別紙１

機器等の要求仕様書

（県南振興局ネットワーク構築業務委託）

令和７年４月

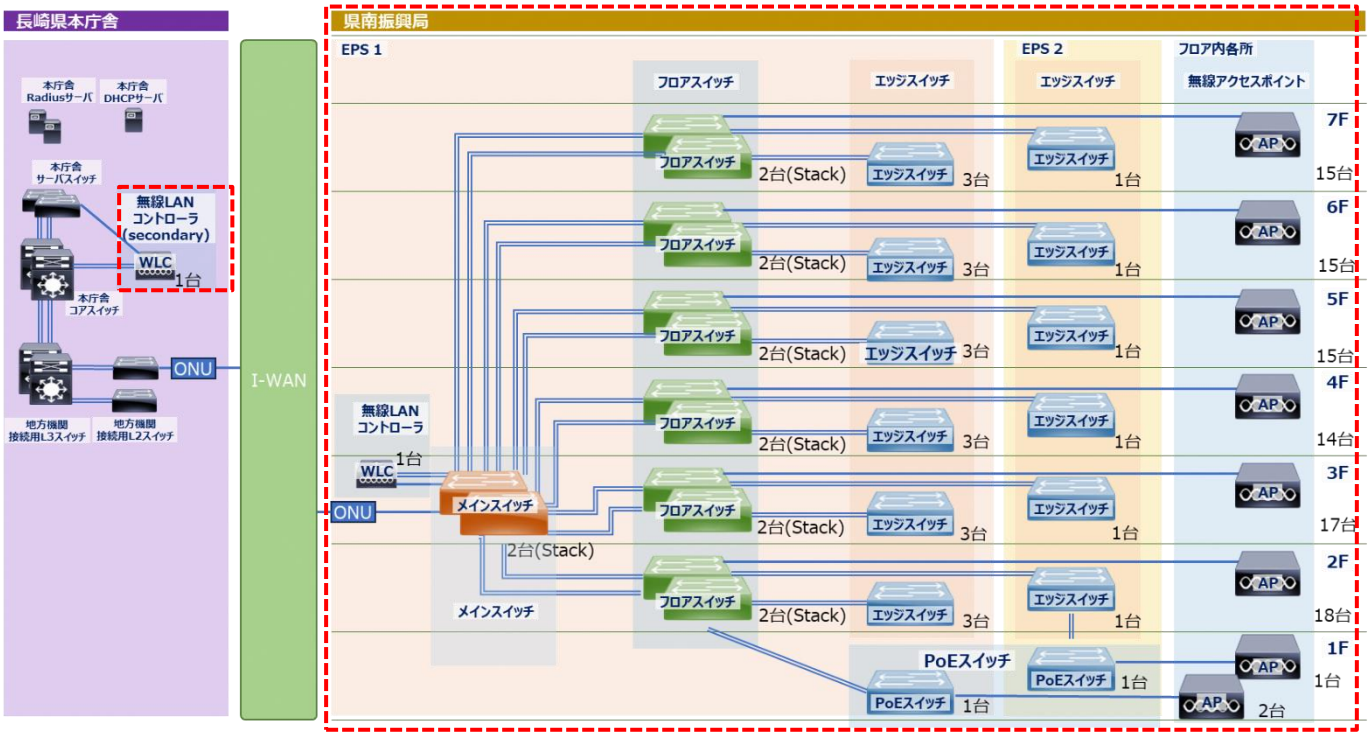
長崎県総務部スマート県庁推進課

目次

1. システム構成

1.1. ネットワークシステム全体構成図

・県南振興局ネットワークシステム全体構成図を以下に示す。（新規構築範囲：赤色破線）



・新規構築範囲のうち、メインスイッチから AP・WLC までの青色線（LAN ケーブル）は建設工事で敷設するため、当該 LAN ケーブル敷設は、本調達の対象外となる。本調達では、調達したネットワーク機器に、敷設された LAN ケーブルを接続する必要がある。

・「建設工事で設置する情報コンセント」用の LAN ケーブルをフロアスイッチ又はエッジスイッチ・PoE スイッチへ接続するが、その接続本数は、概ね次のとおりである（無線 AP を除く）。

フロア	情報コンセント用 LAN ケーブル接続本数
１Ｆ	20
２Ｆ	140
３Ｆ	120
４Ｆ	120
５Ｆ	120
６Ｆ	120
７Ｆ	120
８Ｆ	10

・本調達により調達するハードウェア数量は次のとおりとする。

	数量	備考
メインスイッチ	2	
フロアスイッチ	12	
エッジスイッチ	27	予備機含む
PoE スイッチ	3	予備機含む
無線 LAN コントローラ	1	
無線アクセスポイント	103	予備機含む

2. ハードウェア構成

2.1. ネットワーク機器共通要件

調達対象とするハードウェア要件を以下に示す。

2.1.1. 県南振興局メインスイッチ(CoreSwitch) ※一台あたりの仕様とする。

(1) 10/100/1000 Base イーサネットポートを 24 ポート以上実装していること。
(2) 95.23Mpps 以上のパケット処理能力を有すること。
(3) サイズは 5cm x 40cm x 44.5cm(高さ x 奥行 x 幅)以下であること。
(4) 機材の重量が 5.5kg 以下であること。
(5) 公表している MTBF 値が、587,000 時間以上であること。
(6) 128Gbps 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。
(7) スタック機能を有すること。
(8) IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
(9) IEEE802.1D に準拠したスパニングツリー機能を有すること。
(10) 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。
(11) IEEE802.1s に準拠したマルチプル・スパニングツリー機能を有すること。
(12) IEEE 802.3ad に準拠した Link Aggregation 機能を有すること。
(13) ユニキャストルーティングとして、RIP、OSPF、EIGRP stub に対応していること。
(14) ポートにてリンクフラップ等の障害を検知した際、ポートを一時的に使用不可能な状態にし、一定時間経過後、自動で再度利用可能にする機能を有すること。
(15) VRRP ゲートウェイ冗長プロトコル機能を有すること。
(16) IGMP Filtering、IGMP snooping 機能を有すること。
(17) MLDv1/v2 snooping 機能を有すること。
(18) 4000 以上の VLAN ID を利用可能なこと。また、アクティブな VLAN の数が 1000 個以上利用可能であること。
(19) スイッチ仮想インタフェースを 1000 個以上利用可能であること。
(20) 9000 バイト以上のジャンボフレームに対応していること。
(21) ポートあたり 8 個のキューを有すること。
(22) 設定情報レート(CIR)または最大情報レート(PIR)でレート制限が行えること。
(23) トラフィックを照合し、パケットラベル(DSCP)に基づき、一致するパケットを自動的に QoS グループに割り当てる機能を有すること。
(24) モジュラー型 QoS 機能を有すること。
(25) Class-Based Shaping 機能を有すること。
(26) Priority Queueing 機能を有すること。
(27) IEEE802.1p の CoS 優先制御機能を有すること。
(28) 2 階層以上の QoS 機能を有すること。
(29) ACL、IP Precedence、DSCP、COS によってトラフィックを分類する機能を有すること。
(30) 輻輳回避の仕組みとして、WTD、WRED を有すること。
(31) アクセスまたはトランクポートにて学習される MAC アドレスの数やアドレスにより制限する機能を有すること。
(32) IEEE802.1X および IEEE802.1X-REV 認証機能を有すること。
(33) VLAN、ルータ、およびポートの ACL 機能を有すること。
(34) 最大 1,500 個のセキュリティ ACL をエントリできること
(35) CPU(コントロールプレーン)への通信のレート・リミッタ機能を有すること。
(36) 同一 VLAN 上でブロードキャストドメインの分割をし、通信制限を行うセキュリティ機能を有すること。
(37) 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。
(38) ネットワーク管理者の予期しないエッジ 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。
(39) 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。
(40) ARP Spooping などの攻撃を防止するため、ARP パケットを検査する機能を有すること。
(41) 管理者の想定しない DHCP サーバによる、DHCP サービスを防止するため、DHCP サービスを提供できるインタフェースを指定できること。
(42) ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム制御機能を有すること。

