

提案書（正本）

令和 年 月 日

公立大学法人大阪
理事長 様

大阪公立大学医学部附属病院 病院情報システムネットワーク機器等購入・運用保守
業務委託について、提案書を提出します。

【提案者（入札参加者）】

住所又は
事務所所在地

商号又は名称

代表者職氏名

印

【連絡先】

担当者

所属

電話番号

FAX

E-mail

提案書（副本）

令和 年 月 日

公立大学法人大阪
理事長 様

大阪公立大学医学部附属病院 病院情報システムネットワーク機器等購入・運用保守
業務委託について、提案書を提出します。

(様式第4号)

技術審査資料届出書

令和 年 月 日

公立大学法人大阪 理事長 様

入札案件名	大阪公立大学医学部附属病院 病院情報システムネットワーク機器等購入・運用保守業務委託
-------	---

所在地

商号又は名称

代表者氏名 印

問合せ先

(担当者氏名：)

(電話番号：)

(FAX番号：)

様式第 5 号 技術審査資料 要件対応表（記載要領）

記載箇所
①実現方法
各項目について、下記の○・▲・×から対応方法を選択すること。
○ 対応可能：提案構成に含まれる機器の機能により、要件どおり実現できる。コnfig設定による実現を含む。
▲ 一部代替により対応：要件の一部又は全部について、記載の方式によらず、代替手段（他機器での実現や運用回避など）により同等の目的を達成できる。
× 対応不可能
ライセンスやオプションモジュールの追加により実現する場合は○とし、必要なライセンス等を提案構成に含めた上で、補足事項にその旨を記載すること。
なお、上記以外の記載（空欄・不明を含む）は全て×評価とする。
機能要件一覧において、水色の行はヘッダであり、対応方針の記入は不要である。

②③メーカー名、機器名（型番） 各項目を実現する機器名（型番）と、その機器を提供するメーカー名称を記載すること。

④補足事項
対応方法等について、補足説明がある場合に記載すること。
▲を選択した場合には、代替手段の具体的な内容（実現方式や運用手順など）を記載すること。

					①	②	③	④	
項番	大分類	中分類	小分類	要件	備考	実現方法	ベンダ名	ソリューション名	補足事項
1.1.1.1	スイッチ	共通	スパンニングツリー	IEEE802.1Q（旧IEEE802.1D／802.1w／802.1s）に準拠したスパンニングツリー機能（RSTP／MSTPを含む）を有すること。					
1.1.2.1	スイッチ	共通	リンク冗長	IEEE802.1AX（旧IEEE802.3ad）に準拠したリンクアグリゲーションに対応していること。					
1.1.3.1	スイッチ	共通	ジャンボフレーム	9,000バイト以上のジャンボフレームに対応していること。					
1.1.4.1	スイッチ	共通	接続認証	IEEE802.1X認証及びMAC認証に対応し、認証サーバと連携したダイナミックVLANにより端末を所属セグメントへ収容できること。					
1.1.5.1	スイッチ	共通	ループ・不正対策	ストーム制御、BPDUガード相当のループ防止、DHCPスヌーピングやARP検査などの不正対策を有すること。					
1.1.6.1	スイッチ	共通	障害検知	ループ等のネットワーク障害の原因となるポートの異常を検知し、当該ポートを自動閉塞できること。閉塞したポートは、自動又は運用手順により復旧できること。					
1.1.6.2	スイッチ	共通	障害検知	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）を検出できること。					
1.1.7.1	スイッチ	共通	自己診断	装置の異常を検知し、ログ出力等により確認できること。					
1.1.8.1	スイッチ	共通	マルチキャスト制御	IGMPスヌーピング及びMLDスヌーピングに対応していること。					
1.1.9.1	スイッチ	共通	解析支援	トラフィック解析のためのポートミラーリングができること。					
1.1.10.1	スイッチ	共通	QoS	IEEE802.1Q（旧IEEE802.1p）及びDSCPによる分類と優先制御ができ、ポートあたり8キュー以上を有すること。					
1.1.11.1	スイッチ	共通	管理機能	Syslogサーバへのログ送信、SSHによるリモート管理及びNTPによる時刻同期に対応していること。					

