

機能分類	機能名	仕様内容	南富良野町 設置場所等	中川町 設置場所等
新インターネット接続系ネットワークの構築	ネットワークの新規構築	1. 既設のインターネット接続系ネットワーク、LGWAN接続系ネットワークとは論理分離して構築すること。 2. 特定の通信に限定して、既設のLGWAN接続系ネットワークと相互に通信できること。 3. IPアドレス、サブネットマスク等の設定値に関しては、参加団体から提供されるデータを基に設計すること。 4. サーバとクライアントは異なるL3ネットワークに構築すること。		
新インターネット接続系ネットワークの構築	無線LANアクセスポイント	1. 既設のLGWAN接続用無線LANアクセスポイントは、(a)メーカー保守が運用期間（令和13年3月まで）中に継続可能、(b)Wi-Fi 6相当以上の性能を満たす、(c)WPA3-Enterprise/802.1Xに対応し証明書認証が実現可能、(d)VLAN/SSID分割及び管理方式（集中管理/クラウド管理等）が本業務の設計と両立する、の全てを満たす場合に限り流用候補とする。流用可否は受託者が評価結果（根拠、リスク、代替案）を提示し、参加団体の承認により決定する。 2. 受託者は、現地サイトサーベイ（電波測定・干渉確認・設置可否）を実施し、5GHz帯で-67dBm以上の受信強度を目標として、参加団体ごとの対象範囲全体をカバーする配置・台数・チャネル計画を設計すること。 3. Wi-Fi 6（IEEE802.11ax）に対応していること。 4. WPA3-Enterprise/802.1Xに対応していること。 5. 新規設置及び流用する全アクセスポイントについて、新インターネット接続系及びLGWAN接続系へ無線接続するための設定（SSID、VLAN、認証方式、暗号方式、ログ取得、管理者権限）を行うこと。 6. 接続するネットワーク単位（新インターネット接続系/LGWAN接続系）にSSID及びVLANを分離し、相互にブリッジされないこと。	・役場庁舎：1F建設課※、1F企画課※、1F総務課①②※、2F大会議室※、2F教育委員会※、2F議事事務局、2F議場 ・保健福祉センター：1F執務室①②※、1Fみくろホール、1F相談室、1Fトレーニングルーム、2Fエントランス※ ・焼養保育所：職員室、ホール・各教室共通、相談室・支援センター共通 ※既設あり（AT-TQ6702 GEN2）	■既設 役場庁舎内→①1階建設水道課付近（WAPM-1266R） ②1階住民課社会福祉係付近（MR36） ③2階総務課付近（WAPM-1266R） ④大会議室前（MR36） ⑤議場（MR36） 生涯学習センター→①1階職員室 ②2階大会議室 幼児センター→①職員室 ■要新設・更新箇所 ・役場庁舎内→1階①建設水道課付近②農林課付近③住民生活係付近 ④健康推進係付近⑤集団検診室 2階①地域振興課付近②総務課付近③議場 ④議事事務局⑤町長室 ・生涯学習センター ・幼児センター ・エコミュージアムセンター
新インターネット接続系ネットワークの構築	無線LAN用認証サーバ	1. 既設のLGWAN用認証サーバは、(a)メーカー保守が運用期間中（令和13年3月まで）に継続可能、(b)RADIUS（802.1X）で証明書認証が実現可能、(c)新インターネット接続系とLGWAN接続系の双方で論理分離（別インスタンス又は別テナント/設定分離）が可能、の全てを満たす場合に限り流用候補とする。流用可否は受託者が評価結果を提示し、参加団体の承認により決定する。 2. 無線LAN認証は、証明書認証（EAP-TLS等）により実現し、証明書の発行・失効（CRL/OCSP）・更新手順を設計書及び手順書に明記すること。 3. 新インターネット接続系のみ及びLGWAN接続系のみへ接続する端末を考慮し、各ネットワークごとに証明書及び認証ポリシーを分離すること（同一証明書の使い回しを禁止）。	・役場庁舎機械室 ※既設あり（NetAttest EPS-ST05-A）	・役場庁舎電算室
新インターネット接続系ネットワークの構築	無線AP用L2 PoEスイッチ	1. 指定した場所に設置すること。 2. ポート数は、接続対象機器数（アクセスポイント等）に対し予備10%以上を加えた数以上とすること。 3. PoEはIEEE802.3at（PoE+）以上に対応すること。 4. 新インターネット接続系ネットワークとLGWAN接続系ネットワークをVLANで論理分割できること（VLANの許可リスト及びポート設定を含む）。 5. 無線LANアクセスポイントへPoE方式で給電できること。	・役場庁舎機械室 ・保健福祉センター ・焼養保育所	・役場庁舎 ・生涯学習センター ・幼児センター
新インターネット接続系ネットワークの構築	L3スイッチ	1. 指定した場所に設置すること。 2. 下記ネットワークに接続すること。 ・新インターネット接続系 ・LGWAN接続系 ・共同調達基盤接続装置 3. LGWAN接続系ネットワークには、LGWAN境界FWを介して接続すること。 4. 参加団体間の分離（VLAN/VRF等）及び通信要件に従い、必要なVLAN、ルーティング、ACL等の設定を行うこと。	・役場庁舎機械室	・役場庁舎電算室
