千代田区全庁LAN基盤整備及び運用保守業務

要求水準書

1. 業務件名

千代田区全庁LAN基盤整備及び運用保守業務

2. 業務概要

2.1 新基盤整備の背景と目的

千代田区では、令和3年度より全庁LANシステムおよび内部事務機能を統合した総合行政システムのリプレースを段階的に進めてきました。令和6年度からは、β´モデル環境における運用が開始され、Microsoft365 などのクラウドサービスを活用しながら業務の効率性と利便性の向上が一定の成果を見せています。

一方で、業務端末が複数存在することにより業務効率が停滞していること、クラウドサービスの利用に柔軟性が欠けていること、情報資産の保護や認証・権限管理の最適化、外部サービスとの連携におけるセキュリティ確保など端末の適切な利用やセキュリティ対策の強化が求められるなど、新たな課題が顕在化しています。

これらの課題を踏まえ、新たな全庁LAN基盤では、クラウドベースのアーキテクチャを中心に据え、ゼロトラストセキュリティの導入を行います。EntraIDによる認証の一元化、SASEによる通信・クラウドアクセスの制御、EDRやMDMによるエンドポイント保護など、多層的な対策を講じることで、「ひとり1台の端末で業務完結できる環境」、「三層分離を意識しない環境」、「情報資産を適切に保護しながら、どこでも働ける環境」を目指します。さらに、職員一人一人の負担軽減を図り、業務の効率化を実現するとともに、災害時等にも業務継続ができる環境整備を推進していきます。

これらの取り組みは、職員の生産性向上だけでなく、区民サービスの質的向上にも寄与するものであり、今後の行政運営における基盤強化の一環として位置づけられます。これまでの運用実績と課題を踏まえ、持続可能で安全な情報システムの構築を目指します。

さらに、千代田区では、ワークプレイス変革にも重点を置き、今後取り組んでいく方針です。これは単なる職場環境の改善にとどまらず、職員一人ひとりのパフォーマンスを最大化し、組織全体で協働する働き方への転換を意味しています。「働きやすい職場づくりを進めることで区民サービスを向上させる」という理念が、区のパーパス「挑戦＿千代田らしさを、わたしらしく」として明確に打ち出されています。職員は自らの業務を能動的に捉え、時には集中して働き、時には他部署とコラボレーションして効率的に業務を進めることが期待されています。

本要求水準書では、これまでの運用実績と課題を踏まえ、次期基盤に求められる要件と方向性を明確にし、持続可能かつ安全な情報システムの構築を目指します。千代田区の行政運営における基盤強化の一環として、職員の業務効率化と区民サービスの質的向上を両立させる次期リプレースの実現に向けた指針を示すものです。

2.2 解決したい主な課題

(1) 業務端末の複数利用による非効率の解消（1台の端末で業務完結できる環境の実現）
(2) クラウドサービス等の活用による柔軟な業務拡張と事務効率化の推進
(3) 認証・権限管理の最適化および高度なセキュリティレベルの確保
(4) 外部システムやクラウドサービスとの安全かつ円滑な連携の確保
(5) ワークスタイル、ワークプレイス変革を支援・推進する仕組みの構築
(6) 災害時を含む業務継続性（BCP）の確保
(7) 全庁LAN基盤の見直しによる運用・保守経費の削減および最適化
(8) サイバー攻撃や内部情報窃取など新たなセキュリティ脅威への対策強化
(9) 管理部門（情報システム課）職員の業務負担軽減および専門性向上の促進
(10) 勉強会・研修等の実施による職員の能力開発およびITスキルの向上
(11) ネットワーク監視の一元管理および通信可視化によるセキュリティ強化
(12) ヘルプデスク機能の向上によるワンストップ対応体制の構築・対応の迅速化
(13) ヘルプデスク体制の見直しによる問い合わせ内容の集約化及びナレッジ蓄積の推進
(14) ヘルプデスク強化による職員業務量の削減および人材不足の解消
(15) ヘルプデスクにおけるAI等の活用によるオペレーションの高度化・効率化

2.3 調達方針

(1) クラウドサービスを前提とした職場環境の整備

働く場所や時間にとらわれない働き方を可能とする、職員同士のコミュニケーションやデータ共有の仕組みを構築すること。

(2) 強靭化モデル（三層の対策（β´モデル））を意識しない業務空間の整備

三層分離を抜本的に見直し、これまでの境界型のセキュリティ対策からゼロトラストネットワークモデルへシフトし、クラウドサービスの有効活用できる環境を整備すること。

(3) 高度な情報セキュリティの確保

最新の「千代田区情報セキュリティポリシー対策基準」及び「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の対策基準」に準拠すること。また、セキュリティの脆弱性を最小限に抑えるため、定期的な脆弱性診断やセキュリティパッチの適用を含む運用保守体制を構築すること。

(4) 業務継続性の確保

システムの可用性を最大化するため、冗長化構成や障害時の迅速なリカバリ機能を組み込むこと。24時間365日の稼働を前提に、SLAに基づいた可用性の基準を設定し、それに対応した技術的対応をすること。

(5) 全庁LAN運用管理の簡素化と自動化

システム運用に必要な管理機能は、できるだけ自動化され、効率化されるべきであり、監視、ログ管理、障害対応などの運用業務は、ダッシュボードやアラートシステムを活用して簡便に行えるようにすること。

(6) 外部監査への対応

外部監査(セキュリティ監査、コンプライアンス監査、ISO 等の認証監査)に対応できる設計と運用体制を持つこと。変更管理やリリース管理の履歴を追跡できる仕組みを導入し、監査結果に基づく改善提案や指摘事項への対応がスムーズに行えるようにすること。

(7) 管理部門(情報システム課)の運用負荷低減への対応

システム切り替え時及びシステム稼働後の安定稼働を担保するサポート体制及び窓口の整備、迅速なインシデント対応、定期的なアップデート及びパッチ適用等が行えること。

(8) 調達コスト最適化への対応

システムの導入・運用にかかる総所有コストを最小化することを基本方針とし、本調達において重要視する。初期導入費用だけでなく、保守費、運用人件費、ライセンス更新費、クラウド利用費など、長期的なコストを含めて総合的に最適化を図ること。不要な機能や過剰なスペックを排除した“スリムかつ効果的な構成”とし、調達後においても定期的にコストをレビューし、利用状況や業務変化に応じて構成等の見直しを行うことで、継続的なコスト最適化の実現を目指すこと。

2.4 業務範囲

(1) 要件定義

本システムで実装する機能および性能・信頼性・セキュリティ・運用保守等の非機能要件、導入時の制約条件を整理し、要件として定義し、提案内容と現状との Fit&Gap にて現状との差異を確認するため、要件定義工程を計画すること。

(2) 基本設計

システム全体の構成や機能要件を整理し、設計方針を決定すること。職員の業務要件を踏まえ、システムの概要、構成要素等を定義すること。

(3) 詳細設計

基本設計を基に、サービスや機器等の技術要素の仕様を具体化すること。画面設計、処理手順などを明確にし、開発や構築に必要な情報を整備すること。

(4) 調達機器等における技術的支援

機器やソフトウェアの選定・調達に関する技術的な助言を行うこと。性能要件や互換性、セキュリティなどを確認し、適切な製品選定を支援すること。

(5)　システム構築

設計に基づき、機器の設定やソフトウェアのインストール等を実施すること。合わせてネットワークやサーバ構成を整え、システムを稼働可能な状態にすること。

(6)　システム移行

既存システムから新システムへのデータ移行や設定変更を行うこと。業務停止を最小限に抑え、安全かつ確実な移行を実現すること。

(7)　システムテスト

構築したシステムが設計通りに動作するか検証すること。単体・結合・総合テストを実施し、品質と安定性を確認すること。

(8)　ユーザ操作支援

職員がシステムを円滑に操作できるよう、操作説明やサポートを行うこと。導入時のフォローや問い合わせ対応も行うこと。

(9)　プロジェクト管理

進捗管理、課題管理、品質管理を行い、プロジェクト全体を円滑に進めること。関係者との調整や報告も適宜適切に行うこと。

(10) マニュアル・研修等の資料作成

システム利用や運用に関するマニュアルを作成し、研修資料等を整備すること。利用者教育やスキル定着を支援すること。

(11) 運用保守業務

システム稼働後の安定運用を維持し、障害対応や定期メンテナンスを行うこと。

(12) ヘルプデスク

職員からの問い合わせに対応し、問題解決を支援すること。トラブルシューティングや操作案内を迅速に行うこと。

(13) 業務及び運用改善業務

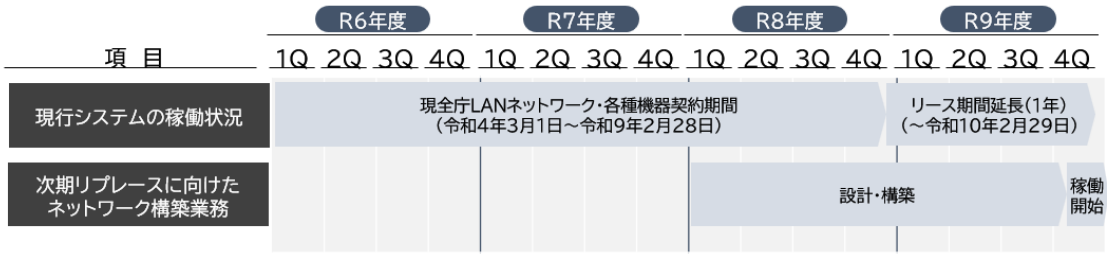
業務効率化や運用の最適化を目的に、改善提案や設定変更を行うこと。

(14) その他

上記に含まれない付随業務や随時対応を行うこと。新技術の検討や緊急対応など、柔軟に対応すること。

2.5 全体スケジュール

次期全庁 LAN システムの構築・運用スケジュールは下記のとおり。



2.6 全庁ネットワークセキュリティ基盤の概要

本業務では以下の 3 つの機能を統合した集合体を「全庁ネットワークセキュリティ基盤」と定義し設計・運用することを想定している。

①ゼロトラストモデルに基づく認証・認可、暗号化通信、侵入検知・防御、セキュリティポリシー管理・ログ監査を統合した「ネットワークセキュリティ基盤」

②クラウドサービス利用時の ID 管理・アクセス制御・データ保護、冗長構成・バックアップ体制による業務継続性確保、ガバナンス運用を実現する「クラウド業務基盤」

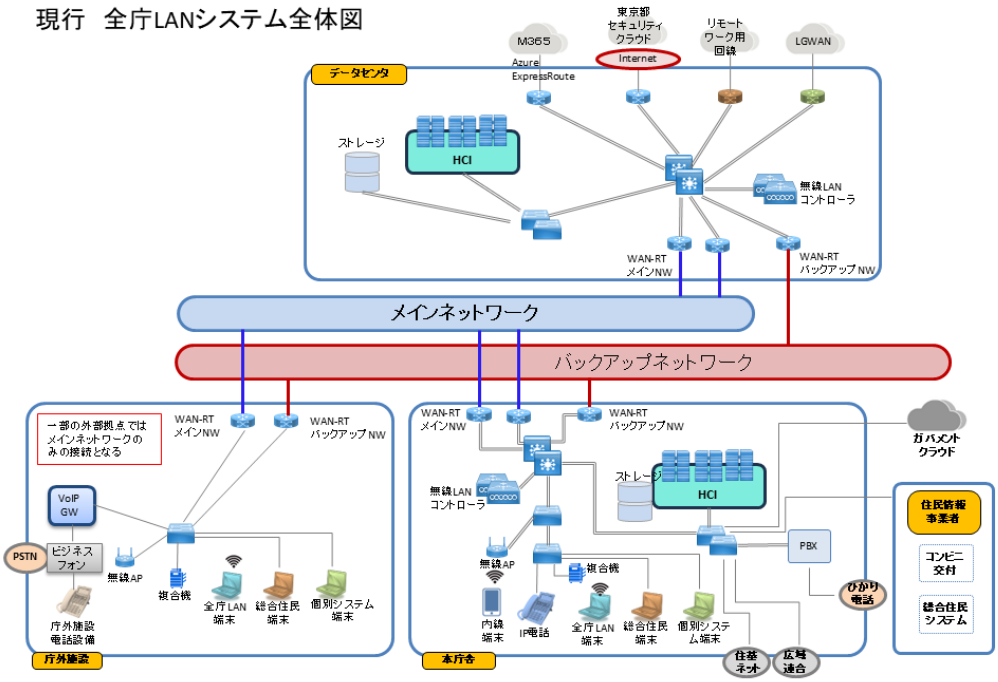
③拠点間通信の安全・効率化、回線の自動最適化・冗長化による業務継続性強化を図る「広域ネットワーク基盤」