様式第5号 技術審査資料 要件対応表

項番	大分類	中分類	小分類	要件	備考	実現方法	ベンダ名	ソリューション名	補足事項
1.1.1.1	スイッチ	共通	スパンニングツリー	IEEE802.1Q（旧IEEE802.1D／802.1w／802.1s）に準拠したスパンニングツリー機能（RSTP／MSTPを含む）を有すること。					
1.1.2.1	スイッチ	共通	リンク冗長	IEEE802.1AX（旧IEEE802.3ad）に準拠したリンクアグリゲーションに対応していること。					
1.1.3.1	スイッチ	共通	ジャンボフレーム	9,000バイト以上のジャンボフレームに対応していること。					
1.1.4.1	スイッチ	共通	接続認証	IEEE802.1X認証及びMAC認証に対応し、認証サーバと連携したダイナミックVLANにより端末を所属セグメントへ収容できること。					
1.1.5.1	スイッチ	共通	ループ・不正対策	ストーム制御、BPDUガード相当のループ防止、DHCPスヌーピングやARP検査などの不正対策を有すること。					
1.1.6.1	スイッチ	共通	障害検知	ループ等のネットワーク障害の原因となるポートの異常を検知し、当該ポートを自動閉塞できること。閉塞したポートは、自動又は運用手順により復旧できること。					
1.1.6.2	スイッチ	共通	障害検知	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）を検出できること。					
1.1.7.1	スイッチ	共通	自己診断	装置の異常を検知し、ログ出力等により確認できること。					
1.1.8.1	スイッチ	共通	マルチキャスト制御	IGMPスヌーピング及びMLDスヌーピングに対応していること。					
1.1.9.1	スイッチ	共通	解析支援	トラフィック解析のためのポートミラーリングができること。					
1.1.10.1	スイッチ	共通	QoS	IEEE802.1Q（旧IEEE802.1p）及びDSCPによる分類と優先制御ができ、ポートあたり8キュー以上を有すること。					
1.1.11.1	スイッチ	共通	管理機能	Syslogサーバへのログ送信、SSHによるリモート管理及びNTPによる時刻同期に対応していること。					
1.1.12.1	スイッチ	共通	管理者認証	機器管理者の認証を認証サーバと連携し、管理者以外による設定の参照や変更を防止できること。					
1.1.13.1	スイッチ	共通	保守性	設定情報及びファームウェアのバックアップ及び復元ができること。					
1.1.13.2	スイッチ	共通	保守性	故障による交換の際に、交換機へ設定を自動で復元できること。					
1.1.14.1	スイッチ	共通	監視連携	SNMPv3に対応し、機器の異常時には監視サーバが速やかに障害を検知できること（SNMP v1／v2cは既設機器との互換のため任意対応とする）。					
1.1.15.1	スイッチ	共通	環境条件	動作温度0～40℃に対応し、VCCI（クラスA又はクラスB）に適合していること。					
1.1.16.1	スイッチ	共通	付属品	実装に必要なアダプタ類やケーブル類等を全て含むこと。					
1.2.1.1	スイッチ	コアシッチ	形状	シャーシ型又はボックス型のL3スイッチであり、19インチラックに搭載できること。					
1.2.2.1	スイッチ	コアシッチ	構成	複数のスイッチを1台の仮想スイッチとして構成できること（MLAG、Virtual Chassis等の複数台統合仮想化機能相当）。					
1.2.3.1	スイッチ	コアシッチ	ポート構成	1G SFPポートを合計102口以上実装できること。					
1.2.3.2	スイッチ	コアシッチ	ポート構成	1台あたり、10G SFP+ポートを11口以上及びダイレクトアタッチ接続12口を実装できること。					
1.2.4.1	スイッチ	コアシッチ	FW接続	内部ファイアウォールとの接続用に、10G以上のポートを4口以上確保すること。					
