I	**ネットワーク基盤整備**
	ネットワーク基盤整備 本ネットワーク基盤は広島市立大学の情報ネットワークを構成し、インターネット接続を提供するとともに、大学の教育、研究、事務に必要なデジタル化されたサービスが利用できるプラットフォームとして機能する。また、安全なプラットフォーム利用のため、セキュリティ機構や認証機構をもつ。以下はこのネットワーク基盤の全体や構成要素の要件を示すものである。
1.0	**情報セキュリティポリシに関する要件** 本システムは本学情報セキュリティポリシーに準拠すること。また、本学のクラウドサービスチェックリストによりチェックすること。当該チェックリストは別途配付する。なお、セキュリティ対策規定は本学Webサイトに提示しており、実施基準、対策手順は契約後に提示する。
1.1	**ネットワーク基盤共通要件**
(1)	学内の既存ネットワーク接続を維持しつつ、基幹ネットワークの集約と高度化を行うこと。
(2)	機器の二重化等の冗長構成により、耐故障性を高めること。
(3)	現行と同様に学内の全ての組織・施設から利用可能な接続性を持つこと。
(4)	学内の通信トラフィックに対応可能な帯域を持つこと。
(5)	組織構成の変更に柔軟に対応したネットワークトポロジを実現可能であること。
(6)	運用管理性も考慮し、より高度なセキュリティ対策が実現可能であること。
(7)	AC100V電源に対応していること。
(8)	別紙1「ネットワーク構成図」を参考に個別の構成要素を構成すること。別紙1が必要な場合は、依頼に応じて提供する。
1.1.1	**基幹スイッチ　2式（DC設置）** 基幹スイッチは1式あたり、以下の仕様を有すること。
(1)	1,080Gbps以上のスイッチング容量を実装するボックス型のL3スイッチ製品であること。
(2)	最大8台までのスタッキングに対応し、スタックされた全ての筐体は1台の論理ユニットとして設定・管理できること。
(3)	複数のスイッチをスタックした構成で、異なるスタックスイッチ間でリンクアグリゲーション構成可能なこと。
(4)	インターフェースは10ギガビットイーサネットSFP+24ポート以上実装していること。
(5)	800Mpps以上の転送レート(パケット処理性能)を持つこと。
(6)	Media Access Control（MAC）エントリ として 112,000 あること。
(7)	ARPエントリを 24,000 サポートすること。
(8)	装置内で複数のルーティングポリシーを独立して保有するVRF（Virtual Routing and Forwarding）機能を有していること。
(9)	IPv4/IPv6デュアルスタック機能を有すること。
(10)	IPv6 MulticastおよびMLDv1/MLDv2 Snooping機能をサポートすること。
(11)	不正なIPv6 RA（Router Advertisment）を廃棄する機能を保有すること。
(12)	コントロール プレーン ポリシングを含むCPU レート リミッタ（DoS 攻撃対策）に対応可能なこと。
(13)	同一筐体内で電源の二重化機能を有すること。
(14)	光ファイバやツイストペアケーブルの単一方向リンク検出機能（UDLD）を有すること。
(15)	ブロードキャスト、マルチキャストのストーム制御機能を有すること。
(16)	GUIを使用して設定を行える機能を有すること。
(17)	シリアル接続によるコンソールポートを有すること。
(18)	SSH等によるセキュアなリモート・コンソール機能を有すること。
(19)	ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードが可能であること。
(20)	NTPクライアントとして、一貫したタイムスタンプを刻む機能を有すること。
(21)	Syslogサーバにメッセージを送信する機能を有すること。
(22)	SNMPv1/v2c/v3による管理機能を有すること。
(23)	隣接するデバイスのと間で、トポロジの管理を行うためのプロトコル（CDP、LLDP等)を実装していること。
(24)	トラフィック解析のためポートのミラーリング機能を有し、同一筐体内のみならず、他の筐体のポートもミラーリングできる機能を有すること。
(25)	トランシーバを必要数有すること。
1.1.2	**キャンパス集約スイッチ　2式** キャンパス集約スイッチは1式あたり、以下の仕様を有すること。
(1)	800Gbps以上のスイッチング容量を実装するボックス型のL3スイッチ製品であること。
(2)	最大8台までのスタッキングに対応し、スタックされた全ての筐体は1台の論理ユニットとして設定・管理できること。
(3)	複数のスイッチをスタックした構成で、異なるスタックスイッチ間でリンクアグリゲーション構成可能なこと。
(4)	10ギガビットイーサネットSFP+ポートを4ポート以上実装していること。
(5)	1ギガビットイーサネットSFPポートを16ポート以上実装していること。
(6)	600Mpps以上の転送レート(パケット処理性能)を持つこと。
(7)	19インチラックマウント可能であり、1U以下のサイズであること。
(8)	IEEE802.1Q VLAN Tagging機能を有すること。
(9)	IEEE802.1wに準拠した高速スパニングツリー機能を有すること。
(10)	IEEE 802.3ad Link Aggregation機能を有すること。
(11)	BPDUを期待しないポートでBPDUを受信した際、ループを防ぐためにそのポートを自動的にダウンする機能を有すること。
(12)	スイッチングハブの追加等により期待されていないBPDUを受けルートブリッジが変更されてしまう事態を防止する機能を有すること。
(13)	光ファイバやツイストペアケーブルの単一方向リンク検出機能（UDLD）を有すること。
(14)	ポートごとに通信可能なMACアドレス、またはMACアドレス数を制限する機能を有すること。
(15)	MACアドレスとIPアドレスのマップをスイッチ上で管理することによって偽造ARPによる不正な通信盗聴を防止する機能を有すること。
(16)	信頼されないDHCPメッセージを破棄するDHCP snooping機能を有すること。
(17)	ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること。
(18)	GUIを使用して設定を行える機能を有すること。
(19)	シリアル接続によるコンソールポートを有すること。
(20)	SSH等によるセキュアなリモート・コンソール機能を有すること。
(21)	ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードが可能であること。
(22)	NTPクライアントとして、一貫したタイムスタンプを刻む機能を有すること。
(23)	Syslogサーバにメッセージを送信する機能を有すること。
(24)	SNMPv1/v2c/v3による管理機能を有すること。
(25)	隣接するデバイスのと間で、トポロジの管理を行うためのプロトコル（CDP、LLDP等)を実装していること。
(26)	トラフィック解析のためポートのミラーリング機能を有し、同一筐体内のみならず、他の筐体のポートもミラーリングできる機能を有すること。
(27)	管理性、操作性等を考慮し各機器のコマンドラインは基幹スイッチと同一であること。
1.1.3	**キャンパスサーバ集約スイッチ　2式** キャンパスサーバ集約スイッチは1式あたり、以下の仕様を有すること。
(1)	最大300Gbps以上のスイッチング容量を実装するボックス型のL2スイッチ製品であること。
(2)	最大8台までのスタッキングに対応し、スタックされた全ての筐体は1台の論理ユニットとして設定・管理できること。
(3)	複数のスイッチをスタックした構成で、異なるスタックスイッチ間でリンクアグリゲーションを構成可能なこと。
(4)	10/100/1000イーサネットポートを48ポート以上実装していること。
(5)	10ギガビットイーサネットSFP+ポートを4ポート以上実装していること。

(6) 200Mpps以上の転送レート(パケット処理性能)を持つこと。
(7) 19インチラックマウント可能であり、1U以下のサイズであること。
(8) IEEE802.1Q VLAN Tagging機能を有すること。
(9) IEEE802.1wに準拠した高速スパニングツリー機能を有すること。
(10) IEEE 802.3ad Link Aggregation機能を有すること。
(11) GUIを使用して設定を行える機能を有すること。
(12) シリアル接続によるコンソールポートを有すること。
(13) SSH等によるセキュアなリモート・コンソール機能を有すること。
(14) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードが可能であること。
(15) NTPクライアントとして、一貫したタイムスタンプを刻む機能を有すること。
(16) Syslogサーバにメッセージを送信する機能を有すること。
(17) SNMPv1/v2c/v3による管理機能を有すること。
(18) 隣接するデバイスのと間で、トポロジの管理を行うためのプロトコル(CDP、LLDP等)を実装していること。
(19) トラフィック解析のためポートのミラーリング機能を有し、同一筐体内のみならず、他の筐体のポートもミラーリングできる機能を有すること。
(20) 管理性、操作性等を考慮し各機器のコマンドラインは基幹スイッチと同一であること。

1.1.4 建屋集約スイッチ 18式

建屋集約スイッチは、以下の仕様を有すること。
(1) 導入するスイッチの台数は、機種毎に以下の通りとする。
・48ポートUTP 建屋集約スイッチ x4式
・48ポートSFP 建屋集約スイッチ x3式
・24ポートUTP 建屋集約スイッチ x11式

各機種個別の仕様は以下の通りとする。

48ポートUTP 建屋集約スイッチ x4式

(2) 10/100/1000 イーサネットポートを48ポート以上実装していること。
(3) 200Mpps以上の転送レート(パケット処理性能)を持つこと。

48ポートSFP 建屋集約スイッチ x3式

(5) 1ギガビットイーサネット SFPポート を36ポート以上実装していること。
(6) 10ギガビットイーサネットSFP+ポートを4ポート以上実装していること。
(7) 600Mpps以上の転送レート(パケット処理性能)を持つこと。

24ポートUTP 建屋集約スイッチ x11式

(8) 10/100/1000 イーサネットポートを24ポート以上実装していること。
(9) 200Mpps以上の転送レート(パケット処理性能)を持つこと。

共通仕様は以下の通りとする。

(10) 最大8台までのスタッキングに対応し、スタックされた全ての筐体は1台の論理ユニットとして設定・管理できること。
(11) 複数のスイッチをスタックした構成で、異なるスタックスイッチ間でリンクアグリゲーション構成可能なこと。
(12) 19インチラックマウント可能であり、1U以下のサイズであること。
(13) IEEE802.1Q VLAN Tagging機能を有すること。
(14) IEEE802.1wに準拠した高速スパニングツリー機能を有すること。
(15) IEEE 802.3ad Link Aggregation機能を有すること。
(16) BPDUを期待しないポートでBPDUを受信した際、ループを防ぐためにそのポートを自動的にダウンする機能を有すること。
(17) スイッチングハブの追加等により期待されていないBPDUを受けルートブリッジが変更されてしまう事態を防止する機能を有すること。
(18) 光ファイバやツイストペアケーブルの単一方向リンク(片対障害)検出機能を有すること。
(19) ポートごとに通信可能なMACアドレス、またはMACアドレス数を制限する機能を有すること。
(20) MACアドレスとIPアドレスのマップをスイッチ上で管理すること。によって偽造ARPによる不正な通信盗聴を防止する機能を有すること。