(43) サプリカントとして上位スイッチにて IEEE802.1X を用いて認証される機能を有すること。
(44) 日時や時間帯を指定できるアクセスリスト機能を有すること。
(45) IEEE802.1X ユーザ認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
(46) IEEE802.1X 未対応端末に対応するため、ゲスト VLAN 機能を有すること。
(47) IEEE802.1X 認証ユーザに対し、ユーザ単位で異なるアクセスリストを適用できること。
(48) 送信元/受信元 MAC アドレスの任意の組み合わせに基づくパケットフィルタを行う機能を有すること。
(49) 送信元/受信元 IP アドレス、TCP/UDP ポート番号、またはこれらのフィールドの任意の組み合わせに基づくパケットフィルタを行う機能を有すること。
(50) 製品の正当性を保証し個体を一意に識別する仕組みを、十分な耐改ざん性を備えたハードウェアで提供すること。

例示品：シスコシステムズ合同会社製　Catalyst9200-24T

型名	内容	数量
C9200-24T-E	Catalyst 9200 24-port data only, Network Essentials	2
C9200-NW-E-24	C9200 Network Essentials, 24-port license	2
CAB-TA-JP	Japan AC Type A Power Cable	2
C9200-DNA-E-24	C9200 Cisco DNA Essentials, 24-Port Term Licenses	2
C9200-DNA-E-24-3Y	C9200 Cisco DNA Essentials, 24-Port, 3 Year Term License	2
PWR-C6-125WAC=	125W AC Config 6 Power Supply	2
CAB-TA-JP	Japan AC Type A Power Cable	2
C9200-STACK-KIT=	Cisco Catalyst 9200 Stack Module	2

2.1.2. 県南振興局フロアスイッチ(DistributionSwitch) ※一台あたりの仕様とする。

(1) 10/100/1000 Base イーサネットポートを 24 ポート以上実装していること。
(2) 95.23Mpps 以上のパケット処理能力を有すること。
(3) サイズは 5cm x 40cm x 44.5cm(高さ x 奥行 x 幅)以下であること。
(4) 機材の重量が 5.5kg 以下であること。
(5) 公表している MTBF 値が、587,000 時間以上であること。
(6) Power over Ethernet(PoE)給電を除く、スイッチの消費電力が 60W 以下であること。
(7) 128Gbps 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。
(8) スタック機能を有すること。
(9) IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
(10) IEEE802.1D に準拠したスパニングツリー機能を有すること。
(11) 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。
(12) IEEE802.1s に準拠したマルチプル・スパニングツリー機能を有すること。
(13) IEEE 802.3ad に準拠した Link Aggregation 機能を有すること。
(14) ユニキャストルーティングとして、RIP、OSPF、EIGRP stub に対応していること。
(15) ポートにてリンクフラップ等の障害を検知した際、ポートを一時的に使用不可能な状態にし、一定時間経過後、自動で再度利用可能にする機能を有すること。
(16) VRRP ゲートウェイ冗長プロトコル機能を有すること。
(17) IGMP Filtering、IGMP snooping 機能を有すること。
(18) MLDv1/v2 snooping 機能を有すること。
(19) 4000 以上の VLAN ID を利用可能なこと。また、アクティブな VLAN の数が 1000 個以上利用可能であること。
(20) スイッチ仮想インタフェースを 1000 個以上利用可能であること。
(21) 9000 バイト以上のジャンボフレームに対応していること。
(22) ポートあたり 8 個のキューを有すること。
(23) 設定情報レート(CIR)または最大情報レート(PIR)でレート制限が行えること。
(24) トラフィックを照合し、パケットラベル(DSCP)に基づき、一致するパケットを自動的に QoS グループに割り当てる機能を有すること。
(25) モジュラー型 QoS 機能を有すること。
(26) Class-Based Shaping 機能を有すること。
(27) Priority Queueing 機能を有すること。
(28) IEEE802.1p の CoS 優先制御機能を有すること。

(29) 2 階層以上の QoS 機能を有すること。
(30) ACL、IP Precedence、DSCP、COS によってトラフィックを分類する機能を有すること。
(31) 輻輳回避の仕組みとして、WTD、WRED を有すること。
(32) アクセスまたはトランクポートにて学習される MAC アドレスの数やアドレスにより制限する機能を有すること。
(33) IEEE802.1X および IEEE802.1X-REV 認証機能を有すること。
(34) VLAN、ルータ、およびポートの ACL 機能を有すること。
(35) 最大 1,500 個のセキュリティ ACL をエントリできること
(36) CPU(コントロールプレーン)への通信のレート・リミッタ機能を有すること。
(37) 同一 VLAN 上でブロードキャストドメインの分割をし、通信制限を行うセキュリティ機能を有すること。
(38) 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。
(39) ネットワーク管理者の予期しないエッジ 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。
(40) 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。
(41) ARP Spooping などの攻撃を防止するため、ARP パケットを検査する機能を有すること。
(42) 管理者の想定しない DHCP サーバによる、DHCP サービスを防止するため、DHCP サービスを提供できるインタフェースを指定できること。
(43) ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム制御機能を有すること。
(44) サプリカントとして上位スイッチにて IEEE802.1X を用いて認証される機能を有すること。
(45) 日時や時間帯を指定できるアクセスリスト機能を有すること。
(46) IEEE802.1X ユーザ認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
(47) IEEE802.1X 未対応端末に対応するため、ゲスト VLAN 機能を有すること。
(48) IEEE802.1X 認証ユーザに対し、ユーザ単位で異なるアクセスリストを適用できること。
(49) 送信元/受信元 MAC アドレスの任意の組み合わせに基づくパケットフィルタを行う機能を有すること。
(50) 送信元/受信元 IP アドレス、TCP/UDP ポート番号、またはこれらのフィールドの任意の組み合わせに基づくパケットフィルタを行う機能を有すること。
(51) 製品の正当性を保証し個体を一意に識別する仕組みを、十分な耐改ざん性を備えたハードウェアで提供すること。

例示品：シスコシステムズ合同会社製　Catalyst9200-24P

型名	内容	数量
C9200-24P-E	Catalyst 9200 24-port PoE+, Network Essentials	12
C9200-NW-E-24	C9200 Network Essentials, 24-port license	12
CAB-TA-JP	Japan AC Type A Power Cable	12
C9200-DNA-E-24	C9200 Cisco DNA Essentials, 24-Port Term Licenses	12
C9200-DNA-E-24-3Y	C9200 Cisco DNA Essentials, 24-Port, 3 Year Term License	12
PWR-C6-600WAC=	600W AC Config 6 Power Supply	12
CAB-TA-JP	Japan AC Type A Power Cable	12
C9200-STACK-KIT=	Cisco Catalyst 9200 Stack Module	68

2.1.3. 県南振興局エッジスイッチ(AccessSwitch) ※一台あたりの仕様とする。

(1)　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。
(2)　1G SFP ポートを 4 ポート以上有していること。
(3)　USB ポートを 1 ポート以上有していること。
(4)　USB-C のコンソールポートを有していること。
(5)　104Gbps 以上のスイッチング容量を有すること。
(6)　77.3Mpps 以上のパケット転送能力を有すること。
(7)　8000 個以上の MAC アドレスを自動学習可能であること。
(8)　メインメモリ 4GB 以上、フラッシュメモリ 16GB 以上を有していること。
(9)　物理ポートごとにブロードキャスト/マルチキャストトラフィックを抑制する機能を有すること。
(10)　パケットサイズが 9,000byte 以上の Jumbo Frame 転送が可能であること。

