

DNS・DHCP サービスアプライアンス 一式
調達仕様書

国立大学法人 一橋大学

2026 年 2 月 6 日

I 概要

1 件名

DNS・DHCP サービスアプライアンス 一式

2 調達の背景及び目的

一橋大学キャンパスネットワークにおいて、ドメインや IP アドレス資源を管理・運用するシステムを改修し、安定したサービス提供とネットワークセキュリティの強化を行う。各システムはアプライアンスにより構築し、集中管理機能と組み合わせて、保守・メンテナンスの簡易化と停止時間の短縮をはかる。

3 調達の対象及び範囲

- ◆ 本仕様書に基づく物品及び役務の提供
- ◆ 案件全体のプロジェクト管理、ドキュメント管理、スケジュール管理、品質管理の提供
- ◆ 案件全体に関する必要な作業の提供
- ◆ 完成図書（機器接続表、機器設定表、機器収容図・写真の提供等）
- ◆ 日本語化された機器マニュアルの提供
- ◆ 5 年分のサブスクリプションライセンス及び保守の提供

4 調達物品及び構成内容

- ◆ 国立キャンパス 設置分
 - ◆ 権威 DNS サービスアプライアンス 2 台
 - ◆ DNS Cache/DHCP サービスアプライアンス 1 組
 - ◆ サービス管理アプライアンス 1 組
 - ◆ UPS
- ◆ 千代田キャンパス 設置分
 - ◆ DNS Cache/DHCP サービスアプライアンス 1 組
 - ◆ UPS

II 全般的要件

1 納入期限及び納入場所

- 1.1 納入期限は、2026 年 9 月 15 日（火）とする。
- 1.2 納入場所は、一橋大学国立キャンパス及び千代田キャンパス内とする。
- 1.3 指定する期日までに本学の指定する場所に納入物を納入し、本学の希望する状態にすること。すべての機器及び機能について稼動を確認し受入検査が完了していることを想定する。
- 1.4 その他納入に関すること
 - 1.4.1 納入品の搬入及び設置に関しては、本学施設に損害を与えないように、また本学業務の妨げにならないよう配慮し計画的に行うこと。
 - 1.4.2 受注業者が故意または過失により、本学の建物、機器類等の一部または全部を、滅失または毀損した場合は、受注業者の負担により直ちに原状に復すること。
 - 1.4.3 搬入、据付、配線、調整、既設設備との接続に要する全ての費用は、本調達に含まれる。

2 スケジュール及び実施体制

案件に関するスケジュール及び実施体制については、事前に受注業者で提案を行い、本学の承認を得ること。

3 作業環境及び作業場所

案件に係る作業用資源（機器類等）、作業場所その他必要となる環境や費用については、受注業者の負担で用意すること。ただし、据えつけ前の一時保管場所についてはその限りではない。

4 仕様変更及び未定義事項

案件を遂行する上で役務内容、仕様もしくは条件に疑問点や変更が生じた場合、または仕様書に記載のない内容については、直ちに受注業者と本学で協議し、解決に向けて最善の努力を行うこと。

5 情報セキュリティ要件

- 5.1 受注者が実施する作業、提示する納入物等、受注者の責任範囲にある役務、物品及びシステムに対し、受注者は本仕様書の要件の範囲において本学の指示に基づいて責任をもってセキュリティ対策を実施すること。かかる諸経費は受注者で負担すること。また、本業務に係る情報セキュリティ対策の実施内容及び管理体制について、事業開始までに本学に承認を得ること。
- 5.2 本業務の実施に当たり、受注者又はその従業員、若しくはその他の者による意図せざる不正な変更が本業務で納入する情報システムのハードウェアやソフトウェア等に加えられないため