1.2.4.2	スイッチ	コアシッチ	FW接続	11ヶ所障害時及び片系ファイアウォール停止時にも、セグメント間通信のピーク需要を収容できるネットワーク構成・帯域設計とすること。					
1.2.5.1	スイッチ	コアシッチ	性能	スイッチング容量は6Tbps以上であること。					
1.2.6.1	スイッチ	コアシッチ	MACアドレス	32,000以上のMACアドレスに対応できること。					
1.2.7.1	スイッチ	コアシッチ	VLAN	IEEE802.1QタグVLANに対応し、VLAN IDを4,000以上利用できること。					
1.2.8.1	スイッチ	コアシッチ	ルーティング	スタティック及び動的ルーティング（OSPF等）に対応していること。					
1.2.8.2	スイッチ	コアシッチ	ルーティング	VRFによる経路分離、ゲートウェイ冗長及びDHCPリレーができること。					
1.2.9.1	スイッチ	コアシッチ	ルート数	IPv4ルートを10,000以上収容できること。					
1.2.10.1	スイッチ	コアシッチ	フロー可視化	sFlow相当のフロー情報を出力できること。					
1.2.11.1	スイッチ	コアシッチ	解析支援	他筐体へのリモートミラーリング又は障害解析及びトラフィック監視を実現できる機能若しくは構成を有すること。					
1.2.12.1	スイッチ	コアシッチ	電源	電源モジュール及びFANを二重化し、稼働中に交換できること。					
1.3.1.1	スイッチ	サーバスイッチ	形状	1RUの2スイッチであり、19インチラックに搭載できること。					
1.3.2.1	スイッチ	サーバスイッチ	構成	2台のスタックを6組構成できること。					
1.3.3.1	スイッチ	サーバスイッチ	ポート構成	1G BASE-Tポートを48口実装していること。					
1.3.3.2	スイッチ	サーバスイッチ	ポート構成	10Gアップリンク（ダイレクトアタッチ）を2口実装できること。					
1.3.4.1	スイッチ	サーバスイッチ	性能	スイッチング容量は176Gbps以上、パケット処理能力は130Mpps以上であること。					
1.3.5.1	スイッチ	サーバスイッチ	MACアドレス	16,000以上のMACアドレスに対応できること。					
1.3.6.1	スイッチ	サーバスイッチ	VLAN	IEEE802.1QタグVLANに対応し、アクティブVLANを1,000以上利用できること。					
1.3.7.1	スイッチ	サーバスイッチ	フロー可視化	sFlow相当のフロー情報を出力できること。					
1.3.8.1	スイッチ	サーバスイッチ	電源	冗長電源に対応していること。					
1.4.1.1	スイッチ	エッジスイッチA／B	形状	1RUの1.2スイッチであり、19インチラックに搭載できること。					
1.4.2.1	スイッチ	エッジスイッチA／B	ポート構成	1G BASE-Tポートを、Aは24口、Bは48口実装していること。					
1.4.2.2	スイッチ	エッジスイッチA／B	ポート構成	1G SFPアップリンクを2口以上実装できること。					
1.4.3.1	スイッチ	エッジスイッチA／B	性能	スイッチング容量とパケット処理能力は、Aは56Gbps以上かつ41Mpps以上、Bは104Gbps以上かつ74Mpps以上であること。					
1.4.4.1	スイッチ	エッジスイッチA／B	MACアドレス	16,000以上のMACアドレスに対応できること。					
1.4.5.1	スイッチ	エッジスイッチA／B	VLAN	IEEE802.1QタグVLANに対応し、アクティブVLANを1,000以上利用できること。					
1.5.1.1	スイッチ	PoEスイッチA／B	形状	1RUの1.2スイッチであり、19インチラックに搭載できること。					
1.5.2.1	スイッチ	PoEスイッチA／B	ポート構成	PoE給電に対応した1G BASE-Tポートを、Aは24口、Bは48口実装していること。					
1.5.2.2	スイッチ	PoEスイッチA／B	ポート構成	1G SFPアップリンクを2口以上実装できること。					