(11) ループ検出パケットを使用したループ検知機能を有し、ループににによるネットワークへの影響を抑えることができること。またループ検知時は検知のみ、ループ検知パケットを送信したポートのみ無効、送信ポート及び受信ポートの両方を無効にするアクションが選択できること。
(12) 送信または受信しかできないリンク状態を検出し、該当ポートを自動的にダウンさせる機能を有すること。
(13) 4,000 個以上の VLAN を登録可能であり、また同時に 512VLAN 使用が可能なこと。
(14) ポートベース、802.1Q ベースの VLAN をサポートしていること。
(15) IP アドレスの設定が可能なインターフェースは 16 以上を有すること。
(16) 同一 VLAN 内でのポート間の通信を不可にする機能を有すること。
(17) MVRP(Multiple VLAN Registration Protocol)をサポートすること。
(18) IEEE802.3ad に準拠した LACP による Link Aggregation をサポートしていること。
(19) IEEE802.1D スパニングツリー及び IEEE802.1w ラピッドスパニングツリーに準拠していること。
(20) IEEE802.1s マルチプルスパニングツリーに準拠していること。
(21) VLAN ごとに独立したスパニングツリーを構成可能な機能を有していること。
(22) IEEE802.1p に準拠した QoS 機能を有すること。また、ポートあたり 8 つ以上のキューを有すること。
(23) キューイング方式として SP(Strict Priority)をサポートしていること。
(24) IPv4 ACL(Access Control List)および IPv6 ACL(Access Control List)をサポートしていること。
(25) IPv4 および IPv6 ルーティングをハードウエアで実行すること。
(26) サポート可能なルーティングテーブル数は IPv4 が 512、IPv6 は 512 以上であること。
(27) IPv6 アドレスにてホストアドレスの設定が可能であること。
(28) IEEE802.1x 認証機能を有すること。
(29) MAC アドレスベースでの認証機能を有すること
(30) MAC アドレスベースで認証した殆ど通信しない端末で、端末自身がログオフするか切断するまで認証状態を維持する機能を有すること。
(31) RADIUS サーバと連携し、ユーザ/デバイス毎に認証の結果に応じたロールというセキュリティポリシーを割り当てアクセス制御が行えること。
(32) 接続済み端末に対しての動的なアクションを行うため、RADIUS CoA (Change of Authorization)をサポートすること。
(33) DHCP Snooping 機能を有すること。
(34) SNMPv1,SNMPv2c,SNMPv3 エージェント機能を有すること。
(35) Secure Shell(SSH) v2.0 にてリモートログイン可能であること。
(36) CLI で現在操作している階層のみのコンフィグを表示可能なこと。
(37) ポートミラーリング機能を有すること。
(38) スイッチ単体でのパケットキャプチャ機能を有すること。
(39) LLDP をサポートしていること。
(40) sFlow をサポートしていること。
(41) コンフィグを自動的にチェックポイントとして保存し、装置の再起動なしでコンフィグのロールバックができること。
(42) プログラミングによる制御に対応するため REST API をサポートしていること。
(43) メーカーが提供するオプションソフトウェアを使用することで設定の自動化や管理が集中的に行えること。
(44) Web GUI を有すること。
(45) DHCP サーバーと TFTP サーバーを使用した ZTP (Zero Touch Provioning)に対応し、自動的にスイッチのコンフィグとファームウェアのダウンロード及び適用が可能なこと。
(46) スイッチメーカーが提供するクラウドサービスからスイッチ単体のモニタリング、設定を行う機能を有すること。クラウドサービスを利用するためのサブスクリプションは別途購入するとする。
(47) 機器のサイズは 1U 以内であること。
(48) 動作保証温度は 0-45℃をサポートすること。
(49) RoHS 指令に対応していること。
(50) スイッチ単体でサポートする機能はライセンス等の追加を必要とすることなく利用可能なこと。
(51) スイッチ本体のハードウェア障害発生時、製品が販売されている期間及び販売終了から 5 年間は無償で同等製品との機器交換が可能であること。

例示品：日本ヒューレット・パッカード合同会社製　Aruba CX6000 48G 4SFP スイッチ

型名	内容	数量
R8N86A#ACF	Aruba CX6000 48G 4SFP	27

2.1.4. 県南振興局 PoE スイッチ(AccessSwitch) ※一台あたりの仕様とする。

(1) 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。
(2) アップリンクとして 1/10 ギガビットイーサネット SFP/SFP+を 4 ポート以上を実装できること。
(3) コアスイッチとの接続は、10 ギガビットイーサネット SFP+を利用し、10GBASE-LRM SFP Module を各スイッチに対して 1 個用意すること。
(4) 95Mpps 以上のパケット処理能力を有すること。
(5) サイズは 5cm x 30cm x 44.5cm(高さ x 奥行 x 幅)以下であること。
(6) 機材の重量が 6kg 以下であること。
(7) 公表している MTBF 値が、390,000 時間以上であること。
(8) Power over Ethernet(PoE)給電を除く、スイッチの消費電力が 55W 以下であること。
(9) 使用可能な PoE 電力が 370W 以上であること。
(10) 最大 100Gbps 以上の転送帯域幅を実装する固定型の L2 スイッチ製品であること。
(11) IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
(12) IEEE802.1D に準拠したスパニングツリー機能を有すること。
(13) 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。
(14) IEEE802.1s に準拠したマルチプル・スパニングツリー機能を有すること。
(15) IEEE 802.3ad に準拠した Link Aggregation 機能を有すること。
(16) ユニキャストルーティングとして、RIP、OSPF、EIGRP stub に対応していること。
(17) ユニキャストルーティングとして、OSPF、EIGRP、IS-IS に対応していること。
(18) ポートにてリンクフラップ等の障害を検知した際、ポートを一時的に使用不可能な状態にし、一定時間経過後、自動で再度利用可能にする機能を有すること。
(19) VRRP ゲートウェイ冗長プロトコル機能を有すること。
(20) IGMP Filtering、IGMP snooping 機能を有すること。
(21) MLDv1/v2 snooping 機能を有すること。
(22) 4000 以上の VLAN ID を利用可能なこと。また、アクティブな VLAN の数が 1000 個以上利用可能であること。
(23) スイッチ仮想インタフェースを 512 個以上利用可能であること。
(24) 9000 バイト以上のジャンボフレームに対応していること。
(25) ポートあたり 8 個のキューを有すること。
(26) 設定情報レート(CIR)または最大情報レート(PIR)でレート制限が行えること。
(27) トラフィックを照合し、パケットラベル(DSCP)に基づき、一致するパケットを自動的に QoS グループに割り当てる機能を有すること。
(28) モジュラー型 QoS 機能を有すること。
(29) Class-Based Shaping 機能を有すること。
(30) Priority Queueing 機能を有すること。
(31) IEEE802.1p の CoS 優先制御機能を有すること。
(32) 2 階層以上の QoS 機能を有すること。
(33) ACL、IP Precedence、DSCP、COS によってトラフィックを分類する機能を有すること。
(34) 輻輳回避の仕組みとして、WTD、WRED を有すること。
(35) アクセスまたはトランクポートにて学習される MAC アドレスの数やアドレスにより制限する機能を有すること。
(36) IEEE802.1X および IEEE802.1X-REV 認証機能を有すること。
(37) VLAN、ルータ、およびポートの ACL 機能を有すること。
(38) 最大 1,500 個のセキュリティ ACL をエントリできること。
(39) CPU(コントロールプレーン)への通信のレート・リミッタ機能を有すること。
(40) 同一 VLAN 上でブロードキャストドメインの分割をし、通信制限を行うセキュリティ機能を有すること。
(41) 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。
(42) ネットワーク管理者の予期しないエッジ 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。
(43) 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。
(44) ARP Spooping などの攻撃を防止するため、ARP パケットを検査する機能を有すること。
(45) 管理者の想定しない DHCP サーバによる、DHCP サービスを防止するため、DHCP サービスを提供できるインタフェースを指定できること。
(46) ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム制御機能を有すること。
(47) サプリカントとして上位スイッチにて IEEE802.1X を用いて認証される機能を有すること。

