千代田区全庁LAN基盤整備及び運用保守業務

共通仕様書

令和８年１月

目次

目次

1. 背景と目的

1-1. 背景

令和 2 年 1 月に感染拡大が始まった新型コロナウイルス感染症への対応においては、オンライン環境の整備不足により、給付金等の申請手続や感染者情報の把握・集計に遅れが生じたほか、押印・対面規制やシステム環境の不備によるテレワーク推進の阻害など、国や自治体のみならず社会全体のデジタル化の遅れが顕在化した。

その後の 5 年間で、こうした課題を教訓とし、国や自治体ではデジタル化・DX 推進の取り組みが大きく加速した。千代田区（以下、「本区」という。）においても、行政手続のオンライン化やクラウドサービスの活用、テレワーク環境の整備、情報セキュリティ対策の強化など、デジタル技術を活用した業務改革が進められている。また、区民サービスの利便性向上や職員の働き方改革、デジタルデバイド対策など、多様な分野で DX の実現に向けた取り組みが展開され、社会全体のデジタル化が着実に進展している。

本区では、令和 7 年 4 月に改定した「千代田区 DX 戦略」に基づき、職員の生産性向上と安全性の確保を両立させた DX 推進の重点方針を掲げている。その一環として、β´モデル環境下でのさらなる業務効率化に加え、全庁 LAN システムの次期リプレースに向けて、現状の課題整理や今後の働き方を見据えた環境整備、ゼロトラストセキュリティアーキテクチャの考え方に基づくセキュリティ強化など、新たな業務環境の構築への移行を目指している。

あわせて、人口減少・少子高齢化の進行に伴い、行政ニーズの多様化や課題の複雑化が進む一方で、自治体としての経営資源が今後ますます制約を受けることが想定される。こうした状況を踏まえ、本区ではデジタル技術の活用によって課題解決を図り、持続可能な行政運営の実現に向け、職員の意識改革やデジタルスキル向上といった「人材育成」と、デジタル技術の利活用を支える「基盤整備」を両輪として位置付け、積極的な施策展開に取り組んでいる。

1-2. 目的

本区では、行政 DX の推進に向けた「基盤整備」として、業務効率と生産性の向上、区民目線の行政サービスの継続的な提供を実現することを目的に、職員の柔軟で多様な働き方や、迅速な情報共有・意思決定、さらには、データ利活用を前提とした政策立案や行政サービス提供を可能にする「全庁ネットワークセキュリティ基盤」（以下、「セキュリティ基盤」という。）を整備する。