2.7 全庁 LAN システム

本業務における全庁 LAN システムとは全庁ネットワーク（個人番号利用事務系ネットワーク・LGWAN 接続系ネットワーク・インターネット接続系ネットワーク・個別ネットワーク）及び全庁ネットワーク上で動作するシステムの総称をいう。

（1） 全庁LANシステム全体図

現行 全庁LANシステム全体図



（2）　利用拠点及び通信回線

現在の利用拠点を以下に示す。

No.	拠点名称	住所
1	千代田区役所	九段南 1-2-1
2	麹町出張所	麹町 2-8
3	富士見出張所	富士見 1-6-7
4	神保町出張所	神田神保町 2-40
5	神田公園出張所	神田司町 2-2
6	万世橋出張所	外神田 1-1-11
7	和泉橋出張所	神田佐久間町 1-11-7
8	千代田保健所	九段北 1-2-14
9	西神田コスモス館 （西神田児童センター、西神田保育園）	西神田 2-6-2
10	麹町保育園	一番町 4
11	神田保育園	神田淡路町 2-109
12	富士見みらい館（富士見小学校、ふじみこども園）	富士見 1-1-3
13	ちよだパークサイドプラザ （和泉小学校、いずみこども園、まちかど図書館）	神田和泉町 1
14	麹町小学校（麹町幼稚園）	麹町 2-8
15	九段小学校（九段幼稚園）	三番町 16
16	番町小学校（番町幼稚園）	六番町 8
17	お茶の水小学校（お茶の水幼稚園）	神田猿楽町 1-1-1
18	麹町中学校	平河町 2-5-1
19	神田一橋中学校	一ツ橋 2-6-14
20	九段中等教育学校（前期課程）	富士見 1-10-14
21	九段中等教育学校（後期課程）	九段北 2-2-1
22	日比谷図書・文化館	日比谷公園 1-4
23	四番町図書館（仮施設）	三番町 14-7
24	昌平童夢館 （昌平小学校、昌平幼稚園、神田児童館、まちかど図書館）	外神田 3-4-7
25	神田さくら館 （千代田小学校、千代田幼稚園、まちかど図書館、児童・家庭支援センター）	神田司町 2-16

26	四番町児童館(四番町保育園)	四番町 5-8
27	一番町児童館	一番町 10
28	千代田土木事務所	一ツ橋 2-1-1
29	千代田土木事務所 神田橋分室	内神田 1-1-3
30	スポーツセンター	内神田 2-1-8
31	九段生涯学習館	九段南 1-5-10
32	ちよだプラットフォームスクウェア (まちみらい千代田、ゆとりちよだ)	神田錦町 3-21
33	千代田清掃事務所	外神田 1-1-6
34	千代田清掃事務所飯田橋車庫	飯田橋 3-13-2
35	千代田清掃事務所三崎町中継所	神田三崎町 3-9-3
36	高齢者あんしんセンター神田	神田淡路町 2-8-1
37	高齢者あんしんセンター麹町	一番町 12
38	高齢者総合サポートセンター(かがやきプラザ)	九段南 1-6-10
39	千代田会館	九段南 1-6-17
40	児童・家庭支援センター、教育研究所	神 田 須 田 町　1-4-4 PMO 神田須田町
41	旧今川中学校	鍛冶町 2-4-2
42	四番町複合施設(新設:令和 9 年 4 月 共用開始)	
43	都内データセンター	―

現在の通信回線の構成を以下に示す(参考)

No	拠点名称	LGWAN 系 インターネット系回線 (帯域保障)	個人番号利用事務系回線	
			主回線 (帯域保障)	副回線 (ベストエフォート)
1	千代田区役所	(1Gb/s)　2回線	(100Mb/s)1 回線	(100Mb/s)1 回線
2	麹町出張所	(100Mb/s)1回線	(10Mb/s)1回線	(100Mb/s)1 回線
3	富士見出張所	(100Mb/s)1回線	(10Mb/s)1回線	(100Mb/s)1 回線

4	神保町出張所	(100Mb/s)1回線	(10Mb/s)1回線	(100Mb/s)1回線
5	神田公園出張所	(100Mb/s)1回線	(10Mb/s)1回線	(100Mb/s)1回線
6	万世橋出張所	(100Mb/s)1回線	(10Mb/s)1回線	(100Mb/s)1回線
7	和泉橋出張所	(100Mb/s)1回線	(10Mb/s)1回線	(100Mb/s)1回線
8	千代田保健所	(100Mb/s)1回線	(10Mb/s)1回線	(100Mb/s)1回線
9	西神田コスモス館(西神田児童センター、西神田保育園)	(100Mb/s)1回線	—	—
10	麹町保育園	(100Mb/s)1回線	—	—
11	神田保育園	(100Mb/s)1回線	—	—
12	富士見みらい館(富士見小学校、ふじみこども園)	(100Mb/s)1回線	—	—
13	ちよだパークサイドプラザ(和泉小学校、いずみこども園、まちかど図書館)	(100Mb/s)1回線	—	—
14	麹町小学校(麹町幼稚園)	(100Mb/s)1回線	—	—
15	九段小学校(九段幼稚園)	(100Mb/s)1回線	—	—
16	番町小学校(番町幼稚園)	(100Mb/s)1回線	—	—
17	お茶の水小学校(お茶の水幼稚園)(仮校舎)	(100Mb/s)1回線	—	—
18	麹町中学校	(10Mb/s) 1回線	—	—
19	神田一橋中学校	(10Mb/s) 1回線	—	—

20	九段中等教育学校(前期課程)	(100Mb/s)1回線	―	―
21	九段中等教育学校(後期課程)	(100Mb/s)1回線	―	―
22	日比谷図書･文化館	(100Mb/s)1回線	―	―
23	四番町図書館(仮施設)	(100Mb/s)1回線	―	―
24	昌平童夢館 (昌平小学校、昌平幼稚園、神田児童館、まちかど図書館)	(100Mb/s)1回線	―	―
25	神田さくら館 (千代田小学校、千代田幼稚園、まちかど図書館、児童･家庭支援センター)	(100Mb/s)1回線	(10Mb/s)1 回線	(100Mb/s)1回線
26	四番町児童館(四番町保育園)	(100Mb/s)1回線	―	―
27	一番町児童館	(100Mb/s)1回線	―	―
28	千代田土木事務所	(10Mb/s) 1回線	―	―
29	千代田土木事務所 神田橋分室	(10Mb/s) 1回線	―	―
30	スポーツセンター	(10Mb/s) 1回線	―	―
31	九段生涯教育館	(10Mb/s) 1回線	―	―
32	ちよだプラットフォームスクウェア (まちみらい千代田、ゆとりちよだ)	(10Mb/s) 1回線	―	―
33	千代田清掃事務所	(100Mb/s)1回線	―	―
34	千代田清掃事務所	(10Mb/s) 1回線	―	―

	飯田橋車庫			
35	千代田清掃事務所 三崎町中継所	(10Mb/s) 1回線	—	—
36	高齢者あんしんセンター神田	(10Mb/s) 1回線	(10Mb/s)1 回線	(100Mb/s)1回線
37	高齢者あんしんセンター麹町	(10Mb/s) 1回線	(10Mb/s)1 回線	(100Mb/s)1回線
38	高齢者総合サポートセンター (かがやきプラザ)	(100Mb/s)1 回線	(10Mb/s)1 回線	(100Mb/s)1回線
39	千代田会館(8階 商工観光課、生活衛生課)	(100Mb/s)1回線	—	—
40	児童家庭支援センター(教育研究所)	(100Mb/s)1回線	—	—
41	旧今川中学校	(100Mb/s)1回線	—	—
42	千代田会館(10階 研修室)	(10Mb/s) 1回線	—	—
43	四番町複合施設 (新設:令和 9 年 4 月 共用開始)		—	—
44	都内データセンター	(1Gb/s) 2回線	—	—

3. 現行システムの概要

3.1 履行場所、契約期間

【履行場所】千代田区役所本庁舎 (千代田区九段南1丁目2番1号)

※上記場所を原則とし、その他の履行場所については、別途指定する。

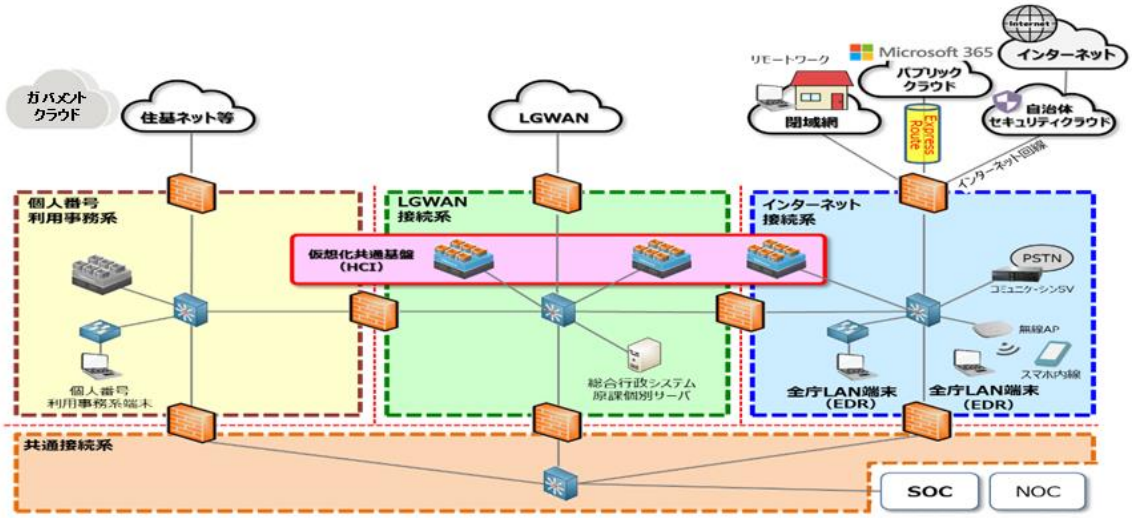
【履行期間】契約締結日の翌日から令和10年2月29 日迄とする。

3.2 現行の全庁ネットワーク

現在の千代田区全庁ネットワークは、「三層の対策」における強靭化のβ´モデルで運用している。本庁舎及び外部拠点を結ぶネットワークで、総務省三層分離に準拠し3つのネットワークにて構成されている。

・業務端末（全庁 LAN 端末）はインターネット系ネットワークに配置されている。
・インターネット接続は、共通接続系に配置されたインターネット接続環境及び東京都セキュリティクラウドを通じて行っている。
・LGWAN へは、共通接続系に配置された LGWAN 接続環境（仮想基盤端末）を通じて行っている。一部の個別システムはLGWAN接続系に配置されており、端末から直接LGWANへアクセスを行っている。
・インターネットからダウンロードされたファイルは、LGWAN 接続系へファイル転送システムにより無害化されて手動にて転送される。
・個人番号利用事務系は、個人番号利用事務系に接続された業務システム及び専用端末により行っている。

現行の全庁ネットワークの構成イメージ



LGWAN 網への接続

地方公共団体情報システム機構が運営する総合行政ネットワーク（Local Government Wide Area Network）（以下「LGWAN」という）とのネットワーク接続

個人番号利用事務系ネットワーク

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータを取扱うネットワーク

（ア）住民基本ネットワークへの接続

（イ）自治体中間サーバネットワークの接続

（ウ）eLTAX・ぴったりサービスシステムへの接続

（エ）ガバメントクラウドへの接続

LGWAN 系ネットワーク

LGWAN に接続された情報システム及びその情報システムで取り扱うデータを取扱うネットワーク(個人番号利用事務系を除く。)