(48) 日時や時間帯を指定できるアクセスリスト機能を有すること。
(49) IEEE802.1X ユーザ認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
(50) IEEE802.1X 未対応端末に対応するため、ゲスト VLAN 機能を有すること。
(51) IEEE802.1X 認証ユーザに対し、ユーザ単位で異なるアクセスリストを適用できること。
(52) 送信元/受信元 MAC アドレスの任意の組み合わせに基づくパケットフィルタを行う機能を有すること。
(53) 送信元/受信元 IP アドレス、TCP/UDP ポート番号、またはこれらのフィールドの任意の組み合わせに基づくパケットフィルタを行う機能を有すること。
(54) 製品の正当性を保証し個体を一意に識別する仕組みを、十分な耐改ざん性を備えたハードウェアで提供すること。

例示品：シスコシステムズ合同会社製　Catalyst9200L-24P-4X

型名	内容	数量
C9200L-24P-4X-E	Catalyst 9200L 24-port PoE+, 4 x 10G, Network Essentials	3
C9200L-NW-E-24	C9200L Network Essentials, 24-port license	3
C9200L-DNA-E-24	C9200L Cisco DNA Essentials, 24-port Term license	3
C9200L-DNA-E-24-3Y	C9200L Cisco DNA Essentials, 24-port, 3 Year Term license	3
C9200L-STACK-KIT=	Cisco Catalyst 9200L Stack Module	3
SFP-10G-LRM=	10GBASE-LRM SFP Module	3

2.1.5. 無線ネットワークコントローラ※一台あたりの仕様とする。

(1) 「2.1.6.無線アクセスポイント」と同一メーカとする。
(2) メインスイッチとの接続は、UTP ケーブルにより接続すること。
(3) 最大 250 台のアクセスポイントを管理できること。
(4) 最大 5,000 台の無線デバイスを管理できること。
(5) 機器自体の性能として、スループット最大 10Gbps を利用可能なこと。
(6) IEEE 802.11 a/b/g/n/ac/ax に対応していること。
(7) IEEE 802.1Q をサポートすること。
(8) 無線コントローラとアクセスポイントの通信が RFC で公開された CAPWAP (RFC5415)プロトコルをサポートしていること。
(9) SNMP v1, v2c, v3 及び Syslog に対応していること。
(10) クライアント側で意識せず、IP サブネットを跨るローミングができること。
(11) 冗長構成として、AP とクライアントの状態を同期する環境に応じて 1 対 1 の Active-Standby 構成または、N 対 1 の Primary-Secondary 構成が出来る機能を有すること。
(12) N+1 構成時にアクセスポイントをグループ化し、グループ単位でソフトウェアアップグレードすることにより、コントローラとアクセスポイントの一部が常に起動している状態で無線システムのソフトウェアアップグレードできること。
(13) アクセスポイントをグループ化し、グループ単位でソフトウェアアップグレードができること。
(14) RF の管理機能として、動的なチャネル割り当て，カバレッジ ホールの検出と修正，出力制御ができること。
(15) 常時変動しうる電波環境に対応するため、電波管理機能は定期的に動作すること。
(16) 管理外 AP の検知及びルールに応じた分類が可能なこと。
(17) 無線 LAN クライアント間の通信をブロックすることが可能であること。
(18) IEEE802.1X 無線 LAN 認証が可能なこと。
(19) Web 認証が可能なこと。
(20) MAC 認証可能なこと。

例示品：シスコシステムズ合同会社製　C9800-L

型名	内容	数量
C9800-L-C-K9	Cisco Catalyst 9800-L Wireless Controller_Copper Uplink	1
SC9800LK9-179	Cisco Catalyst 9800-L Wireless Controller	1
C9800-AC-110W	Cisco Catalyst 9800 L Wireless Controller Power Supply	1
CAB-AC-C5-JAP	AC Power Cord, Type C5, Japan	1

2.1.6. 無線アクセスポイント※一台あたりの仕様とする。

(1) 「2.1.5.無線コントローラ」と同一メーカとする。
(2) IEEE 802.11 a/b/g/n/ac/ax に対応していること。
(3) IEEE 802.11ac/ax 80MHz チャネルに対応していること。
(4) IEEE 802.11i に準拠および WPA/WPA2 に対応していること。
(5) WPA3 に対応していること。
(6) 2.4GHz および 5GHz のワイヤレスネットワークの同時運用が可能であること(デュアル無線)。
(7) Dual 5GHz モードおよび 2.4GHz での利用が可能であること。
(8) 2.4GHz/5GHz を自動で切り替えられること。
(9) アップリンクとして、10/100/1000 イーサネット(RJ45)に対応していること。
(10) 無線 LAN のアンテナは内蔵であること。
(11) ビームフォーミングに対応していること。
(12) 802.11n 2x2 MIMO アンテナで 2 空間ストリームをサポート可能なこと。
(13) 802.11ac/ax 2x2 MU-MIMO アンテナで 2 空間ストリームをサポート可能なこと。
(14) レーダー干渉時帯域幅を縮退し回避する機能を有すること(Flex DFS)。
(15) 壁面や天井に設置された状態でも LED が確認でき、LED の色で稼働状態(ブートローダーステータス、アソシエーションステータス、オペレーティングステータス、ブートローダーワーニング、ブートローダーエラー)が判別できること。
(16) 1 本の 802.3af PoE で給電時に 80.11ax で動作可能なこと。
(17) パワーインジェクターや PoE/PoE+など柔軟な電源環境に対応できる製品であること。
(18) 以下の EAP に対応した認証が可能なこと。
- Extensible Authentication Protocol-Transport Layer Security(EAP-TLS)
- EAP-Tunneled TLS(TTLS)または Microsoft Challenge Handshake Authentication Protocol Version 2(MSCHAPv2)
- Protected EAP(PEAP)v0 または EAP-MSCHAPv2
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
- PEAPv1 または EAP-Generic Token Card(GTC)
- EAP-Subscriber Identity Module(SIM)

(19) コントローラと連携して動作可能なこと。
(20) OOOOOJAPAN に対応していること。
(21) 重量が 0.5Kg 以下であること。

例示品：シスコシステムズ合同会社製　Catalyst9105AXI

型名	内容	数量
C9105AXI-Q	Cisco Catalyst 9105AX Series	103
AIR-AP-BRACKET-8	AP Mounting Bracket	103
SW9105AXI-CW-K9	Capwap software for Catalyst 9105AXI	103
NETWORK-PNP-NONE	Network Plug-n-Play Opt Out SKU	103
CDNA-A-C9105	Wireless Cisco DNA On-Prem Advantage, 9105 Tracking	103
DNA-A-7Y-C9105	C9105AX Cisco DNA On-Prem Advantage,7Y Term,Trk Lic	103
AIR-DNA-A	Wireless Cisco DNA On-Prem Advantage, Term Lic	103
AIR-DNA-A-7Y	Wireless Cisco DNA On-Prem Advantage, 7Y Term Lic	103
AIR-DNA-A-T	Wireless Cisco DNA On-Prem Advantage, Term, Tracker Lic	103
AIR-DNA-A-T-7Y	Wireless Cisco DNA On-Prem Advantage, 7Y Term, Tracker Lic	103
AIR-DNA-NWSTACK-A	Wireless DNA Perpetual Network Stack - Advantage	103
SPACES-EXT-T	Cisco Spaces Extend Term License for Cisco DNA Advantage	103
SPACES-EXT-7Y	Cisco Spaces Extend for Cisco DNA Advantage	103