1-3. 本仕様書の位置付け

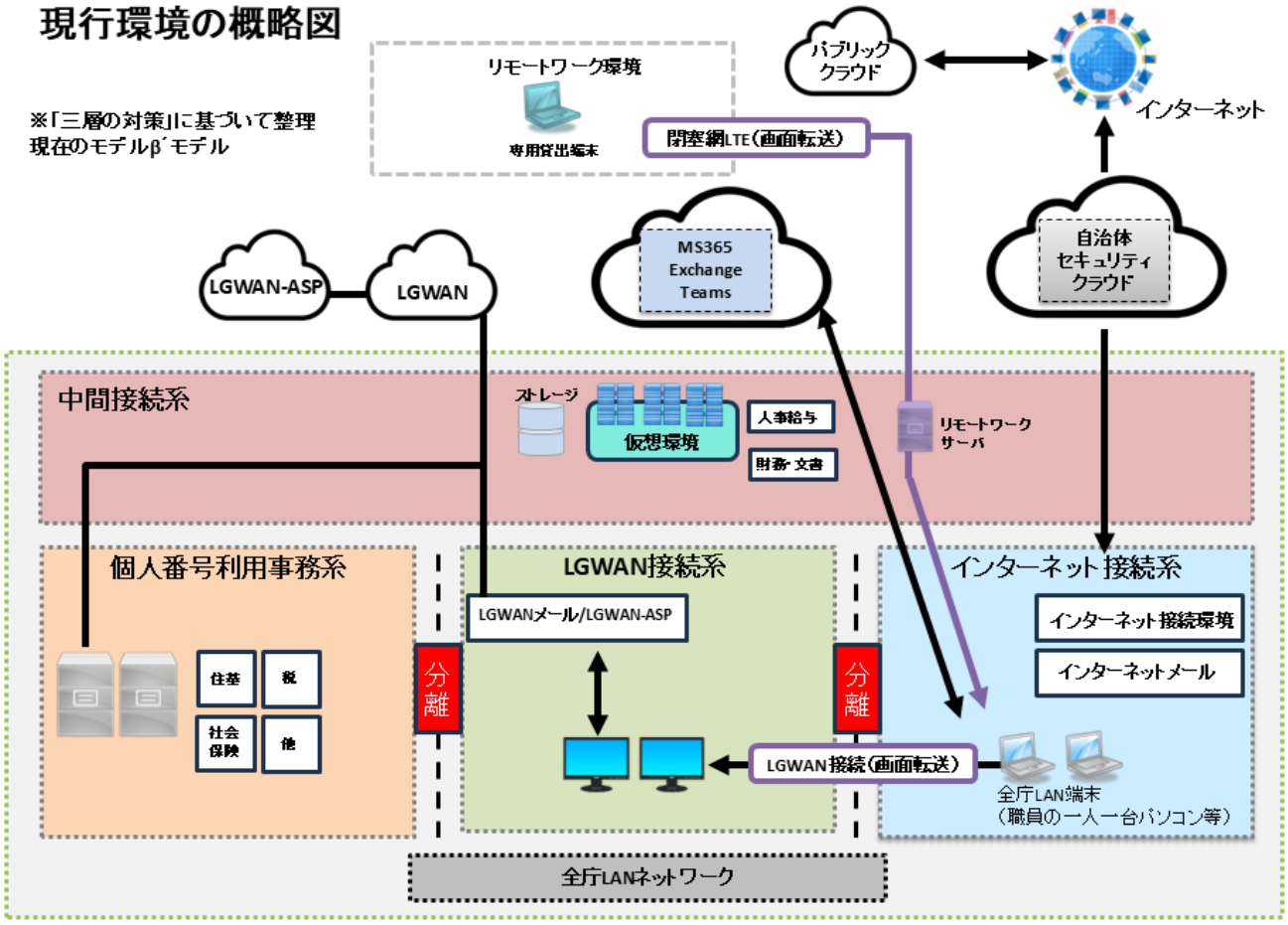
本仕様書は、セキュリティ基盤の整備にあたっての基本事項や調達概要を記述したものである。

2. 現状と課題

2-1. 現状

2-1-1. 現行環境の概略図

庁内システムや全庁 LAN 端末の配置、インターネット接続等にかかる現行の環境については、以下概略図のとおり(全体構成については「三層の対策」に基づいて整理)。



自治体ネットワークを「個人番号利用事務系」「LGWAN 接続系」「インターネット接続系」の三層に分離・分割するセキュリティモデルで、総務省の要請を受けて、本区は平成 28 年度から平成 29 年度にかけて対策を実施した。αモデル、βモデルを経て、現在はインターネット接続系にて、庁内システムや業務端末(一人一台パソコン)配置するβ´モデルとして運用している。なお、β´モデルによる運用を継続してきたが、さらなるセキュリティ強化を図るため、今後はゼロトラストモデルへの移行を推進する。本区の考えるゼロトラストモデルは、ネットワーク境界に依存せず、すべてのアクセス

を検証することを基本とし、内部・外部を問わず脅威に対応できる体制を構築するものとする。これにより、認証・認可の高度化、アクセス制御の厳格化、ログ監視の強化等を通じて、庁内システム及び業務端末に対する不正アクセス防止を徹底し、より安全で信頼性の高い情報環境を実現する。