- の管理体制を整備すること。
- 5.3 受注者は、システムが構築中であるか完成であるかといった状態にかかわらず、システム及び各ファイルの信頼性とセキュリティを十分に考慮して、以下のセキュリティ対策を施し、システムへの不正侵入や攻撃、ウィルス感染等への防止に万全を期すること。また、システムに関する開発、導入等の一連作業においても、受注者は以下のセキュリティ対策を行うこと。詳細については、受注者と本学で協議して決定すること。
- 5.3.1 原則として ISO/IEC 15408 (JIS X 5070)「情報技術セキュリティ評価基準」によるセキュリティにかかる基本設計を行うこと。また、本学からセキュリティポリシー等の提示があった場合は、本学からの提示要件を優先して設計を行うこと。
- 5.3.2 不正アクセス及び悪意のあるソフトウェアによる情報の誤用、破壊、破損、改ざんからシステム及びデータを保護するとともに、他のシステム及びネットワークに影響を及ぼすことのない仕組みを持つこと。
- 5.3.3 システムの動作に必要な IP アドレスや通信ポートからのリクエストを遮断すること。
- 5.3.4 許可しないユーザに不正に侵入されない仕組みを持つこと。
- 5.3.5 コンテンツ、ログ、設定、環境等を改ざんされないよう対策を講ずること。
- 5.3.6 セキュリティホールが発見された場合は、パッチ、サービスパック、レベルアップ等の適用といった必要な対策情報を提供し、本学が実施する作業の支援を行うこと。
- 5.4 前項 5.3.1 に関連し、本調達で導入する機器等の内、経済産業省が策定している「IT 製品の調達におけるセキュリティ要件リスト」に記載されており、且つ前記文書に記載の「セキュリティ上の脅威」が 1 つ以上存在する環境に設置・導入される製品については、前記文書を参照の上、システム稼働環境において存在する脅威に対抗するためのセキュリティ要件を満たす適切な製品を選定すること。
- 5.5 セキュリティ事件、事故及びセキュリティの違反については、本学に速やかに報告し、本学の指示に従って対応を行うこと。
- 5.6 受注者は、契約不適合責任期間中、上記の対策を講じているにもかかわらず、セキュリティ侵害、各種攻撃、ウィルス感染またはそれらが推測される兆候があった場合は、本学と協議の上、速やかに必要な作業、対策を講じ、サービスを維持すること。
- 5.7 システムへのアクセス記録が採取可能であり、必要に応じて参照及び電子データ出力が行えること。
- 5.8 受注者の資本関係・役員等の情報、事業の実施場所、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）・実績及び国籍等に関する情報提供を行うこと。
- 5.9 納品・保守等における本学の情報処理設備の操作及び施設への立ち入りについては、本学が承認したアクセス方法及びアクセス制御によって行うこと。
- 5.10 受注者は、個人情報の取扱いについて適切な保護措置を講ずる体制を整備しており、ISO/IEC 27001 (JIS Q 27001)「情報セキュリティマネジメントシステム (ISMS)」認証を取得済であること。
- 5.11 暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。

- 5.12 受注者が本調達・役務内容の一部を外部に再委託する場合は、再委託されることにより生ずる脅威に対して、情報セキュリティが十分に確保されるよう本仕様書と同水準の措置の実施を再委託先にも担保すること。

6 守秘義務及び厳守事項

受注業者は、案件及び案件に関連する役務過程において知り得た案件に関する一切の情報（以下「案件に関する情報」という。）について、次に掲げる義務を遵守すること。

- 6.1 本業務の過程で収集・作成する情報は、本業務の目的の他に利用しないこと。ただし、本業務の実施以前に公開情報となっていたものについては除く。
- 6.2 故意又は過失にかかわらず、案件に直接従事する担当者であることを本学が書面にて認めた者以外の者（以下「他者」という。）に案件に関する情報を漏らさないこと。
- 6.3 案件の履行に関連して知り得た本学の秘密情報の加工、改ざん、複写または複製等をしてはならない。ただし、委託契約の範囲内のものや安全管理上必要なバックアップを目的とするものはこの限りではない。
- 6.4 案件遂行中は、案件に関する情報の取扱いに十分留意し、他者に情報を開示しないこと。
- 6.5 案件完遂後は、案件に関する情報を返却し、又は確実に廃棄するとともに、本学の書面による許可なく案件に関する情報を他者に開示しないこと。
- 6.6 案件に関する情報を知り得た者が、異動、転職、退職等の事由によって案件と無関係になった場合でも、本学の書面による許可なく案件に関する情報を他者に開示させないこと。
- 6.7 万が一受注業者先において秘密情報の漏えい等の事故が発生した場合には、直ちに本学へ報告し、また、受注業者先が責任をもって対応すること。
- 6.8 本学秘密情報の取扱いにおいて、再委託をする場合は、本学の了解を得なければならない。
- 6.9 業務の再委託を行う場合、委託先企業についても、本義務を遵守させること。
- 6.10 その他本学の指示に基づいて守秘義務を全うすること。