項番	大分類	中分類	小分類	要件	備考	実現方法	ベンダ名	ソリューション名	補足事項
1.5.3.1	スイッチ	PoEスイッチA／B	性能	スイッチング容量とパケット処理能力は、Aiは128Gbps以上かつ95Mpps以上、Biは176Gbps以上かつ130Mpps以上であること。					
1.5.4.1	スイッチ	PoEスイッチA／B	MACアドレス	16,000以上のMACアドレスに対応できること。					
1.5.5.1	スイッチ	PoEスイッチA／B	VLAN	IEEE802.1QタグVLANに対応し、アクティブVLANを1,000以上利用できること。					
1.5.6.1	スイッチ	PoEスイッチA／B	PoE給電	IEEE802.3at（PoE+）以上に対応し、総電力720W以上を供給できること。					
1.6.1.1	スイッチ	エッジスイッチC／D	形状	1RUの3スロットであり、19インチラックに搭載できること。					
1.6.2.1	スイッチ	エッジスイッチC／D	構成	2台のスタックを構成できること。なお、Dは全数を予備機とする。					
1.6.3.1	スイッチ	エッジスイッチC／D	ポート構成	1G BASE-Tポートを、Cは24口、Dは48口実装していること。					
1.6.3.2	スイッチ	エッジスイッチC／D	ポート構成	アップリンクとして、1G SFPを2口及び10G SFP+を1口以上実装できること。					
1.6.4.1	スイッチ	エッジスイッチC／D	性能	スイッチング容量とパケット処理能力は、Ciは160Gbps以上かつ119Mpps以上、Dは240Gbps以上かつ178Mpps以上であること。					
1.6.5.1	スイッチ	エッジスイッチC／D	MACアドレス	16,000以上のMACアドレスに対応できること。					
1.6.6.1	スイッチ	エッジスイッチC／D	VLAN	IEEE802.1QタグVLANに対応し、アクティブVLANを1,000以上利用できること。					
1.6.7.1	スイッチ	エッジスイッチC／D	ルーティング	スタティック及び動的ルーティング（OSPF等）に対応し、ゲートウェイ冗長及びDHCPリレーができること。					
1.6.8.1	スイッチ	エッジスイッチC／D	電源	冗長電源に対応していること。					
1.7.1.1	スイッチ	PoEスイッチC	形状	1RUの3スロットであり、19インチラックに搭載できること。					
1.7.2.1	スイッチ	PoEスイッチC	構成	2台のスタックを構成できること。					
1.7.3.1	スイッチ	PoEスイッチC	ポート構成	PoE給電に対応した1G BASE-Tポートを24口実装していること。					
1.7.3.2	スイッチ	PoEスイッチC	ポート構成	1G SFPアップリンクを2口以上実装できること。					
1.7.4.1	スイッチ	PoEスイッチC	性能	スイッチング容量は160Gbps以上、パケット処理能力は119Mpps以上であること。					
1.7.5.1	スイッチ	PoEスイッチC	MACアドレス	16,000以上のMACアドレスに対応できること。					
1.7.6.1	スイッチ	PoEスイッチC	VLAN	IEEE802.1QタグVLANに対応し、アクティブVLANを1,000以上利用できること。					
1.7.7.1	スイッチ	PoEスイッチC	ルーティング	スタティック及び動的ルーティング（OSPF等）に対応し、ゲートウェイ冗長及びDHCPリレーができること。					
1.7.8.1	スイッチ	PoEスイッチC	PoE給電	IEEE802.3at（PoE+）以上に対応し、総電力400W以上を供給できること。					
1.7.9.1	スイッチ	PoEスイッチC	電源	冗長電源に対応していること。					
1.8.1.1	スイッチ	機間スイッチ	形状	1RUの3スロットであり、19インチラックに搭載できること。					
1.8.2.1	スイッチ	機間スイッチ	構成	2台のスタックを構成できること。					
1.8.3.1	スイッチ	機間スイッチ	ポート構成	1G SFPポートを17口以上実装できること。					
1.8.3.2	スイッチ	機間スイッチ	ポート構成	10G SFP+を1口以上及びダイレクトアタッチ接続2口を実装できること。					
1.8.4.1	スイッチ	機間スイッチ	性能	スイッチング容量は1.2Tbps以上、パケット処理能力は950Mpps以上であること。					
1.8.5.1	スイッチ	機間スイッチ	MACアドレス	32,000以上のMACアドレスに対応できること。					
1.8.6.1	スイッチ	機間スイッチ	VLAN	IEEE802.1QタグVLANに対応し、VLAN IDを4,000以上利用できること。					
1.8.7.1	スイッチ	機間スイッチ	ルーティング	スタティック及び動的ルーティング（OSPF等）に対応し、ゲートウェイ冗長及びDHCPリレーができること。					