(21) 信頼されないDHCPメッセージを破棄するDHCP snooping機能を有すること。
(22) ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること。
(23) GUIを使用して設定を行える機能を有すること。
(24) シリアル接続によるコンソールポートを有すること。
(25) SSH等によるセキュアなリモート・コンソール機能を有すること。
(26) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードが可能であること。
(27) NTPクライアントとして、一貫したタイムスタンプを刻む機能を有すること。
(28) Syslogサーバにメッセージを送信する機能を有すること。
(29) SNMPv1/v2c/v3による管理機能を有すること。
(30) 隣接するデバイスのと間で、トポロジの管理を行うためのプロトコル(CDP、LLDP等)を実装していること。
(31) トラフィック解析のためポートのミラーリング機能を有し、同一筐体内のみならず、他の筐体のポートもミラーリングできる機能を有すること。
(32) 管理性、操作性等を考慮し各機器のコマンドラインは基幹スイッチと同一であること。
(33) トランシーバを必要数有すること。

1.1.5 エッジスイッチ(情報科学部・国際学部・芸術学部・サテライトキャンパス)

エッジスイッチ(情報科学部・国際学部・芸術学部・サテライトキャンパス)は、以下の仕様を有すること。
(1) 導入するスイッチの台数は以下の通りとする。
・48ポート エッジスイッチ x35式
・24ポート エッジスイッチ x69式

各機種個別の仕様は以下の通りとする。

48ポート エッジスイッチ x35式

(2) 10/100/1000イーサネットポートを48ポート以上実装していること。
(3) 1ギガビットイーサネットSFPポートを4ポート以上実装していること。
(4) 70Mpps以上のパケット処理能力を有すること。
(5) IEEE 802.3adに準拠したLink Aggregation機能を有すること。

24ポート エッジスイッチ x69式

(6) 10/100/1000イーサネットポートを24ポート以上実装していること。
(7) 1ギガビットイーサネットSFPポートを2ポート以上実装していること。
(8) 35Mpps以上のパケット処理能力を有すること。
(9) IEEE 802.3adに準拠したLink Aggregation機能を有すること。

共通仕様は以下の通りとする。

(10) 19インチラックマウント可能であり、1U以下のサイズであること。

(11) BPDUの受信時にスパニングツリーPortFast対応インターフェイスをシャットダウンして、予期せぬトポロジループを阻止する機能を有すること。
(12) ネットワーク管理者の制御下にないエッジ デバイスがスパニングツリープロトコルのルートノードになることを阻止する機能を有すること。
(13) 光ファイバやツイストペアケーブルの単一方向リンク(片対障害)検出機能を有すること。
(14) MACアドレスに基づいてアクセスまたはトランクポートへのアクセスを保護し、学習されるMACアドレスの数を制限する機能を有すること。
(15) 悪意のあるユーザがDHCPサーバをスプーフィングし、偽装したアドレスを送信することを防ぐ機能を有すること。
(16) 悪意のあるユーザがARPプロトコルのセキュリティの弱点を悪用するのを阻止し、ユーザの整合性を保証する機能を有すること。
(17) ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること。
(18) ループ接続が起こった際に、発生したポートを遮断することでループ障害を最小限におさえる機能を有すること。
(19) IEEE802.1X認証、MAC認証、WEB認証の機能を有すること。なお、IEEE802.1X/MAC/WEB認証を1つのポートで同時待ち受け可能であること。
(20) シリアル接続によるコンソールポートを有すること。
(21) SSH等によるセキュアなリモート・コンソール機能を有すること。
(22) トラフィック解析のためポートのミラーリング機能を有すること。
(23) NTPクライアントとして、一貫したタイムスタンプを刻む機能を有すること。
(24) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードする機能を有すること。
(25) Syslogサーバにメッセージを送信する機能を有すること。
(26) SNMPv1/v2c/v3による管理機能を有すること。
(27) 起動時、および稼動中(トラブルシューティング時)に、機器動作の信頼性を維持するための総合的な自己診断機能を有すること。
(28) 「1.3.13 ネットワーク監視機能」等と連携し、動作温度、ハードウェアの稼働時間、その他の重要なイベントやメッセージなどのデータを収集できること。

1.1.6 入退管理用スイッチ 28式
8ポート エッジスイッチ x28式

(1) 10/100/1000イーサネットポートを8ポート以上実装していること。
(2) 1ギガビットイーサネットSFPポートを2ポート以上実装していること。
(3) 14Mpps以上のパケット処理能力を有すること。
(4) IEEE 802.3ad Link Aggregation機能を有し、最大6個のLink Aggregationを設定可能な機能を有すること。

共通仕様は以下の通りとする。

(5) 19インチラックマウント可能であり、1U以下のサイズであること。
(6) BPDUの受信時にスパニングツリーPortFast対応インターフェイスをシャットダウンして、予期せぬトポロジループを阻止する機能を有すること。
(7) ネットワーク管理者の制御下にないエッジ デバイスがスパニングツリープロトコルのルートノードになることを阻止する機能を有すること。
(8) 光ファイバやツイストペアケーブルの単一方向リンク(片対障害)検出機能を有すること。
(9) MACアドレスに基づいてアクセスまたはトランクポートへのアクセスを保護し、学習されるMACアドレスの数を制限する機能を有すること。
(10) 悪意のあるユーザがDHCPサーバをスプーフィングし、偽装したアドレスを送信することを防ぐ機能を有すること。
(11) 悪意のあるユーザがARPプロトコルのセキュリティの弱点を悪用するのを阻止し、ユーザの整合性を保証する機能を有すること。
(12) ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること。
(13) シリアル接続によるコンソールポートを有すること。
(14) SSH等によるセキュアなリモート・コンソール機能を有すること。
(15) トラフィック解析のためポートのミラーリング機能を有すること。
(16) NTPクライアントとして、一貫したタイムスタンプを刻む機能を有すること。
(17) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードする機能を有すること。
(18) Syslogサーバにメッセージを送信する機能を有すること。
(19) SNMPv1/v2c/v3による管理機能を有すること。
(20) 起動時、および稼動中(トラブルシューティング時)に、機器動作の信頼性を維持するための総合的な自己診断機能を有すること。
(21) 「1.3.13 ネットワーク監視機能」等と連携し、動作温度、ハードウェアの稼働時間、その他の重要なイベントやメッセージなどのデータを収集できること。

1.1.7 外部接続L2スイッチ 1式(DC設置)
外部接続L2スイッチは1式あたり、以下の仕様を有すること。
(1) 最大300Gbps以上のスイッチング容量を実装するボックス型のL2スイッチ製品であること。
(2) 10/100/1000イーサネットポートを24ポート以上実装していること。
(3) 10ギガビットイーサネットSFP+を2ポート以上実装していること。
(4) 200Mpps以上の転送レート(パケット処理性能)を持つこと。
(5) 19インチラックマウント可能であり、1U以下のサイズであること。
(6) IEEE802.1Q VLAN Tagging機能を有すること。
(7) IEEE802.1wに準拠した高速スパニングツリー機能を有すること。
(8) IEEE 802.3ad Link Aggregation機能を有すること。
(9) ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること。
(10) GUIを使用して設定を行える機能を有すること。
(11) シリアル接続によるコンソールポートを有すること。
(12) SSH等によるセキュアなリモート・コンソール機能を有すること。
(13) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードが可能であること。
(14) NTPクライアントとして、一貫したタイムスタンプを刻む機能を有すること。
(15) Syslogサーバにメッセージを送信する機能を有すること。
(16) SNMPv1/v2c/v3による管理機能を有すること。
(17) 隣接するデバイスのと間で、トポロジの管理を行うためのプロトコル(CDP、LLDP等)を実装していること。
(18) トラフィック解析のためポートのミラーリング機能を有し、同一筐体内のみならず、他の筐体のポートもミラーリングできる機能を有すること。
(19) 管理性、操作性等を考慮し各機器のコマンドラインは基幹スイッチと同一であること。
(20) トランシーバを必要数有すること。

1.1.8 10Gサーバスイッチ 2式(DC設置)
10Gサーバスイッチは1式あたり、以下の仕様を有すること。
(1) 10ギガビットイーサネットSFP+を24ポート以上実装していること。
(2) 25ギガビットイーサネットSFP28ポートを4ポート以上実装していること。
(3) スイッチング容量が1080Gbps以上であること。
(4) 800Mpps以上の転送レート(パケット処理性能)を持つこと。
(5) 最大8台までのスタッキングに対応し、スタックされた全ての筐体は1台の論理ユニットとして設定・管理できること。
(6) 複数のスイッチをスタックした構成で、異なるスタックスイッチ間でリンクアグリゲーション構成可能なこと。
(7) 19インチラックマウント可能であり、1U以下のサイズであること。
(8) IEEE802.1Q VLAN Tagging機能を有すること。

(9) IEEE802.1wに準拠した高速スパニングツリー機能を有すること。
(10) IEEE 802.3ad Link Aggregation機能を有すること。
(11) コントロール プレーン ポリシングを含むCPU レート リミッタ（DoS 攻撃対策）に対応可能なこと。
(12) 同一筐体内で電源の二重化機能を有すること。
(13) 光ファイバやツイストペアケーブルの単一方向リンク検出機能（UDLD）を有すること。
(14) ブロードキャスト、マルチキャストのストーム制御機能を有すること。
(15) GUIを使用して設定を行える機能を有すること。
(16) シリアル接続によるコンソールポートを有すること。
(17) SSH等によるセキュアなリモート・コンソール機能を有すること。
(18) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードが可能であること。
(19) NTPクライアントとして、一貫したタイムスタンプを刻む機能を有すること。
(20) Syslogサーバにメッセージを送信する機能を有すること。
(21) SNMPv1/v2c/v3による管理機能を有すること。
(22) 隣接するデバイスのと間で、トポロジの管理を行うためのプロトコル（CDP、LLDP等)を実装していること。
(23) トラフィック解析のためポートのミラーリング機能を有し、同一筐体内のみならず、他の筐体のポートもミラーリングできる機能を有すること。
(24) トランシーバを必要数有すること。