7 契約不適合責任及び契約の解除、違約金

- 7.1 契約によって納入された機器の契約不適合責任の期間は、稼働後1年とし、ハードウェア障害、データ及びプログラムの不良、その他セキュリティリスク等によるシステムの再構築並びに修正を保証できるように、受注業者の責任において必要となる物品及び情報の複製を保管すること。
- 7.2 導入作業開始から契約不適合責任期間の終了までの間に、ハードウェア、ソフトウェア、システム構成及び作業に契約不適合があった場合、本学はこれらの修復、代替物への交換、再作業に加え、本学の被った損害の賠償を求めることができるものとする。
- 7.3 本学が仕様書の内容を満たさない機器あるいは作業状況であると判断した場合は、受注業者に対し、口頭または書面により改善要求を行う。それでもなお、改善要求に従わず、仕様を満たさない状況が1ヶ月以上続く場合、本学は契約の解除及び売買代金の10分の1に相当する額を違約金として求めるものとする。

8 その他留意事項

- 8.1 本調達物件に係る性能、機能及び技術等（以下、「性能等」という。）の要求要件（以下、「技術的要件」という）は「Ⅲ 技術的要件」に示すとおりである。
- 8.2 本調達物件に係る導入、設置及び保守の要求要件（以下、「役務要件」という）は「Ⅳ 導入・設置・保守要件」に示すとおりである。
- 8.3 技術的要件及び役務要件は、すべて必須の要求である。
- 8.4 技術的要件及び役務要件を満たしているか否かの判定は、本学が設ける技術審査において、入札機器に係る技術仕様書その他の入札説明書で求める提出資料の内容を審査して行う。
- 8.5 技術審査において提案が技術要件及び役務要件を満たしていないとの判定がなされた場合には不合格となり、落札決定の対象から除外する。
- 8.6 調達物品のうち入札時点で製品化されていないものが含まれる場合には、納期までに製品化され、仕様書に記載する技術的要件を満たすことが可能であることを証明する技術的資料、開発計画書及び確約書を併せて提出すること。
- 8.7 受注者が自社製以外の製品を納入する場合、受注業者は一元的な窓口となり、自社製以外の製品についても自社製品と同様の保証をすること。
- 8.8 以下の業務について再委託を行う場合においても筆頭責任者は受注者とすること。また、業務体制・範囲について本学の承認を得ること。

システムの設計

- ◆ 作業工程の管理
 - ◆ 作業中の対大学窓口
 - ◆ 作業終了後の確認作業
- 8.9 受注者は以下の資格等を有すること。
 - ◆ ISO20000
 - ◆ ISO27001

III 技術的要件

1 アプライアンス共通要件

本仕様書 I-4 の調達物品に共通の技術的要件を示す。なお、原則として全て新品、又は新品と同等の品質を持つもので調達し納品すること。

- 1.1 TIA/EIA-310-D 準拠の 1U サイズ筐体のアプライアンス装置であること。
- 1.2 100-200V AC 電源で動作すること。
- 1.3 DNS/DHCP サービスの提供に利用可能な IEEE802.3 準拠の 10/100/1000BASE-T の Ethernet Port を 2 つ以上有すること。
- 1.4 冗長化に使用する IEEE802.3 準拠の 10/100/1000BASE-T の Ethernet Port を別途有すること。
- 1.5 運用管理に使用する IEEE802.3 準拠の 10/100/1000BASE-T の Ethernet Port を別途有すること。
- 1.6 IPMI 2.0 に準拠した Lights-Out-Management (LOM) Port を別途有すること。インターフェースは IEEE802.3 準拠の 10/100/1000BASE-T の Ethernet Port であること。
- 1.7 アプライアンス筐体と同一のメーカーから提供される独自開発の OS を使用していること。
- 1.8 HTTPS 通信を使用した Web UI により設定変更などのオペレーションが行えること。
- 1.9 SSH を使用して CLI への接続が可能であること。SSH 接続のアクセス制御を内部で行えること。
- 1.10 DNSv4/v6 デュアルスタック、DHCPv4 及び v6、DHCPv6-PD(Prefix Delegation)、TFTP、NTP の各サーバ機能を同一筐体で提供できること。
- 1.11 SNMP に準拠したエージェント機能を有すること。
- 1.12 イベントが発生した際、SNMP Trap 及び電子メールにて通知する機能を有すること。それぞれの通知手段について通知内容をカテゴリー別を選択できること。
- 1.13 CPU やメモリ、ディスクなどの監視項目について、任意に設定した閾値を超えたときに通知する機能を有すること。
- 1.14 SYSLOG 転送機能を有すること。
- 1.15 複数の管理者 ID 及び管理グループを作成でき、グループ毎に管理権限を制限できること。また個々の作業履歴がログで確認できること。
- 1.16 OS のアップデートを WebUI から行う機能を有すること。またアップデートのスケジュール実施機能を有すること。
- 1.17 システム設定を定期的に自動でバックアップし、外部転送を行う機能を有すること。
- 1.18 DNS や DHCP のデータ登録を、CSV ファイルから読み込んで一括実施する機能を有すること。
- 1.19 DNS や DHCP のデータ管理作業のための API を有すること。
- 1.20 HA 構成が可能で、構成した場合のフェールオーバー時間が 5 秒以下であること。