1.8.8.1	スイッチ	機間スイッチ	ルータ数	IPv4ルートを10,000以上収容できること。					
1.8.9.1	スイッチ	機間スイッチ	フロー可視化	sFlow相当のフロー情報を出力できること。					
1.8.10.1	スイッチ	機間スイッチ	電源	電源の二重化に対応していること。					
2.1.1.1	セキュリティ・認証アプライアンス	共通	監視連携	SNMPに対応し、機器の異常時には監視サーバが速やかに障害を検知できること。					
2.1.2.1	セキュリティ・認証アプライアンス	共通	環境条件	動作温度0～40℃に対応し、VCCI（クラスA又はクラスB）に適合していること（仮想アプライアンスの場合は種別基礎の環境条件による）。					
2.1.3.1	セキュリティ・認証アプライアンス	共通	付属品	実装に必要なアダプタ類やケーブル類等を全て含むこと。					
2.2.1.1	セキュリティ・認証アプライアンス	内部ファイアウォール	形状	物理アプライアンスであり、19インチラックに搭載できること。					
2.2.2.1	セキュリティ・認証アプライアンス	内部ファイアウォール	冗長構成	HA構成（2台）とし、系切替時に通信セッションを維持できること。					
2.2.3.1	セキュリティ・認証アプライアンス	内部ファイアウォール	性能	ステートフルインスペクションのスループットは70Gbps以上であること。					
2.2.3.2	セキュリティ・認証アプライアンス	内部ファイアウォール	性能	同時セッション数は5,000,000以上であること。					
2.2.3.3	セキュリティ・認証アプライアンス	内部ファイアウォール	性能	新規セッション処理は50,000セッション／秒以上であること（一斉ログイン時のバーストに対する余裕を含む）。					
2.2.3.4	セキュリティ・認証アプライアンス	内部ファイアウォール	性能	片のみでセグメント間通信の全量を処理できること。					
2.2.4.1	セキュリティ・認証アプライアンス	内部ファイアウォール	セッション制御	ポリシー単位でセッションタイムアウトを設定できること。					
2.2.5.1	セキュリティ・認証アプライアンス	内部ファイアウォール	収容数	アクセスポリシーを1,000件以上、VLANインターフェースを1,000以上設定できること。					
2.2.6.1	セキュリティ・認証アプライアンス	内部ファイアウォール	インターフェース	10G以上のポートを4口以上有すること。					
2.2.7.1	セキュリティ・認証アプライアンス	内部ファイアウォール	ルーティング	スタティック、RIP Ver.2及びOSPF（Ver.2／Ver.3）に対応していること。					
2.2.8.1	セキュリティ・認証アプライアンス	内部ファイアウォール	管理分離	管理用の通信と業務通信のルーティングテーブルを分離して保持できること。					
2.2.9.1	セキュリティ・認証アプライアンス	内部ファイアウォール	機能	ゾーン間のアクセス制御ができ、通信ログを取得できること。					
2.2.10.1	セキュリティ・認証アプライアンス	内部ファイアウォール	ログ	セッションログをSyslogサーバへ転送できること。					
2.2.11.1	セキュリティ・認証アプライアンス	内部ファイアウォール	更新・保守	ソフトウェア等の更新を契約期間中継続して受けられること。					
2.3.1.1	セキュリティ・認証アプライアンス	外部ファイアウォール	形状	物理アプライアンスであり、19インチラックに搭載できること。					
2.3.2.1	セキュリティ・認証アプライアンス	外部ファイアウォール	冗長構成	HA構成（2台）とする。					
2.3.3.1	セキュリティ・認証アプライアンス	外部ファイアウォール	性能	ステートフルインスペクションのスループットは70Gbps以上であること。IPS有効時のスループットを合わせて提示すること。					
2.3.3.2	セキュリティ・認証アプライアンス	外部ファイアウォール	性能	同時セッション数は5,000,000以上であること。					
2.3.3.3	セキュリティ・認証アプライアンス	外部ファイアウォール	性能	新規セッション処理は50,000セッション／秒以上であること。					
2.3.4.1	セキュリティ・認証アプライアンス	外部ファイアウォール	収容数	アクセスポリシーを1,000件以上設定できること。					
2.3.5.1	セキュリティ・認証アプライアンス	外部ファイアウォール	インターフェース	10G以上のポートを4口以上有すること。					
2.3.6.1	セキュリティ・認証アプライアンス	外部ファイアウォール	ルーティング	スタティック、RIP Ver.2及びOSPF（Ver.2／Ver.3）に対応していること。					