1.1.9 1Gサーバスイッチ 2式（DC設置）

1Gサーバスイッチは1式あたり、以下の仕様を有すること。
(1) 最大250Gbps以上のスイッチング容量を実装するボックス型のL2スイッチ製品であること。
(2) 10/100/1000イーサネットポートを48ポート以上実装していること。
(3) 10ギガビットイーサネットSFP+ポートを4ポート以上実装していること。
(4) 190Mpps以上の転送レート(パケット処理性能)を持つこと。
(5) 最大8台までのスタッキングに対応し、スタックされた全ての筐体は1台の論理ユニットとして設定・管理できること。
(6) 複数のスイッチをスタックした構成で、異なるスタックスイッチ間でリンクアグリゲーション構成可能なこと。
(7) 19インチラックマウント可能であり、1U以下のサイズであること。
(8) IEEE802.1Q VLAN Tagging機能を有すること。
(9) IEEE802.1wに準拠した高速スパニングツリー機能を有すること。
(10) IEEE 802.3ad Link Aggregation機能を有すること。
(11) 同一筐体内で電源の二重化機能を有すること。
(12) 光ファイバやツイストペアケーブルの単一方向リンク検出機能（UDLD）を有すること。
(13) ブロードキャスト、マルチキャストのストーム制御機能を有すること。
(14) GUIを使用して設定を行える機能を有すること。
(15) シリアル接続によるコンソールポートを有すること。
(16) SSH等によるセキュアなリモート・コンソール機能を有すること。
(17) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードが可能であること。
(18) NTPクライアントとして、一貫したタイムスタンプを刻む機能を有すること。
(19) Syslogサーバにメッセージを送信する機能を有すること。
(20) SNMPv1/v2c/v3による管理機能を有すること。
(21) 隣接するデバイスのと間で、トポロジの管理を行うためのプロトコル（CDP、LLDP等)を実装していること。
(22) トラフィック解析のためポートのミラーリング機能を有し、同一筐体内のみならず、他の筐体のポートもミラーリングできる機能を有すること。
(23) トランシーバを必要数有すること。

1.1.10 ロードバランサ 2式（DC設置）

ロードバランサは1式あたり、以下の仕様を有すること。
(1) サーバロードバランサー及びSSLアクセラレータとしての機能を有するハードウェアアプライアンスであること。なお、冗長構成であること。
(2) ソースIPアドレスを元にした負荷分散ができること。
(3) URLやHTTPヘッダに含まれる文字列による分散ができること。また、X-Forwarded-Forヘッダを元にした負荷分散ができること。
(4) TCPコネクション、UDP送達確認によるサーバヘルスチェックと組み合わせて、HTTP応答データ確認（返信文字列、ステータスコード）でもヘルスチェックできること。
SSLハンドシェイク、DNS、FTP、IMAP、NTP、POP3、SMTPのヘルスチェックができること。
(5) ソースNAT設定なしでワンアーム構成ができること。
(6) CLI／GUI両方から同じ設定が出来ること。
(7) システムスループット(L4)が7.5Gbps以上であること。
(8) L7負荷分散パケットをキャプチャーできること。
(9) SSL新規トランザクションが15,000トランザクション/秒以上であること。
(10) SSLアクセラレータ機能を有し、TLS暗号スイートに対応していること。
(11) 10BASE-T/100BASE-TX/1000BASE-T 10ポート以上有すること。
(12) 最大消費電力は100W以下であること。

1.1.11 リモートメンテナンス用VPN装置 1式（DC設置）

リモートメンテナンス用VPN装置は1式あたり、以下の仕様を有すること。
(1) 3DES/AES VPNスループットは最大350Mbps以上を有すること。
(2) ClientまたはClientless SSL-VPNコネクション数が最大50対応可能なこと。
(3) リモートアクセスVPNクライアントソフトウェアはWindows、MacOS、Linux、Apple iOS、Android、Blackberry、Chrome OSに対応すること。
(4) RJ45シリアル接続によるコンソールポートを有すること。
(5) SSH等によるセキュアなリモート・コンソール機能を有すること。
(6) GUIによる運用管理機能を有すること。
(7) 8ポート以上の10/100/1000Tインターフェースを有すること。
(8) USB2.0ポートを1ポート以上有すること。
(9) 専用の管理ポートを1ポート以上有すること。
(10) 19インチラックにマウント可能なこと。

1.1.12 コンソールスイッチ 1式（DC設置）

コンソールスイッチは1式あたり、以下の仕様を有すること。
(1) RJ45のシリアルポートを16ポート以上有すること。
(2) 10/100/1000イーサネットポートを2ポート以上実装していること。
(3) シリアルポート接続及びSSHクライアント等のリモートアクセスを提供するポートサーバ機能を有すること。
(4) 接続状況一覧表示、ログ利用状況表示可能な運用支援機能を有すること。

1.1.13 管理集約用L2スイッチ 1式（DC設置）

管理用スイッチは1式あたり、以下の仕様を有すること。
(1) 最大200Gbps以上のスイッチング容量を実装するボックス型のL2スイッチ製品であること。
(2) 10/100/1000イーサネットポートを24ポート以上実装していること。

(3) 100Mpps以上の転送レート(パケット処理性能)を持つこと。
(4) 19インチラックマウント可能であり、1U以下のサイズであること。
(5) IEEE802.1Q VLAN Tagging機能を有すること。
(6) IEEE802.1wに準拠した高速スパニングツリー機能を有すること。
(7) IEEE 802.3ad Link Aggregation機能を有すること。
(8) 光ファイバやツイストペアケーブルの単一方向リンク検出機能（UDLD）を有すること。
(9) ブロードキャスト、マルチキャストのストーム制御機能を有すること。
(10) GUIを使用して設定を行える機能を有すること。
(11) シリアル接続によるコンソールポートを有すること。
(12) SSH等によるセキュアなリモート・コンソール機能を有すること。
(13) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードが可能であること。
(14) NTPクライアントとして、一貫したタイムスタンプを刻む機能を有すること。
(15) Syslogサーバにメッセージを送信する機能を有すること。
(16) SNMPv1/v2c/v3による管理機能を有すること。
(17) 隣接するデバイスのと間で、トポロジの管理を行うためのプロトコル（CDP、LLDP等)を実装していること。
(18) トラフィック解析のためポートのミラーリング機能を有し、同一筐体内のみならず、他の筐体のポートもミラーリングできる機能を有すること。

1.1.14 バックアップDC接続スイッチ 1式（バックアップDC設置）

バックアップDC接続スイッチは1式あたり、以下の仕様を有すること。
(1) 最大200Gbps以上のスイッチング容量を実装するボックス型のL2スイッチ製品であること。
(2) 10/100/1000イーサネットポートを24ポート以上実装していること。
(3) 10ギガビットイーサネットSFP+ポートを4ポート以上実装していること。
(4) 150Mpps以上の転送レート(パケット処理性能)を持つこと。
(5) 19インチラックマウント可能であり、1U以下のサイズであること。
(6) IEEE802.1Q VLAN Tagging機能を有すること。
(7) IEEE802.1wに準拠した高速スパニングツリー機能を有すること。
(8) IEEE 802.3ad Link Aggregation機能を有すること。
(9) 同一筐体内で電源の二重化機能を有すること。
(10) 光ファイバやツイストペアケーブルの単一方向リンク検出機能（UDLD）を有すること。
(11) ブロードキャスト、マルチキャストのストーム制御機能を有すること。
(12) GUIを使用して設定を行える機能を有すること。
(13) シリアル接続によるコンソールポートを有すること。
(14) SSHによるリモートコンソール機能を有すること。
(15) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードが可能であること。
(16) NTPクライアントとして，一貫したタイムスタンプを刻む機能を有すること。
(17) Syslogサーバにメッセージを送信する機能を有すること。
(18) SNMPv1/v2c/v3による管理機能を有すること。
(19) 隣接するデバイスのと間で、トポロジの管理を行うためのプロトコル（CDP、LLDP等)を実装していること。
(20) トラフィック解析のためポートのミラーリング機能を有し、同一筐体内のみならず、他の筐体のポートもミラーリングできる機能を有すること。
(21) トランシーバを必要数有すること。

1.1.15 バックアップ回線利用設備 （DC設置）

(1) 大学とDCを接続する10Gbps光回線（メイン回線）のバックアップ回線(10Gbps 光専用線）を本線障害時の切り替え、または併用するための機能を提供すること。
(2) メイン回線障害時にはバックアップ回線でメイン回線と同様の性能で通信が可能なこと。
(3) メイン回線障害時に自動でバックアップ回線に切り替えて通常通信が可能なこと。メイン回線復旧時には戻すことができること。
(4) メイン回線とバックアップ回線にそれぞれ特定通信の優先制御ができること。
(5) 本機能を提供するための専用装置を設置しても、他のスイッチで兼用することも可能だが。ただし、その場合、兼用されるスイッチの通信性能に影響を及ぼさないこと。
(6) 本機能を提供するための専用装置を設置する場合、19インチラックマウント可能であり、1U以下のサイズであること。

1.1.16 無線LAN管理システム

無線LAN管理システムは1式あたり、以下の仕様を有すること。
(1) 複数の無線アクセスポイント(以下、APという）を集中制御する機能を有すること。クラウドサービスでの提供も可能とする。
(2) APを300台以上管理する機能を有すること。またライセンス追加等で容易に管理台数を拡張できること。
(3) 特定のクライアント端末の通信をブロックする機能を有すること。
(4) 各AP間の自動電波・出力調整機能を有すること。
(5) 周辺の無線LAN環境に応じて、APに対し自動的に最適なチャネルやパワーを調整する機能を有すること。
(6) RFの干渉を検出し、干渉源周囲のワイヤレス電波到達範囲を最適化する自動調整機能を有すること。
(7) チャネル管理の自動化により稼働中でも最適なチャネルへの移動を行う機能を有すること。
(8) APに接続する端末の接続状態をロードバランスする機能を有すること。なお、本機能を有しない場合は、電波調整等で特定のAPに接続が偏らないよう自動制御できる機能を有すること。
(9) デュアルバンド（2.5GHz帯と5GHz帯のどちらもサポートしている端末）対応端末を5GHz帯へ誘導する機能を有すること。
(10) クライアント端末のコンピュータ名、OS種別等を可視化する機能を有すること。
(11) クライアントが利用しているアプリケーション毎の利用状況が可視化できること
(12) IPv4およびIPv6のアクセス制御とL7のファイアウォール機能を有すること。なお、本機能を有しない場合は、経路上のネットワーク機器（ファイアウォール含む）で同等の機能を代替できるよう設計すること。
(13) 時間帯によりSSIDの出力を自動的に制限する機能を有すること。
(14) 学内で利用するSSIDと同一のSSIDを提供する管理外APを自動的に検知する機能を有すること。また、不正なSSIDに接続しているクライアントを強制切断するなど、管理外APによる不正アクセス対策機能を有すること。
(15) 接続する端末に対し、MACアドレス認証、WEB認証、IEEE802.1X認証を行う機能を有すること。
(16) RADIUSサーバを参照して認証する機能を有すること。
(17) 同一SSIDにおいてIEEE802.1X認証によりユーザ毎に割り当てられたVLANで通信を行う機能を有し、設定できるVLAN数は4000以上であること。
(18) ファームウェアを自動アップグレードする機能を有すること。
(19) 端末の無線LAN使用帯域をSSID単位・ユーザ単位で制限する機能を有すること。
(20) ファイアウォールや帯域制御機能は時間帯によってポリシーを可変にできる機能を有すること。なお、本機能を有しない場合は、経路上のネットワーク機器（ファイアウォール含む）で同等の機能を代替できるよう設計すること。
(21) 登録したマップ上に端末の場所を表示する機能を有すること。
(22) クライアント端末のローミング履歴を過去に遡って追跡・表示できる機能を有すること。
(23) 外部Syslogサーバへ送信する機能を有すること。なお、クラウドサービス提供型により、本機能を有しない場合は、特定のアラートをメール通知する機能を有すること。
(24) レポーティング機能を有すること。レポートはメールで送信する機能を有すること。
(25) 端末の障害切り分けのために接続状況診断（接続エラー、パケットロス、ユーザー毎の接続帯域、などが確認、解析できること）を行う機能を有すること。