インターネット系ネットワーク

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータを取扱うネットワーク

共通接続系ネットワーク

共通接続系とは、全庁 LAN において運用・保守機能を集約し、他の接続系(インターネット接続系、LGWAN 接続系、個人番号利用事務系)と論理分離された専用ネットワーク。

全庁 LAN における運用・保守・認証・ID 管理など共通機能を集約する専用ネットワークセグメントであり、セキュリティ確保と運用効率化(保守ネットワーク統合、認証・監視の集中管理)することを目的としている。

図書館システムへのネットワーク機能提供

全庁ネットワーク上で論理分離にてネットワーク機能を提供

会館施設予約システムへのネットワーク機能提供

全庁ネットワーク上で論理分離にてネットワーク機能を提供

個別システムへのネットワーク機能提供

個人番号利用事務系ネットワーク、LGWAN 系ネットワーク、インターネット系ネットワークの各ネットワークに存在する個別システムへのネットワーク機能の提供

3.3 現行の仮想化共通基盤

本区ではネットワークを『インターネット接続系セグメント』、『LGWAN 接続系セグメント』、『個人番号利用事務系セグメント』の3つのネットワークにて分けて構成している。
このうちインターネット接続系セグメント、LGWAN 接続系セグメント及び個人番号利用事務系セグメントにて、仮想化共通基盤(IaaS)を運用している。

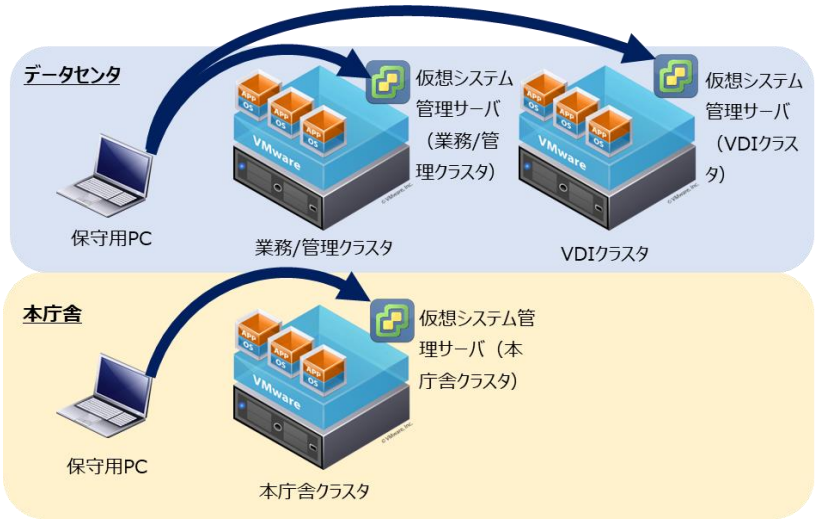
提供している仮想化共通基盤を以下に示す。

1. インターネット接続系(サーバ)
2. インターネット接続系(仮想デスクトップ)
3. LGWAN 接続系(サーバ)
4. 個人番号利用事務系(サーバ)

仮想化共通基盤は、安定したサーバの稼働および集約化を実現するとともに、全てのシステムに対して高可用性・高信頼性を提供し、拡張性・ライセンス適用範囲を制限しコストを考慮したシステム環境を提供することを目的としている。ネットワーク構成については、仮想サーバ間のアクセス経路を L3 や VLAN、ファイアウォールを用いて、論理的にネットワークを分離し制御を行っている。

本システムでは、仮想システム管理サーバ（vCenter Server）を用いて、仮想化基盤ホスト（VMware ESXi）の仮想サーバ、仮想デスクトップを集中・統合管理している。
vCenter を利用することにより仮想サーバの可用性向上させるための vSphere HA 機能、仮想サーバをオンラインのまま別の仮想化基盤ホストへ移動させる vMotion 機能、仮想化基盤ホストの負荷分散及び特定の仮想サーバを特定の仮想化基盤ホストで起動する vSphere DRS 機能を利用することができる。

仮想システム管理の概要



3.4 第二期都区市町村情報セキュリティクラウドサービス（東京都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は、令和 2 年 8 月に総務省が示した「次期自治体情報セキュリティクラウドの標準要件について」を受け、総務省要件を満たす自治体情報セキュリティクラウドサービスを開発し、利用団体へ提供している。
本区では以下のサービスを利用している。

No	機能	サービス名
1	必須機能	Web 閲覧サービス
2	選択型必須機能サービス	メールリレーサービス
3	選択型必須機能サービス	Web 公開サービス
4	オプション機能	外部 DNS サービス
5	オプション機能	振る舞い検知サービス

6	オプション機能	ファイル交換システムサービス

3.5 ID 統合管理システム

①Microsoft Windows Server の Active Directory ドメインを利用し、ユーザ認証及びリソース管理を行うオンプレミス認証基盤を運用している。オンプレミス認証基盤では、グループポリシーを庁内端末に適用することにより、セキュリティ対策等を行っている。

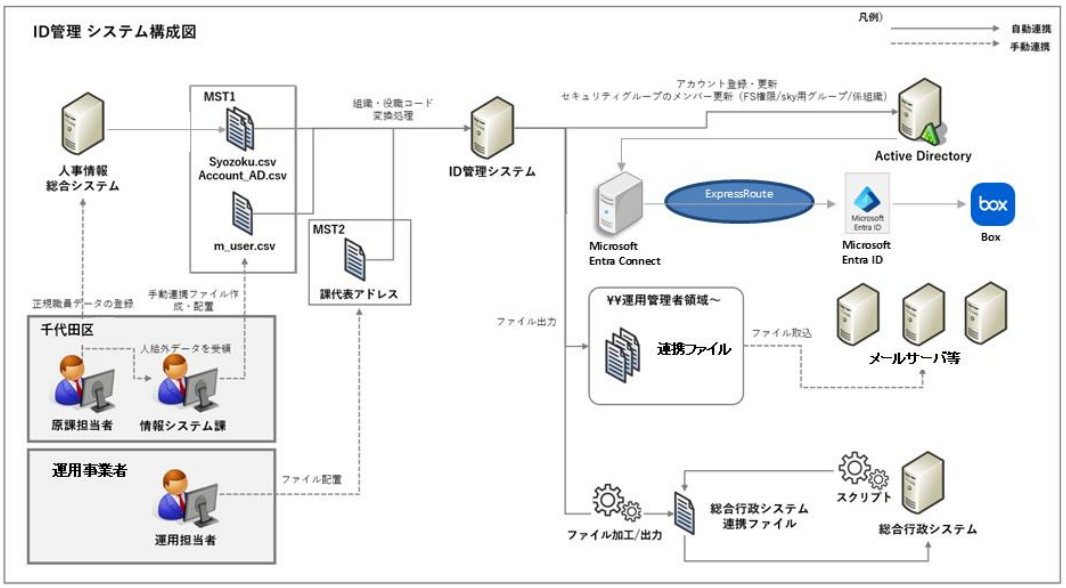
②人事情報総合システムから出力される人事情報ファイルを ID 管理システム(ADMS)にて取り込み、Active Directory に対して AD アカウント等のオブジェクト情報を連携する。また、ファイル交換サービス、メールサーバ、総合行政システム(財務会計、文書管理・電子決裁システム)に対して、各システムが取り込める連携用ファイルを所定のフォルダに出力する。

③Microsoft Entra Connect を利用し、ExpressRoute を経由して Microsoft Entra ID(Ms365)に認証情報を連携している。Microsoft Entra ID(Ms365)は外部テナントからの接続を制限している。

④令和 8 年 4 月から全庁ファイルシステムとして「Box」の利用を開始する。

Box へはシングルサインオン(以下 SSO)にて接続している。

ID 統合管理システムの概要



3.6 インターネット接続環境

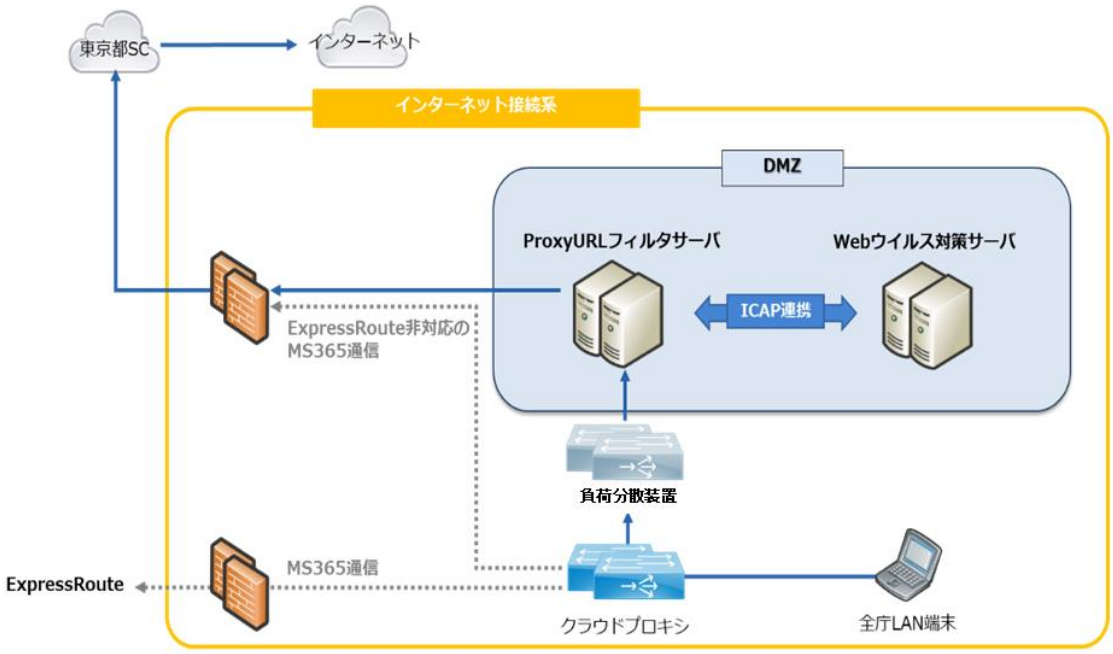
インターネット接続は、ProxyURL フィルタサーバ、Web ウイルス対策サーバで構成する。

ProxyURL フィルタサーバ、Web ウイルス対策サーバは不特定多数から通信があり、サーバ内部にウイルスが侵入する可能性があるため、DMZ に配置している。

インターネットへの接続は東京都セキュリティクラウドの上位プロキシサーバ経由で接続する。

ProxyURL フィルタサーバでは、Web 閲覧のためのプロキシ機能や URL フィルタ機能、HTTPS(SSL)通信復号機能、HTTPS(SSL)通信の復号データを Web ウイルス対策サーバへ送信する機能を提供する。Web ウイルス対策サーバでは、Web 閲覧時のウイルス対策機能を提供している。

インターネット接続環境の概要



3.7 LGWAN 接続環境

LGWAN 接続は ProxyURL フィルタサーバ、Web ウイルス対策サーバで構成する。

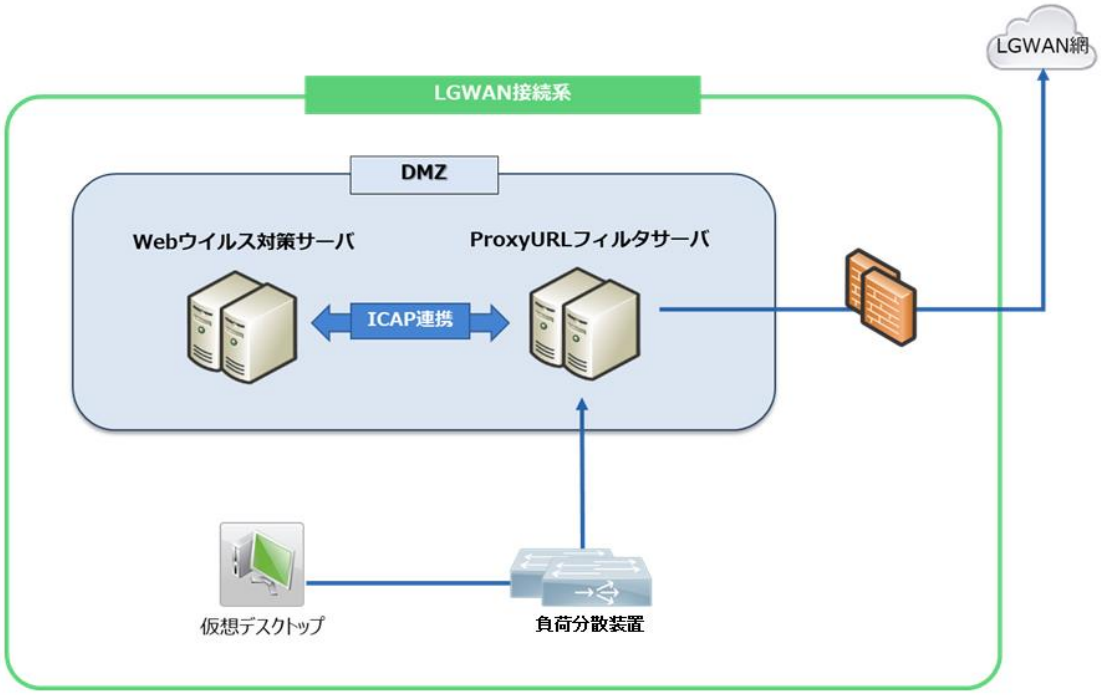
ProxyURL フィルタサーバ、Web ウイルス対策サーバは不特定多数から通信があり、ウイルスが侵入する可能性があるため、DMZ に配置している。

