の調査のための計算機 (調査機) を使っている。調査機の指定された場所 (/src, /usr/local 等) をバックアップすること。
 - (h) ユーザーのアカウント削除時には、該当者の home directory をアーカイブし、指定する場所に保存すること。
 - (i) その他システム固有情報のバックアップを行うこと。
 - (j) バックアップの際には、個人情報の取り扱いや守秘義務に注意すること。
- (3) スケジュールと手順
バックアップを行うための具体的なスケジュールと手順を情報センターと相談し、バックアップルールとして予め文書化しておき、情報センターに報告すること。

- (4) リストア
システムや機器の障害等による設定情報の消失等に対して、あらかじめバックアップされたデータを用いてリストア作業を行うこと。
- (5) バックアップメディアの管理
- (6) バックアップ履歴、世代の管理

12.3.3 情報センターと協議の上で決定する内容

- (1) バックアップあるいはアーカイブすべき内容
- (2) バックアップに使用するメディア
- (3) メディアの保管場所
- (4) バックアップに関するログの作成方法と保存方法
- (5) リストアに関するログの作成方法と保存方法
- (6) 遠隔操作での対応について、実施方法、作業時間等

12.4 運転監視

ネットワーク及びネットワークへ接続される計算機の運転状況監視、異常時の措置、利用ルール違反の監視等を行うこと。情報センターと協議の上、一部の作業について遠隔操作での作業も可とする。

12.4.1 対応の開始

- (1) 運転監視ルールによる対応
- (2) Zabbix による情報提供

12.4.2 対応内容

- (1) 運転監視を行うための具体的なスケジュールと手順を情報センターと相談し、運転監視ルールとして予め文書化しておき、情報センターに報告すること。概ね以下の内容を含めること。
 - (a) 死活監視
 - i. ネットワーク機器の死活監視
 - ii. サーバ等の計算機の死活監視
 - iii. その他機器の死活監視
 - (b) パフォーマンス監視
 - i. ネットワーク機器のパフォーマンス監視
 - ii. サーバ等の計算機のパフォーマンス監視
 - iii. その他機器のパフォーマンス監視
 - (c) トラフィックの監視
 - (d) サーバ等で動作しているデーモンプロセスの死活監視
 - (e) 不必要なプロセスの監視
 - (f) 不具合のあるプロセスの監視
 - (g) 宛て先不明の spam メールに関する確認
 - (h) postmaster 及び管理者アドレス宛への電子メールの確認
 - (i) 電子メールの伝送の確認
 - (j) SPAM フィルタの動作の確認
 - (k) 未使用機器の確認
 - (l) 無線 LAN 環境に於ける電波状況監視
- (2) 学外からの接続に対してもサービスを提供している場合は、(1) と同様にルール化し学外からの通信も監視すること。
- (3) 利用ルール違反の監視については、具体的なスケジュールと手順の相談を行うこと。
 - (a) 長時間の端末の占有について
 - (b) 利用者のディスク使用量について
 - (c) 初期パスワードの変更について

- (4) 運転中の正常か異常かの判断は、情報センターと協議の上、定義しておくこととする。また、情報センターから提供されたツール以外を業務に用いる場合は、予め、インストール場所、動作の概要、入力出力インターフェースを文書化しソースコード等の情報を情報センターに報告すること。
- (5) 上位ネットワーク等、接続先ネットワークからの情報の確認を必要に応じて行うこと。
- (6) 情報センターが提供するサービスが変更される場合には、情報センターと相談の上、運転監視内容について検討し、必要に応じて対応すること。
- (7) 異常を発見した場合、必要があれば情報センターに報告の上、ワークアラウンドを行うこと。
- (8) 情報センターが提供するツールについては、動作を正しく理解した上で使用すること。

12.4.3 情報センターと協議の上で決定する内容

- (1) 遠隔操作で対応について、実施方法、作業時間等

12.5 ソフトウェアおよびユーザ環境管理

教育研究及び管理用で利用する無償ソフトウェアを含むソフトウェアの導入、変更及び削除作業を行うこと。情報センターと協議の上、一部の作業について遠隔操作での作業も可とする。