(26) APが停止した際にアラートを通知する機能を有すること。

1.1.17 アクセスポイント 124式以上

アクセスポイントは1式あたり、以下の仕様を有すること。

(1) 無線LAN管理システムによって制御可能なものであること。
(2) IEEE802.11a/b/g/n/ac/axに準拠及びWi-Fiアライアンス認定を得ていること。
(3) WPA3-Enterprise/Personal準拠及びWi-Fiアライアンス認定を得ていること。
(4) IEEE802.11axを導入すること。ただし、既に導入している端末では、IEEE802.11axに対応していないものもあるため、現在利用している規格(IEEE802.11a/b/g/n/ac)も並行して利用できる機能を有すること。
(5) IEEE802.11a/n/ac/ax においては、W52、W53、W56 に対応すること。
(6) 2.4GHz及び5GHzのワイヤレスネットワークの同時運用を行う機能を有すること。
(7) 2.4GHz 帯 2×2MIMO、2 ストリーム、5GHz 帯 4×4MIMO、4 ストリームに対応していること。
(8) 100/1000/2.5G BASE-T(RJ45)インタフェースを1つ以上有すること。
(9) IEEE802.3at/btに基づくPoE電源供給により動作すること。
(10) APで接続クライアントに対してDHCPとNAT機能を有すること。なお、本機能を有しない場合は、経路上のネットワーク機器で同等の機能を代替できるよう設計すること。
(11) チャネルボンディング機能を有すること。
(12) APを一括でバージョンアップを行う機能を有すること。無線利用者が継続してネットワーク利用できるように、バージョンアップを分散させる機能を有すること。
(13) DHCPでアドレス取得し自動的にコントローラから設定を適用する機能を有すること。
(14) 設置金具を含めること。
(15) アクセスポイント導入で必要となるPoEスイッチは受注者により準備すること。
(16) APの故障時は機器交換のみによる一切の事前設定不要でサービス復旧する機能を有すること。
(17) 別紙2で示すAP設置場所は授業等で高密度接続が想定されるため、別紙2記載の想定利用人数が同時接続してもに支障なく利用できる数のAPを準備すること。別紙2は依頼に応じて、提供する。

1.1.18 認証スイッチ 4式(キャンパス設置)

認証スイッチは1式あたり、以下の仕様を有すること。

(1) DHCP機能を有すること。
(2) ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること。
(3) BPDUの受信時にスパニングツリーPortFast対応インターフェイスをシャットダウンして、予期せぬトポロジループを阻止する機能を有すること。
(4) ネットワーク管理者の制御下にないエッジ デバイスがスパニングツリープロトコルのルートノードになること。を阻止する機能を有すること。
(5) 光ファイバケーブルの接続ミスまたはポート障害に起因する単一方向リンクを検出する機能を有すること。
(6) IPv4 IGMP Snooping機能に対応していること。
(7) 19インチラックマウント可能であり、1U以下のサイズであること。
(8) 悪意のあるユーザがDHCPサーバをスプーフィングし、偽装したアドレスを送信すること。を防ぐ機能を有すること。
(9) ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること。
(10) スイッチポート間にセキュリティと隔離性を提供する機能を有すること。
(11) GUIを使用して設定を行える機能を有すること。
(12) シリアル接続によるコンソールポートを有すること。
(13) SSH等によるセキュアなリモート・コンソール機能を有すること。
(14) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードする機能を有すること。
(15) NTPクライアントとして、一貫したタイムスタンプを刻む機能を有すること。
(16) Syslogサーバにメッセージを送信する機能を有すること。
(17) SNMPv1/v2c/v3による管理機能を有すること。
(18) 取り付けられたケーブルのタイプ(クロスまたはストレート)が不適切な場合は送受信ペアが自動的に調整される機能を有すること。
(19) MACアドレスによる機器認証(MAC認証)を、本調達におけるRadiusサーバを利用して行えること。
(20) WebブラウザによるHTTPSプロトコルを使用した利用者認証(WEB認証)を、本調達におけるRadiusサーバを利用して行えること。
(21) HTTPS認証に関して、本学が指定するサーバ証明書が利用できること。
(22) MAC認証を利用しない端末がスイッチに接続された場合、認証前の状態でブラウザが任意のページへアクセスすると自動的に認証ページを表示する、リダイレクト機能を有すること。
(23) ポート単位およびVLAN単位で認証機能の有無を指定できること。
(24) ダイナミック認証および固定VLAN認証が混在しても対応可能であること。
(25) UserPolicyControl機能を有すること。
(26) 無通信状態が発生してからのエージングタイムによるタイムアウト機能を有すること。
(27) 利用端末側に専用ソフトのインストールが必要でないこと。
(28) 同時20台以上の認証処理を遅延なく実行できる性能を有すること。
(29) イーサネット 10/100/1000Baseを48ポート以上実装していること。
(30) 1ギガビットイーサネット SFP を 4ポート以上実装していること。
(31) 77Mpps以上のパケット処理能力を有すること。

1.1.19 ファイアウォール/IPS 2式

1.1.19.1 ファイアウォール機能

ファイアウォール/IPSは1式あたり、以下の仕様を有すること。

(1) ハードウェアとソフトウェアが一体となったアプライアンス機器であること。
(2) IPv6に対応していること。
(3) 10/100/1000ポートを8ポート以上有すること。
(4) 1G/10G SFP/SFP+ポートを4ポート以上有すること。
(5) 専用の管理用インターフェースを1ポート以上有し、全てのモジュールを一元管理できること。
(6) ファイアウォール、アプリケーション可視化機能を動作させた際、8Gbps以上の処理能力を有すること。
(7) ファイアウォール、アプリケーション可視化機能、IPSを動作させた際、3Gbps以上の処理能力を有すること。
(8) 新規セッション数が秒間あたり、100,000セッション以上を処理可能であること。
(9) 最大同時セッション数が、945,000セッション以上を処理可能であること。
(10) 機器内部にログや設定を保存するためのストレージとして、120GB以上のSSDが搭載されていること。
(11) 19インチ幅のラック搭載型とし、1U以内に収納可能であること。
(12) 管理通信処理用とデータ通信処理用でそれぞれ独立した処理プロセッサを搭載していること。
(13) 本装置はTAPモード(ミラーポート接続)、L1モード(MACアドレスを保持しない)、L2(ブリッジ)モード、L3(ルータ)モードに対応し、一筐体内で複数のモードの混在設定が可能なこと。
(14) NAT機能を有すること。
(15) DoS攻撃防御機能を有すること。
(16) IEEE802.1Q VLANトランク機能をサポートすること。

(17) 専用のアプリケーション識別エンジンを搭載しており、追加設定なく、初期状態（デフォルト）で全てのトラフィックを対象にしたアプリケーションの識別のシグネチャが適用されていること。
(18) 3500種類以上のアプリケーションをポート番号に関わらず識別し可視化できること。
(19) ファイアウォール機能およびIPSなどの脅威防御機能を利用可能な仮想システムを6個以上利用可能であること。
(20) ファイアウォールのポリシーは送信元/送信先とアプリケーション名を元に処理可能であること。
(21) 外部Syslogサーバにログ出力可能であること。また、各Syslogサーバー毎に送出するログフォーマットの設定が可能であること。
(22) ファイアウォール上でログ保存が可能であり、別途管理サーバあり/なしに関わらずファイアウォール上でログが閲覧可能なこと。
(23) セキュリティ機能毎（ファイアウォール、アンチウイルス、IPSなど）で統一された、https対応の管理WebUIを有すること。
(24) sshによるセキュアなコマンドラインインタフェースを有すること。
(25) WebUI上で動的に表示を切り替えることができるリアルタイムレポート機能を搭載し、利用頻度の多いアプリケーション、URLカテゴリ、脅威をランキング形式で表示できること。
(26) 50以上の事前に定義されたレポートテンプレートおよびカスタムレポート機能を有し、それらをPDF形式にして設定されたスケジュールで自動メール送信可能なこと。
(27) インターネット経由でファームウェアならびにシグネチャファイルを製品に直接ダウンロードおよびインストール可能であること。またProxy経由でもこれが可能であること。
(28) IPv4/IPv6通信に対して、脆弱性防御、アンチウィルス、アンチスパイウェア、URLフィルタリング、ファイルフィルタ、データフィルタといったコンテンツスキャニング機能を、シングルエンジンで且つストリームベースで処理できること。
(29) クラウド上の機械学習エンジンを使って、未知のコマンド＆コントロール（C2）の脅威を検出して、防御できること。
(30) HTTP(S)通信のWebページのペイロードをクラウド上で解析し、高度な標的型フィッシング攻撃や、クローキングなどの高度な回避技術を使用するWebベースの攻撃、マルチステップ攻撃、CAPTCHAチャレンジ、これまでに見られなかった1回限りのURLを検出および防御できること。
(31) クライアント端末のウェブブラウザ上でユーザ認証を行い、認証の成否により通信の可否を制御するキャプティブポータル認証機能を有すること。キャプティブポータル認証機能により許可した通信は、ファイアウォール機能により送信元ユーザによる通信の制御が行えること。

1.1.19.2 URLフィルタリング機能
(1) ファイアウォールにURLフィルタリング機能を有すること。
(2) カテゴリベースのURLフィルタリング機能を利用可能であること。
(3) ファイアウォールのセキュリティポリシー上でURLカテゴリを直接指定し、URLカテゴリ毎のアクセス制御が可能であること。
(4) User-Agent、Referer、X-Forwarded-Forの情報が記録できること。