2 権威 DNS サービスアプライアンス (2 台)

- 2.1 同一性能のアプライアンスでプライマリ権威 DNS 及びセカンダリ権威 DNS として構成すること。
- 2.2 RFC1034, 1035, 1995, 1996, 2136, 2317, 2845 に準拠すること。
- 2.3 DNS マスター、スレーブ、フォワーダ、キャッシュサーバとして動作する機能を有すること。
- 2.4 IPv4/v6 デュアルスタック DNS として動作できること。
- 2.5 GSS-TSIG による DynamicDNS 更新を受けることが可能なこと。
- 2.6 NAPTR レコードを設定できること。
- 2.7 NXDOMAIN レコードを設定できること。
- 2.8 WebUI にて複数の VIEW を定義し、それぞれ異なる DNS 応答とアクセスコントロールを設定できること。各 VIEW 間でレコードをコピーする機能を提供すること。
- 2.9 Web ベースの管理 GUI にて DNS64 サーバとして設定し動作させる機能を有すること。
- 2.10 Web ベースの管理 GUI にて AAAA レコード及び IPv6 逆引きゾーンを設定できる機能を有すること。
- 2.11 Web ベースの管理 GUI にて DNSSEC を運用管理できる機能を有すること。
- 2.12 DNSSEC の暗号鍵を、システム全体またはゾーン毎に指定したパラメーターに基づいて自動生成する機能を有すること。
- 2.13 DNSSEC の ZSK (ゾーン署名鍵) 及び KSK(鍵署名鍵)をシステム全体またはゾーン毎に指定したパラメーターに基づいて定期的に自動更新する機能を有すること。
- 2.14 DNSSEC の署名に使用する暗号鍵をハードウェア・セキュリティ・モジュールで管理する機能を有すること。
- 2.15 DNS レコードを登録した際に、RRSIG 及び NSEC (NSEC3) レコードが自動的に作成される機能を有すること。
- 2.16 複数ゾーンの共通情報を一括管理するためのテンプレート機能を提供すること。
- 2.17 ドメイン名乗っ取りを検出して通知する機能を有すること。
- 2.18 DNS 応答性能として最大毎秒 32,000 クエリ以上を有すること。

3 DNS Cache/DHCP サービスアプライアンス (2 組)

- 3.1 2 台一組の冗長構成を組み、国立及び千代田キャンパスに一組ずつ配置すること。
- 3.2 フェールオーバーについて、以下の条件で動作すること。
 - 3.2.1 サービス及び設定情報の自動的な同期
 - 3.2.2 主作動機器の障害発生時に自動で 5 秒以内にフェールオーバーし、同一 IP アドレスでのサービス継続
 - 3.2.3 OS アップデート作業においては、まず Passive 機に対してバージョンアップを実施し、アップデート完了後に自動でフェールオーバーを行うこと。フェールオーバー完了後、新たな Passive 機に対してもバージョンアップを実施すること。
- 3.3 RFC1034, 1035, 1995, 1996, 2136, 2317, 2845 に準拠すること。