ProxyURL フィルタサーバでは、Web 閲覧のためのプロキシ機能や HTTPS(SSL)通信復号機能、HTTPS(SSL)通信の復号データを Web ウイルス対策サーバへ送信する機能、HTTPS(SSL)通信の復号データをネットワーク系路上で HTTP 通信として転送/再生する機能を提供する。

Web ウイルス対策サーバでは、Web 閲覧時のウイルス対策機能を提供する。また、LGWAN ASP サービスを利用し、ウイルスパターンファイルを取得する。

LGWAN 接続ルータはデータセンターに配置しており、令和9年10月に更改予定である。

インターネット接続環境の概要

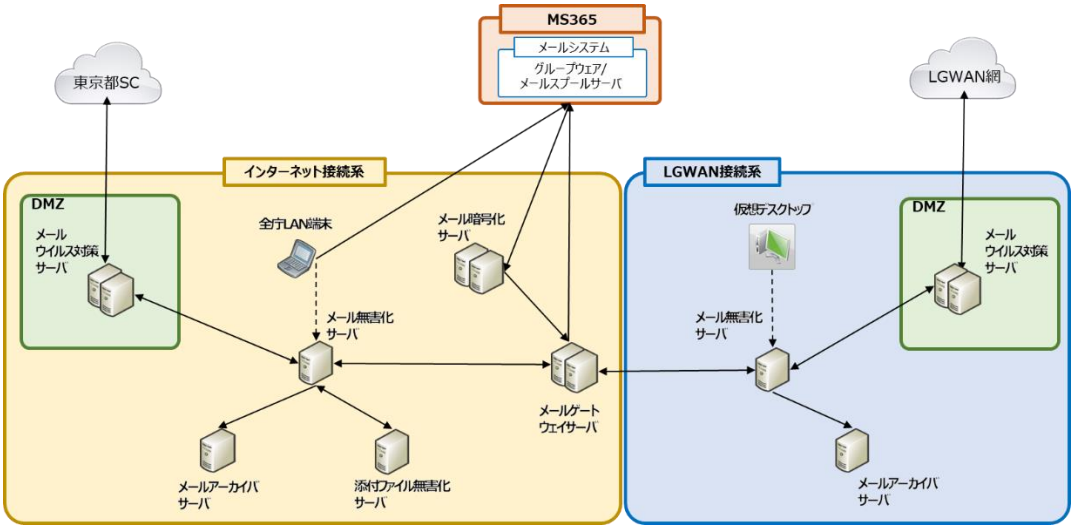


3.8 メールシステム

システムではインターネットとのメール送受信及び LGWAN 内部に閉じたメール送受信を実施している。メールスプールサーバには Microsoft365 のクラウドサービスである Exchange Online を採用し、全庁 LAN 端末上の Outlook をメールクライアントとして、メールの送受信を行う仕組みを提供している。

送受信するメールに対して、ウイルス対策や無害化処理などを行い、インターネット及び LGWAN と送受信するメールに対して安全性を高めている。また、インターネットへの送信時には、誤送信防止の自己チェック、添付ファイル付きメールの上長承認、添付ファイル暗号化の処理を行い、メール送信による情報漏洩対策を実施している。

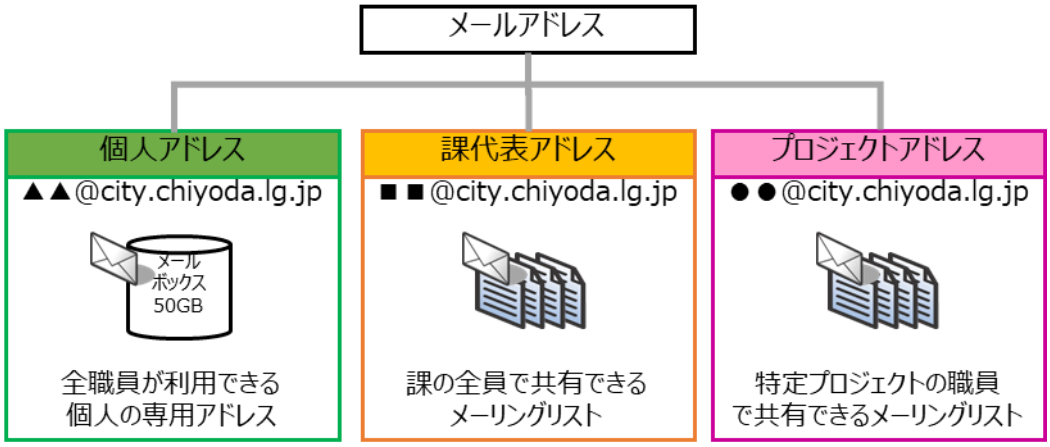
メールシステム概要



構成装置	セグメント	提供機能
グループウェア/ メールスプールサーバ Exchange Online	インターネット接続系	・メールスプール ・会議室予約 ・予定表
メール無害化サーバ	インターネット接続系 LGWAN 接続系	・メールの無害化 ・原本メールのスプール、及び原本メールの閲覧（送受信機能なし） ・メールウィルス対策
添付ファイル無害化サーバ	インターネット接続系	・インターネットから受信したメールの添付ファイルを無害化する
メールアーカイバサーバ	インターネット接続系 LGWAN 接続系	・送受信されたメールをすべてバックアップ保管
メールウィルス対策サーバ	インターネット接続系 LGWAN 接続系	・メールウィルス対策
メール暗号化サーバ	インターネット接続系	・インターネットへの送信メールアドレス制限 ・インターネットに送信する添付ファイルの暗号化 ・添付ファイル付きメールの上長承認、誤送信防止
メールゲートウェイサーバ	インターネット接続系	インターネット及び LGWAN メールの振り分け

3.9 メールアドレスの種類

本区のメールシステムで使用するメールドメインは「city.chiyoda.lg.jp」を利用している。
メールアドレスは 個人アドレスを基本とし、必要に応じて課代表アドレスやプロジェクトアドレスを送信者として選択できるようにし、区民や事業者とのメール送受信を可能としている。
課代表アドレスおよびプロジェクトアドレスは、メールボックスを持たないメーリングリスト形式で運用している。



※個人アドレスメールボックスは運用にて 10GB に制限している

種別	説明
個人アドレス	・区民、事業者等外部、他自治体とのメール送受信に使用する。
課代表アドレス	・課全員で共有するためのメーリングリストとして使用する。（送信者として選択可能）
プロジェクトアドレス	・特定プロジェクトの職員にて共有するためのメーリングリストとして使用する。（送信者として選択可能）

3.10　仮想デスクトップ

全庁 LAN 端末から LGWAN 網へ接続するには、LGWAN 接続系仮想デスクトップ環境を利用する。仮想デスクトップの展開方式としてインスタントクローン方式を採用している。
デスクトップ環境を一括集中管理することにより、標準化/高セキュリティなデスクトップ環境、効率的な運用管理、運用コスト削減を実現している。
全庁 LAN 端末にインストールされた仮想デスクトップアプリケーションにて接続を行う。
※仮想デスクトップ機能は全庁 LAN 端末の LGWAN 網への接続にのみ提供される機能であり、他の個別システムや個人番号利用事務系への提供は行っていない。

仮想デスクトップ接続フロー

① ユーザが仮想デスクトップにログオンを実施

② 負荷分散装置経由で Connection サーバに接続

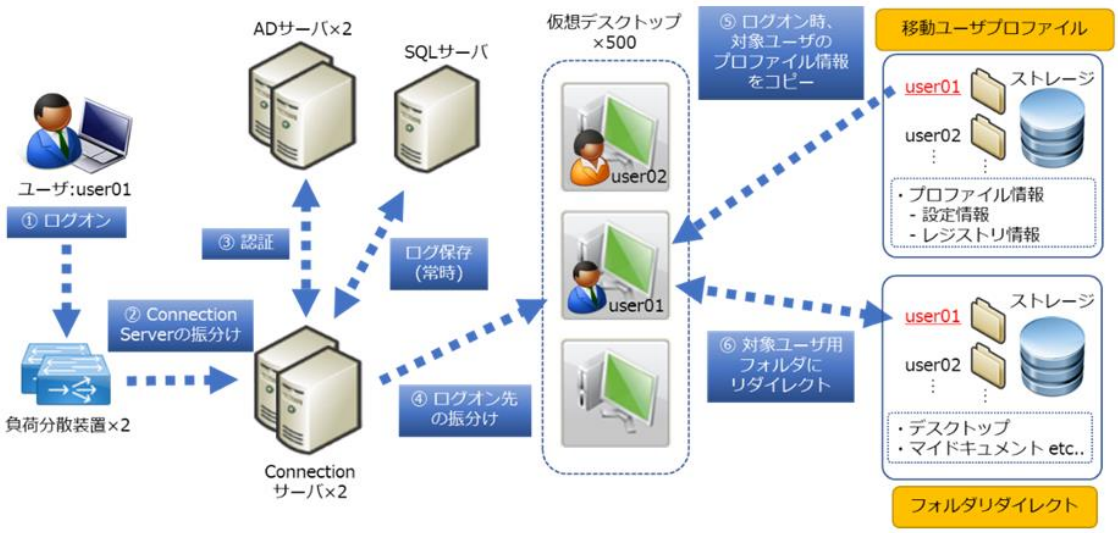
③ AD サーバと連携してユーザ認証を実施

④（AD 認証成功後）ユーザを適切な仮想デスクトップに接続/ログオン

⑤ ログオン時、対象ユーザのプロファイル情報をストレージより読込みを行い、ユーザ個別のデスクトップ環境を用意

⑥ 特定のユーザフォルダ（デスクトップ/マイドキュメントなど）はフォルダリダイレクトを行い、ストレージ上に保存

仮想デスクトップ接続フローの概要



3.11　グループウェアシステム

職員の生産性向上と協働の強化を目的としてメール・予定・会議・ドキュメント共有・業務アプリを一体で提供し、庁内標準のコラボレーション基盤としてMs365 を利用している。

①Exchange Online（メール／予定／連絡先）

全庁 LAN 端末の Outlook をクライアントとし、個人アドレス・課代表アドレス・プロジェクトアドレスを運用（代表／プロジェクトは ML 形式、送信者の切替が可能）。

Outlook予定表（会議室予約含む）と連携し、会議招集・出欠管理・リソース予約を一元化。

②Microsoft Teams（コラボレーションのハブ）

チャット／チャンネル／オンライン会議／音声通話を統合。

ファイル共有・共同編集(後述の SharePoint／OneDrive と連携)。
内線通話・会議録画・文字起こしなど、各種拡張機能を提供。

③SharePoint Online(文書管理・情報共有)
部局・課・プロジェクト単位のサイトで文書ライブラリ／ポータルを提供。権限管理・版管理・通知。
OneDrive for Business:個人用ストレージ。共有リンクを用いた共同編集、PC と自動同期。