1.1.19.3 SSL-VPN機能
(1) ファイアウォールにSSL-VPN機能を有すること。
(2) クライアント端末(Windows、 Mac OS X)の接続先ネットワークを自動識別し、外部ネットワークに接続された場合に自動的に最寄りのファイアウォールに対してVPN接続を行う機能を有すること。
(3) Apple iOSや Google Androidベースのスマートフォン、タブレット等のモバイル端末の接続先ネットワークを自動識別し、外部ネットワークに接続された場合に自動的に最寄りのファイアウォールに対してVPN接続を行う機能を有すること。
(4) クライアント端末(Windows、 Mac OS X)のシステム環境(ホスト・インフォメーション・プロファイル)状態に応じたアプリケーションレベルの通信アクセス制御を行う機能を有すること。
(5) クライアントレスVPN機能を有すること。
(6) VPNクライアントのユーザ認証について、LDAP サーバに対する LDAP bind 認証による認証連携および 共通認証基盤との SAML 認証連携を行える機能を有すること。
(7) デバイスにインストールしたエージェントソフトウェア（以下「エージェント」という。）によりユーザ認証をすることでユーザを識別する機能を有すること。また、エージェントを利用できるユーザ数および端末数は、無制限であること。
(8) VPN クライアントによりユーザ認証した通信は、1.1.19.1のファイアウォール機能により送信元ユーザによる通信の制御が行えること。

1.1.20 セキュリティ監視サービス
(1) サービス提供事業者は、監視対象機器が発するセキュリティアラートやログの監視・分析を24時間365日リアルタイムで実施すること。
(2) 定期的にルールチューニングを実施し、新しい攻撃への対応と過検知・誤検知の削減を図ること。
なお、サービスとして提供できない場合は、ファイアウォール/IPS等の機能で、外部から提供されるIPアドレス、FQDN、URLのリストを自動的に取り込み、ルールチューニングを実施する機能を有すること。
(3) サービス開始前にルールチューニング期間を設けること。
(4) アラートやログの監視・分析は、サービス提供事業者が運用するログ分析システムを利用すること。
(5) 緊急度・危険性が高いと判断される場合には、契約先へメールにて通知すること。
(6) 危険度の高いセキュリティインシデントについて、詳細情報（危険度、イベントの内容、送信元IPアドレス、宛先IPアドレス/ホスト名）、推奨される対処方法とURL情報を、サービス提供事業者が提供するカスタマーポータル上及びメールで提供すること。
(7) 危険度の高いセキュリティインシデントを検知した際、リモートから遮断設定（送信元IP等特定トラフィックの遮断）を実施すること。
(8) インシデントの対応状況の確認や問い合わせ、レポートの閲覧を行う事ができる、カスタマーポータルを準備すること。
(9) サービス提供事業者は、検知したセキュリティインシデント等について、月次報告書を作成すること。
(10) 月次報告書には、全体の傾向を把握できるような情報（サービス提供事業者がサービス提供を行う顧客全体の傾向を含めたセキュリティインシデント件数推移等）及び契約元個別の情報（契約元で検知したセキュリティインシデント件数、緊急度の高いイベントの詳細情報等）を含めること。
(11) 月次報告書は、翌月第10営業日以内を目途にカスタマーポータルで提供すること。
(12) サービス提供事業者は、セキュリティインシデント検知や、カスタマーポータルで契約元に提供している情報等に関する契約元からの問合せに対し、24時間体制で受け付け、翌営業日に回答すること。なお、リアルタイム分析サービスにおけるセキュリティインシデントの内容に関する技術的な問い合わせに対応すること。
(13) インシデントの対応状況の確認や問い合わせ、レポートの閲覧を行う事ができる、カスタマーポータルを準備すること。
(14) 収集したログは圧縮、暗号化されて保管されること。
(15) ログ管理/分析ツールのWebUI及び出力レポート、取扱説明書を含むすべてのドキュメント類は全て日本語表記であること。

(16) IPSから出力されたログを自動分析し、月次でサマリレポートを自動作成。
なお、サマリレポートには以下の統計情報を含めるものとし、全て日本語で記載されていること。
① 攻撃内容
② 対象外シグネチャ
③ 不正アクセス(外部→内部)
④ 悪質なIP

1.2 サーバ・ストレージ基盤共通要件

(1) 本調達で実現する全てのサーバおよび機能は、1.2.1仮想サーバ基盤または同等のサービスレベルのクラウドサービスを用いて提供すること。

(2) 原則として全てのサーバ機能は仮想化で統合すること。ただし、クラウドサービスや管理機能は仮想化の範囲から除いても良い。

(3) 本調達で実現するサービスの認証は、「共通認証基盤」にて統一的に管理し、利用者がどこからでも安全なサービス利用ができること。

(4) AC100V電源に対応していること。

1.2.1 仮想サーバ基盤

1.2.1.1 仮想サーバ基盤ソフトウェア要件

(1) 仮想化方式は、ハイパーバイザ型とし、VMware vSphere 8.0 Essentials Plus以上以上の機能を持つと判断されること。
(2) 仮想マシンをグループ化し、CPU、メモリのリソースコントロール(予約、制限、比例配分)が可能なこと。
(3) 物理ホストのリソースを論理的に統合する機能を有すること。
(4) 物理ホストに依存せず、論理的に分割されたグループに対してアクセス管理が可能であること。
(5) サービスを停止せずに物理サーバ間で仮想マシンを移動させるのライブ マイグレーションが可能であること。
(6) ホストサーバと仮想マシンを監視し、ハードウェアとゲスト OS の障害を検出する機能を有すること。
(7) 物理サーバの障害時には別の物理サーバ上で仮想マシンが作成され、サービスの継続が可能なこと。
(8) ハードウェアやオペレーティング システムに障害が発生した場合でも、仮想マシンを自動的に再起動し、アプリケーションのダウンタイムを回避する機能を有すること。
(9) サービスを停止せずに、コンピューティング リソースを拡張および管理する機能を有すること。

1.2.1.2 仮想サーバ基盤ハードウェア要件

(1) 仮想サーバ基盤の運用・管理など環境の維持に必要となるサーバを必要数有すること。
(2) 物理サーバ1台当たり以下の要件を満たすこと。
・プロセッサーとして、Intel Xeon Gold 6430 相当以上のプロセッサーを2個以上有すること。
・256GB以上のメモリを有すること。
・内蔵ディスクとして、RAID構成により冗長化された容量600GB以上のディスクを有すること。
・ネットワークインターフェースは、10GbE に対応した イーサネットポートを2ポート以上有したものを2枚以上搭載すること。
・通常の通信に利用するNICから独立した1000base-Tの管理ポートを搭載していること。
(3) 電源モジュールは冗長化構成とすること。
(4) 物理サーバのシングル障害時にも仮想サーバ基盤の機能が継続できる構成であること。

1.2.2 プライマリストレージ 1式

(1) 仮想サーバ基盤/ファイルサーバのストレージとして利用できること。
複数台の装置で構成する場合も全体で(2)以降の要件を満たすこと。
(2) 仮想サーバ領域として、10TBを超える実効容量を確保すること。
(3) ファイルサーバ領域として、10TBを超える実効容量を確保すること。
(4) ファイルサーバ領域として、10,000 IOPS(SequentialWrite100% 32kブロックサイズ前提)を超える処理が可能なコントローラーであること。

(5) ローカルバックアップ領域として、ローカルデータ領域を過不足なくバックアップ可能なローカルバックアップ領域を確保した構成とすること。
(6) ファイルサーバとデータベースのストレージとしての利用時には、以下の項目を満たすこと。
・Active Directory、LDAPクライアントとして動作する機能を有すること。
・ファイルサーバストレージとしての利用時には、CIFS(SMB1.0、SMB2.x、SMB3.x)/NFS v3、v4、v4.1/iSCSI/FCP/FCoEプロトコルがサポートされていること。
・NASサーバ利用時は、SANストレージにNASゲートウェイを接続する構成でないこと。
・論理ボリューム管理機能を有すること。
・シンプロビジョニング機能を有すること。
・CIFS、NFS領域において、論理ボリュームの拡張・縮小をオンラインで実行する機能を有すること。
(7) バックアップに関連する機能として、以下の項目を満たすこと。
・仮想サーバ基盤ファイルサーバのバックアップが可能であること。
・遠隔サイトのストレージへのバックアップが可能であること。
・遠隔サイト用バックアップサーバへは本学で準備する回線を利用したバックアップができること。
・バックアップ機能としてフルバックアップおよび増分バックアップが可能なこと。
・増分バックアップはファイル単位の増分ではなく変更されたブロックのみの増分でバックアップできること。
・任意の時点の状態にリストアすることが可能であること。
・ストレージ上で重複排除された状態でバックアップできること。重複排除はブロック単位で処理されること。
・ストレージ上のバックアップ対象のデータを圧縮してバックアップする機能を有すること。
・日次・週次・月次でのバックアップスケジュールの設定が可能であること。
(8) サポートドライブの種別としては少なくとも3.8TBをもつNVMe SSD、または少なくとも1.8TBをもつ2.5型SAS HDDに対応したストレージ装置であること。
(9) RAIDレベルは同一RAIDグループ内でのディスクの二重障害時でもデータ消失が無いようにすることとし、RAID6相当には対応していること。
(10) コントローラ筐体とドライブ筐体間のドライブインターフェースは、12GbE以上に対応していること。
(11) ストレージコントローラが冗長化されており、耐障害性と処理能力を考慮し、フェイルオーバーが実現可能であること。
また、Active-Activeの冗長化構成で運用が可能であること。
(12) ホストとの接続インタフェースは16Gbps以上のFibre Channelと10Gbps Ethernet以上のiSCSIとNFSに対応していること。

(13) 接続インタフェースとして、16Gbps以上の Fibre Channelポートを4ポート以上、または10Gbps以上のEthernetポートを4ポート以上有すること。
(14) ディスク障害の兆候を監視し、障害が発生する前にスペアディスクに自動的にデータコピーを行なう機能を有すること。

(15) 主要部位(高速バス、キャッシュメモリ、ファン、電源、バッテリ等)は二重化、冗長化されていること。

(16) ハードウェアの障害発生時に、障害内容を電子メールで通知する機能を有すること。
(17) システム無停止でアレイコントローラのファームウェアのアップデートができること。
(18) プロセッサ、キャッシュメモリ、ファン、ディスク、電源、バッテリはシステムを止める事なく、ホットスワップでの交換が可能なこと。
(19) ホットスワップ可能なスペアディスクを1台以上有すること。
(20) 容量が不足した際、接続されるサーバーおよびストレージが稼働中に特定RAIDグループに対してディスクを1本から追加できること。