- 3.4 DNS マスター、スレーブ、フォワーダ、キャッシュサーバとして動作する機能を有すること。
- 3.5 IPv4/v6 デュアルスタック DNS として動作できること。
- 3.6 GSS-TSIG による DynamicDNS 更新を受けることが可能なこと。
- 3.7 NAPTR レコードを設定できること。
- 3.8 NXDOMAIN レコードを設定できること。
- 3.9 WebUI にて複数の VIEW を定義し、それぞれ異なる DNS 応答とアクセスコントロールを設定できること。各 VIEW 間でレコードをコピーする機能を提供すること。
- 3.10 Web ベースの管理 GUI にて DNS64 サーバとして設定し動作させる機能を有すること。
- 3.11 Web ベースの管理 GUI にて AAAA レコード及び IPv6 逆引きゾーンを設定できる機能を有すること。
- 3.12 Web ベースの管理 GUI にて DNSSEC を運用管理できる機能を有すること。
- 3.13 DNSSEC の暗号鍵を、システム全体またはゾーン毎に指定したパラメーターに基づいて自動生成する機能を有すること。
- 3.14 DNSSEC の ZSK (ゾーン署名鍵) 及び KSK(鍵署名鍵)をシステム全体またはゾーン毎に指定したパラメーターに基づいて定期的に自動更新する機能を有すること。
- 3.15 DNSSEC の署名に使用する暗号鍵をハードウェア・セキュリティ・モジュールで管理する機能を有すること。
- 3.16 DNS レコードを登録した際に、RRSIG 及び NSEC (NSEC3) レコードが自動的に作成される機能を有すること。
- 3.17 複数ゾーンの共通情報を一括管理するためのテンプレート機能を提供すること。
- 3.18 ドメイン名乗っ取りを検出して通知する機能を有すること。
- 3.19 RFC1531, 1534, 2131, 2132 に準拠した DHCP サーバ機能を有すること。また以下の機能を有すること。
 - 3.19.1 ISC-DHCPD Ver.3 相当の機能
 - 3.19.2 クライアントに割り当てる Default Gateway, Broadcast Address, Subnet Mask, リース時間を DHCP レンジ毎に指定できる機能
 - 3.19.3 特定の MAC アドレスに対して静的な IP アドレスをリースする機能
 - 3.19.4 MAC アドレスリストを作成し、登録された MAC アドレスにのみ IP アドレスをリースする機能
- 3.20 GSS-TSIG による Dynamic DNS 更新を権威 DNS に送信する機能を有すること。
- 3.21 DHCP 要求を分析して要求元クライアントの OS 種別を判別する機能を提供し、その機能はクライアント側エージェントや DHCP 以外のプロトコルによる検査などを必要としないこと。
- 3.22 DHCP 要求を分析して判別した OS 種別をもとにして IP アドレス払い出しを制御するフィルターを提供できること。そのフィルターは MAC アドレスや DHCP オプションのフィルターと組み合わせて詳細な払い出し制御を記述できること。
- 3.23 Web ベースの管理 GUI にて DHCPv6 及び DHCPv6-PD サーバとして設定し動作させる機能を有すること。
- 3.24 IP アドレスのリース状況を監視し、空きアドレス不足等のサービス停止につながる問題を警告する機能を持つこと。

- 3.25 冗長構成を組む機器間でリース情報をリアルタイム同期し、フェールオーバー動作前後で相違なく IP アドレス払い出しが行えること。
- 3.26 DNS 応答性能として最大毎秒 37,500 クエリ以上を満たすこと。
- 3.27 DHCP リース性能として最大毎秒 200 リース以上を満たすこと。

4 サービス管理アプライアンス (1 組)

- 4.1 2 台一組の冗長構成とし、以下の条件で動作すること。
 - 4.1.1 サービス及び設定情報の自動的な同期
 - 4.1.2 主作動機器の障害発生時に自動で 5 秒以内にフェールオーバーし、同一 IP アドレスでのサービス継続
 - 4.1.3 OS アップデート作業においては、まず Passive 機に対してバージョンアップを実施し、アップデート完了後に自動でフェールオーバーを行うこと。フェールオーバー完了後、新たな Passive 機に対してもバージョンアップを実施すること。
- 4.2 本仕様書 III-2「権威 DNS サービスアプライアンス」及び III-3「DNS Cache/DHCP サービスアプライアンス」(以下、あわせて「アプライアンス群」という。)と連動し、一元的な設定管理及び制御を行う機能を有すること。また以下の機能を含めること。
 - 4.2.1 アプライアンス群の個々の設定のバックアップを保持し、常時同期をとる機能
 - 4.2.2 アプライアンス群の故障交換時において、故障機が保持していた設定を自動復元する機能
 - 4.2.3 WebUI を介してアプライアンス群へ一括でファームウェア等のバージョンアップを行う機能
 - 4.2.4 禁止されたドメインへの DNS リクエストの回答を、指定した IP アドレスに設定できる機能。
 - 4.2.5 CSV 形式の DNS ブラックリストを Web ベースの管理 GUI から登録する機能。
 - 4.2.6 DNS ブラックリストをアプライアンス群で自動同期する機能。
 - 4.2.7 DHCP の MAC アドレスフィルターをアプライアンス群で自動同期し一元管理する機能。
 - 4.2.8 DNS 及び DHCP のクエリ応答状況を監視するため、成功数、失敗数、再帰検索数等の処理累積数を表示し、またそれぞれ秒間処理数の履歴をグラフ表示する機能
 - 4.2.9 各拠点の DHCP サーバで発行された IP アドレスの発行状況と、IP アドレスが発行されたデバイスの情報を Web インターフェースで、一元的に集中管理する機能
 - 4.2.10 各ネットワークセグメントの IP アドレス使用率を可視化する機能
- 4.3 前項で構成される機器間の設定情報、データ同期はリアルタイムで行われ、その通信は VPN 通信を介して暗号されること。また、機器間で行われる DNS ゾーン転送や DHCP リース情報についても例外なくリアルタイムで同期が行われ、その通信は VPN 通信を介して暗号されること。
- 4.4 III-2.1 権威 DNS のマスタサーバーとして稼働し、各権威 DNS アプライアンスに DNS ゾーン転送を行うこと。その際公開する DNS ゾーンデータに自身が NS レコードとして登録され