2-1-2. 関連する現行システム等

セキュリティ基盤の整備と関連する現行システム等は下表のとおりである。

関連する現行システム等

システム名	概要	使用者
全庁ネットワーク	庁舎や出張所、データセンターの各拠点を結ぶ基幹ネットワークであり、国・全国自治体を結ぶ総合行政ネットワーク（**LGWAN**）等を接続する物理的ネットワークである	区職員等
東京都自治体情報セキュリティクラウド（第二期都区市町村情報セキュリティクラウド）	「三層の対策」の一環として、東京都及び都内市区町村等のインターネット接続を集約し、高度なセキュリティ監視を行うシステムである。 令和10年1月より「第三期都区市町村情報セキュリティクラウド」として運用開始を予定している。	区職員
LGWAN 接続環境	「三層の対策」の一環として、全庁 LAN 端末からの LGWAN 接続を画面転送方式（仮想化）による間接的な接続とするシステムである。	区職員
グループウェアシステム（**MS365**）	Teams チャット、電子職員録や Outlook スケジュール管理、施設予約、文書共有等の機能を中心に全職員が活用するシステムである。	区職員
インターネットメールシステム	庁内及び外部関係者とのメール（インターネット及び LGWAN）の送受信を行うためのシステム。ウイルスチェックによる添付ファイルの分離機能及び原本保管機能のほか、誤送信対策の機能を有する。	区職員

システム名	概要	使用者
リモートワークシステム	専用端末(貸出端末:200 台)を活用したリモートワークシステムを運用している(同時接続数 100 台)。LTE の閉塞回線を利用して、画面転送方式にて 運用している。	区職員
業務端末 (一人一台パソコン)	全庁 LAN システムで使用する職員用の業務端末(ノートパソコン)である端末2000台と、各所属で調達する個別システム用端末約600台が庁内ネットワークに接続している。	区職員
総合行政システム	全庁 LAN システムの仮想サーバ上に構築され、財務会計システムおよび文書管理システムとして稼働しています。利用にあたっては、全庁 LAN 端末からブラウザを介してアクセスします。	区職員
人事情報総合システム (正規職員・非常勤職員)	全庁 LAN システムの仮想サーバ上に構築され、勤怠管理および旅費精算の業務システムとして稼働しています。利用にあたっては、全庁 LAN 端末からブラウザを介してアクセスします。	区職員
人材情報システム	全庁 LAN システムの仮想サーバ上に構築され、職員のキャリア意向・昇進希望の申告機能を担うものとして稼働しています。利用にあたっては、全庁 LAN 端末からブラウザを介してアクセスします。	区職員

システム名	概要	使用者
千代田区ポータルサイト	オンライン申請、予約、決済、相談、情報発信などの機能を集約し、区民と区役所をつなぐ役割を担います。インターネット上に配置され、庁内業務システムとの連携にあたっては、全庁 LAN システムを介した安全な通信を確保しています。これにより、区民サービスの利便性向上と、庁内システムとの連動による業務効率化を両立しています。	区職員
Box(クラウドサービス)	Box は、庁内外での安全なファイル共有と共同作業を目的に導入されています。全庁 LAN 端末からブラウザでアクセスし、SSO 認証により利用します。庁内システムとの連携はセキュリティポリシーに基づき、安全な通信を確保しています。	区職員

2-2. 課題

1. クラウドサービス利用の柔軟性不足

【背景】

β´モデルへの移行後、クラウドサービスの利用は急速に拡大しているが、既存のセキュリティ基盤はオンプレミス中心の設計思想に依存しており、クラウド特有の柔軟な拡張性や多様なサービス連携に十分対応できていない。また、ネットワーク設計が従来型の集中接続に依存しているため、トラフィックの逼迫や拠点からの直接的なクラウド接続(ローカルブレークアウト)の不足が顕在化している。

【具体的課題】

・新規クラウドサービス導入時のセキュリティ審査・接続要件が煩雑で、導入スピードが遅延。

・SaaS 利用における認証・アクセス制御が統一されておらず、利用部門ごとに異なる運用ルールが存在。

・クラウド利用拡大に伴い、従来の境界防御型セキュリティではリスク管理が困難。

・ネットワークトラフィックが集中し、帯域不足に起因する業務処理の遅延や、利用環境の安定性が損なわれている。

・拠点からクラウドサービスへのローカルブレークアウトが未整備であり、通信経路が非効率となり、応答速度や可用性に課題が残る。

【影響】

行政サービスの迅速なデジタル化が阻害され、住民サービスの改善や業務効率化に遅れが生じている。さらに、ネットワーク性能の制約により、クラウド活用の効果が十分に発揮されず、職員の業務環境や住民向けサービスの品質低下につながっている。