(21) ディスク追加の際、パフォーマンス影響を避けるためパリティの再計算などのデータ再配置が起こらないこと。

(22) 同一RAIDグループ内でディスク二重障害が発生してもサービス停止しないこと。また三重障害にも対応できる構成が可能なこと。

(23) 容量と性能との2つの観点で最適なデータ配置となるように、仮想LUNのデータを再配置する機能を有すること。

(24) 業務間のストレージリソースを分割する事により、相互にアクセスを制限できる機能を有すること。
(25) 本ストレージ装置は19 インチラックEIAに準拠し、ラックマウント型であること。
(26) ボリュームにおいて、ポイントインタイム方式を利用した世代管理が可能なスナップショット作成機能を有し、スナップショットは30世代以上の管理が可能であること。
(27) スナップショット作成機能は、スケジュール管理が可能なこと。
(28) 同一ボリューム内で重複したブロックを排除可能な機能および圧縮の機能を有すること。
(29) 現行のストレージのうち、必要なデータを誤りなく移行すること。

1.2.3 遠隔サイト用バックアップストレージ
(1) 本ストレージは大学が指定する場所（比治山にあるデータセンター）に設置し、プライマリストレージから大学が提供する回線を用いてバックアップできること。複数台の装置で構成する場合も全体で(2)以降の要件を満たすこと。
(2) プライマリストレージに復旧不能な障害が発生した場合には、バックアップストレージから復旧できること。
(3) バックアップは講義等業務時間に支障のない時間で終了すること。
(4) プライマリストレージのローカルバックアップ領域以上の実行容量を有するディスクを準備すること。
(5) ストレージコントローラが冗長化されていること。
(6) 同一RAIDグループ内でのディスクの二重障害時でもデータ消失が無いこと。
(7) 12台以上のHDD/SSDドライブを搭載可能なこと。
(8) 1000BASE-Tおよび10GBASE-Tに対応したイーサネットインターフェースを2ポート以上有すること。
(9) 主要部位(高速バス、キャッシュメモリ、ファン、電源、バッテリ等）は二重化、冗長化されていること。
(10) ホットスワップ可能なスペアディスクを有すること。
(11) 容量が不足した際、接続されるサーバーおよびストレージが稼働中に特定RAIDグループに対してディスクを1本から追加できること。
(12) ハードウェアの障害発生時に、障害内容を電子メールで通知する機能を有すること。
(13) 本ストレージは19 インチラックEIAに準拠し、ラックマウント型であること。

1.2.4 各種サーバ
1.2.4.1 ウィルス対策サーバ
(1) 仮想サーバ基盤上で動作し、サーバおよびクライアントからのリクエストに対する動作に支障がないリソースを有すること。

(2) 現在、導入しているウィルス対策ソフト（Trend Micro Security）用の既存サーバ機能を、本調達の仮想サーバ基盤で動作するようにすること。

1.2.4.2 ライセンス管理サーバ
(1) 仮想サーバ基盤上で動作し、サーバおよびクライアントからのリクエストに対する動作に支障がないリソースを有すること。
(2) 既存サーバ機能を、本調達の仮想サーバ基盤で動作するようにすること。

1.2.4.3 知のトライアスロン用サーバ
(1) 仮想サーバ基盤上で動作し、サーバおよびクライアントからのリクエストに対する動作に支障がないリソースを有すること。
CPU：2コア以上
メモリ：12GB以上
ストレージ：300GB以上
(2) 以下の環境を用意すること。各種バージョンは2024年6月時点の最新版を使用すること。
Rocky Linux、Apache、PHP
(3) ミドルウェアについてはOS標準パッケージの最新版に対応すること。
(4) 本サーバに必要なその他のソフトのインストールや動作確認は本調達の範囲外とする。

1.2.4.4 ファイルサーバ 1式
(1) サーバ上に個人フォルダ及び各グループの共有フォルダを有すること。
(2) 稼動後に個人フォルダ、共有フォルダを事務局管理者が追加できること。
(3) 事務局各室・各グループ、学部、学科、研究室単位等（以下「所属」という。）ごとに共有フォルダを作成し文書を格納できること。

(4) 各フォルダには次のアクセス権が付与できること。（ファイル参照権限・ファイル登録権限・ファイル削除権限・フォルダ作成権限）

(5) アクセス権は本基盤系システムのActiveDirectoryと連携して、ユーザ単位、所属単位など、任意のグループ単位で設定できること。

(6) 他のユーザや他の所属からはアクセスできない、参照できない設定が可能なこと。
(7) キーワードでファイルの絞り込み検索ができ、検索結果は一覧で表示できること。
(8) データを復元できるようにバックアップを保持し、システム管理者によりバックアップからの復元が可能であること。

(9) 既設の事務用ファイルサーバのデータを移行すること。
(10) 事務用端末からもアクセスできること。
(11) ファイルサーバの総容量として10TBの容量が使用できること。
(12) ログの取得等によりセキュリティを確保すること。
(13) 外部ネットワークから本ファイルサーバを利用する際は、本基盤系システムのSSL-VPNで接続し、事務用セグメントにアクセス出来るユーザのみが利用出来るようにすること。

1.3 ネットワークサービス機能
1.3.1 全学用DNS機能
(1) 仮想サーバ基盤上で動作し、学内外からのリクエストに対する動作に支障がないリソースを有すること。
(2) DNS機能としてbind9相当以上の機能を有すること。
(3) 既存DNSサーバのデータ・設定を移行し、学内および学外からの名前解決を行うこと。
(4) サーバはプライマリ、セカンダリとして2台構築し、安定した名前解決機能を提供すること。

(5) 脆弱性の対策等セキュリティに考慮した構成とすること。

1.3.2 学生用メール機能

(1) 現在、本学が運用中の Microsoft365（以降、M365と記載）上のメールサービスを利用すること。M365のライセンスはM365 Education A3、A5を別途調達する。
(2) M365の利用に必要なメールアドレスやSSOに必要な属性について、「共通認証基盤」と連携して自動更新が可能な構成とすること。
(3) メールアドレスを変更した場合であっても、変更前に受信したメールデータの引き継ぎが行えること。
(4) メールセキュリティ機能をM365のサービスを使用して提供すること。

1.3.3 教職員用メール機能

(1) M365 上のメールサービスを利用すること。
(2) M365の利用に必要なメールアドレスやSSOに必要な属性について、「共通認証基盤」と連携して自動更新が可能な構成とすること。
(3) 現行のメールアドレス(xxxxx@hiroshima-cu.ac.jp)をM365で使用可能とすること。
(4) メールアドレスを変更した場合であっても、変更前に受信したメールデータの引き継ぎが行えること。
(5) 教職員メール環境を新システムに切り替えるにあたり、過去の受信済みメールは利用者の操作によって移行が可能であること。
(6) 共有メールアドレスをMicrosoft Exchangeの共有メールボックスなどを用いて共通パスワードを設定せず、共有メンバーのメールボックスに受信メールが複製保持されることなく、利用可能とすること。また、その設定や利用の支援をすること。
(7) メールセキュリティ機能をM365のサービスを使用して提供すること。

1.3.4 メーリングリスト機能

(1) M365の機能を用いてSaaSで提供すること。その際、動作に影響のないSaaSのリソースを有すること。
(2) 管理者によってメーリングリストの作成、編集、削除、検索（メンバーによる検索を含む）が行えること。
(3) 既存のメーリングリストの移行を行うこと。移行対象のメーリングリストと、そのメンバーリストは大学側より提供するものとする。
(4) メーリングリストの一部（大学から指定）は前述の共有メールアドレスを使って提供すること

1.3.5 文書管理機能

(1) 文書管理機能としてMicrosoft SharePointを利用する。
(2) 現行の文書管理システム(サイボウズ)からの移行は本学で実施する。移行に対する支援を行うこと。

1.3.6 LDAPサーバ機能

(1) 仮想サーバ基盤上で動作し、サーバおよびクライアントからのリクエストに対する動作に支障がないリソースを有すること。
(2) 2台以上の仮想サーバで冗長化構成とすること。
(3) LDAPサーバはOpenLDAPと同等以上の機能を有すること。
(4) 複数のディレクトリサーバで、ディレクトリの自動的な複製・同期（レプリケーション）が相互に更新ができること。
(5) ディレクトリサーバに障害が発生した場合、負荷分散装置によりディレクトリサービスを継続させ、ディレクトリサービスが停止しないこと。
(6) トランザクションのログ機能を持ち、障害時の復旧に利用できること。
(7) ディレクトリサービスを停止することなくデータベースのバックアップができること。
(8) クライアント等からの接続、読み出し、書き込み、参照及び検索を行った履歴、時刻、操作者及びアクセス結果等を記録可能なこと。
(9) ディレクトリサービスを停止することなく属性の追加ができること。
(10) ディレクトリデータへのアクセス権限を属性レベルまで設定できること。
(11) ユーザ単位での読み出し・書き込み・検索・比較ができること。
(12) ユーザのID単位、グループ単位、IPアドレス及びドメイン名に基づくアクセスコントロールが設定できること。
(13) ユーザID／パスワードによる認証以外に、X.509バージョン3デジタル証明書による認証ができること。
(14) 平均して毎秒4000クエリのLDAP検索処理ができること。
(15) パフォーマンス評価のための情報が出力できること。
(16) LDAPクライアントからのアクセスの際には暗号化を行い通信すること。

1.3.7 ActiveDirectory認証機能

(1) 仮想サーバ基盤上で動作し、サーバおよびクライアントからのリクエストに対する動作に支障がないリソースを有すること。
(2) 2台以上の仮想サーバで冗長化構成とすること。
(3) OSはWindows Server 2022相当以上の機能を有すること。
(4) Active Directory 2016と同等以上の機能を有すること。
(5) LDAPサーバとActive Directoryとのパスワード同期すること。
(6) ActiveDirectoryに対するグループメンテナンス機能を有すること。
(7) 職員利用の事務用端末（FAT端末）のデバイス管理にM365のIntuneを使用する。デバイスの登録はIntuneとAzureADとするため、オンプレADとAzureADのハイブリッドで事務用端末が参加できるようにすること。Intune利用のための設計や運用は本調達の範囲外とする。
(8) 既存のユーザ情報を移行すること。