ないこと。また通信経路は SSL で暗号化されていること。

- 4.5 本学が提供を受けている SINET 分散セカンダリ DNS サービスに対し、DNS ゾーン転送を行うこと。
- 4.6 自身が本仕様書 III-3 の DHCP サーバ機能を有し、DHCP サーバとしても稼働できること。その際、冗長構成の 1 台が停止しても同サービスの更新業務が継続できること。
- 4.7 Web ベースの管理 GUI にてネットワーク内の IP アドレス利用状況を図示し、空きアドレスや接続ホストの情報を確認できること。
- 4.8 Web ベースの管理 GUI にてネットワークの設定状況を図示し、ネットワークの追加、削除、分割、結合などが行えること。
- 4.9 ネットワーク内のホストについて、管理者名、設置場所など任意の属性情報を付与して記録、表示、検索、フィルター等の管理を行えること。
- 4.10 Active Directory と連携することでユーザー名を取得して IP アドレス管理画面に表示する機能を有すること。
- 4.11 ホスト情報を属性によってグループ化し、階層構造でグループに属するホストの最新情報を表示する機能を有すること。
- 4.12 VMWare 等の仮想マシン情報を取得し、IP アドレスの利用状況を図示及び管理する機能を有すること。

5 UPS

国立・千代田の各拠点に UPS を設置し、各サービスアプライアンスの電源管理を行うこと。

- 5.1 入力電源は単相 100V とすること。各サービスアプライアンスの電源供給に必要な出力コンセントを有すること。
- 5.2 停電後 10 分までにすべてのサービスアプライアンスのシャットダウンを終了するよう設定調整し、その間に必要な電源容量を確保すること。
- 5.3 復電時の自動起動設定を行うこと。
- 5.4 UPS と各サービスアプライアンスの連携には RS-232C、USB または Ethernet を使用すること。Ethernet を使用する場合は学内 LAN から独立した経路とし、サービスアプライアンスの IPMI ポートを使用すること。連携に必要なケーブル類、機器類は調達に含めること。
- 5.5 TIA/EIA-310-D 準拠のラックにマウントすること。バッテリーを含めた使用ユニット数は以下とすること。
 - ◆ 国立: 4U 以下
 - ◆ 千代田: 2U 以下
- 5.6 UPS 本体の期待寿命は 10 年以上、内蔵バッテリーの期待寿命は 5 年以上であること。
- 5.7 負荷機器への給電を停止することなく、オンライン状態でのバッテリー交換作業が可能なこと。
- 5.8 インバータモジュール等の主要部品交換時においても、負荷機器への給電を継続すること。