新インターネット接続系ネットワークの構築	LGWAN境界FW	1. 指定した場所に設置すること。 2. 新インターネット接続系ネットワークとLGWAN接続系ネットワークの境界に配置すること。 3. 通信要件に従い、新インターネット接続系ネットワークとLGWAN接続系ネットワーク間のアクセス許可、制限を行うこと。	・役場庁舎機械室	・役場庁舎電算室
新インターネット接続系ネットワークの構築	外局接続用VPNルータ	1. 既設のVPNルータは、メーカー保守が運用期間中（令和13年3月まで）に継続可能である場合に限り流用候補とする。流用可否は受託者が評価結果を提示し、参加団体の承認により決定する。 2. 設置場所の外局は左記とすること。 3. 役場庁舎と外局間はフレックスタイムVPNワイドでVPN接続し、オーバーレイネットワークはL2ブリッジ、もしくはL3ルーティングで接続すること。 4. 外局から共同調達基盤への接続に必要なVLAN、ルーティング等の設定を行うこと。	・役場庁舎機械室 ・保健福祉センター ・焼養保育所 ・金山複合施設（金山保育所・和楽園） ・焼養診療所 ・消防署 ・南富良野小学校 ・南富良野西小学校 ・南富良野中学校 ・南富良野高校	・生涯学習センター ・幼児センター ・エコミュージアムセンター ・中央小学校 ・中川中学校 ・中川消防支所
新インターネット接続系ネットワークの構築	共用サーバ	1. 指定した場所に設置すること。 2. 性能は、Active Directory、DNS/DHCP、RADIUS等の同時稼働を前提に、利用ユーザ数（調達数量）及び冗長構成を踏まえて受託者がサイジングし、参加団体の承認を得ること。 3. 19インチラックマウント型（2U型以内）であること。 4. HDDは冗長構成とすること。 5. LANインターフェースは1000BASE-T 2ポート以上（用途別に論理分離可能）を具備すること。 6. LCDコンソールユニットを用意すること。 7. ラック型無停電電源装置を用意すること。 8. OSはWindows Server 2025を利用すること。 9. 利用ユーザ数は参加団体毎に調達数量を参照すること。 10. 以下機能を実装すること。 ・電源管理ソフトウェア ・Active Directory機能 ・DNS/DHCP機能 ・RADIUS機能 ・その他必要な機能 11. 別途参加団体が提供するEDRソフトウェアを導入すること。	・役場庁舎機械室	・役場庁舎電算室
新インターネット接続系ネットワークの構築	NAS	1. 指定した場所に設置すること。 2. 19インチラックマウント型（2U型以内）であること。 3. RAID構成後の実効データ容量として4TB以上を確保すること。 4. HDDはRAID 5以上の冗長構成とし、1台故障時でもデータ消失・サービス停止が生じない構成とすること。 5. HDDに障害（故障および故障の手兆を含む）が発生した場合、電子メール等により管理者へ自動的に通知する機能を有すること。 6. 保守期間(5年間)中にHDDが故障した場合、先出しセンドバック方式により無償で交換品を提供すること。交換品は、故障連絡を行った日から3営業日以内に発送すること。	・役場庁舎機械室	・役場庁舎電算室
コミュニケーションツールの設定	全般	1. 参加団体から提供するコミュニケーションツール（クラウドサービス）のドメインに対し設定を行うこと。 2. 参加団体が指定するドメインでの環境管理が可能であること。 3. 利用サービス（機能範囲、外部共有可否、生成AI等）の対象は、詳細設計開始前までに参加団体が提示する一覧に基づき設定すること。受託者は、一覧が未確定の場合、要件ヒアリングシートを提示し、確定期限を計画書に明記すること。 4. テレワーク環境及びBYODを除き、庁外からのアクセスを拒否すること。例外（庁外利用が必要な業務）を許可する場合は、対象者・対象機能・許可期間を参加団体が承認した上で条件付きアクセス等で実装すること。 5. クライアントのコンテキスト（端末状態、ネットワーク、場所等）に応じたアクセス制御を実施すること。 6. 庁内に構築するActive Directoryとアカウント同期を行うこと。 7. アカウントの管理（追加、削除など）は参加団体のネットワーク管理者がコンソールを使って実施できるよう、権限分掌（ロール）を設計し、手順書を作成すること。 8. BYODの利用に際し、コミュニケーションツール以外に必要なサービスがある場合は、必要要件・費用・運用影響を明示して提案し、参加団体の承認を得た上で設計・構築すること。 9. 情報漏洩防止（DLP）は、外部共有・外部送信・ダウンロード・印刷・コピー等の制御条件をポリシーとして設定し、例外の申請/承認/記録手順を定めること。		