1.3.8 Radius機能

(1) 仮想サーバ基盤もしくはアプライアンス上で動作し、サーバおよびクライアントからのリクエストに対する動作に支障がないリソースを有すること。
(2) RadiusAAAプロトコルをサポートすること。
(3) LDAP 認証転送がサポートされており、Microsoft などの主要ディレクトリ ベンダーが提供するディレクトリに格納されたユーザ プロファイルを認証できること。
(4) WEBベースGUIによる簡単な管理ができること。
(5) 管理者毎に異なるアクセスレベルの設定が可能なこと。
(6) EAPベースにしたIEEE802.1x標準をサポートしていること。
(7) 既存Radiusサーバデータ・設定を移行すること。
(8) 学外のeduroamを提供している場所で、本学のアカウント/パスワードで認証し無線LANが利用できること。

1.3.9 SAML SP/IdP機能

(1) 仮想サーバ基盤上もしくはIDaaSで動作し、サーバおよびクライアントからのリクエストに対する動作に支障がないリソースを有すること。
(2) M365をIdPとした外部IdP連携を行い、M365の多要素認証(SMS、TOTP)に対応すること。
(3) サービス提供のためのSP環境やサービス利用のための必要なIdP環境を構築し、運用すること。
(4) 学術認証フェデレーション[学認」で利用可能な認証が使えるようにすること。
参考：現在使用しているものは、附属図書館の契約サービス(CUP、Elsevier、IEEE、ProQuest、Springer)、学認クラウドゲートウェイサービス、eduroam、他大学で提供しているサービス(広島大学 無線LANゲスト利用)
(5) 本学の認証システム (SAML2.0) と連携すること。
(6) アクセスするIPアドレスによって、多要素認証の要否を制限できること。

1.3.10 Radiusプロキシ機能

(1) 仮想サーバ基盤上で動作し、サーバおよびクライアントからのリクエストに対する動作に支障がないリソースを有すること。
(2) Radiusプロキシを利用して、eduroam対応もできること。

1.3.11 全学用WEBサーバ・情報処理センターWebサーバ機能

(1) 本サーバ機能はクラウドサービスで提供すること。
(2) 外部クラウドサービスではCMS（WordPress）が利用できること。
(3) 合格発表時のアクセス集中に対応できる性能を有すること。（想定されるアクセス数としては1分間に2000アクセスである）
(4) 既存サーバ機能を、クラウドサービスに移行すること。

1.3.12 ホスティング機能

(1) ホスティング機能はクラウドサービスで提供すること。
(2) ホスティング機能として、次の機能が利用できること。
・CMS機能
・Web機能
・マルチドメイン機能
・SSL通信
・ウェブアプリケーションファイアウォール機能
・IPアドレスフィルタ機能
・メール機能
・迷惑メールフィルタ機能
・メーリングリスト機能
(3) 現行のホスティングサーバで利用しているホスティングドメイン（約70ドメイン）を引き続き利用できること。
(4) 既存サーバ機能を、クラウドサービスに移行できること。なお、クラウドサービスへの移行によりIPアドレスの変更などで現行の利用から制限が生じる場合は事前に提示し、本学と解決策を協議すること。
(5) サブドメインの名前解決が可能なDNS機能を有すること。または、全学用DNS機能にてサブドメインの名前解決が可能であること。
(6) 利用者がデータ移行を行うための手順書を整備すること。

1.3.13 ネットワーク監視機能

(1) 仮想サーバ基盤上で動作し、学内外からのリクエストに対する動作に支障がないリソースを有すること。
(2) トラフィック監視機能を有し、ネットワーク機器のトラフィックを監視すること。
(3) SNMPを利用したパフォーマンス監視機能を有すること。
(4) IP/TCP/UDPを利用したサービス監視機能を有すること。
(5) 各種サーバ、サーバ上のサービス、ネットワーク機器の死活監視が行なえること。
(6) 異常を検知した場合には、管理者へ通知する機能を有すること。
(7) 標準MIBおよびプライベートMIB情報があらかじめテンプレート化されていて、Web GUI画面上での操作によって容易に設定し情報収集が可能であること。
(8) 監視項目の設定については、予めツールによって定義された監視項目の優先度をもとに自動登録する機能を有すること。
(9) 取得トラフィック等の各種リソース情報を、間引きすること無く3年間～5年間、非圧縮で保存できること。
(10) 監視間隔は監視項目単位にて、1分～10分の間で任意に変更ができること。

1.3.14 システムログサーバ機能

(1) 仮想サーバ基盤上で動作し、学内ネットワーク機器からのSyslog受付リクエストに対する動作に支障がないリソースを有すること。
(2) Syslogサーバ機能を有し、ネットワーク機器のSyslogを収集すること。
(3) MRTGによるトラフィック情報を収集する機能を有すること。

1.3.15 DHCPサーバ機能

(1) 仮想サーバ基盤上で動作し、サーバおよびクライアントからのリクエストに対する動作に支障がないリソースを有すること。
(2) 学内施設からのリクエストに対してサービスを提供できるようにすること。
(3) 既存のネットワーク認証機器と連携して、ネットワーク認証時にIPアドレスの払い出しが動的、固定的にできること。
(4) 冗長化構成をとること。

1.4 共通認証基盤

1.4.1 共通認証基盤機能

(1) 複数のシステム（アカウント発行、学内NW利用認証、電子メール、学務システム、外部電子メール、外部教育用プラットフォーム（MS365やGoogle WorkSpace（以降GWS）など）が認証可能な共通の認証基盤を構築すること。このとき、各種システムとの連携概要を示す別紙3「認証連携」をもとに構築すること。別紙3は依頼に応じて提供する。
(2) 共通認証基盤は「1.3.6 LDAPサーバ機能」、「1.3.7 ActiveDirectory認証機能」、「1.3.9 SAML SP/IdP機能」と連携を行いそれぞれで認証が可能なこと。
(3) 共通認証基盤は学生情報や教職員情報を管理する部署においてアカウントの追加、削除、変更などの操作が可能なこと。
(4) 「1.3.6 LDAPサーバ機能」、「1.3.7 ActiveDirectory認証機能」、「1.3.9 SAML SP/IdP機能」の間で、アカウントやパスワードを自動的に同期すること。
(5) アカウントの有効期間が切れている、パスワード変更をしていない、セキュリティガイダンスを未受講などのケースにおいて指定した期間や日時で特定のアカウントを停止できる機能を有すること。この場合のパスワードの再設定は利用者に情報処理センターの特定端末のWeb画面で設定して変更できるようにすること。
(6) 授業開始時など、ユーザからの一斉の認証要求に対しても、適切な処理が継続して行える処理性能を持つこと。
(7) 持込みPC等のネットワーク接続時に、LDAPまたはRADIUSにより、Webブラウザを介して認証が行えること。
(8) 認証のログ情報が保存出来ること。
(9) 既存の認証データを新システムに適した形式で移行すること。
(10) 移行の際には利用者のパスワードを変更させること無く移行できることが望ましい。変更が必要な場合には最良な方法を提案すること。

(11) 以下のアカウント種別を管理できること。
・学生アカウント
・教員アカウント
・職員アカウント
・ゲストアカウント
・その他アカウント

(12) 利用者ごとに1アカウント(ID)ずつ発行する。ただし、現行まで発行している学生、教員、職員の1人につき2アカウント（HUNETアカウントとサービスアカウント）によるサービスの使い分けが実現できるようアクセス権限設定や利用認証をLDAP及びSMAL IdPの設定を用いて実現すること。

1.4.2 共通認証基盤管理機能

(1) 教職員・学生番号情報を管理するためのWebブラウザでアクセス可能な管理者画面機能を有すること。
(2) 管理者画面へのログイン時に、共通認証基盤による認証連携が行えること。
(3) 学生の利用者登録時には、学籍番号に紐づく、以下のアカウント情報を自動生成すること。
・HUNETアカウント
・uidNumber
・gidNumber
・シェル
・パスワード
・ホームディレクトリパス
(4) 自動生成するデータの生成ルールは定義可能とすること。
(5) アカウントは別途導入される学務システムから出力されるアカウント情報のCSVファイルを取り込み、自動的にアカウントを作成すること。

(6) 利用者を検索して得た利用者情報を検索結果として画面に表示する機能を有すること。
(7) 利用者情報を教務システムからのデータ出力に応じて、取り込み、登録・更新・削除・ロック・ロック解除の一括処理を行うことが可能であること。

(8) 利用者を検索後、対象の利用者を登録・更新・削除・ロック・ロック解除する機能を有すること。
(9) 利用者を検索後、対象者のパスワードを強制的に初期化する機能を有すること。また、初期化するパスワードは自動生成、手動入力から選択可能であること。

(10) 対象利用者情報のCSVファイルを取り込み、パスワードの一括変更を行うことが可能であること。
(11) CSVファイルで取り込んだ利用者情報については、画面で個別確認及び編集が可能であること。
(12) 入力データ取り込み時にデータ不備のプレチェックを行う機能を有すること。
(13) 上位システムからデータ連携によって利用者情報を登録する際に、利用者区分、所属毎の共通初期値を自動設定する機能を有すること。

(14) 管理者グループを設定でき、パスワード強制変更のみ行える権限を与える機能を有すること。
(15) 各管理機能につき利用者種別毎・所属毎に管理者グループの設定が可能であること。
(16) 管理者グループには、管理機能単位での管理者権限の委譲設定を行える機能を有すること。
(17) 管理者に各種メール(バッチ実行結果、処理エラー)を通知する機能を有すること。
(18) 管理者や利用者が操作した作業ログが、5年間分保存でき、過去に遡って検索が行えること。
(19) 利用者ID及びパスワード通知書を生成することができる機能を有すること。
(20) 管理者端末・利用者端末との通信を暗号化すること。
(21) ゲスト用アカウントを管理者からの登録により作成する機能を有すること。
(22) 講習受講済みユーザCSVを取り込み、対象アカウントのパスワード有効期限を無期限とする機能を有すること。

1.4.3 他システム連携機能

(1) 上位システムとのデータ連携の際、CSVファイルで受信出来ること。取り込むCSVに必要な項目情報を本学に提示すること。

(2) 処理方式として上位システムから全件データを受け取り、利用者の変更点(新規登録、内容変更、削除、ロック、ロック解除)をデータベース上で判断、抽出し、メタデータリポジトリ内に格納する機能を有すること。
(3) M365のクラウドサービスに対しても、AzureADConectを利用して提案する機器や他システムと連携して自動処理が行われること。
(4) GWS（GWS for Education Fuundamentals を利用）のクラウドサービスに対しても、Google Cloud Directory Syncを利用して提案する機器や他システムと連携して自動処理が行われること。
(5) 「1.3.9 SAML SP/IdP機能」により、Shibboleth（SAML2.0以降）対応のサイトにSSO連携ができること。