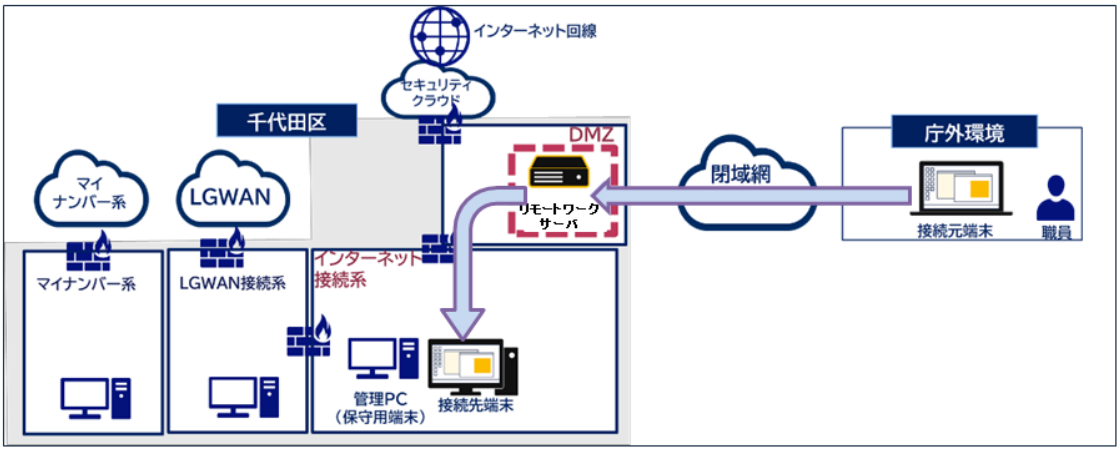
④タスク・業務可視化
Planner(グループタスク)／To Do(個人タスク):案件・作業の進捗を共有。Teams から直接利用可能。

⑤申請・アンケート・自動化
Forms:アンケート／申請フォームの作成・集計。
Power Automate:承認フローや通知、ファイル処理などの業務自動化。メール承認・回覧との連携で日常業務を効率化。
Power Apps:ローコードで庁内業務アプリを構築(例:備品貸出、来庁者受付)

3.12 リモートワークシステム

本システムは、閉域回線を利用し、リモート端末から庁舎内 PC(全庁 LAN 端末)へ安全に接続する「画面転送方式」のリモートデスクトップ基盤を構築している。端末認証・ユーザ認証を実施し、画面および音声の転送(Teams 会議)のみを許可することで、データの持ち出しを防止している。
さらに、リモートワーク専用端末には SIM を搭載し、モバイル回線経由で閉域網へ接続可能とすることで、在宅や外出先でも安全な業務環境を提供している。

リモートワークシステムの概要



3.13　業務端末

情報システム課で配布している業務端末(全庁 LAN 端末:1900 台)、災害用端末:70 台 、リモートワーク用端末:200 台、さらに各課で購入・管理している業務端末(個別システム端末:390 台)が導入されている。

なお、VDI の同時接続数は 500 台としている。

・千代田区全庁ネットワークに接続されており、VRF、VLAN 等技術を用いて適切に論理分離されている。

・全庁 LAN 端末においては、庁内の認証基盤(オンプレミス版 AD)により、ログイン認証を行い、ID 統合管理システムを経由して Ms365 とも連携を行っている。

・インターネットへは、インターネット接続環境を通じてアクセスしている。

・全庁 LAN 端末は、Microsoft 365 Apps for enterprise がインストールされている。

・全ての端末に EPP としてトレンドマイクロ社 Apex One がインストールされている。

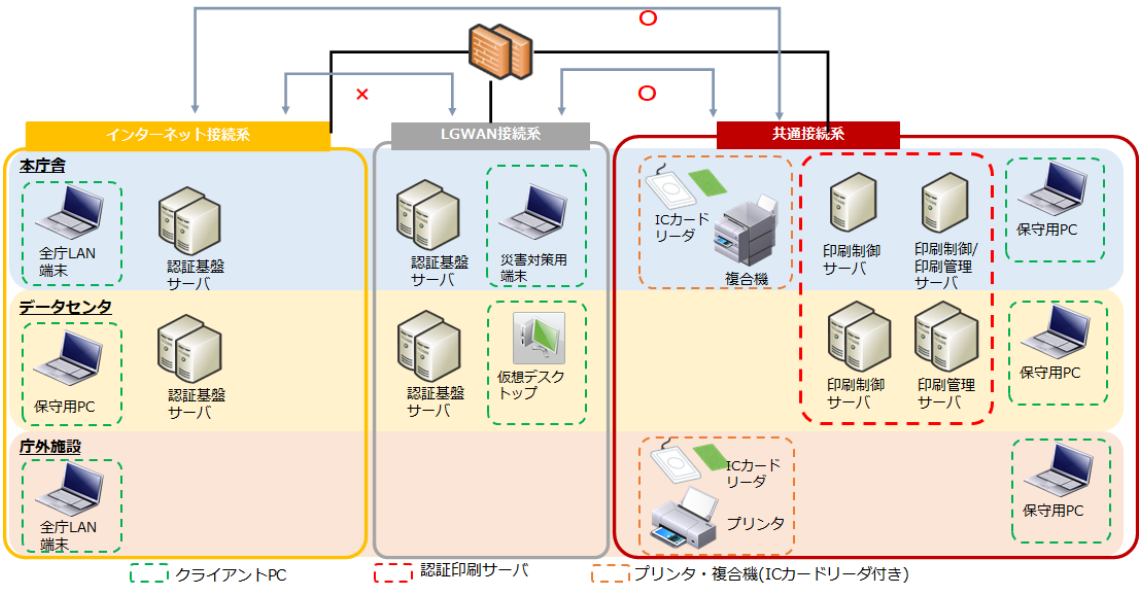
・全庁 LAN 端末には EDR としてサイバーリーズン合同会社の cybereason がインストールされている。

3.14　認証印刷

認証印刷システムは、IC カードで正規のユーザであることを確認した場合のみ、印刷、コピー、ファクス、スキャンを可能とすることで、印刷時の秘密情報の覗き見や情報漏えいを防止するシステムである。本システムは、全庁 LAN 端末からのみ利用可能となる。

認証印刷システムは共通接続系セグメントに配置している。

認証印刷システムの全体構成イメージ



認証印刷の利用者向け機能一覧

機能名		サービス概要
認証印刷		クライアント PC へのマルチプリンタドライバの導入により、IC カードで正規のユーザであることを確認した場合のみ、プリンタ・複合機で印刷できる。 併せて、下記の機能を提供する。 ・印刷設定の一元管理 ・印刷ジョブのキャンセル ・放置された印刷ジョブの自動キャンセル
	全庁共通プリント	プリンタ・複合機を指定せず、IC カードで認証した任意のプリンタ・複合機で印刷できる。
	ベンダ純正ドライバ固有の詳細な印刷設定利用時の対処用	
	特定プリント	印刷範囲の拡張、複数の手差しトレイの選択など「全庁共通プリント」のマルチプリンタ対応ドライバで対応できない書類を印刷する場合に備え、メーカ純正ドライバを使用した認証印刷ができるようにしておく。 ※利用する場合は、PC にメーカ純正ドライバの導入が必要
認証コピー・ファクス・スキャン		IC カードで正規のユーザであることを確認した場合のみ、コピー・ファクス・スキャンが利用できるようにする。
課金ログの集計		印刷・コピー・ファクス・スキャンの使用ログをセグメント毎に集計する機能を具備する。

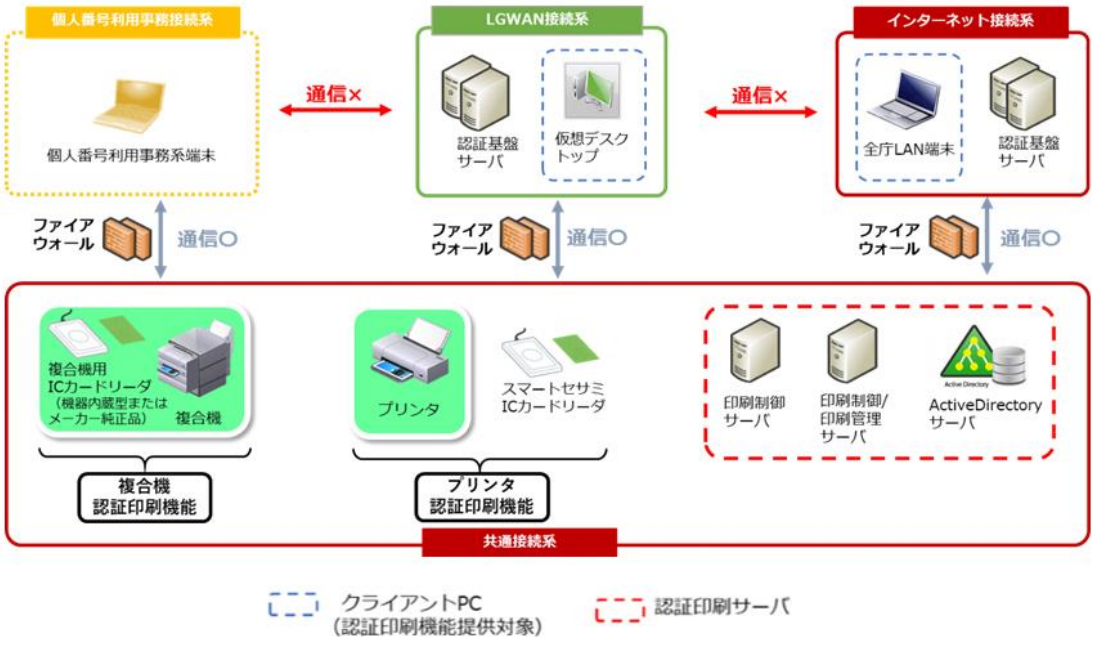
認証印刷システム製品名および製品のバージョン

製品	製品バージョン情報等
㈱シーイーシー SmartSESAME SecurePrint!Suite	SecurePrint!Suite Ver4.0.6.0 SecurePrint!Suite 複合機連携 Ver4.0.6.0 Ms eye 統合ログ Ver4.0.5.0
認証カード	認証カードについては Felica カード（配布済の職員証または印刷カード）を利用している。 る。

3.15　デジタル複合機・プリンタ機器

全庁ネットワークに接続する共通接続系（LGWAN接続系・インターネット系）パソコンにおける印刷・スキャン、また業務全般のコピーおよびFAX等の利用を目的とした、IC カードリーダー内蔵デジタル複合機およびプリンタを設置している。（個人番号利用事務系パソコンからの印刷については対象外）

デジタル複合機・プリンタ機器の概要



印刷機器種類と設置台数

機器		本庁	庁外	予備機	総計
デジタル複合機	Apeos C2570	2	28		30
	Apeos C3570		9		9
	Apeos C5570（2トレイモデル）		1		1
	Apeos C5570	23	10		33
	Apeos C7070	4			4
モノクロプリンタ	ApeosPrint 3360S(A3)	4	1	9	14
	ApeosPrint 4830(A4)	1	17		18
合計		34	66	9	109

3.16　現行の複合機スキャン機能

現行の複合機スキャン機能は、庁内ネットワーク環境において紙文書を電子化し、指定された宛先に送信する仕組みを提供している。スキャンしたデータは、利用者が後続処理を行うために取得可能な状態で保持される。

現行方式には以下の 2 種類がある。

CyberMail 経由方式

複合機でスキャンしたデータを LGWAN 接続系の CyberMail に送信し、職員総合ポータル経由でダウンロードする方式。

・認証は IC カード認証と CyberMail 認証を組み合わせて実施

・通信経路は LGWAN 接続系内で完結し、セキュリティを確保

親展ボックス（インターネット経由）方式

複合機内の親展ボックスにスキャンデータを保存し、インターネット接続系のブラウザからアクセスして取得する方式。

・利用者は各課のフォルダアクセス時に暗証番号を入力して認証を行う

・通信はインターネット接続系内で完結し、セキュリティを担保

新方式として以下の方式を令和8年4月より運用を開始する。

Box へのスキャン方式

本方式は、複合機からクラウドストレージサービス「Box」へスキャンデータを直接送信する仕組みを提供する。従来の CyberMail 経由や親展ボックス方式と比較して、操作性と利便性を大幅に向上させるとともに、ゼロトラスト環境に準拠したセキュリティを確保する。