- (1) 無償ソフトウェアに関しては、情報センターから指示された導入手順に従って、導入、動作検証などを行うこと。
- (2) 有償ソフトウェアに関しては製品マニュアル等に従った導入、動作検証などを行うこと。
 - (a) 動作不具合については、ワークアラウンドを検討すること。
- (3) セキュリティパッチ適用などの安定的な維持管理を行うこと。

12.5.1 対応の開始

情報センターからの依頼

12.5.2 対応内容

- (1) 日常のソフトウェアの導入と変更で、原則として情報センターが作成した手順書に基づき、下記の項目を作業すること。
 - (a) インストール
 - i. ソースファイルが提供されているソフトウェア
 - A. ソースファイルの取得
 - B. アーカイブ展開
 - C. コンフィギュレーション
 - D. コンパイル
 - E. インストール
 - ii. バイナリパッケージとして提供されるソフトウェア
 - A. 開発元やリポジトリ等からのバイナリパッケージの取得
 - B. コンフィギュレーション
 - C. インストール
 - (b) 環境設定
 - (c) 動作確認
 - (d) 配布
 - (e) 配布終了後、所定の情報の更新
 - (f) 上記 (a)-(e) に関する作業記録の作成を行い、情報センターに報告すること。
- (2) ソフトウェアの削除で、下記の項目を作業すること。
 - (a) アンインストール
 - 申請書または情報センターの依頼により、他のサービスに影響を与えないようにソフトウェアを削除する。削除できない場合は、使用できないようにする。
 - (b) 作業後、所定の情報の更新を行うこと。
 - (c) (a)-(b) に関する作業記録の作成を行い、情報センターに報告すること。
- (3) ソフトウェアの安定的な維持管理
 - (a) 教育研究及び管理用として利用する有償ソフトウェアおよび情報センターが指定する定期更新確認ソフトウェアのバージョンアップの有無を含めた事前調査/動作検証を行うこと。

- (b) セキュリティパッチ適用などの安定的な維持管理を行うこと。パッチ適用や各種ソフトウェアのバージョンアップにあたっては事前に綿密な計画を立て、情報センターに了承を得て作業すること。
 - (c) (a)-(b) の作業記録の作成を行い、情報センターに報告すること。
 - (d) ベンダが提供する OS の更新プログラムについては、ベンダから提供される度に、適用の可否、システム構成の確認を行い、情報センターに報告すること。適用時期等については、情報センターと協議すること。一般ユーザが利用する Linux, macOS, Windows 端末およびサーバ等については更新プログラムの提供毎、その他のサーバについては 4 半期毎の適用を予定している。
 - (e) インストール指示書に基づいたソフトウェアの導入、動作検証を行うこと。
- (4) 標準的なユーザ環境 (stdskel) の作成・検証・管理
- (5) ソフトウェアの一括変更作業。(年 1 回程度を想定) ハードウェア等の更新や OS のバージョンアップなどによる変更で、原則として情報センターが作成した手順書に基づき下記の項目を作業すること。
- (a) インストール
 - i. ソースファイルが提供されているソフトウェア
 - A. ソースファイルの取得
 - B. アーカイブ展開
 - C. コンフィギュレーション
 - D. コンパイル
 - E. インストール
 - ii. バイナリパッケージとして提供されるソフトウェア
 - A. 開発元やリポジトリ等からのバイナリパッケージの取得
 - B. コンフィギュレーション
 - C. インストール
 - (b) 環境設定 (必要に応じて、起動スクリプトの作成、保守も行うこと)
 - (c) 動作確認
 - (d) 配布
 - (e) 配布終了後、所定の情報の更新
 - (f) 上記 (a)-(e) に関する作業記録の作成を行い、情報センターに報告すること。
- (6) ライセンスサーバの構築と運用管理