項番	大分類	中分類	小分類	要件	備考	実現方法	ベンダ名	ソリューション名	補足事項
2.3.7.1	セキュリティ-認証アプライアンス	外部ファイアウォール	機能	IPS機能を有効化し、外部との通信を監視又は遮断できること。					
2.3.8.1	セキュリティ-認証アプライアンス	外部ファイアウォール	ログ	セッションログ及び検知ログをSyslogサーバへ転送できること。					
2.3.9.1	セキュリティ-認証アプライアンス	外部ファイアウォール	更新・保守	シグネチャ等の更新を契約期間中継続して受けられること。					
2.4.1.1	セキュリティ-認証アプライアンス	透過型IPS（小型UTM）	形状・設置	透過型の物理アプライアンスであり、保守回線の特定点と院内ネットワークの間に設置できること。					
2.4.2.1	セキュリティ-認証アプライアンス	透過型IPS（小型UTM）	性能	監視対象の通信量に対して十分なスループットを有すること。					
2.4.3.1	セキュリティ-認証アプライアンス	透過型IPS（小型UTM）	インターフェース	保守回線側及び院内側に、1G以上のポートを各1口以上有すること。					
2.4.4.1	セキュリティ-認証アプライアンス	透過型IPS（小型UTM）	機能	不審な通信や脆弱性を悪用した攻撃などを検知又は遮断できること。					
2.4.5.1	セキュリティ-認証アプライアンス	透過型IPS（小型UTM）	ログ	検知又は遮断した通信の日時、送信元・宛先及び処理結果を記録できること。					
2.4.6.1	セキュリティ-認証アプライアンス	透過型IPS（小型UTM）	更新・保守	シグネチャ等の更新を契約期間中継続して受けられること。					
2.5.1.1	セキュリティ-認証アプライアンス	IPS集中管理コンソール	形状	サーバ又は仮想アプライアンスとして構成できること。					
2.5.2.1	セキュリティ-認証アプライアンス	IPS集中管理コンソール	管理範囲	導入するIPSの全台を一元的に管理できること。					
2.5.3.1	セキュリティ-認証アプライアンス	IPS集中管理コンソール	機能	IPSの稼働状態、検知・遮断イベント、シグネチャ更新状況及びポリシー設定を確認できること。					
2.5.3.2	セキュリティ-認証アプライアンス	IPS集中管理コンソール	機能	シグネチャやファームウェア等の更新を一元管理できること。					
2.5.4.1	セキュリティ-認証アプライアンス	IPS集中管理コンソール	ログ	各IPSのログを検索・確認できること。					
2.5.5.1	セキュリティ-認証アプライアンス	IPS集中管理コンソール	付属品	必要なサーバ、ソフトウェア及びライセンス等を全て含むこと。					
2.6.1.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	形状（無線LANコントローラ）	物理機器であり、19インチラックに搭載できると（RADIUSサーバとの同一筐体・別筐体のいずれの構成も可とする）。					
2.6.2.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	形状（RADIUSサーバ）	物理機器であり、19インチラックに搭載できると（無線LANコントローラとの同一筐体・別筐体のいずれの構成も可とする）。					
2.6.3.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	冗長構成（無線LANコントローラ）	単一障害時にも、接続中クライアントの通信の維持に加え、障害中の新規クライアントの接続・認証を含めて無線LANの利用を継続できること（実現方式は問わない、これを満たす場合、冗長構成は必須としない）。					
2.6.4.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	冗長構成（RADIUSサーバ）	冗長構成（2台以上）とすること。					
2.6.5.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	可用性（無線LANコントローラ）	認証サーバ機能との通信途絶時又は認証サーバ障害時にも、コントローラに保持した認証情報又は認証サーバの冗長構成等により、認証サービスを継続できること。					
2.6.6.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	性能（無線LANコントローラ）	コントローラを経由してデータ転送を行う構成の場合、スループットは20Gbps以上であること（データ転送に間与しない構成には適用しない）。					
2.6.7.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	収容数（無線LANコントローラ）	アクセスポイントを2,000台以上管理できること。					
2.6.8.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	収容数（RADIUSサーバ）	同時デバイス3,200台以上を認証できる性能及びライセンスを有すること。					
2.6.9.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	認証処理性能（RADIUSサーバ）	コアシッチの切替等に伴い再認証が集中した場合にも、同時デバイスの再認証を業務に支障のない時間内に完了できること（達成状況は総合テストにおいて確認する）。					