コミュニケーションツールの設定	クラウドストレージ	1. 個人用及び共有ストレージを利用可能とする設定を行うこと。 2. 共有ストレージは全庁、及び課毎に分割すること。 3. 新規追加・削除（組織改編等を含む）に係る運用手順（申請/承認/設定/記録）を手順書として提供すること。 4. コミュニケーションツール標準機能及び参加団体が別途提供するバックアップサービスを用いて、バックアップを1日1回以上実施すること。受託者は当該サービスとの連携設定及び運用引継ぎを行うこと。 5. バックアップからのデータ復元手順及び復元試験の実施方法を手順書に明記すること。		
コミュニケーションツールの設定	カレンダー・チャット・Web会議	1. 他ユーザ、会議室及び備品リソースを予約・確認できる設定を行うこと。 2. コミュニケーションツール標準機能及び参加団体が別途提供する業務支援サービスを用いて、設定を行うこと。受託者は当該サービスとの連携設定及び運用引継ぎを行うこと。 3. 外部（ドメイン外）宛でのファイル送付は原則禁止とし、DLP又は共有設定により技術的に制御すること。業務上やむを得ず例外を設ける場合は、対象者・対象期間・送付先ドメイン等を参加団体が承認した上で、例外ポリシーとして実装・記録すること。		
コミュニケーションツールの設定	移行	1. データ移行（ファイル・メール）の実施主体は職員とする。ただし、受託者は、移行計画（対象、手順、代替手順、ロールバック、並行運用期間）、移行手順書及び各サービス利用手順書を作成し、職員が実施可能となるよう移行リハール（代表データの試行）及び問い合わせ対応を行うこと。 2. クラウドサービスと既存環境の並行運用期間を設け、受託者が定める確認項目（送受信、権限、共有、ログ等）を満たすことを確認後に本切替を実施すること。 3. 移行前に職員向け、管理者向けのトレーニングを実施すること（オンライン・オンラインいずれも可）。 4. 職員が後日振り返るために、庁内に配信できる録画データを提供すること。		
メールの統合と無害化		1. 別途指定するコミュニケーションツールを使ってメールの送受信ができること 2. メールクライアントとして、新インターネット接続系端末のブラウザ、及びMicrosoft Outlookを利用可能とすること。 3. 統合後のメールドメインはLGWANドメイン（lg.jp）を利用すること。 4. LGWAN用メール、インターネット用メールのいずれの宛先ともメールの送受信を可能とするために振り分けを行うこと。 5. LGWANを経由しメールを送信する場合、メール本文や添付ファイルに対し無害化処理を行うこと。 6. インターネットを経由するメールを中継するために北海道セキュリティクラウドのMTAを利用すること。 7. メール経路の設計及び既存のメール経路からの切り替えに必要な作業（ドメイン移行等）を行うこと。		

ネットワーク間のファイルの転送と無害化		<ol style="list-style-type: none"> 1. 新インターネット接続系とLGWAN接続系との間でファイル転送ができること。 2. 新インターネット接続系からLGWAN接続系への転送時は、原則として無害化処理を実施すること。無害化処理を省略できる例外は、(a)対象ファイル形式が事前に無害化済みであることを技術的に検証できる、又は(b)参加団体が指定する承認者が事前に例外として承認した場合に限る。例外の承認・転送履歴はログとして保存すること。 3. 無害化対象のファイル形式（拡張子）を指定できること。 4. 無害化できないファイル形式の場合、予め指定した管理者が承認した場合に限り転送できるようにすること（承認・転送履歴を保存）。 		
BYOD環境の構築		<ol style="list-style-type: none"> 1. 職員の私用端末（Windows/Android/iOS）からアクセス可能なこと。 2. 管理者により許可された端末以外が接続できないよう制御すること。 3. ユーザ毎に、管理者が指定したコミュニケーションツール機能のみ利用できるように制限すること。 4. コミュニケーションツールへのアクセスには、多要素認証（MFA）を必須とすること。 5. ファイルのダウンロード及び画面キャプチャは原則禁止とし、アプリ保護ポリシー等により技術的に制御すること。例外を設ける場合は、参加団体の承認により対象者・期間・機能を限定し、設定と記録を行うこと。 		
外部監査の実施		<ol style="list-style-type: none"> 1. 「地方公共団体における情報セキュリティポリシーに関するガイドライン」に記載のB¹モデルに準拠することを監査すること。 2. 外部監査は、当該ネットワークの設計、構築、運用保守等を受託した事業者及びその関係事業者以外であって、当該監査の独立性及び客観性を確保できる者が実施すること。 3. 外部監査の実施後、監査実施者は監査結果報告書を作成し、参加団体へ提出すること。 4. 受託者は、監査結果報告書において是正又は改善が必要な指摘事項に対して、対応方針、対応期限を記載した是正計画書を参加団体へ提出すること。 5. 指摘事項に対し是正措置を行い、必要に応じて再監査を行うこと。 		