12.5.3 情報センターと協議の上で決定する内容

- (1) 遠隔操作での対応について、実施方法、作業時間等

12.6 障害対応

情報センターおよびシステム納入業者と連携した復旧措置を行うこと。

12.6.1 対応の開始

- (1) 情報センターからの依頼
- (2) 運転監視による不具合の発見
- (3) 利用者からの報告

12.6.2 対応内容

- (1) 想定可能なシステム障害に対する手順を情報センターと相談し予め文書化しておき、情報センターに報告すること。
- (2) 障害が発生した場合には、直ちに情報センターに報告後、情報センターが指定したメーリングリストに報告すること。保守業者と連携し復旧措置を行い、その結果を情報センターに報告すること。
- (3) ワークアラウンドによって、被害が軽減すると判断する場合には、ワークアラウンドを行い報告すること。ワークアラウンドはあくまで、応急処置なので、以下の報告や作業を行うこと。
 - (a) ワークアラウンドの対象となる障害、対応をおこなった日時、対応内容を記録し、情報センターに報告
 - (b) ワークアラウンドの対象となったものがシステム障害と判断した場合、情報センターに報告し、復旧または改善に向けた作業
- (4) 障害によって情報センターが提供するサービスが変更される場合、情報センターと相談し、考えられるシステム障害に対する手順を文書化し、情報センターに報告すること。
- (5) 情報センター指示の下、該当するユーザ向けに障害発生との連絡をすること。
- (6) 情報センター指示の下、端末等故障時に予備機への入れ替え等作業を行うこと。

12.7 セキュリティ対策および対応

全学的無線 LAN を含むシステム全体の堅牢性の確保、ユーザによる不正・不適切な利用への対処と調査、学外からの不正アクセスに対する対応を行うこと。

12.7.1 対応の開始

- (1) 情報センターからの依頼
- (2) SOC からのインシデント連絡
- (3) 運転監視による不具合の発見
- (4) 受託業者が独自に入手した情報 (詳細は情報センターと協議し対応すること)

12.7.2 対応内容

- (1) セキュリティ情報の調査および実現方法を相談の上、実施すること。
 - (a) 代表的なセキュリティ情報サイト等を調査し、AINS に対し脅威となる情報があつた場合は脅威の程度及び現実的な対応策とそのスケジュールを検討し、情報センターと相談し作業を行うこと。
 - (b) 脅威を取り除ける場合は取り除き、それができない場合はワークアラウンドを情報センターに相談の上行うこと。
- (2) 想定可能なセキュリティインシデントに対する手順を相談の上、実施すること。
 - (a) ユーザによる不正利用の発生確認時の解析と原因の除去
 - i. 許可されていないディスクの使用
 - ii. 法令や学内規則を犯す行為
 - iii. 個々のアプリケーションのライセンス契約に反する行為
 - (b) ユーザの低リテラシーに起因する問題の解析と原因の除去
 - i. 不適切なファイル属性 (パーミッション UID, GID 他) のチェックと修正
 - ii. mail address に関する設定
 - iii. 法令や学内規則に抵触する行為
 - iv. その他許可無くシステムに負荷をかける行為
 - (c) ユーザの異動にともなう作業
 - i. 不適切なファイル属性 (パーミッション UID, GID 他) のチェックと修正
 - ii. mail address に関する設定
 - iii. 法令や学内規則に抵触する行為
- (3) ユーザによる不正利用の再発可能性の判断と可能性がある場合の対策を情報センターと相談の上、実施すること。
- (4) セキュリティインシデントによって、情報センターが提供するサービスが変更される場合、対応方法を情報センターと相談し、考えられるセキュリティインシデントに対する手順を文書化し、情報センターに報告すること。
- (5) システムの停止、性能の極度の低下及び会津大学の名誉を傷付けるようなセキュリティインシデントの対応を情報センターと相談の上、実施すること。
- (6) インシデント発生時には、インシデントレポートを作成し、情報センターに報告すること。インシデントレポートは電子的、検索閲覧できるようにして保管すること。インシデントレポートの書式や項目については、情報センターと協議すること。
- (7) SOC からのインシデント連絡への対応を実施すること。
 - (a) SOC による端末隔離が実施された場合
 - i. 利用者に端末隔離の第一報を通知すること。
 - ii. 利用者に SOC による解析結果の報告し、当該通信の報告を依頼すること。
 - iii. 利用者から受理した報告を情報センターに引き継ぐこと。
 - (b) SOC による端末隔離が実施されない場合
 - i. 放置すると深刻なセキュリティインシデントであると判断された場合、情報センターとの協議により、ワークアラウンドを実施し、作業内容について情報センターに報告すること。