2.6.10.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	インターフェース（無線LANコントローラ）	データ転送に關する構成の場合、2.6.4の性能に見合うインタフェースを有すること。					
2.6.11.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	インターフェース（RADIUSサーバ）	認証通信及び管理通信に必要なインタフェースを有すること。					
2.6.12.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	認証機能	WPA2 Enterprise以上に対応し、EAP認証（EAP-TLSなど）及びMAC認証ができること。					
2.6.12.2	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	認証機能	認証結果に応じたダイナミックVLANにより、端末を所属セグメントへ収容できること。					
2.6.13.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	無線管理	アクセスポイントの構成を一括管理できること。					
2.6.13.2	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	無線管理	電波のチャネル及び出力を自動で最適化できること。					
2.6.13.3	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	無線管理	サブネットをまとめてローミングに対応していること。					
2.6.13.4	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	無線管理	管理外のアクセスポイントを検知できること。					
2.6.14.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	証明書	電子証明書の発行・管理に対応し、現行端末の証明書認証を移行できること。					
2.6.15.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	更新・保守	更新イメージをアクセスポイントへ事前配布し、停止時間を抑えて更新できること。					
2.6.16.1	セキュリティ-認証アプライアンス	無線LANコントローラ／RADIUSサーバ	ログ	認証ログをSyslogサーバへ転送できること。					
3.1.1.1	無線アクセスポイント	無線アクセスポイント	無線規格	IEEE802.11ax（Wi-Fi 6）以上に対応し（11a/b/g/n/acの下位互換）、2.4GHz帯と5GHz帯を同時に利用できること。					
3.1.2.1	無線アクセスポイント	無線アクセスポイント	アンテナ	内蔵アンテナ4本による4x4 MIMOに対応していること。					
3.1.3.1	無線アクセスポイント	無線アクセスポイント	転送速度	2.4GHz帯で1,147Mbps以上、5GHz帯で2,400Mbps以上に対応していること。					
3.1.4.1	無線アクセスポイント	無線アクセスポイント	同時接続数	各バンド400台に対応し、設置エリアごとの想定端末数を収容できること。					
3.1.5.1	無線アクセスポイント	無線アクセスポイント	セキュリティ	WPA2 Enterprise以上に対応し、EAP認証（EAP-TLS又はEAP-PEAP）とAES暗号化による通信ができること。					
3.1.6.1	無線アクセスポイント	無線アクセスポイント	有線側	1G BASE-Tポートを有し、IEEE802.3at（PoE+）以上による受電で動作すること。					
3.1.7.1	無線アクセスポイント	無線アクセスポイント	運用	コントローラを自動検出し、設定を自動取得できること（ゼロコンフィグ）。					
3.1.7.2	無線アクセスポイント	無線アクセスポイント	運用	コントローラとの通信断の間も、接続中クライアントの通信を継続できること（ローカルブリッジ/トンネル転送等の構成方式は問わない）。					
3.1.8.1	無線アクセスポイント	無線アクセスポイント	設置	天井面又は壁面へ取り付けられ、落下防止措置に対応していること。					
3.1.9.1	無線アクセスポイント	無線アクセスポイント	環境条件	動作温度0～40℃に対応し、VCCI（クラスA又はクラスB）に適合していること。					
3.1.10.1	無線アクセスポイント	無線アクセスポイント	監視連携	SNMPに対応し、機器の異常時には監視サーバが速やかに障害を検知できること。					
3.1.11.1	無線アクセスポイント	無線アクセスポイント	付属品	実装に必要なアダプタ類やケーブル類等を全て含むこと。					
4.1.1.1	サーバ	共通	CPU	調達仕様書「3.機能要件」「4.非機能要件」「6.運用要件」に定める仕様等をもとに、必要なCPU性能を試算し提供すること。					
4.1.2.1	サーバ	共通	メモリ	調達仕様書「3.機能要件」「4.非機能要件」「6.運用要件」に定める仕様等をもとに、必要なメモリ容量を試算し提供すること。					