3. ソフトウェア構成

3.1. 共通要件

(1) 全てのソフトウェアは高い信頼性を有するものであり、メーカー・ベンダ等の保証又は動作確認済のものであること。
(2) 本調達に含むネットワーク機器を運用するに当たって必要数分のソフト・ライセンスを用意すること。
(3) ソフトウェアを導入するサーバ機器に関しては、既存のサーバ統合基盤上に構成することを想定している。
(4) ソフトウェアの選定・導入構築作業に於いては、既存導入ベンダと十分協議の上対応すること。
(5) 豊富な利用実績を有するとともに、十分な稼働期間を背景とし安定した動作を客観的に証明可能な市販パッケージ製品の標準機能を利用して構築すること。ただし、オープンソースソフトウェアを利用する場合、市販アプリケーションと同等の信頼性が認められ、継続的な保守対応が望めるものに限り認めるものとし、利用にあたっては受注者にて保証すること。
(6) ISO、JIS、ANSI 等の公的な規格に定めのある製品については、当該規格に準拠したものであること。
(7) 機器等を構成するソフトウェアは、同種の機器毎にバージョン等を統一すること。
(8) サービスパックまたはパッチ類に関しては発注者と協議のうえ、最新のものを適用すること。

3.1.1. 無線運用管理・可視化（CiscoDNA）

(1) 現行本庁舎ネットワーク環境にて導入済の Cisco DNA Center 上で、無線ネットワークコントローラ・無線アクセスポイントを登録すること。
(2) 無線 AP、不正 AP(管理外 AP)、干渉源(非無線 LAN 機器)について位置情報をマップ上に表示できること。また、物理位置に加え、稼働状況、ヒートマップ、干渉源の影響度を可視化できること。
(3) 本庁舎既設の Cisco DNA Center 上で無線接続端末の位置情報を図示するため CMX を導入すること。
(4) CMX のライセンスについては必要数を購入すること。

3.1.2. ネットワーク監視ソフト（OpManager）

(1) 現行本庁舎ネットワーク環境にて導入済の OpManager にて、本調達のネットワーク機器を監視登録すること。

4. プロジェクト管理

4.1. プロジェクト管理要件

システム構築・導入作業期間中に以下の文書を作成し、文書の記載に基づき各種管理を行い、プロジェクト管理を実施すること。また、プロジェクト管理については、受注者の品質マネジメントシステムを活用して品質の向上を図ること。

(1)　作業着手前に、「要求仕様書」7(1)に記載する“事前提出資料”を作成すること。
(2)　作業着手前に、前項で作成した事前提出資料のレビューを受け承認を貰うこと。
(3)　事前提出資料のうち、プロジェクト実施計画書に記載すべき事項は以下のとおりである。
　（ア）用語定義
　（イ）適用範囲
　（ウ）プロジェクト実施体制
　（エ）会議体
　（オ）スケジュール
　（カ）成果物
　（キ）制約条件及び前提条件
　（ク）レビュー実施方針
　（ケ）文書管理要領
　（コ）情報セキュリティ対策要領
　（サ）進捗管理要領
　（シ）課題・問題管理要領
　（ス）変更管理要領
　（セ）品質管理要領
　（ソ）コミュニケーション要領
　（タ）リスク管理要領
　（チ）プロジェクト実施計画書の改訂手順

(4)　プロジェクト管理
　（ア）受注者は、遅延なく業務を完遂するためにプロジェクト管理を行うこと。
　（イ）受注者は、本プロジェクトの実行にあたり、構築方針、実施体制、役割分担、実施内容(設計・構築・試験・評価等)、作業スケジュール、納入成果物、進捗管理方法、プロジェクトの意思決定手順、変更情報取り扱いの管理方法や手順を定めたプロジェクト実施計画書を作成し、長崎県の承認を得た上でプロジェクトの包括的な管理を行うこと。

(5)　進捗・課題管理
　（ア）受注者は、プロジェクトの進捗について計画と実績の確認および管理を行うこと。
　　併せて、作業遂行上で発生した課題を把握し、早期に解決を図るため検討を行うこと。

(6)　報告会議
　（ア）受注者は、各工程における詳細な打ち合わせの他、プロジェクト期間中は隔週（2025 年 12 月までは月 1 回で可とする。）で進捗報告会議を開催すること。
　　また、長崎県の求めがある場合はこれに応じ、必要な打ち合わせに参加すること。
　　なお、打ち合わせ及び進捗会議の議事録は受注者が作成し、長崎県の承認を得た上で、保管すること。

(7)　その他
　（ア）長崎県と受注者との役割分担を明確にし、長崎県が実施する必要のある作業は全て、プロジェクト実施計画書に明記すること。
　　機器の搬入・設置、配線工事・機器撤去等、全ての作業実施においては、長崎県に対し事前に作業計画書を提出し、レビュー・承認を得てから作業を実施すること。

5. システム構築・導入

5.1. 基本要件

信頼性・可用性・保守性・安全性の高いネットワークシステムの構築を基本方針とし、以下に示す項目を本調達に含めて実施すること。
なお、以下に示す項目は主要な事項について定めたものであり、この他にシステム構築・導入に際して当然に必要となる事項については本調達に含めて実施すること。

(1) 本庁舎既存ネットワーク機器の設定変更に当たっては、現行の長崎県県庁情報基盤運用サービス業務委託業者（以下、「庁内ネットワーク保守業者」という。）と協議すること。
(2) ネットワークシステムは 24 時間 365 日の稼働を求められることから、厳重な稼働監視により障害の早期発見及び迅速な復旧を行い、信頼性・可用性の向上を図ること。
(3) 本調達に含まれるネットワーク構築等については、必要なソフトウェア等をインストールし、別途指示する内容により、IP アドレス、ドメイン名(FQDN)及びセキュリティの確保に必要な設定を行った状態で納入すること。
(4) 今後の調達の公平性を鑑み、データ保持の必要性があるなど継続性の高いと考えられる機器及びソフトウェアについては、製造元の企業と資本関係のない企業によって、導入実績の多数ある製品を採用すること。また、ソフトウェアについては、ソフトウェアの製造元等の特定の製造元製機器のみでなく、他社製品等の機器においても稼働保証がされている製品を採用すること。
(5) 十分な実績、品質及び信頼性を有するものを採用すること。

5.2. 構築・導入要件

導入するハードウェア、OS 及びミドルウェアを現行ネットワークとの接続を考慮した上で実施すること。
なお、長崎県本庁舎設置機器については、今回の調達範囲外とする。

(1) 構築・導入に関する作業内容
　（ア）導入に関する作業内容については、設計レビューの中で長崎県担当者と合意を図りながら決定すること。
　（イ）本庁舎設置済の無線 LAN コントローラ(Catalys　t9800-L-F)1 台を、県南振興局設置の無線 LAN コントローラ予備となるよう構築すること。
(2) 構築・導入作業の実施時間帯
　（ア）原則業務に影響のない時間帯に実施すること、ただし業務影響がある作業を実施する必要がある場合は、長崎県担当者と合意を図りながら決定すること。
(3) 構築・導入に関する文書の作成
　（ア）「要求仕様書」7(1)“事前提出資料”及び「要求仕様書」7(2)“成果品”に記載された文書を作成すること。
(4) 構築・導入結果報告書の作成
　（ア）導入手順書の作業完了確認方法の合否結果を記した上で、導入作業全体を総括した導入結果報告書を作成すること。
(5) 機器搬入
　（ア）本プロジェクトにて調達するネットワーク機器の設置場所への搬入は、事前に詳細な施工及び作業内容、範囲、作業者名、スケジュールを長崎県に報告して承認を得ること。作業日当日は長崎県担当者の立ち合いのもと、作業を行うこと。
　　平日時間外や土日祝日を含めた時間外の作業が必要である場合は、事前に届け出を行うこと。
　（イ）搬入に際して長崎県に依頼する作業がある場合は、作業依頼書を提出すること。搬入作業後に排出される梱包材等、納入物品に付帯するもので、長崎県が指定する不要なものは受注者にて処分を行うこと。
(6) 機器設置・据付
　（ア）受注者は、本プロジェクトにて調達するネットワーク機器を長崎県が指定する箇所に設置・据付を行うこと。
　　設置箇所は、無線アクセスポイントは各フロア天井、スイッチは EPS 室へ設置するものとし、詳細な設置位置については事前に長崎県と協議の上で決定すること。
　（イ）導入機器には、長崎県の指示に従って管理用シールを作成・貼付し、ケーブル等にはケーブルラベル・タグの取り付けを行うこと。
　（ウ）設置を行う際は、既存システムへの影響を及ぼさないよう万全を期すこと。
　（エ）EPS 内各機器間の LAN 接続、フロア内無線アクセスポイントの取り付け、LAN 接続を行うこと。