12.8 AINS のシステムの更新/変更作業

システムの更新によって AINS のシステムが必要とされる機能・性能が確実に実現できる作業を行うこと。情報センターと協議の上、一部の作業について遠隔操作での作業も可とする。

12.8.1 対応の開始

情報センターからの依頼

12.8.2 対応内容

- (1) 情報センター指示の下、システム更新作業に向けた調整、調査、準備作業を行い、情報センターに報告すること。
- (2) 情報センターの指示の下、ハードウェア、ソフトウェアの動作テストを行うこと。なお、システムの更新にあたっては、各機器が適正な動作をするようにインストレーションとコンフィギュレーションを行い、既存システムと不整合が無いことを確認し報告すること。また、何らかの理由で、機器が安定せず、ワークアラウンドが必要な場合、これを実施すると共に情報センターに報告すること。
- (3) 管理マニュアル変更の必要が生じた場合には、情報センター指示の下、変更に伴う補助作業を行うこと。また、ユーザが直接操作する機器の場合、ユーザ向けの利用手順を作成すること。何れも情報センターに報告すること。
- (4) 各機器の更新があった場合には、情報センターと協議の上、整合性のある運用管理手順や業務体制の見直しを行い、情報センターに報告すること。
- (5) 情報センター指示の下、システム更新またはシステム検証で導入する仮想サーバ上に、以下のサービスを構築し、チューニング、データ移行等を行うこと。
 - (a) 更新予定の OS および指定するパッケージソフトウェア等による検証環境の構築を行うこと。
 - (b) Zabbix, Redmine, カレンダーサーバを計算機システム 1,2 の納入業者による構築・導入後に引き継ぎ、チューニングや運用等を行うこと。
 - (c) その他必要となる作業については、情報センターと協議する。
- (6) その他、所定の情報の更新を行い、情報センターに報告すること。

12.8.3 情報センターと協議の上で決定する内容

- (1) 遠隔操作での対応について、実施方法、作業時間等

12.9 資産管理等の支援

会津大学の教育・研究活動に必要な AINS システムが支障なく機能するための資産管理等の作業を行うこと。

12.9.1 対応の開始

- (1) 消耗品交換時
- (2) 情報センターからの依頼

12.9.2 対応内容

- (1) 設置機器情報等の管理を行うこと。
 - (a) 機器の設置、更新または撤去があった場合、情報センターが管理している機器リストを更新し、情報センターに報告すること。
 - (b) 利用状況調査を行うための具体的なスケジュールと手順を情報センターと相談し、利用状況調査ルールとして予め文書化しておき、情報センターに報告すること。
 - (c) 計算機等から値の取得を行う場合、情報センターから提供されたツール以外を用いる場合は、予め、インストール場所、動作の概要、入力出力インターフェースを文書化しソースコード等を明らかにすること。
 - (d) 機器にセットされた消耗品が交換時期になった場合、保持してある消耗品と交換すること。
- (2) 必要となる消耗品費等の概算を行うこと。消耗品使用量の統計履歴データをリソースの消費予測ができるように管理し、情報センターに報告すること。
- (3) 利用状況の調査を行い、情報センターに報告すること。
- (4) 情報センター提供の web ページの更新および支援を行うこと。詳細については情報センターと協議すること。