2. 業務端末の整備と事業継続性（BCP）への対応不足

【背景】

災害や感染症流行など、業務継続性を脅かす事象が増加している中、「いつでも、どこでも」業務を遂行できる端末環境の整備が十分ではない。さらに、β´モデルへの移行に伴い、クラウドサービスや分散型ネットワークの利用が拡大しているが、端末環境の整備が追随できておらず、モデル移行後の新しい業務様式に適合していない。

また、現状ではシステムごとに専用端末を保有しているため、職員は複数の端末を切り替えて運用しており、業務効率や管理負荷の面で課題が顕在化している。

【具体的課題】

・テレワーク用端末の配備が限定的であり、災害時に庁舎外で業務を継続できる職員が限られる。

・端末のセキュリティ管理（パッチ適用、暗号化、認証強化）が不十分で、外部接続時のリスクが高い。

・モバイル環境での業務アプリ利用が制約され、緊急時の意思決定や情報共有が遅延。

・現状はテレワーク専用端末を配布し、画面転送方式で業務を行っているため、操作レスポンスやシステム利用の即応性に欠け、迅速な業務遂行が困難。

・β´モデル移行後に求められる「クラウド前提の業務遂行」に対して、端末環境が十分に最適化されておらず、クラウドサービス利用の柔軟性が制限されている。

・災害時や非常時における端末の可搬性・冗長性が不足し、BCP 対応力が限定的。

・システムごとに端末を保有しているため、複数端末の切り替え運用が必要となり、職員の負担や管理コストが増大しさらに、端末の重複配備により導入コストや維持コストも増加している。

【影響】

災害時・緊急時に行政機能が停止するリスクが高まり、住民への迅速な対応が困難となる。加えて、β´モデル移行後に期待される「クラウド活用による柔軟な業務継続」が十分に発揮されず、行政サービス全体の信頼性・可用性が低下している。

今後は、全庁 LAN 端末への統合を進めることで、端末の集約・標準化を図り、「いつでも、どこでも」安全かつ効率的に業務を遂行できる環境を整備する方針である。これにより、クラウドサービスの柔軟な活用や BCP 対応力の強化、端末管理の効率化を実現し、新しい業務様式への円滑な移行を目指す。

3. レガシーPBX によるコミュニケーション制約

【背景】

既存の PBX 環境は老朽化しており、クラウドやモバイル環境との親和性が低い。音声通話中心の設計であり、現代的な業務スタイルに適合していない。さらに、業務用スマートフォンと無線 LAN 環境を活用した電話システムも導入されているが、現状では子機的利用にとどまっており、十分な業務基盤として機能していない。また、本区の BCP 戦略においては、外部拠点ごとに独自の PBX を導入しているため、全体最適化が困難であり、拠点間の連携に制約が生じている。

【具体的課題】

・電話システムが庁舎内中心に設計されているため、災害時やテレワーク環境での利用に制約が生じ、BCP 対応力が十分ではない。

・音声通話以外のコミュニケーション（チャット、ビデオ会議、ファイル共有）との統合ができず、業務効率が低下。

・PBX の保守コストが高く、更新・拡張に柔軟性がない。

・業務用スマートフォンと無線 LAN 環境を利用した電話システムが限定的に運用されており、子機的利用にとどまっているため、モバイルワークやクラウド連携に十分対応できていない。

・外部拠点ごとに独自の PBX を導入しているため、BCP 戦略上の全体的な統合運用が困難となり、拠点間のコミュニケーションに制約が生じている。

【影響】

職員間のコミュニケーションが限定され、テレワークやクラウド連携に適した業務スタイルへの移行が阻害されている。さらに、BCP 戦略における外部拠点の独自運用が全体最適化を妨げ、災害時や緊急時における迅速かつ一貫した情報共有・意思決定が困難となっている。