・複合機の操作パネルで「スキャン」機能を選択、送信先として「Box」を選択。

・Entra ID による SSO 認証を実施

（初回ログイン時のみ ID・パスワード入力、以降はキャッシュ利用）。

・スキャンデータの格納先フォルダを指定

・スキャン実行後、データは Box 上に保存される

複合機スキャンデータの格納・アクセス方式			
項目	現行方式① CyberMail経由(LGWAN系)	現行方式② 複合機親展ボックス(インターネット系)	新方式(Box移行後) (令和8年度4月より)
格納先	LGWAN接続系 CyberMailde受信トレイ	複合機内の親展ボックス	クラウドストレージ Box
アクセス方法	LGWAN系へVDI接続 → CyberMail (LGWAN) で受信→ダウンロード	インターネット系からブラウザアクセス → 暗証番号入力 → ダウンロード	複合機操作パネルでBox選択 → フォルダ指定→Boxからアクセス
認証方式	ICカード認証(複合機)	ICカード認証＋暗証番号	ICカード認証＋手動にてID/PASS入力
通信経路	庁内ネットワークLGWAN内のみ	庁内ネットワークインターネット系のみ	庁内ネットワーク→ FWポリシー → Box(インターネット)
セキュリティ対策	庁内ネットワーク閉域＋ CyberMail認証	庁内ネットワーク閉塞＋ 進展ボックス暗証番号	https(暗号化)＋BoxへのSSO ＋通信経路制限(MAC/IP/Port)
操作性	煩雑(複数ステップ)	煩雑(暗証番号入力必須)	シンプル(複合機から直接Boxへ) 複合機からBoxへ経由するクラウドサービスがSSOに対応していない部分が課題
導入時期	現在運用中	現在運用中	令和8年4月予定

3.17　コールセンター用システム

PC 中継台／中継台支援システムは、PC 端末と電話帳データや交換機からの呼情報を格納する中継台統計サーバで構成して、機能提供を実現する。

PC 中継台は代表着信及びコールセンター受付業務で利用する PC 端末であり、複数番号の着信に対して応答が可能であり、応答した通話の要件に応じて庁内の各部署へ通話の転送等の中継台機能を提供する。必要となる主な機能を以下に記載する。

1:交換機と連携及び、ヘッドセットによる対応を可能とさせる機能

2:電話帳機能を具備し、内線情報を検索して、転送操作ができること機能

3:転送の際に転送先が話中状態なのか確認出来る機能

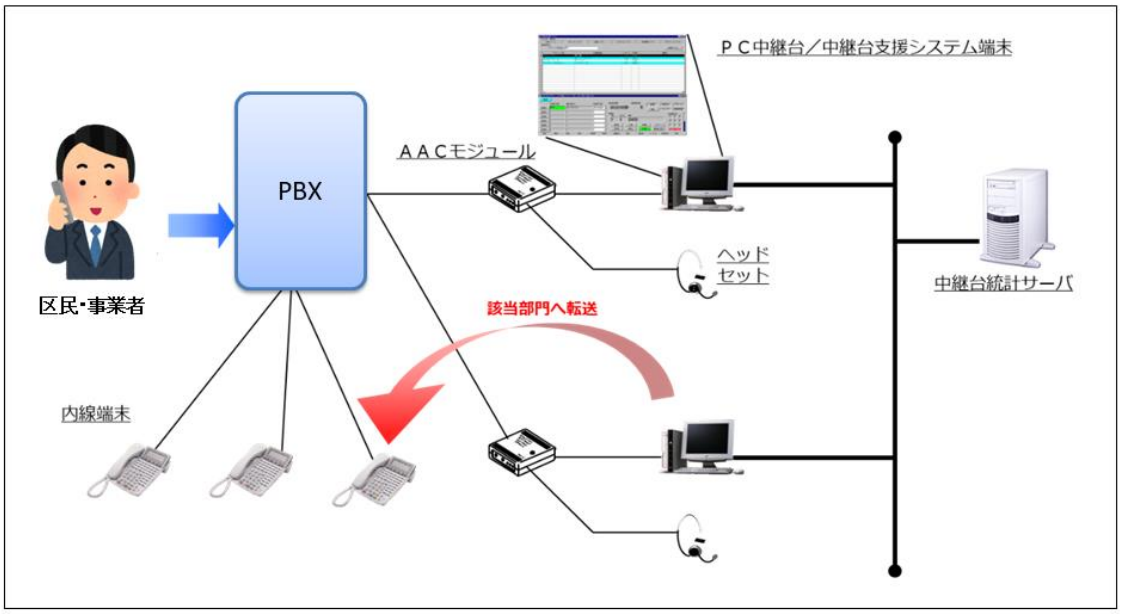
4:取扱件数や操作履歴・通話時間記録を Excel ファイルで出力できる機能

5: FAQ システム(コールセンターへの質問内容を蓄積し外部公開)機能

6:コールセンターの応対履歴システム機能

※上記1～4の機能はオンプレミス環境で構築、5, 6の機能はクラウドサービスを利用

コールセンター用システムの概要



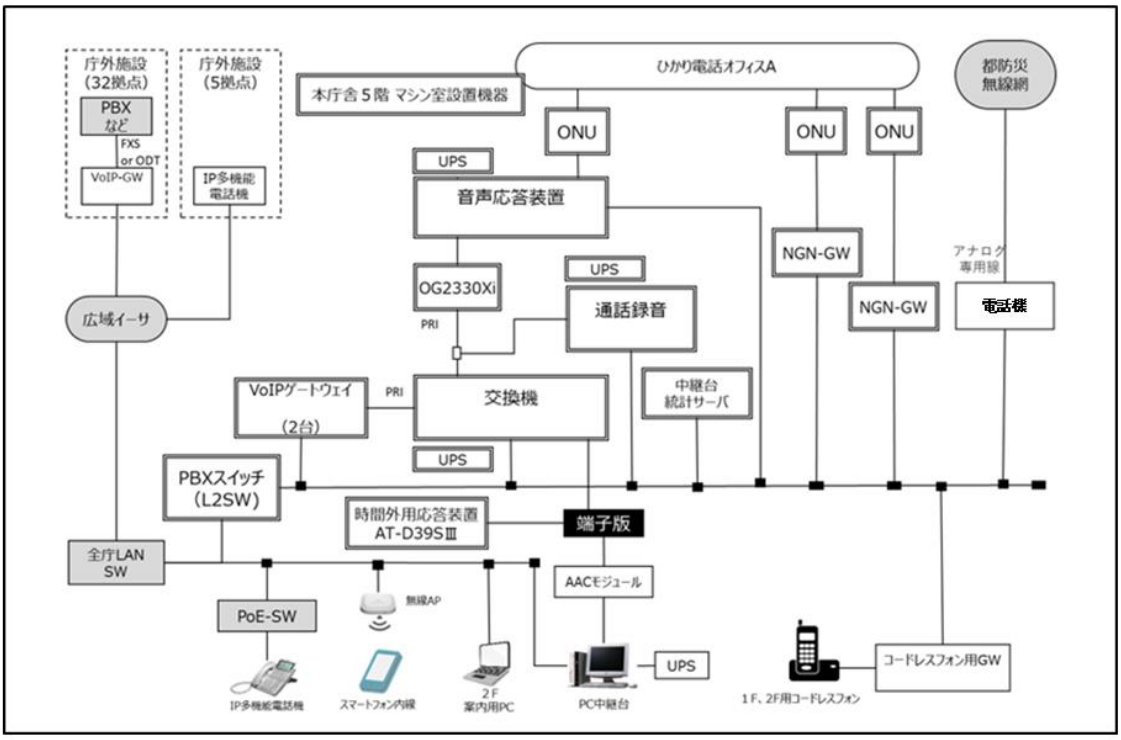
取扱件数や操作履歴・通話時間記録を Excel ファイルで出力できる統計レポートの種類

統計レポート種類	内容
オペレータごと統計レポート	①　日別レポート、②月別レポート オペレータごとの中継台応答処理を①日ごと、②月ごと、時間単位で集計する
全オペレータレポート	全オペレータの受付処理を月ごと、オペレータ単位で集計する
全中継台統計レポート	①　日別レポート、②月別レポート 全 PC 中継台の受付状況を①日ごと、②月ごと、時間単位で集計する
中継履歴レポート	オペレータごとの中継台処理履歴の概要を出力する
時間別取扱件数レポート	１ヶ月の時間帯別の中継処理件数を時間帯別に出力する

3.18　音声系システム

本システムは、本庁舎で利用する IP 電話およびコールセンターで利用する中継台機能を提供している。現行では、有線 LAN 接続による IP 電話の提供に加え、無線 LAN 接続によるスマートフォンでの内線機能も実現している。また、庁外施設との施設ごとの PBX との内線通話接続に加え、都防災無線など外部拠点との接続も提供している。

音声系システムの概要



構内交換機に収容すべき回線数／端末数の概要

No	種別	内容	数量	備考
1	回線	ひかり電話オフィス A（ダイヤルイン用）	46ch/2 契約	直収
2	回線	ひかり電話オフィス A（代表着信、CC 用）	23ch/1 契約	PRI 収容
3	回線	庁外施設接続 GW	2台	PRI 収容（23ch × 2 台）
4	回線	都防災用 GW	1 台	CCIS専用線接続:12ch
5	端末	IP 多機能電話機	350 台	24 ボタン
6	端末	スマートフォン端末	900台	android OS
7	端末	PC 中継台・ヘッドセット	5台	

3.19 Box(クラウドサービス)

本区では令和 8 年 4 月より Box を全庁ファイルサーバ機能として利用を開始する予定である。「Box」はクラウド上で提供される SaaS 型ファイル共有サービスであり、本サービスの導入により、職員の業務効率化とセキュリティ強化を両立し、千代田区内外におけるコンテンツ共有の活性化を実現する

運用用効率化の取り組み

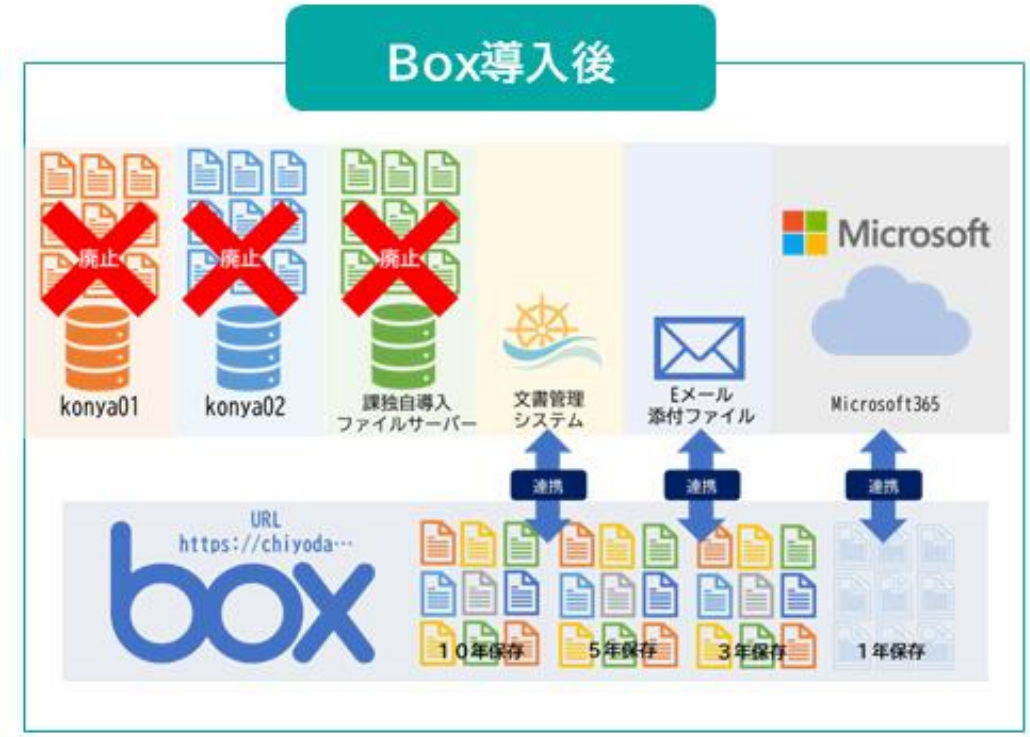
運用の効率化を目的として、以下のシステムと Box の連携を実施している。

・Entra ID

クラウドベースの ID およびアクセス管理サービス、Entra ID の自動プロビジョニング機能を活用し、ユーザ・グループ情報を Box 側と同期する。これにより、アカウントの作成・更新・削除を自動化する。