12.10 利用支援

会津大学の教育・研究活動ならびに行事を行う上で必要なシステムに関する作業を行うこと。

12.10.1 対応の開始

情報センターからの依頼

12.10.2 対応内容

- (1) 以下の会津大学の行事について、AINS システムにかかる事前準備、設定変更、動作確認、後処理を行い、情報センターに報告すること。
 - (a) 会津大学の電気設備定期点検に伴う全停電時
 - (b) 会津大学の電気設備定期点検に伴う全停電以外の停電時
- (2) 以下の教育、研究活動について、AINS システムにかかる事前準備、設定変更、動作確認、後処理を行い、情報センターに報告すること。機器設定、ユーザ ID 管理、ソフトウェア管理、バックアップ等の作業を想定している。
 - (a) 学期開始前などで、情報センターが支援が必要だと判断した場合
 - (b) 学会または学会に準じる会合のうち、情報センターが支援が必要だと判断したもの
 - (c) 公開講座のうち、情報センターが支援が必要だと判断したもの

13 主な申請書一覧

- 【様式 1】 ユーザアカウント申請書 (教職員)
- 【様式 4】 ユーザアカウント申請書 (学外者)
- 【様式 14】 ユーザアカウント申請書 (学生)
- 【様式 16】 ユーザアカウント休止申請書
- 【様式 12】 ゲストアカウント申請書
- 【様式 8】 UNIX グループ利用申請書
- 【様式 31】 ファイル共有サービス利用申請書
- 【様式 3】 機器接続申請書
- 【様式 22】 機器接続申請書 (無線専用)
- 【様式 24】 イベント用無線 LAN 申請書
- 【様式 17】 AINS 設定申請書
- 【様式 25】 LDAP 認証サービス利用申請書
- 【様式 26】 無線 LAN 用固定 IP アドレス申請書
- 【様式 7】 メーリングリスト申請書
- 【様式 27】 メールフォワード申請書 (教員用)
- 【様式 23】 SPAM メール隔離申請書
- 【様式 19】 Web サーバ運用申請書
- 【様式 20】 メールサーバ登録申請書
- 【様式 21】 SSH サーバ登録申請書
- 【様式 29】 ファイアーウォール・インバウンド通信許可申請書
- 【様式 50】 SSL サーバ証明書申請書
- 【様式 13】 教育用ソフトウェア・インストール申請書
- 【様式 85】 ネットワーク・遠隔講義室利用申請書
- 【様式 41】 ポスター印刷依頼申請書
- 【様式 60】 PDF Studio Pro License 申請書
- 【様式 80】 Microsoft Windows and Office ライセンス (MAK) 申請書
- 【様式 70】 iOS Developer University Program 参加申請書
- 【様式 71】 iOS Developer University Program デバイス登録申請書
- 【様式 28】 Eduroam 認証連携 ID Activation 申請書

ここに記述した以外にも運用方針により申請書が増減する場合もある。

14 主な運用管理対象機器一覧

2021 年 4 月 1 日時点の主な運用管理対象機器を以下に示す。
計算機システムの更新予定については、「1.3 システムの更新予定」(4 頁)を参照のこと。

14.1 主な教育用端末、サーバ

システム名称	システム区分	明細	OS	台数
教育用計算機システム 1	演習室 1,2 端末	(FAT)	CentOS8 / Windows 10	94 台
教育用計算機システム 1	演習室 3,4 端末	(FAT)	CentOS8	104 台
教育用計算機システム 3	演習室 5,6 端末	Apple iMac	macOS 10.14	100 台
教育用計算機システム 3	CALL 教室端末	Apple iMac	macOS 10.14	68 台
教育用計算機システム 3	iLab 教室端末	Apple iMac	macOS 10.14	98 台
教育用計算機システム 1	実験室 1,2 端末	(FAT)	Windows 10 / CentOS8	100 台
教育用計算機システム 1	実験室 3,4 端末	(FAT)	Windows 10 / CentOS8	52 台
教育用計算機システム 1	遠隔講義室	(FAT)	Windows 10 / CentOS8	21 台
教育用計算機システム 1	講義室用端末	(FAT)	CentOS8 / Windows 10	13 台
教育用計算機システム 1	実験室回路設計用サーバ	(物理)	RHEL7	4 台
教育用計算機システム 1	標準環境サーバ	(仮想)	CentOS8	6 台