1.4.4 パスワード管理機能

(1) WEBインタフェースを用い、「共通認証基盤」のユーザーアカウントのパスワードが変更可能であること。
(2) 「共通認証基盤」と連携しユーザ認証が行えること。
(3) パスワードに使用できる文字を設定する機能を有すること。禁則文字、必須文字種の組合せ、最小・最大文字長による制限が可能であること。

(4) パスワード自動生成は、禁則文字、必須文字種の組合せ、最小・最大文字長による制限を設け、その制限内でランダムに生成可能とすること。また、パスワードに使用できる文字(パスワードポリシー)とは、設定を別にすることが可能であること。
(5) セキュリティ強化の目的で、パスワード文字列に利用者IDが含まれている場合は、パスワード変更を拒否すること。

(6) 過去に使用したパスワードを設定回数分、再使用を禁止できること。
(7) 利用者パスワードの有効期限を設定する機能を有すること。
(8) 指定期間以上パスワード変更しない利用者、または利用停止が必要な者に対してパスワードロックする機能を有すこと。また、ロックやその解除の設定は個別、一括登録ともにできること。

(9) パスワード有効期限切れでロックされた状態になった場合、パスワード変更すればパスワードロックが解除されること。

(10) パスワード有効期限前にパスワード変更を促し(メール送信等)、超過後にロックする機能を有すること。
(11) パスワード有効期限切れの通知メールを自動で送信する機能を有すること。
(12) 通知メールの配信タイミングを複数回設定できる機能を有すること。
(13) 通知メールのテンプレートは複数個用意可能であること。
(14) 管理者端末・利用者端末との通信を暗号化すること。

1.4.5 利用者機能

(1) 利用者が自身のパスワードや管理者によって許可された個人情報の一部変更を行う為の利用者画面を利用者の属性（教職員、学生、その他）に応じて有すること。

	(2)	利用者画面はWebブラウザからアクセスできること。ブラウザは、Microsoft Edge、Google Chrome、Mozilla Firefox、Apple Safariに対応すること。
	(3)	利用者画面へのログイン時にユーザ認証が行えること。
	(4)	利用者がログインした後にパスワード有効期限を表示できること。
	(5)	長期間パスワード変更を行っていない利用者に対して、警告メッセージの表示、または通知メッセージのメール送信により警告ができること。
	(6)	利用者が自らの個人情報を変更することができること。利用者区分(学生・教員・職員など)に応じて、変更可能な項目が管理者により設定できること。
	(7)	大学のメールアドレスとクラウドメールアドレスのエイリアス登録や変更できる機能を有し、ユーザ自身がWebブラウザを介して変更を行えること。
	(8)	アカウントやメールアドレス登録、変更時には以下の入力チェックが実施できること。 ・NULLチェック ・一意チェック ・入力許可文字タイプ ・入力最小長/最大長 ・入力不可文字
	(9)	メールアドレスを変更した際、変更前のメールアドレスを凍結状態とし、一定期間後に自動的に削除する機能を有すること。本機能によってメールアドレスの変更を行っても、クラウドメール（M365）のメールボックスは変更されることなく、変更前のアドレスで受信済みのメールデータを引き続き参照できること。
	(10)	変更内容に応じて「共通認証基盤」やメールシステム（学生用メール、教職員用メール）と連携し、必要な更新が自動的に行えること。
	(11)	管理者端末・利用者端末との通信を暗号化すること。
	(12)	メタデータリポジトリ上の利用者情報を管理する場合、任意のフィールドを暗号化して保存できること。
	(13)	約250名が利用者画面で同時に利用者機能を使用できること。
1.5		**外部教育・業務支援プラットフォーム利用機能**
	(1)	教務・学習支援プラットフォームとしてM365とGWS for Education Fundamentalsを用いる。これらのプラットフォームで提供されるサービスを使える機能を提供すること。(M365の利用ライセンス契約は別途調達とする。)
	(2)	これらのプラットフォームは、大学のアカウントで認証し、共通認証基盤のSAML IdPで認証を行うこと。
	(3)	学生の教育利用のストレージとして、M365の環境を利用出来るようにすること。
	(4)	事務支援のプラットフォームにM365を使うとき、チーム単位で提供サービスが使えるようにすること。
	(5)	これらのプラットフォームのアカウント設定等利用のための導入作業をすること。
	(6)	これらのプラットフォームの利用のための技術支援をすること。具体的な支援内容を示すこと。

Ⅱ 搬入・据付・調整・撤去

搬入・据付・調整・撤去

2.1 搬入、据付、調整条件

(1) 各機器は本学指定の場所(サーバ類においては、本学が利用する学外データセンターに設置された19インチラック2本を含む)に設置すること。
(2) 機器設置に関しては、現行システムからの移行をスムーズに行うことを前提に考え、併設運用を行ってもよい。なお、併設運用を行うに当たっては現行システムに発生する設定変更費用を本調達に含めること。
(3) 移行にあたり、現行システムの情報取得などが必要な場合には本学の承認を得た上で実施すること。また、情報取得のために発生する費用は本調達に含めること。
(4) 事務用端末をVDIからFAT端末利用するための環境移行の支援をおこなうこと。
(5) 本システムの構築作業は、各作業工程における本学職員の負荷軽減に十分留意し、品質の確保、納期を厳守すること。
(6) 各機器、システム構成に必要なケーブル等を含めること。
(7) 搬入、据付、調整、ソフトインストール、システム運用テストまで全て受注者の負担で行うこと。
(8) システムの移行については既存の環境設備、システム、ネットワークなどの継続性について配慮すること。
(9) 同時期にデータセンターで稼働するHUNET2019、物品管理システム、等が円滑に動作するようにスケジュール管理や協力して動作検証を行うこと。
(10) 検収完了後速やかに完成図書を作成し提出すること。完成図書とは以下の通りである。
・システム構成表および構成図
・システム運用マニュアル
・システム操作マニュアル
・システム検証結果報告書

(11) 完成図書作成に関わる費用はすべて受注者の負担とする。
(12) システムの操作性については、本学と十分に協議を行い　要望に応じて改修・調整を行うこと。
(13) 納入後、本格運用前に最低1回以上の取扱説明会を実施すること。
(14) システム構築においてデータセンターの事前使用は6月上旬から開始し、バックアップの10Gbpsの回線は8月1日からとする。

2.2 撤去条件

(1) 契約終了時には、調達機器を撤去すること。

2.3 移行条件

(1) 将来的に本システムから他システムへデータ移行の必要が発生した際には、本システムからデータを抽出すること。ただし、対象システムは共通認証基盤とし、データフォーマットは本調達の受注業者側にて規定されたものとする。
なお、データの抽出作業に必要な費用は本調達に含めること。

Ⅲ	**稼動維持支援サービス**
	稼動維持支援サービス　1式
3.1	**稼動維持支援サービスの概要**
(1)	本調達にて導入されるハードウェア及びソフトウェア製品の安定運用のため、システム全体の稼動維持支援を行うこと。
(2)	稼動維持支援サービスを提供する組織・部門は、財団法人日本適合性認定協会または海外の認定機関によりISO9001の認証を得ていること。
3.2	**稼動維持支援サービスの要件**
3.2.1	**全般**
(1)	本学又は常駐システムエンジニアからの問合せに対し、問題解決のための調査・検討を行うこと。
(2)	問合せは、電話またはメールにて受付を行えること。
(3)	問題解決のためにシステムの設定変更・インストール作業が必要となった場合には、本学と協議の上実施すること。
3.2.2	**定例会議・セキュリティミーティングへの参加**
(1)	月1回の定例会議に出席し、主要な関連ベンダを取りまとめて、障害対策状況や懸案事項に関する報告を行うこと。
(2)	問合せの調査・検討結果は、問合せ者に電話・メールで回答するとともに、定例会にて報告を行うこと。
3.2.3	**障害発生時対応**
(1)	障害発生時には速やかに業務を再開できるよう支援すること。
(2)	障害切り分け、対策方法の提示を行い、最終的な判断のみを本学に仰ぐこと。
(3)	障害対策により他システム等に影響を与える場合には、本学にその詳細を報告するとともに、本学との協議に速やかに応じること。
(4)	障害対応においては再発防止の為の対策案を提示すること。
(5)	障害対応状況・対策結果については、問合せ者に電話またはメールにて回答するとともに、定例会にて報告を行うこと。
3.2.4	**予防保守**
(1)	納入システムにおいて、予防保守を目的とした対策が必要となった場合には、具体的対策方法を計画立案の上、本学へ報告を行うこと。
(2)	システム停止を伴う予防保守の場合には、事前にその重要性、影響範囲、影響時間等を本学に報告し、実施の有無については本学の指示に従うこと。
3.2.5	**その他**
(1)	年1回の計画停電時は、運用停止・再開などの作業に協力すること。
(2)	本システムとは別にシステムを調達（増設）する場合があるので、システム連携が必要な場合には本学に協力すること。
3.3	**保守・運用の要件**
3.3.1	**全般**
(1)	導入システムのハードウェア・ソフトウェアの保守費用及びシステムエンジニアのサポート費用は本調達に含めること。
(2)	システムが安定稼働するまで、専任の技術者を派遣して対応すること。
(3)	本学が導入システム上でシステム開発、変更を行う際、本学の要求に応じて支援を行うこと。
(4)	システム管理と運用に関して、技術的なサポートを行うこと。
(5)	システムのOS・アプリケーションに関する不具合対策版パッチが各ベンダーからリリースされた際に、速やかに業務システムに与える影響やリスクを判断し、本学と協議の上で必要に応じたパッチを適用できること。
(6)	本学職員の指示により、計画停電・障害対応に伴うシステムの起動、停止時には協力すること。
3.3.2	**障害対応**
(1)	本学からの障害発生連絡により原因切り分け、調査、復旧作業を行うこと。遠隔操作による対応で解決できない場合には、現地対応を行うこと。
(2)	障害対応において技術員の派遣の必要がある障害内容の時は、平日昼間であれば障害発生連絡から1時間以内に本学に派遣できること。
(3)	障害発生時にネットワーク、業務システム等の各事業者と連携し障害対応を行い、対応完了時に報告を行うこと。また、保守対象が障害の起因でない保守事業者に対しても復旧に必要な対応を求めた場合、対応すること。
(4)	障害発生時以外でも本学から導入システムに関する電話・メールによる質問・問合せに対応すること。
(5)	障害対応においては再発防止の為の対策案を提示すること。
(6)	障害対応状況・対策結果については、問合せ者に電話またはメールにて回答するとともに、定例会にて報告を行うこと。