3. セキュリティ基盤の基本事項

3-1. 全庁ネットワークセキュリティ基盤

3-1-1. 基本的な考え方

本区が今回構築する「全庁ネットワークセキュリティ基盤」は、以下の 3 つの機能を統合した集合体として、ベンダーのクラウド上での設計・運用することを想定している。

① ネットワークセキュリティ基盤

庁内ネットワークにおける通信の安全性を確保するため、ゼロトラストモデルを基本とした認証・認可、暗号化通信、侵入検知・防御機能を実装する。また、セキュリティポリシーの一元管理とログ監査を可能とする仕組みを提供することを想定する。

・認証・認可

端末・利用者・アプリケーションに対する強固な認証（多要素認証を含む）及び属性に基づく認可を実装すること。

・通信保護

庁内外の通信について暗号化を標準とし、機微データの取り扱いに応じた保護レベルを適用すること。

・脅威対策

不正アクセス、マルウェア、指令通信等を検知・遮断する機能を有し、継続的な脅威知見の反映を可能とすること。

・ゼロトラスト適用

ネットワーク境界に依存せず、常時検証・最小権限・セグメンテーションを実現すること。

・ポリシー一元管理

ネットワーク、ID、端末、アプリケーションのポリシーを統合管理し、変更履歴及び承認記録を保持すること。

・ログ・監査

認証、通信、設定変更、検知イベントのログ収集・保管・検索・改ざん防止を実装し、監査に資するレポート出力を提供すること。

② クラウド業務基盤

クラウドサービス利用に伴うセキュリティリスクを低減するため、ID 管理、アクセス制御、データ保護機能を強化する。さらに、業務継続性を確保するため、冗長構成とバックアップ体制を整備し、ガバナンスに準拠した運用を実現することを想定する。

・ID・アクセス管理

職員等のアカウントライフサイクル管理、権限付与・剥奪、委託先を含む外部利用者のガバナンスを提供すること。

・データ保護

保管・転送・利用時のデータ暗号化、情報分類に応じた防護ルール（持ち出し制御、透かし、共有制限等）を適用すること。

・業務継続性

冗長構成、定期バックアップ、復旧手順の整備及び復旧時間目標（RTO）・復旧時点目標（RPO）の設定と検証を行うこと。

・準拠運用

役割分担、変更管理、構成管理、脆弱性管理、定期レビュー等のガバナンスプロセスを実施すること。

・監査機能

アクセス・共有・外部連携の監査証跡を保持し、証憑として提出可能な形式で出力すること。

・連携性

庁内認証基盤、ネットワーク制御、資産管理、チケット管理、脅威インテリジェンス等と連携可能なこと。

③ 広域ネットワーク基盤

庁内外の拠点間通信を安全かつ効率的に行うため、複数の回線を柔軟に組み合わせ、通信経路を自動的に最適化する仕組みを導入する。これにより、暗号化された安全な接続を確保しつつ、回線障害時の冗長性を確保し、業務継続性を高めることを想定する。