14.2 教育用計算機システム 1

システム区分	明細	OS 等	台数
演習室 1,2	端末 [Fat] (モニタ、キーボード、マウス、アンチウィルスソフト)	CentOS, WinPro	94 台
	プリンタ	—	4 台
演習室 3,4	端末 [Fat] (モニタ、キーボード、マウス、アンチウィルスソフト)	CentOS	104 台
	UPS (端末 2 台につき 1 台)	—	52 台
	プリンタ	—	4 台
実験室 1,2	端末 [Fat] (モニタ、キーボード、マウス、アンチウィルスソフト)	WinPro, CentOS	100 台
	UPS (端末 4 台につき 1 台)	—	26 台
	FPGA ボード	—	50 台
	プリンタ	—	4 台
実験室 3,4	端末 [Fat] (モニタ、キーボード、マウス、アンチウィルスソフト)	WinPro, CentOS	52 台
	プリンタ	—	2 台
遠隔講義室	端末 [Fat] (モニタ、液晶アーム、キーボード、マウス、アンチウィルスソフト)	WinPro, CentOS	21 台
	プリンタ	—	1 台
	遠隔講義システム	Proprietary	1 台
講義室	端末 [Fat] (モニタ、キーボード、マウス、アンチウィルスソフト)	CentOS, WinPro	13 台
	UPS (端末 1 台につき 1 台、2 箇所不要)	—	11 台
修学支援室	端末 [Fat] (モニタ、キーボード、マウス、アンチウィルスソフト)	CentOS, WinPro	11 台
	プリンタ	—	1 台
図書館	端末 [Thin] (モニタ、キーボード、マウス、USB Dock、L2 ハブ)	Proprietary	12 台
【後方支援】 仮想用サーバ	サーバ	ESXi	5 台
	- 仮想化ソフトウェア		
	サーバストレージ	—	1 式
	ロードバランサー	仮想	2 台
	サーバスイッチ	—	2 台
	バックアップ用 NAS	—	1 台
	仮想ゲストサーバ (CentOS 43 台、RHEL 4 台、WinSv 8 台、vCenter)	—	56 台
	- ウィルス対策: 仮想ゲストサーバ		
	- LDAP: オープンソース・ソリューション・テクノロジー株式会社製 OpenLDAP		
	- ID マネージャ: オープンソース・ソリューション・テクノロジー株式会社製 Unicorn ID Manager		
	- NetBoot: 株式会社アルファシステムズ製 V-Boot		
	- バックアップ: Veritas 社製 NetBackup		
Solaris サーバ	サーバ	Solaris	2 台
回路設計演習用 サーバ	サーバ (アンチウィルスソフト)	RHEL	4 台
バックアップ サーバ	サーバ (LTO チェンジャー ×1: 内蔵ドライブ ×1 台、アンチウィルスソフト)	RHEL	1 台
	サーバ (LTO ドライブ ×1、アンチウィルスソフト)	RHEL	1 台
DNS/DHCP /IPAM	アプライアンス	NIOS	1 式
他	イメージ作成 端末 [Fat] (モニタ、キーボード、マウス、アンチウィルスソフト)	CentOS	3 台
	教室環境検証 端末 [Fat] (モニタ、キーボード、マウス、アンチウィルスソフト)	CentOS, WinPro	3 台
	運用委託業務 端末 [Fat] (モニタ、キーボード、マウス、アンチウィルスソフト)	CentOS	6 台
	予備 端末 [Fat] (モニタ、キーボード、マウス)	CentOS	3 台
	運用委託業務 端末 [Thin] (モニタ、キーボード、マウス)	Proprietary	9 台
	予備 端末 [Thin] (モニタ、キーボード、マウス、USB Dock)	Proprietary	1 台
	予備 キーボード、マウス、USB Dock、附帯品		4 式
	KMV スイッチ	—	2 台
	監視装置 端末 [Raspberry Pi] (70 インチ液晶テレビ 、ネットワーク監視表示灯)	RPiOS	2 式
	後方支援 プリンタ	—	2 台
	事務局 プリンタ	—	4 台
	シリアルコンソール用ノート PC (統合セキュリティソフト)	WinPro	4 台
	インタラクティブディスプレイシステム	Proprietary	1 式
	遠隔サポートシステム	Proprietary	1 式
	液晶プロジェクト	—	3 台
	消耗品 プリンタトナー	—	200 本