項番	大分類	中分類	小分類	要件	備考	実現方法	ベンダ名	ソリューション名	補足事項
4.1.3.1	サーバ	共通	ディスク	調達仕様書「3.機能要件」「4.非機能要件」「6.運用要件」に定める仕様等をもとに、必要なディスク容量を試算し提供すること。					
4.1.4.1	サーバ	共通	電源	冗長電源を有すること。					
4.1.5.1	サーバ	共通	監視連携	SNMPによる死活監視及びR/Sソース監視に対応していること。					
4.1.6.1	サーバ	共通	付属品	実装に必要なケーブル類やライセンス等を全て含むこと。					
4.2.1.1	サーバ	監視サーバ	導入ソフトウェア	ネットワーク管理・監視ソリューションを導入すること。なお、ハイパーバイザー上で動作させるか物理サーバとするかは、仕様書調達仕様書の非機能要件の水準に従い、コスト効率及び可用性を考慮して選定すること。					
4.2.2.1	サーバ	監視サーバ	機能	全機器の死活監視とR/Sソース監視ができること。					
4.2.2.2	サーバ	監視サーバ	機能	監視対象をカテゴリに分けて表示し、機器ごとの設置場所や利用状況を把握できること。					
4.3.1.1	サーバ	Syslogサーバ	導入ソフトウェア	Syslogサーバソフトウェア及び最新OS（Windows Server 2025以上など）を導入すること。					
4.3.2.1	サーバ	Syslogサーバ	容量	厚生労働省等の方針に基づき12か月以上のログ保存に必要な容量を確保すること（外部記憶装置との併用を含む）。					
5.1.1.1	周辺機器	ネットワーク監視用PC	機能	ネットワーク監視サーバの管理コンソール及び運用管理機能を利用できること。					
5.1.2.1	周辺機器	ネットワーク監視用PC	付属品	実装に必要なアダプタ類やケーブル類等を全て含むこと。					
5.2.1.1	周辺機器	ネットワーク監視用バトランプ	機能	ネットワーク監視サーバと連携し、障害の検知時に点灯して異常の発生を視認できること。					
5.2.2.1	周辺機器	ネットワーク監視用バトランプ	付属品	実装に必要なアダプタ類やケーブル類等を全て含むこと。					
5.3.1.1	周辺機器	UPS	機能	接続機器への給電を無停電で維持し、電源の瞬断・停止時にも安全に運転を継続できること。					
5.3.2.1	周辺機器	UPS	容量	接続する機器の消費電力と必要なバックアップ時間を満たす容量を有すること。					
5.3.3.1	周辺機器	UPS	保守	バッテリーは、履行期間中の点検及び予防的交換を含むこと（調達仕様書6.4.2参照）。					
5.4.1.1	周辺機器	NAS	機能	Syslogサーバから退避したログを保存し、必要な際に参照できること。					
5.4.2.1	周辺機器	NAS	容量	12か月以上のログ保存に必要な容量を、Syslogサーバとの合計で確保できること。					
5.5.1.1	周辺機器	サーバ室ラック	形状	調達仕様書「3.6.共通機能（6）サーバ室ラック」に定める仕様によること。					