・複数回線の柔軟な利用：

拠点毎に複数の回線を併用し、品質・遅延・輻輳等の指標に基づき通信経路を自動選択する仕組みを提供すること。

・暗号化及び分離：

拠点間通信は暗号化トンネルを用い、部局・業務系・個人情報系等の論理的分離を実現すること。

・障害時の自動切換機能

回線障害や品質低下時に、自動的に代替経路へ切替し、業務継続を確保すること。

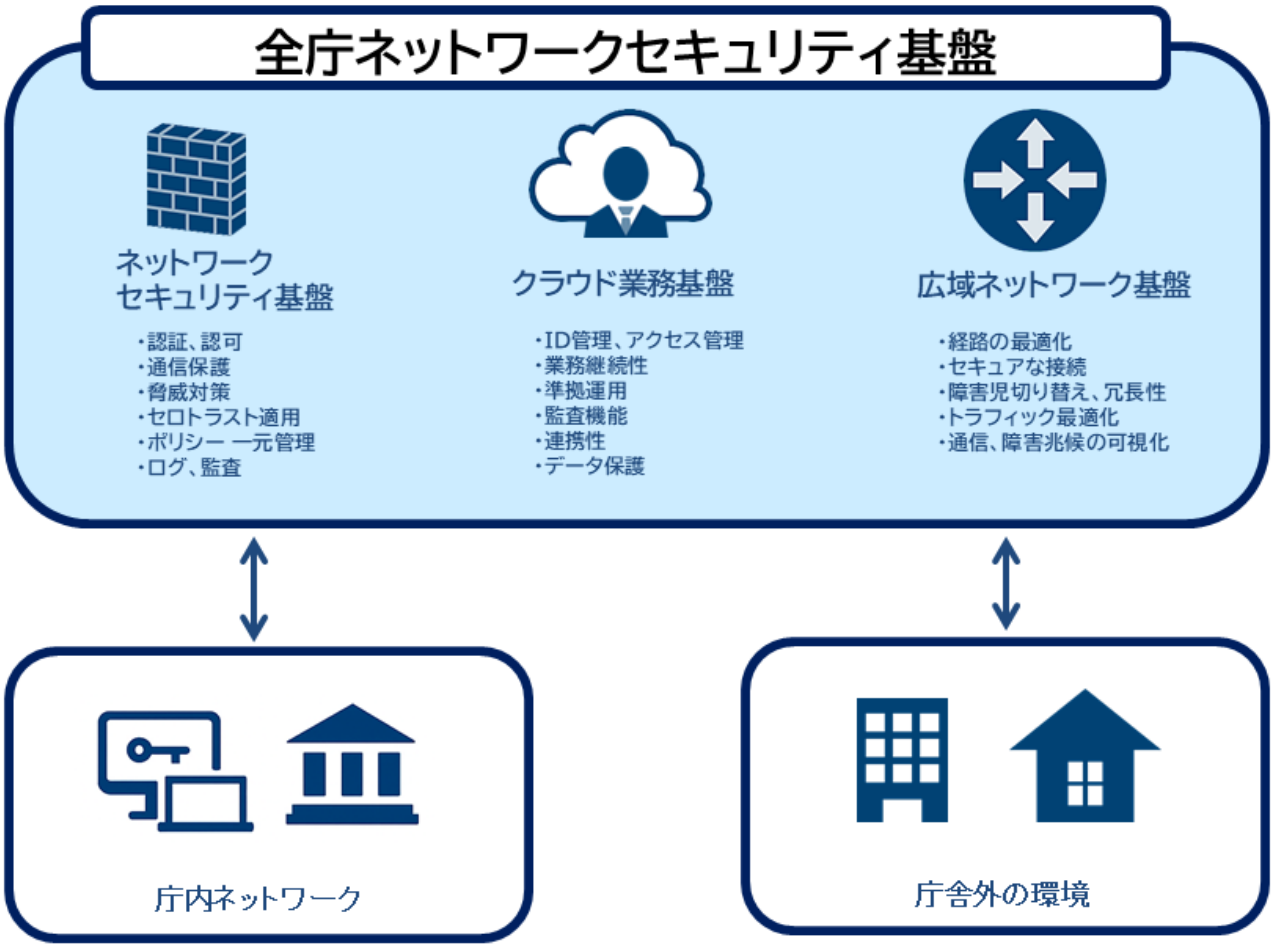
・トラフィック最適化

アプリケーション毎の優先度設定、帯域制御、遅延対策、キャッシュ活用等により最適な品質を担保すること。

・可視化：

運用：拠点毎の通信状況、障害兆候、設定差分を統合的に可視化し、遠隔からの標準化された運用を可能とすること。

概略図（イメージ）



3-2. Box への対応

本区では、情報資産の保護と業務効率化を目的として、令和 8 年 4 月よりクラウドストレージサービス「Box」の利用を全庁にて開始する。Box の導入に際しては、文書管理の精度を高めるため、Box 内でラベル管理機能を活用し、文書の分類やアクセス制御を適切に行う。