5.3. 庁内ネットワーク接続に係る要件

（1） 基本方針

（ア）庁内ネットワークへの接続時は、業務継続性に影響を与える事なく接続を行えるよう、ネットワークの停止可能時間の調整も含めて、長崎県及び庁内ネットワーク保守業者と十分な協議を行った上で、事前の試験を含む接続計画を立案すること。

（イ）安全で確実な作業を行うため、庁内ネットワークへの接続時は、万が一ネットワークへの接続後に障害が発生した場合の対応策を準備しておくこと。

（2） 庁内ネットワークとの接続

（ア）庁内ネットワークへの接続後は、業務に支障がないように安定した運用ができるよう構築すること。

（イ）庁内ネットワークと接続するにあたり、設定変更作業及び停止が発生する場合、長崎県及び庁内ネットワーク保守業者と対応を協議し、実施すること（本庁舎ネットワーク機器設定変更、DHCP サーバ設定変更、認証サーバ設定変更等）。本項にかかる庁内ネットワーク保守業者に作業を依頼する必要がある場合は、庁内ネットワーク保守業者に対する作業費用も本調達に含まれるものとする。

（ウ）ネットワーク構築に伴い、既存ネットワーク監視システム等のメンテナンス（ノード追加、syslog 設定追加等）についても、庁内ネットワーク保守業者と対応を協議し、実施すること。本項にかかる庁内ネットワーク保守業者に作業を依頼する必要がある場合は、庁内ネットワーク保守業者に対する作業費用も本調達に含まれるものとする。

5.4. 教育に係る要件

導入するハードウェア、OS 及びミドルウェアを含めた全ての機器の教育を下記内容にて実施すること。実施時期や内容等については、設計レビューの中で長崎県担当者と合意を図りながら決定すること。

（1） 教育の種類

受注者は、(2)(ア)の対象者に対し、調達設備等に係る運用等(機器の操作等の訓練を含む)に関する研修を行うこと。なお、当該研修費用は本調達に含まれるものとする。

（2） 教育実施方法

（ア）対象者：長崎県スマート県庁推進課、庁内ネットワーク保守業者等(10 名程度)

（イ）研修内容：

① 県南振興局ネットワークの概要

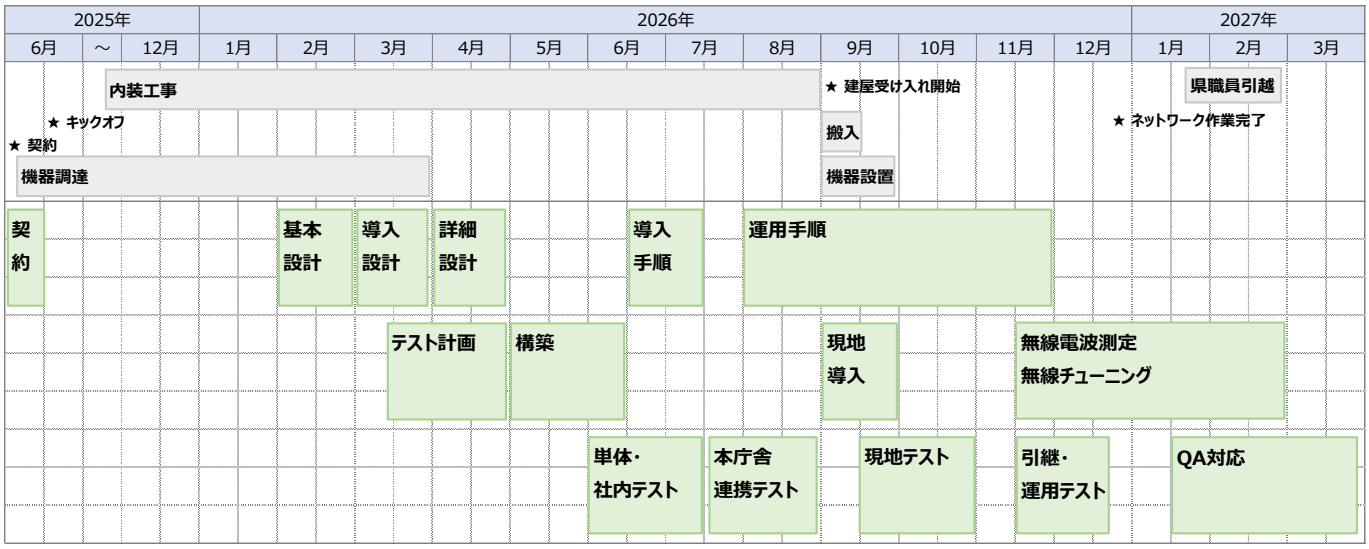
② 県南振興局ネットワーク運用における対応事項

③ 各機能の運用操作手順

（ウ）教材：運用等に関する研修において使用する研修用テキストを事前に作成し、県の確認を得ること。

5.5. 導入スケジュールについて

県南振興局ネットワーク本稼働までの工程を下記に記す。今回の作業を概ね下記スケジュールにて作業を実施すること。



6. テスト内容

6.1. 基本要件

機器の初期不良の検出および「要求仕様書 7(2)成果品」として作成する各種設計図書等の妥当性を確認するため、テストを実施すること。

(1) テスト開始時において、システムの適切な稼働が確認できる最新のバージョンのファームウェア・パッチが適用されていること。
(2) 単体テスト、結合テストは受注者側の設備にて行うこと。なお、セキュリティテスト、障害テスト及び運用テストは、本番環境にて実施すること。
(3) テストの実施に当たっては、現行システムを停止せずに実施すること。
(4) テスト時の動作確認にあたり、庁内ネットワーク保守業者及び各システムの保守運用業者に作業を依頼する必要のある場合は、依頼内容を取りまとめの上、事前に通知すること。

6.1.1. テスト内容

テスト内容に記載する事項は以下を想定しているが、設計レビューの中で県担当者と合意を図りながら決定すること。

(1) 単体テスト
機器の初期不良の検出及び機器単体レベルでの設計内容の妥当性を検出するテストを実施すること。
(2) 結合テスト
今回の調達範囲内における機器相互間の稼働が適切であることを確認すること。
(3) セキュリティテスト
設計書と同等の設定を施した状況において、導入するシステムにセキュリティ上の脆弱性がないか確認すること。
(4) 障害テスト
障害発生時に障害を適切に検出し、ログへの書き出しが適切に行われるか、アラートが適切に通知されるか及び冗長構成の切り替わりが適切に行われるかを確認すること。
(5) 運用テスト
システム運用及び運用業務が適切に実施できるか、運用設計書及び運用手順書の妥当性を検証すること。
(6) 総合テスト
県南振興局で構築したネットワークを庁内ネットワークへ接続し、基幹システムやポータルサイト等他のシステムへの接続等、県南振興局ネットワークが庁内ネットワークの一部として稼働することを検証すること。なお庁内ネットワークへの接続の詳細(日時、手順、範囲等)については長崎県担当者と協議し業務に支障が無いように実施すること。

6.1.2. テスト計画

テスト計画書は、テストの実施方針やテスト項目を記載するものである。
テスト計画書に記載する事項は以下を想定しており、設計レビューの中で長崎県担当者と合意を図りながら決定すること。
(1) テスト実施体制
(2) テストスケジュール
(3) テスト実施環境
(4) 合否判定基準
(5) テスト実施項目一覧

6.1.3. テスト結果報告書

テスト結果報告書は、テスト計画書において用意したテスト項目の実施結果とテストにおいて合否判定が否となったものの対応状況及びテストの結果を受けた品質見解を記載するものである。
尚、テスト結果報告書の提出に関して、プロジェクト責任者による承認を持って提出すること。