14.3 教育用計算機システム 2

システム区分	明細	OS	台数
ストレージシステム	大規模ストレージサーバ (教員・学生用)	Ontap	1 台
	大規模ストレージサーバ (バックアップ用)	Ontap	1 台
	小規模ストレージサーバ (事務局用)	Ontap	1 台
メールシステム	メールシステム用サーバ (VMware, NSX)	VMware	5 台
	メール中継サーバ	RHEL/仮想	2 台
	教員用メールサーバ	RHEL/仮想	1 台
	学生用メールサーバ	RHEL/仮想	4 台
	事務局用メールサーバ	RHEL/仮想	1 台
	転送用メールサーバ	RHEL/仮想	1 台
	メーリングリストサーバ	RHEL/仮想	1 台
	事務局用 MUA サーバ (Active!mail)	RHEL/仮想	2 台
	事務局用認証サーバ (SECUREMATRIX)	RHEL/仮想	1 台
	事務局用 MUA サーバ用ロードバランサー	仮想	1 式
	学生用メールロードバランサー	仮想	1 式
	仮想環境用ストレージサーバ	Tintri OS	1 台
	仮想環境用スイッチ	Network OS	2 台
Web 系システム	Web 系システム用サーバ (VMware)	VMware	3 台
	学外向け Web コンテンツサーバ	Solaris/仮想	1 台
	学外向け Web サーバ	Solaris/仮想	1 台
	学内向け Web サーバ	Solaris/仮想	1 台
	学内向け Web 認証サーバ	Solaris/仮想	1 台
	事務局用サーバ	Solaris/仮想	1 台
	ファイル共有サーバ (WebDav, DAViCal, Proself)	RHEL/仮想	1 台
	システム管理用サーバ (パトライト、Zabbix)	RHEL/仮想	1 台
	運用支援用サーバ	Solaris/仮想	1 台
	図書館用プリンタサーバ	Solaris/仮想	1 台
	演習室 3,4 プリンタサーバ	Solaris/仮想	1 台
	仮想環境用ストレージサーバ	Ontap	1 台
後方支援システム	ソフトウェア開発環境サーバ	Solaris/仮想	1 台
	ログサーバ (ログ解析ツール)	RHEL	2 台
	ログ解析サーバ (ALog Converter ANY)	WindowsServer	1 台
	バックアップサーバ 1 (NetBackup)	RHEL	1 台
	テープライブラリ / 24 スロット+LTO7 ドライブ ×2 LTO7 ドライブ ×1		
	バックアップサーバ 2 LTO6 ドライブ ×1, LTO7 ドライブ ×1	RHEL	1 台
	KVM 装置	—	3 台
	シリアルコンソール用ノート PC	Windows10	4 台
	サーバ用無停電装置	—	6 台
サービス提供用システム	ポスター印刷用プリンタ	—	2 台
	図書館用プリンタ	—	1 台
運用管理用システム	業務用デスクトップ PC Monitor(27inch)	Windows10	5 台
	業務用ノート PC	Windows10	3 台
	運用支援用端末 Monitor(23inch)	—	14 台
	検証用 iMac	macOS	2 台
	検証用 Macbook	macOS	2 台
	SOFT: Qoppa Software / PDF Studio Pro	—	—