IV 導入・設置・保守要件

1 導入・設置要件

- 1.1 調達機器は、本学が指定する場所(ラック)に収容すること。収容に必要な部材は本調達に含むこと。
- 1.2 作動に必要な配線を行うこと。
- 1.3 電源供給に必要な作業を行うこと。
- 1.4 既存機器からの設定移行、本調達の各機器の連動試験を行うこと。既存機器からの追加機能設定がある場合は本学の指示に従って設定を行うこと。
- 1.5 既存機器でサービス中の DNS 及び DHCP を停止することなく作業を行うこと。
- 1.6 UPS 連動作業を行うこと。
- 1.7 設定と運用に必要な設定手順書を提出すること。手順書には、設定画面を図示した上で、必要な操作を具体的に日本語で記述すること。また手順書には以下の項目を含むこと。
 - 1.7.1 システム操作(起動、終了、バックアップ、基本操作、システム監視)
 - 1.7.2 ライセンス操作
 - 1.7.3 DNS 設定
 - 1.7.4 DHCP 設定
 - 1.7.5 冗長構成の設定と障害時の復旧手順
 - 1.7.6 障害発生時の確認事項と対応手順
- 1.8 前項を含め、本調達において受注者が作成する成果物の著作権（著作権法第 21 条から第 28 条に定める全ての権利を含む。）は、既存の製品付属のマニュアル、ドキュメント部分（受注者が既に著作権を保有しているもの（以下「受注者著作物」という。）が組み込まれている場合は、当該受注者著作物の著作権を含む。）を除き、本学に帰属するものとする。

なお、受注者は、成果物に関する著作者人格権（著作権法第 18 条から第 20 条までに規定された権利をいう。）を行使しないものとする。

あわせて、前述の受注者著作物について、本システムへ利用する目的の範囲に限り、本学は受注者に権利留保された著作物を自由に複製し、及びそれらの利用を第三者に許諾することができるものとする。ただし、成果物に第三者の権利が帰属するときはこの限りでないものとし、この場合には複製等ができる範囲やその方法等について協議するものとする。また、成果物に第三者が権利を有する著作物が含まれる場合には、**⑧** 受注者が当該著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続きを行うものとする。

2 保守要件

- 2.1 5 年分のサブスクリプションライセンスを提供すること。またライセンス期間において平日 9 ～17 時のオンサイト保守を実施すること。
- 2.2 不具合発生時には、平日 9 時から 17 時まででは通報から 4 時間以内、17 時以降は翌営業日の朝から対応作業を開始すること。

- 2.3 製造元または販売代理店が運営する保守サポート専用の Web サイトのアカウントを提供すること。本学が既にアカウントを所有しサブスクリプションの追加登録が可能な場合は、既存のアカウントに当該ライセンスを追加すること。

Web サイトにはセキュリティ対策、重要なソフトウェアの不具合、新 OS のバージョンのリリース等を掲載し、内容変更時には速やかに電子メールにて運用担当者へ情報提供すること。

- 2.4 保守連絡体制を明示すること。受注業者と異なる製造元、販売代理店の製品を組み合わせで納入する場合には、受注業者が本学との窓口になること。

V 提案書提出要項

提案書提出は、「DNS・DHCP サービスアプライアンス 一式」の導入を行う受注業者を選定するために求めるものである。本学が必要としている物品、役務等の内容については、本仕様書で説明しているので、提案書提出希望者は、仕様書に提示されている事項について十分留意し、以下の提案書作成要項に従って提案書を作成し提出すること。

1 提案書記述項目

- 1.1 本仕様書に提示している各項目内容を要件とし、その対応、方策、性能データを具体的に提案すること。
- 1.2 既存のシステムとのデータ連携については、本学及び本学が指定する企業から必要な資料を入手し十分な調査検討を行った上で提案すること。
- 1.3 提案書においては、提案システムまたは類似システムによる納入・運用実績を明示するか、要件を満たすことが可能であると判断する根拠となった資料の一覧を明記すること。
- 1.4 別途、下記事項についても提案書に含めること。
 - ① システム構成：提案システムの全体構成図
 - ② ハードウェアの構成：機器毎に名称、型名、規格、機能、性能、寸法、消費電力、ライセンス形態、数量など。
 - ③ ネットワークの構成：納入機器類に関係するネットワークなど。
 - ④ 必要な床面積及び床に係る荷重：内訳、レイアウト案を含む。
 - ⑤ 電源及び空調の仕様：電源プラグの形状、消費電力及び発熱量を含む。
 - ⑥ 定常的保守の内容と緊急的保守の体制。
 - ⑦ 本学の要望に対する作業体制、方法及びメンテナンス等について、営業日及び営業日外の作業人数、体制、方法など。
 - ⑧ 障害発生時の連絡先と対応体制、本学に到着するまでの必要所要時間の概算など。
 - ⑨ マニュアル：種類、記述言語など。
 - ⑩ 納入実績：提案システムあるいは類似システムに関する実績（機関名、構築概要、構築期間、導入した機器類等）の一覧
 - ⑪ 作業区分：詳細な作業日程及び受注業者と本学との作業の区分
 - ⑫ ランニングコスト：本仕様書に記されている要件以外に機器やシステムなどを運用・管理し続けるために継続的に必要な経費がある場合は、その項目と内容、金額
 - ⑬ 提出資料に関する照会先：提出された内容等に関して、問い合わせやヒアリング、デモンストレーションを要求する場合の照会先など。