7. 保守・運用要件

7.1. 保守要件

7.1.1. ハードウェア保守要件

(1) 機器故障時の修理
機器に故障が発生した場合は、「9. 保守サービスレベル」に示した目標復旧時間以内に復旧するように、オンサイト保守による対応が可能であること。

(2) ドライバおよびファームウェア等の提供
提供するハードウェアは、保守期間全体にわたって、BIOS、ドライバ及び OS(ファームウェア)の最新データ及びパッチが継続的に提供されること。

(3) 保守期間
機器の保守期間は 5 年とし、本稼働前構築期間における保守は受託業者にて担保すること。

7.1.2. ソフトウェア保守要件

(1) 修正ソフトウェアの提供
(ア) 提供するソフトウェアは、保守契約期間全体にわたって、セキュリティホール等に対する情報及びプログラムの修正モジュールが継続的に提供されること。
(イ) 構築及び保守契約期間を通じて、当該情報を無償にて速やかに提供する体制を構築すること。

(2) 障害発生時の問い合わせ対応
(ア) 保守契約期間を通じて、ソフトウェア保守サポートが実施可能であること。
(イ) ソフトウェアに関連する障害が発生した場合、ログの解析等、詳細の切り分けに関する対応窓口を用意し、支援すること。なお、対応時間帯は、9 時-17 時の対応とする。尚、影響度の高い障害時は状況に応じて、真摯に対応すること。

7.1.3. 特記事項

(1) 保守の実施について、保守契約期間中は追加費用が発生することなく契約金額内で対応すること。
(2) 通常使用の状況において、障害が発生した場合についても、機器費用・作業費用・出張旅費などの追加費用が発生することなく受注金額内で対応すること
(3) 高所作業となるため、無線 AP の取り外し、取り付けについては、本調達対象外とする。
(4) 障害発生時は 2 時間以内に現地へ駆け付け、対応を開始すること。
(5) 部品が必要となった際、1 時間以内で搬入可能な場所にパーツセンターを有していること。

7.2. 運用要件

7.2.1. 運用管理要件

庁内ネットワーク保守業者が行うマニュアルの整備に必要な各種情報提供を行うこと。
なお、以下に示す内容は、主要な業務を定めたものであり、この他に運用管理業務の遂行に際して当然に必要となる情報については、県の求めに応じて資料を追加して作成し、提出するものとする。

(1) 庁内ネットワーク保守業者作業内容

(ア) 運用管理業務

① ITIL フレームワークに則ったネットワークシステムの管理
② ネットワークシステムの設定変更や構成管理
1. VLAN 変更
2. ファイアウォールルール変更
3. 認証ユーザの追加
4. セグメント追加
③ ネットワークシステムの安定稼働に必要な定期的な点検及び調整作業
④ 運用における各種連絡体制の管理
⑤ 要望・QA 発生時の受付、対応内容についての協議・実施可否
⑥ 下記、サービス稼働後の運用サービスが実施できる環境に必要なドキュメントの整備
1. 運用条件変更時の運用仕様書更新
2. イベント管理(計画停電/業務追加)
3. 改善提案

(イ) 障害受付業務

① ネットワークシステムに関する Q/A 問合せ受付
② 障害発生時の受付

(ウ) 障害管理業務

① 障害発生時のハード/ソフトの切り分・対応(保守対応含む)
② 原因調査・障害復旧対応の電話対応
③ 障害履歴管理を行い、定例会時の報告業務。

(エ) 構成/維持管理業務

① 庁内ネットワークの構成管理・ドキュメント/ネットワーク機器の設定情報の維持管理
② 定期的なネットワークシステムの環境監視・リソース報告(トラフィック状況、エラー内容)
③ 定期的なセキュリティ状況の報告(認証エラー件数、ウィルス検出状況)

(オ) 予防保守業務

① アプリケーション障害時、修正モジュールの適用
② ネットワーク OS 管理、修正モジュールの情報提供

7.2.2. 特記事項

(1) 保守の実施について、保守契約期間中は追加費用が発生することなく契約金額内で対応すること。
(2) 通常仕様の状況において、障害が発生した場合についても、機器費用・作業費用・出張旅費などの追加費用が発生することなく受注金額内で対応すること

8. 作業体制

8.1. 作業体制

8.1.1. 受注者側作業体制

システム構築・導入時の受注者側の担当者及び役割分担は下表のとおりとする。
なお、ここで示す担当者および役割は県が想定する体制で記載しているため、県と協議の上、プロジェクト進行に支障のない範囲で、役割内容の変更および兼務を認めることとする。

受注者側の担当者及び役割分担

担当者	役割
プロジェクト管理者 （必要に応じて補佐を配置することを認める。）	・ 県南振興局ネットワーク構築プロジェクト全体を統括する ・ プロジェクト実施計画書を作成する。 ・ 進捗報告書を作成する。 ・ 定例会議の議事を運営する。 ・ 成果品の作成に関する業務を総括する。 ・ 構築期間中の運用の月次報告を行う。 ・ 各グループの進捗状況の確認を行い、工程に変更を要する場合は、影響度合い等のリスク分析を行い、変更計画を立案する。 ・ 課題管理表の管理を行い、各グループに課題の解決を促す調整
ネットワーク設計管理者	・ ネットワーク関係の成果品の作成に関する業務を管理する。 ・ 成果品レビューのレビューイとして、関係者へのレビューを行う。
構築作業従事者	・ ネットワーク設計管理者およびファシリティ管理者の指示に従い、成果品の作成を行う。 ・ 調達システムの構築を行う。

8.1.2. 主要担当者

(1) プロジェクト管理者

次の（ア）（イ）両方を満たすプロジェクト管理者を配置すること。

（ア）プロジェクトマネジメントに関する以下のいずれかの資格又はこれに準ずる公的な資格を有すること。

プロジェクトマネージャ、技術士(情報工学部門)、技術士(総合技術管理部門(情報工学を選択科目とする者))、PMP(Project Management Professional)

（イ）官公庁ネットワークインフラ環境(有線および無線、クライアント数 2000 台以上)の設計又は構築業務におけるプロジェクト管理者の実績を有すること。

(2) プロジェクト管理者補佐(必要に応じて配置)

（ア）今回実施する作業内容と同様の作業経験を有したものであること。

(3) ネットワーク設計管理者

（ア） ネットワーク設計管理者は、官公庁ネットワークインフラ環境(有線および無線、クライアント数 2000 台以上)の設計又は構築業務における同様の作業実績を有すること。

8.1.3. 作業方法

(1) 県に提出する文書の作成作業においては、受注者側設備において実施すること。

(2) 今回新規に調達する機器以外のテストに必要な機器については、受注者にて手配すること。

(3) 単体テスト、結合テストを実施する場所は、受注者側の設備にて行うこと。なお、セキュリティテスト、障害テスト及び運用テストは、本番環境にて庁内ネットワークと接続した状況で実施すること。

(4) 受注者側でテストを実施する場所は、県に機密保持に関する誓約書を提出した者以外が入室できない環境で行うこと。これによらない場合は、県で使用するホスト名、IP アドレス等を機器の設定情報に登録せずに、テスト内容が担保できる設定情報にて検証を行うこと。

(5) 破損等に関する対応

受注者の責において機器の搬入･設置に関して起きた一切の事故･障害及び諸設備の破損等は、県担当者が指定する者の指示に従い、受注者が無償にて当該設備の復旧又は交換を速やかに行うこと。

(6) 機器の搬入及び搬出

（ア）機器の搬入及び搬出に当たっては、県担当者と搬入ルート及び入構車両に関する調整を行うこと。

（イ）庁舎内の搬入ルートにおいて、県から指示のあった箇所については、養生を行うこと。

(7) 作業場所

（ア）県の定めた場所において、作業を行なうこと。

9. 保守サービスレベル

サービスレベルアグリーメント(以下、「SLA」と記載)とは、受注者と発注者の間に結ばれるサービスの水準(定義・範囲・内容・品質など)に関し合意することをいう。本調達では、高いサービスレベルを維持するために SLA を導入する。