14.4 教育用計算機システム 3

システム区分	明細	OS	台数
iLab1,2 システム	iLab1,2 端末: iMac	macOS	98 台
	21.5 インチ、109/US キーボード、3 ボタンマウス		
	授業支援用端末: iMac (ARD)	macOS	2 台
	27 インチ、109/US キーボード、3 ボタンマウス、DVD ドライブ iLab1,2 プリンタ		4 台
CALL1,2 システム	CALL1,2 端末: iMac	macOS	68 台
	21.5 インチ、109/US キーボード、3 ボタンマウス		
	授業支援用端末: iMac (ARD)	macOS	2 台
	27 インチ、109/US キーボード、3 ボタンマウス、DVD ドライブ CALL1,2 プリンタ		(4 台)
演習室 5,6 システム	演習室 5,6 端末: iMac	macOS	98 台
	21.5 インチ、109/US キーボード、3 ボタンマウス 演習室 5,6 プリンタ		4 台
後方支援システム	OS イメージ配信サーバ	RHEL	2 台
	端末管理サーバ (端末管理、セキュリティ管理)	WindowsServer	1 台
	KVM 装置	—	1 台
	ディスクイメージ管理用端末: iMac	macOS	2 台
	21.5 インチ、109/US キーボード、3 ボタンマウス		
	運用支援用端末: iMac	macOS	4 台
	21.5 インチ、109/US キーボード、3 ボタンマウス		
	運用管理用端末: iMac (ARD)	macOS	1 台
	27 インチ、109/US キーボード、3 ボタンマウス、DVD ドライブ		
	iLab/CALL プリンタサーバ、ライセンスサーバ 1 : Mac mini	macOS	1 台
	演習室 5,6 プリンタサーバ、ライセンスサーバ 2 : Mac mini	macOS	1 台
	DiLL 用サーバ: Mac mini	macOS	1 台
	SOFT: Swift Education / DiLL	—	—

14.5 ネットワークシステム

システム区分	明細	OS	台数
SINET5 接続用ルータ	ルータ	IOS	2
ドメイン間接続スイッチ	L3 スイッチ	IOS	2
次世代ファイアウォール装置	ファイアウォール	PAN-OS	2
事務局用ファイアウォール装置	ファイアウォール	ASA	2
セキュリティ装置 1	セキュリティ・アプライアンス		1
セキュリティ装置 2	セキュリティ・アプライアンス		1
コアスイッチ	L2 スイッチ	Arista EOS	2
サーバ用スイッチ	L2 スイッチ	IOS	8
フロアスイッチ	L2 スイッチ	IOS	77
電子メールセキュリティアプライアンス	メールア・プライアンス		2
無線 LAN コントローラ	アプライアンス		2
無線 LAN アクセスポイント	アプライアンス		195
端末認証装置	アプライアンス		2
タイムサーバ	アプライアンス		1
ログ収集サーバ	サーバ		1
仮想基盤システム	サーバ		3
無線 LAN 統合管理装置	アプライアンス (仮想サーバ)		1
無線 LAN 可視化装置	アプライアンス (仮想サーバ)		1
証明書発行装置	アプライアンス (仮想サーバ)		1
無線 LAN テスター	計測機		1
無停電電源装置	UPS		12
保守用スイッチ	L2 スイッチ		10
遠隔監視	サービス		1
SOC サービス	サービス		1

14.6 その他システム

以下のシステムについては、ハードウェアの管理、ヘルプデスク、バックアップ等は当該システムの納入業者が行うため必要ないが、LDAP 等の認証やネットワークに障害が発生した場合は、問題の切り分けが必要となる。

- (1) 学務システム
- (2) LMS
- (3) 履修計画システム
- (4) 電子申請システム
- (5) 年報業績登録システム
- (6) 図書システム
- (7) 人事給与システム
- (8) 財務会計システム