2 使用言語、書式など

- 2.1 日本語とすること。
- 2.2 A 4 判、縦、横書き、左とじ、ワープロ印刷を原則とすること。
(図表等については、必要に応じて A 4 判横置き of 形式も可とする。)

2.3 技術的な説明等のために、既存の資料を使用する場合は、提案書本体とは別綴じとし「参考資料」と明記すること。

2.4 項目番号の付け方は以下のとおりとすること。

- ① 章……1.
- ② 節……1.1
- ③ 項……1.1.1

(注1) 上記の項目番号で不足が生じる場合は、適宜設定して構わない。

(注2) 図表番号の付け方は、「章番号－連番」の形式とし、図表題名を付与すること。

(例) 図 1-1 ○○○○○○

表 2-1 ○○○○○○

3 要求仕様対応表の記載時の注意

3.1 提案書は約 50 ページ以内を目途とし、簡潔かつ明瞭に記述すること。ただし、別綴の「参考資料」については、このページ数に含めない。

3.2 仕様書の各章、節、項で定義されている要求仕様、提案する物品の仕様等を対比させて記載すること。

(例1)

章・節・項	要求仕様	○○の仕様
2.1.1 ○○要件について	○○について機能を有すること。	○○の方法にて対応します。
3.1 設置、搬入	(1)メンテナンス性を考慮…	○○により、メンテナンス…
	②△△	…

(例2)

章・節・項	要求仕様	○○の仕様
2.3.1 基本機能	2つ以上の…備えること…	4つの○○を備えて…
2.3.2 ハードウェア構成 …	(1) 本体…	○cm×○cm×○…
	(2) C P U…	○○社製○○を○台、○GHz…

4 体裁

4.1 提案書及び参考資料を含む提出物は、すべて冊子の体裁で提出すること。

4.2 提出するすべての冊子の表紙に、タイトル、案件名及び会社名を明記すること。

4.3 提案書には、次の項目を明記及び押印すること。

- ① 住所
- ② 会社名
- ③ 社印

- ④ 代表者名
- ⑤ 代表者印

5 提案書等に関する留意事項

- 5.1 単に「できます」、「有ります」などのみの提案では、評価に支障をきたすので、提案システムが本仕様書の要求要件をどのように満たすか、あるいはどのように実現するかを要求要件ごとに具体的かつ、わかりやすく資料等を添付するなどして説明すること。
- 5.2 カタログ等については、各メーカーが自社のカタログと同等のものとして公開している Web ページであれば、当該ページの印刷出力でも代替可能とする。
ただし、Web ページの印刷出力による当該代替物については、印刷時のレイアウト崩れや文字化け、内容や日付等の意図的な改竄等によって、「代替する資料と同等であると認められない」と本学が判断した場合は、代替できない。
- 5.3 記載内容が不明確である場合は、有効な提案書としてみなさない。
特に審査するに当たって、提案の根拠が不明確、説明が不十分で技術審査に重大な支障があると本学が判断した場合は、要求要件を満たしていないものとみなす。
- 5.4 調達物品を構成するソフトウェアについて、カスタマイズによる開発によって仕様書に記載する技術的要件を満たす場合には、これに係る技術的資料、開発計画書及び確約書を併せて提出すること。
- 5.5 必要に応じてヒアリングあるいはデモンストレーションなどを要求した場合は、真摯に対応すること。
- 5.6 提案書の提出、納品及び保守サービスの過程において知り得た案件に関する一切の情報に対して、故意または過失にかかわらず、本学の許可無く第三者に開示しないこと。
- 5.7 提案書作成に要する費用負担は行わない。
- 5.8 原則として提案書は返却しない。

VI 技術審査

1 技術審査の方法

「DNS・DHCP サービスアプライアンス一式 調達仕様書」に示した内容について、仕様を満たす提案がなされているかどうかを評価する。この審査の結果、発注が可能と判断できた提案者を技術審査通過者とする。

2 提案内容のヒアリング

必要に応じ、提出を受けた提案書について、指定した日時にヒアリングを実施する場合がある。

3 提案物品のデモンストレーション

必要に応じ、提案物品について、指定した日時にデモンストレーションを要求する場合がある。

4 異議申立て

技術審査結果に対する異議申立ては、一切認めない。