・Forest Magic Operation Tool

Box の運用自動化ツールであり、Entra ID 側のアカウント情報を基に、個人フォルダの自動作成を行う。



4. プロジェクト推進

4.1 プロジェクト管理

・プロジェクト全体管理

プロジェクト管理業務の遂行に当たり、PMBOK(Project Management Body Of Knowledge)等のプロジェクト管理体系に準拠したプロジェクト管理を実施することを推奨する。

・プロジェクト計画書の作成

契約締結後、速やかに本区と協議し、プロジェクトキックオフを実施すること。その際には、本書記載事項に基づき具体的な体制、スケジュール、プロジェクト管理方針、品質管理方針、課題管理方針、進捗管理方針等を含んだプロジェクト計画書を作成すること。
記載内容は、本区及び受託者で協議・決定の上、本区の承認を受けること。

・進捗管理

進捗管理については、プロジェクト計画書に基づき、各タスクの状況把握及びスケジュール管理を行うこと。進捗管理は定量的に分析し、定期的に報告すること。
WBS にて各工程の詳細を明示し、スケジュール化すること。
計画に遅れが生じた場合は、遅れの原因を調査分析し、速やかに改善策を提示すること。また改善策については本区の承認を得ること。

・課題管理

業務の遂行上、発生した課題について、定められた課題管理ルールに従い管理すること。
課題管理にあたっては、発生日、課題内容、対応方針、対応者、対応期限、重要度、進捗状況等が分かるように管理台帳を用いて管理すること。
課題管理の状況については、定期的に報告すること。

・リスク管理

各工程におけるリスクを最小限にすることを目的とし、リスクを管理すること。
業務の遂行に影響を与えるリスクを識別し、発生確率や影響等を整理すること。また、リスクの優先度を決定し、「回避」「転嫁」「軽減」「受容」の戦略で対応策を講じること。
リスクについては定期的に監視・評価を行うこと。
特定したリスクについて、分析結果・対応策を定期的に報告すること。

・セキュリティ管理

セキュリティに関する事故及び障害等の発生を未然に防ぐことを目的とし、以下のとおりセキュリティの管理を行うこと。
本区が提示する「千代田区情報セキュリティポリシー対策基準」の内容を理解し、遵守すること。
セキュリティ対策の内容については、本区の承認を得ること。また、対策については状況に応じて適宜改善策を検討すること。
セキュリティに関する事故及び障害が発生した場合は、速やかに本区担当職員に報告し、対応策について協議すること進捗管理は定量的に分析し、定期的に報告すること。

・品質管理

本システムが本要求水準書及び共通仕様書で定義された品質・性能を満たすことを保証することを目的とするため、以下のとおり品質基準を定義し管理を行うこと。

品質管理計画書を定め、本区の承認を得ること。品質の評価指標、品質目標を定めること。

品質管理の責任者を定めること。

品質管理計画書に基づき、検証及び品質改善策の検討、実施を管理する体制を構築すること、また品質状況については定期的に報告すること。

4.2 要件定義

本業務において提案内容と現状との Fit&Gap 分析により差異を確認するため、要件定義工程を計画すること。

本システムで実装する機能について整理し、要件として定義すること。

性能や信頼性、セキュリティ、運用・保守等の非機能要件を整理し、定義すること。

本システム導入における制約条件について明らかにし、定義すること。

4.3 基本設計・詳細設計

基本設計並びに詳細設計工程では、提出する設計書や各種資料類などは本区と事前に協議すること。

・基本設計

基本設計工程では、要件定義での課題点が解決できるよう進め、基本設計書を作成すること。

・詳細設計

本区より基本設計書の承認を得た後、受託者は本システムの構築が可能となるように詳細化し、詳細設計書を作成すること。

4.4 テスト設計

・テスト計画書の作成

本業務におけるテスト工程では、次期システムへの移行が速やかに実施されるよう、テスト計画書を作成し、本区の承認を得てから実施すること。

・テスト実施

受託者は、テストの管理主体としてテストの管理を実施するとともに、その結果と品質に責任を負い適切に対応すること。また、テスト実施にあたって品質管理責任者を配置すること。

テスト工程では、本区へ定期的に進捗報告及び不具合発生時の随時報告を行うこと。不具合が確認された場合は、管理表等で管理を行い、原因と対策を検討のうえで修正を行うこと。なお、スケジュールに大きく影響を及ぼす不具合が確認された場合は、速やかに本区に報告し、協議の

うえで対応方針を検討すること。

・テスト実施報告書

テスト終了時に、実施内容、品質評価結果及び次工程への申し送り事項についてとりまとめたテスト実施報告書を、速やかに提出すること。テストに必要となるプログラム及びツールは、受託者にて用意すること。

4.5 システム移行・データ移行

システム移行・データ移行に係る作業手順・スケジュール・役割分担・移行判定基準等を具体的に記載した移行計画書を作成し、十分に本区と協議し、承認を得てから開始すること。

4.6 運用・保守設計

運用・保守設計は、本業務のプロジェクト開始時より並行して業務を進めること。そのための体制を整備すること。

運用・保守設計書を作成し、運用開始後に内容の変更が発生した場合は、随時更新し、最新版にすること。

4.7 マニュアル作成・操作研修等

必要なマニュアルについては本区と協議し作成すること。特に導入研修が必要とするものについてはマニュアル等の作成を実施し、研修計画をもって本区と協議し実施すること。

本システム稼働において必要となるサーバや端末、クラウドサービス等のマニュアル等については、受託者にて用意すること。

5. 設計・構築等業務

5.1 受託事業者が実施する業務

・本要求水準書及び共通仕様書に基づき受託事業者が導入するハードウェア、ソフトウェア及びクラウドサービス等の要件定義・設計・構築・テストを行うこと。

・現行のシステムから必要なデータの移行を行うこと。

・業務端末（全庁 LAN 端末・個別システム端末の移行支援）の移行を行うこと。

・運用、監視、保守業務への引き継ぎを行うこと。

5.2 作業体制

作業体制

・受託事業者は、設計・構築等業務全体を計画的かつ円滑に進めるため、十分な人数を確保するとともに、作業体制を構築する。さらに、設計・構築等業務を遂行できる知見を有する技術者を確保すること。

・構成要素単位にプロジェクトを立ち上げ、それぞれ緊密に連携を図りながら作業を行う体制とする。

・受託事業者は、本業務の履行に係る実施責任者を選定する。実施責任者はプロジェクトリーダ及び開発リーダを選任し、氏名等を書面で本区へ通知すること。

・人員の中に業務の遂行に著しく不適当な者がいると認める場合には、本区は受託事業者に対してその理由を付して通知し、必要な措置を要求することができ、受託事業者はその趣旨に従い、誠実に対応すること。

主任担当者に関する要件

プロジェクトリーダとは、本業務の統括・運営管理に係る責任を持つ者である。なお、プロジェクトリーダに求める要件を以下に示す。

・クラウドサービスを活用したゼロトラストセキュリティ・ネットワーク基盤の設計・構築におけるプロジェクト管理の経験を有すること。

・プロジェクト管理の実務経験を 5 年以上有すること。

・ウォーターフォール又はアジャイル開発プロセス管理の実務経験を 3 年以上有すること。

開発リーダの資格要件

開発リーダとは、システムの設計・開発作業において、主体となって本区と調整する者である。なお、開発リーダに求める要件を以下に示す。

・クラウドサービスを活用したゼロトラストセキュリティ・ネットワーク基盤の設計・構築におけるプロジェクト管理の経験を有すること。

・設計・開発の実務経験を 5 年以上有すること

・高度情報処理技術者（試験区分は問わない）の資格を有するか、又はこれと同等の能力がある

こと。
・提案するクラウド基盤に関する資格（例：AWS Solutions Architect Professional 相当）を有するか、又はこれと同等の能力があることが望ましい。

5.3 設計・構築業務の管理

管理要件

・設計・構築管理の遂行にあたり、本要求水準書に基づき、進捗管理を行うこと。
・計画から遅れが生じた場合は、原因を調査のうえ本区に改善策を速やかに提示し、承認を得た上で、対策を実施すること。
・構築業務で発生する問題について、課題の認識、対策の責任者、対策の検討、解決状況を明確にするために、課題管理を行うこと。
・発生している課題については、会議体等を通じて本区と随時協議し対応状況の報告を行うこと。
・各工程の達成を妨げるリスクを最小限にするためのリスク管理を行うこと。
・リスクは影響度合いを、識別し、優先度を決定した上で対応を実施すること。
・構築する全庁ネットワークセキュリティ基盤の各システムが、本要求水準書に記載の機能要件を満たすことを確認するため品質管理を行うこと。

5.4 設計

基本事項

・全庁ネットワークセキュリティ基盤の設計にあたっては、本要求水準書のほか「共通仕様書」に基づき、DX 推進に向けた、業務効率化及び生産性のさらなる向上に向けて、現状の課題解決や、共通仕様書で示す 3 つの機能（ネットワークセキュリティ基盤・クラウド業務基盤・広域ネットワーク基盤）を用いた新たな取組の実現に主眼を置いた設計とすること。ただし、その実現方法については、受託事業者の創意工夫による提案を求める。
・現行のネットワーク環境や関連システムの構築・運用事業者との協議等を本区の調整のもと実施した上で、要件を踏まえた最適な全体設計（基本設計及び詳細設計）を行うこと。
・本要求水準書のほか「共通仕様書」に基づき選定したクラウドサービスが適切に利用できるよう設計を行うこと。
全庁ネットワークセキュリティ基盤を構成する各構成要素の正常な稼働を確認するためのテスト設計を行うこと。
・現行システムから全庁ネットワークセキュリティ基盤への移行を行うための移行設計を行うこと。
・全ての設計内容については、本区に対してレビューを実施し、本区の承認を得たうえで次の工程に進むこと。

基本設計書・詳細設計書の作成

・本要求水準書にもとづき導入する各構成要素に係るハードウェア、ソフトウェア及びクラウドサ

ービス等の基本設計書及び詳細設計書を作成し、本区の承認を得た上で作業を行うこと。
・設計の妥当性をプロトタイプにより検証し、その結果を本区に提示し承認を得ること。
・本業務に伴って導入するハードウェア、ソフトウェア、技術、構成の概要等、以下の情報を基本設計書に記述すること。

（ア）　導入するハードウェア及びソフトウェア、クラウドサービスの選定結果
（イ）　ハードウェア一覧
（ウ）　ソフトウェア一覧
（エ）　利用するクラウドサービスの一覧
（オ）　クラウドサービス及びコンポーネントごとの設計内容
（カ）　機器設置計画（ラック配置、機器実装、必要な電源工事の仕様）
※機器設置計画書に基づいて実装されたラック配置及び機器実装の最終結果をラック配置図及び機器実装図として提出すること

・本業務に伴って導入するハードウェア及びソフトウェア、クラウドサービスにおける以下の設定内容等を、詳細設計書に記述すること。
（ア）ネットワーク接続図
（イ）パラメータ・規定値の一覧
（ウ）その他、必要となる詳細設計情報

運用・保守設計書の作成

・受託事業者は運用を開始するまでに、運用・監視・保守業務運用業務及び保守業務の実現方法について検討し、運用・保守設計を行うこと。なお、本区職員が実施する各種業務について、現行システムと同程度、もしくは、軽減されるよう十分配慮すること。
以下の（ア）から（サ）を含む運用・保守設計を行うこと

（ア）　運用計画書
（イ）　運用年次計画書
（ウ）　運用手順書
（エ）　運用フロー
（オ）　保守実施要領（切り分け手順・復旧方法）
（カ）　セキュリティインシデント対応要領（連絡・対応手順）
（キ）　各種管理台帳
（ク）　各種ひな形
（ケ）　取り扱い説明書
（コ）　運用テスト計画書
（サ）　運用テスト報告書