9.1. 保守サービスレベルの項目と設定値

項	項目	項目の説明	対象機器	サービスレベル
1.	障害対応要員到着時間	障害を通知してから障害対応要員が到着するまでの時間を表す。 障害対応要員到着時間＝長崎県での切り分け後、保守窓口に連絡してから到着するまでの時間	すべての機器等	2 時間以内
2.	障害復旧時間	障害の発生箇所を特定後、障害が復旧するまでの作業時間を表す。 なお、障害復旧時間には「IOS のリストア作業時間」は含まれないものとする。 障害復旧時間＝障害の発生箇所を特定後、障害が復旧するまでの作業時間 ・障害停止時間には、オンサイトサポート外の時間を含まない。 ・二重化冗長化部分は、一部障害が発生してもサービス提供可能な場合には障害停止としない。 ・ソフトウェアおよびハードウェアの潜在的なバグに起因する障害についてはサービス稼働率に起因しない。	ハードウェア	4 時間以内
			ソフトウェア	4 時間以内
3.	サービス提供時間帯 (障害対応)	問い合わせについて、障害に関する受付対応時間帯を表す。 サービス提供時間帯(障害対応)＝問い合わせについて、障害に関する受付対応時間帯	ハードウェア (メインスイッチ)	24 時間 365 日
			ハードウェア (メインスイッチを除く)	平日 9 時～17 時
			ソフトウェア	平日 9 時～17 時
4.	保守時間	ハードウェア及びソフトウェア保守作業の開始から、保守作業完了後の動作確認を実施しサービス提供が再開されるまでの時間を表す。 保守時間＝ハードウェア及びソフトウェア保守作業の開始から、保守作業完了後の動作確認を実施しサービス提供が再開されるまでの時間	すべての機器等	3 時間以内
5.	ハードウェア保守サポート期間	ハードウェアの故障を修理する保守サポート保証期間を表す。 ハードウェア保守サポート期間＝サポート保証期間	すべての機器等	本稼働から 5 年

9.2. 保守サービスレベル策定における除外項目

以下の事由により生じた事情については、サービスレベル算定の際、対象から除外する。

(1) 受注者の責任で制御できない事由
  （ア）電力供給の障害
  （イ）通信回線の障害
  （ウ）調達範囲外の機器の障害
  （エ）自然災害の不可抗力
(2) 発注者の責任に帰する事由
  （ア）発注者の作為または不作為
  （イ）本契約に定める発注者の義務不履行
  （ウ）発注者の誤った作業依頼
(3) 発注者と受注者との間での合意事由
  （ア）定期保守のための停止
  （イ）機器の導入やシステムの構成変更作業
  （ウ）その他発注者の要求に基づく業務上必要な停止等
(4) その他、受注者の責めに帰さない事由
  （ア）受注者が保証したシステム環境以外での使用
  （イ）他システムに起因する事象
  （ウ）悪意ある第三者による不正行為

9.3. 保守サービスレベルアグリーメントに係る是正措置

サービスレベルが未達成の場合は、以下の是正措置を行う。

(1) サービスレベルが未達成の場合は、県と受注者で協議の上、改善を実施する。
(2) サービスレベルの未達成が頻繁に繰り返される場合や、サービスレベルが極めて低水準となる場合は、県は契約を解除できるものとする。
(3) サービスレベルの程度の変更については、県、受注者ともに相手側に変更を要求することができるものとし、この場合相手側は誠意をもって協議に応じるものとする。

10. 特記事項

10.1. 全般

(1) 本要求仕様書は、受注者に業務遂行を求める最低限の基準を示したものである。したがって、本要求仕様書に記述していない事項であっても、本業務に必要と認められる事項は、県と協議の上、これを行うこと。
(2) 受注者は、県の指示に従い、本要求仕様書の内容について業務を行うこと。また、本要求仕様書の内容等に疑義が生じた場合は、県と協議の上、決定するものとする。
(3) 受注者は、常に作業場所を整理・整頓し、安全に留意して事故の防止に努めるとともに、労働基準法、労働安全衛生法を遵守して安全の徹底を図り、作業を行うこと。
(4) 機器の搬入・設置に関して起きた一切の事故・障害及び諸設備の破損等は、県及び県が指定する者の指示に従い、受注者が当該設備を無償にて速やかに復旧又は交換すること。
(5) 受注者が行う提案や報告及び相談等はすべて書面をもって実施し、内容について県の承認を得ること。
(6) 受注者は、本契約の全部又は一部を第三者に委託してはならない。ただし、書面により、事前に県の承諾を得た時にはこの限りではない。
(7) 現地調査、構築作業等、各拠点に入室を要する際には、県及び県が別途委託する県南振興局建設工事関係者と協議を行い、受注者の監理下において実施すること。

10.2. 情報セキュリティ対策

(1) 県の情報セキュリティポリシーに基づき、セキュリティ対策を実施すること。
(2) 受注者は、本業務の実施時において知り得た情報の取り扱いに十分留意し、他に漏えい等が行われないようにすること。
(3) 本業務に従事する全員と個別に守秘義務契約を締結していること。
(4) 会社全体としてセキュリティポリシーの策定・運用・教育を行い、適切な文書管理・情報管理が行われていること。
(5) 受注者側設備においては、十分な情報セキュリティを確保していることを設計・構築実施計画書の情報セキュリティ対策要領の中で明記すること。
(6) 次の事項を必ず定め、設計・構築実施計画書及び運用設計書に記載すること。
（ア）県から貸し出された資料又は支給を受けた物品等については、善良なる管理者の注意をもって保管及び管理するものとし、紛失又は破損の場合は直ちに県に報告し、県の指示に従って措置を講ずること。
（イ）責任者及び監督者を定めること。
（ウ）業務体制及び従事者を明確にすること。
（エ）従事者の担当範囲を明確にすること。
（オ）作業場所等に関して、情報の漏えい等の防止及び情報システムのセキュリティ確保のための措置を講ずること。

10.3. 受注者に関する条件

(1) 構築業務の実施部門が、品質マネジメントシステムである ISO 9001:2008 認証を取得していること。または、ISO 9001:2008 に準拠した品質マネジメントシステムを運用していること。
(2) 委託を行う場合においては、受注者の品質、情報セキュリティ及び IT サービスの各マネジメントシステムに従って、再委託先についても受注者と同等の取り組みを実施させること。

10.4. 担当者に関する条件

(1) 本業務を遂行させるために必要な知識及び経験を有するものを担当させること。
(2) 十分な体制を確保した上、責任体制を明確にし、全社的対応を図ること。なお、体制について具体的な資料を提出すること。
(3) 体制を変更する必要が生じた場合には、1 か月前までに設計・構築実施計画書の改訂案を提示し、事前に長崎県の承認を得ること。なお、担当者の異動が発生する場合には、後任の担当者に対して、本業務に支障をきたさないように十分な訓練を実施した後に業務の引継ぎを行い、長崎県に引継ぎ結果を報告すること。
(4) 担当者の病気により欠務が生じる場合は、その旨及び代行する担当者を速やかに長崎県へ報告し、承認を得ること。なお、代行する担当者は当日の業務に支障をきたさないようにすることができる者を担当させること。
(5) 県は、以下の場合においてプロジェクト管理者の交代を求めることができる。
（ア）作業計画に 2 週間以上の遅れが生じ、その遅れを 1 か月以上解消できない時。
（イ）同一の問題が、1 か月以上継続した時。
（ウ）作業計画の遅れや問題の原因として、作業実施者が必要な技能を習得していないと認められ、その状況が 1 か月以上解消できない時。
(6) 県は、以下の場合において担当者の交代を求めることができる。
（ア）十分なコミュニケーション能力がない時。
（イ）業務品質が低く、問題を指摘したにもかかわらず改善が見られない時。