セキュリティレベルの一層の向上を図るため、令和 8 年度中に Microsoft 365 E3 ライセンスを活用し、Microsoft Purview の秘密度ラベル（Sensitivity Labels）の運用を開始する予定である。これにより、機密情報の取り扱いに関するポリシーを強化し、情報漏えいリスクを低減することを目的としている。本取り組みにより、文書の機密度に応じた適切な管理が可能となり、職員が安心して業務を遂行できる環境を整備する。

【提案書記載時の留意事項】

情報資産保護の観点を明確化

・機密情報の取り扱いに関するポリシーを遵守する提案であること。
・セキュリティ強化策（暗号化、アクセス制御、監査ログなど）を具体的に記載すること。

ラベル管理の実装方針

・Box のラベル管理機能を活用した文書分類・アクセス制御の仕組みを提案すること。

・Microsoft Purview の秘密度ラベルとの連携方法を明示すること。

プラットフォーム間の整合性確保

・Box ラベルと Microsoft 365 秘密度ラベルの紐づけ方法を具体的に示すこと。
・両サービス間で一貫した情報保護ポリシーを適用する仕組みを提案すること。

運用・管理の容易性

・ラベル付与の自動化や標準化の仕組みを提案すること。
・誤分類防止策や運用負荷軽減策を記載すること。

職員の利便性向上

・ユーザ操作性を考慮した UI/UX 設計を提案すること。
・ラベル運用ルールやセキュリティポリシーの周知・教育計画を含めること。

拡張性・将来性

・他クラウドサービスとの連携やゼロトラストモデルへの対応を視野に入れた設計を提案すること。
・法令改正やセキュリティ基準変更への柔軟な対応策を記載すること。

リスク管理と対策

・情報漏えい、誤分類、システム障害などのリスクを洗い出し、対策を明示すること。
・事業継続計画（BCP）や障害時の復旧手順を提案すること。

4.音声系システムの基本事項

本区では、次期音声系システムの導入にあたり、既存環境を最大限活用しつつ、FMC サービスや UC 連携を追加することで、庁内外・リモート・ABW 環境に対応できる柔軟な構成を目指しています。スマートフォンや PC 端末を活用し、内線・外線通話を円滑に行えるハイブリッド型の仕組みを検討しています。

4-1. ID および端末管理に関する要件

・全庁 LAN に接続する PC（約 2,300ID）および IP 電話機（約 200 台）を対象とした、規模に応じ ID 管理機能を備えること
・上記端末を適切に管理できる仕組み（端末管理機能）を提供すること

4-2.通話録音に関する要件

・コールセンターや原課ダイヤルインでの発着信時に、通話録音が可能であること

・録音告知ガイダンスを設定できる機能を備えること

4-3. セキュリティ要件

・ID 管理において、認証・認可の強化（多要素認証、ロールベースアクセス制御）を実装すること

・端末管理において、資産情報の暗号化および不正アクセス防止策を講じること

・通話録音データの暗号化保存およびアクセス権限管理を徹底すること

・操作ログ・通話録音ログを取得し、一定期間安全に保管できること

・セキュリティポリシーに準拠した脆弱性対策（OS・アプリケーションの定期更新）を実施できること

5. 注意事項ほか

5-1. 注意事項

本業務について、契約書及び要求水準書・共通仕様書に明示されていない事項でも、双方で協議し合意した事項については、受託事業者が責任を持って対応すること。

・ 受託事業者は、運用開始までの作業スケジュールを本区と協議の上、決定すること。

・ 要求水準書・共通仕様書に記載されている全ての業務に対し、いかなるケースにおいても本区に対し、別途費用を請求することはできない。ただし、本区の要求仕様変更による追加費用については別途協議を行うこととする。

・ 要求水準書・共通仕様書に定めのない事項が発生した場合及び疑義が発生した場合は、本区と協議の上、定めるものとする。

・ 現行システムまたはネットワークの停止を伴う作業は閉庁日、もしくは夜間での実施を前提に本区と協議のうえ決定すること。