ユーザビリティ/アクセシビリティに関する事項

・本業務で導入・整備する各種ツール類については、利便性を重視するため、ユーザビリティ・アクセシビリティの確保に向けた配慮を行うこと。

（ア）　ユーザビリティ

ユーザビリティ要件については以下のとおりである。

No	分類	要件
1	画面の構成	直感的にわかりやすい画面構成であること
2	操作方法のわかりやすさ	直感的にわかりやすい画面構成であること
3	指示の状態のわかりやすさ	直感的にわかりやすい画面構成であること

（イ）　アクセシビリティ

アクセシビリティ要件については以下のとおりである。

No	分類	要件
1	基準等への準拠	・JIS（日本産業規格） 「JIS X 8341-3：2016『高齢者・障害者等配慮設計指針－情報通信における機器、ソフトウェア及びサービス－ 第 3 部:ウェブコンテンツ』」 ・総務省 公共分野におけるウェブアクセシビリティの確保の取り組みの充実に関する調査研究報告書「みんなの公共サイト運用ガイドライン（2016 年版）」 ・W3C 「ウェブ・コンテンツ・アクセシビリティ・ガイドライン（WCAG）2.0」
2	指示や状態のわかりやすさ	例えば、色の違いを識別しにくいユーザを考慮し、メッセージを表示する等、色のみで判断するような設計は行わないこと
3	言語対応	本業務は日本語対応のみとする

5.5 構築

（1） 基本事項

・受託事業者は、詳細設計書に基づき、ネットワークやハードウェア・ソフトウェア及びクラウドサービスの設定・構築作業を行うこと。

・必要に応じて、ソフトウェアのインストールを行うこと。
・機器の設置等のため、執務室に立ち入る場合は、原則として、平日の午前 8 時 30 分から午後 5 時 15 分とすること。その際、事前に作業スケジュールを示した上で本区の許可を得ること。
・機器及び必要資材の搬入等を行う場合、詳細な施工方法、施工範囲、作業員名、スケジュール及び使用車両について、あらかじめ定めた書面をもって作業申請を行い、本区承認を得ること。また、本区が行うべき作業がある場合には、これを明示すること。
・その他必要事項については、適宜本区と協議の上、決定すること。

（2） 構築方式及び構築手法

・構築方式としては、ウォーターフォール型の管理工程とアジャイル型の柔軟な仕様変更対応を組み合わせることを想定している。ウォーターフォール型による工程の明確化及び、アジャイル型による本区の要求に合致したシステム構築を行うこと。
・アジャイル型におけるプロトタイプとしては、標準パッケージシステムを活用した詳細仕様検討のプロトタイプ及び、処理方式などのシステム基盤面でのプロトタイプ検証などを想定している。そのため、要件定義段階から実際に稼働するシステム（プロトタイプ）をクラウド上で一部利用者へ開放し、一部利用者が操作しながら、アイデア、要望をヒアリングしていくこと。
・プロトタイプ検証の内容及びスケジュールは受託事業者の提案によるものとするが、プロトタイプ検証を最低 2 回は行うこと。（本区の想定するマイルストーンは下表を参照すること）
・想定プロトタイプ検証の途中段階においては、本要求水準書で示す全要件を満たす必要はない。
・生産性と品質の向上および、柔軟な変更対応のため、可能な限り Infrastructure as Code（コードによるインフラ構築：以下 IoC）にて実装すること。

No	想定マイルストーン	想定する検証等の概要
1	一次機能検証	情報担当部門による機能性検証を実施し、抽出した要件を改修により反映させる。
2	二次機能検証	一般利用者による操作検証を実施し、抽出した要件を改修により反映する。
3	三次機能検証	一次及び二次検証を踏まえた三次機能性検証を実施する

5.6 テストに関する事項

（1） 基本事項

・テスト設計に基づき、テストの内容、スケジュール等を詳細に記載したテスト仕様書、テスト計画書及び手順書を作成すること。また、アジャイル型で開発を進める部分については、スプ

リント単位で本区の承認を受けること。
・機能の動作確認だけでなく、性能や可用性、セキュリティなどの非機能項目に対しても検証を行うこと。
・必要なシステムについては、バックアップデータからのリストア作業の検証を行うこと。
・考えられる障害に対する対応策の検証を行うこと。
・必要に応じて試行運用期間を設定するなど、本番までに十分なテストを行うこと。
・各種テストにおいて必要なツール等の設計、作成または取得、導入等を行うこと。

（2） テストの実施

・テストは受託事業者が行い、本区は必要に応じて任意のテストに立ち会うことができることとする。
・受託事業者によるテストとは別に、本区は任意の機能について動作検証を行うことができることとする。その場合、受託事業者は操作方法等についてサポートを行うこと。
・テストの実施にあたり作成、使用した不要なテストデータは、受託事業者において削除すること。

（3） テストの結果

・全ての検証が問題なく終了したことを記録したテスト報告書を作成し、本区の承認を得ること。テスト報告書を本区が受理した後、本番運用に移行するものとする。
・テスト結果が期待されるものと異なる場合は、速やかに原因究明と改修を行った後、期待される結果となるまで繰り返し検証を行うこと。

5.7 移行に関する事項

（1） 基本事項

・受託事業者は、現行システムにおける各システムの設定ファイル等、全庁ネットワークセキュリティ基盤に引き継ぐデータの種類を本区に提示した上で、最新のデータを収集し、引き継ぐこと。
・移行が必要となるデータ（対象システムのファイル、設定ファイル、ユーザデータ等）の調査を行い、移行対象となるデータを確定すること。移行対象データの抽出に際し対象データの提供方法、時期、フォーマットを指定した上で、本区に対して依頼、調整を行うこと。
・現行システムで作業が必要になる場合は、事前に本区へ必要となる作業内容を提示し承認を得ること。
・安全性の確保と効率を考慮し、順次、移行を実施すること。
・移行計画書に基づき実施した移行結果を報告書として取りまとめ、本区に提出すること。
・本区の職員が自身でデータ移行を行う場合の問い合わせ対応についても適切に対応できる体制を構築すること。

・複数回に分けて実施する移行作業を含め、全ての移行工程（総合テスト前、受け入れテスト前、稼働開始前）を令和 10 年1月3日までに完了すること。

（2） 移行計画書及び手順書の作成

・移行設計に基づき、現行システムとの一時的な並行運用、業務システムとの連携、業務端末の変更点等も考慮した具体的な移行計画書及び手順書を作成し、本区の承認を得ること。

・移行計画書及び手順書には、以下の項目を含めること。

（ア） 方針、概要

（イ） 前提条件

（ウ） 移行方法

（エ） スケジュール、フェーズの説明

（オ） 作業項目と作業担当者

（カ） 移行対象システム、機器、データ

（キ） 移行作業時の体制表及び役割分担

（ク） 移行作業後の試験項目、合否判定基準

（ケ） 移行を中断・切り戻す場合の切り戻し手順

（コ） 移行期間中の運用体制

・移行計画の策定にあたり、現行システムの利用者に対して、可能な限り影響を与えない方法を検討すること。移行にあたり、本要求水準書等に記載した機能以外の機器等が一時的に必要な場合には、受託事業者の費用負担において用意すること。

（3） 仮想マシン移行方針（V2V）

・既存仮想基盤から新仮想基盤への移行は、V2V 方式を採用し、業務影響を最小化するオンライン移行を基本とする。

・移行後は OS・ネットワーク・アプリの正常性を確認し、運用設定を最新化する。

（4） 業務端末について

・全庁ネットワークセキュリティ基盤にて利用する業務端末（全庁 LAN 端末）は原則として新規調達端末にて運用する想定である。

・新規端末（全庁 LAN 端末）は合計 2000 台程度を想定している。

・受託事業者が指定するエージェント等（EDR、EMM 等）をインストールする必要がある場合は、新規業務端末（全庁 LAN 端末）合計 2000 台とする。

現行システムでは個別システムで利用している個別システム端末、約 500 台にもウイルス対策ソフト、資産管理ソフト（ログ収集、媒体書き出し管理）をインストールしセキュリティ対策を実施している、これらの端末数も提案に含めること。

・全庁ネットワークセキュリティ基盤への移行に伴う業務端末の設定変更は、必要事項を定め、

本業務内で受託事業者の責任において、作業に必要となる機材の準備も含め、全て行うこと。
ただし、対象端末の把握、端末の利用者への連絡、日程調整等の本区が実施すべき作業は除く。

・遠隔操作で設定変更できない業務端末については、現地作業等を行うこと。

なお、現地作業等は以下の項目を想定している。

（ア）　マスタイメージの作成

端末のソフトウェア及び設定に係るマスタイメージを作成すること。

新規業務端末マスタイメージの作成

（イ）　既存端末の回収

本区が指定する既存業務端末を職員から回収すること。

（ウ）　設定

新規業務端末（ア）で作成したマスタイメージを新規業務端末に展開すること。

（エ）　新規端末の配布及び既存端末の再配付

本区が指定する職員に新規端末を配付すること。

既存業務端末の各庁舎別端末設置台数（令和8年1月現在）は以下のとおり。

※新規業務端末の配布、既存業務端末の再配布を計画する参考資料とすること

No.	拠点名称	住所	台数
1	千代田区役所	九段南 1-2-1	約 1239 台（予備機約 271 台含む）
2	麹町出張所	麹町 2-8	約 11 台
3	富士見出張所	富士見 1-6-7	約 10 台
4	神保町出張所	神田神保町 2-40	約 8 台
5	神田公園出張所	神田司町 2-2	約 7 台
6	万世橋出張所	外神田 1-1-11	約 8 台
7	和泉橋出張所	神田佐久間町 1-11-7	約 8 台
8	千代田保健所	九段北 1-2-14	約 70 台
9	西神田コスモス館（西神田児童センター、西神田保育園）	西神田 2-6-2	約 35 台
10	麹町保育園	一番町 4	約 19 台
11	神田保育園	神田淡路町 2-109	約 21 台
12	富士見みらい館（富士見小学校、富士見子ども園）	富士見 1-1-3	約 40 台
13	ちよだパークサイドプラ	神田和泉町 1	約 32 台

	ザ （和泉小学校、いずみこども園、まちかど図書館）		
14	麹町小学校（麹町幼稚園）	麹町 2-8	約 17 台
15	九段小学校（九段幼稚園）	三番町 16	約 15 台
16	番町小学校（番町幼稚園）	六番町 8	約 15 台
17	お茶の水小学校（お茶の水幼稚園）（仮校舎）	富士見 1-1-6	約 15 台
18	麹町中学校	平河町 2-5-1	約 6 台
19	神田一橋中学校	一ツ橋 2-6-14	約 6 台
20	九段中等教育学校（前期課程）	富士見 1-10-14	約 14 台
21	九段中等教育学校（後期課程）	九段北 2-2-1	約 2 台
22	日比谷図書・文化館	日比谷公園 1-4	約 13 台
23	四番町図書館（仮施設）	三番町 14-7	約 0 台
24	昌平童夢館 （昌平小学校、昌平幼稚園、神田児童館、まちかど図書館）	外神田 3-4-7	約 22 台
25	神田さくら館 （千代田小学校、千代田幼稚園、まちかど図書館、教育研究所、 児童・家庭支援センター）	神田司町 2-16	約 63 台
26	四番町児童館（四番町保育園）	四番町 5-8	約 29 台
27	一番町児童館	一番町 10	約 11 台
28	千代田土木事務所	一ツ橋 2-1-1	約 5 台
29	千代田土木事務所 神田橋分室	内神田 1-1-3	約 2 台
30	スポーツセンター	内神田 2-1-8	約 0 台

31	九段生涯学習館	九段南 1-5-10	約 0 台
32	ちよだプラットフォームスクウェア （まちみらい千代田、ゆとりちよだ）	神田錦町 3-21	約 1 台
33	千代田清掃事務所	外神田 1-1-6	約 33 台
34	千代田清掃事務所飯田橋車庫	飯田橋 3-13-2	約 7 台
35	千代田清掃事務所三崎町中継所	神田三崎町 3-9-3	約 0 台
36	高齢者あんしんセンター神田	神田淡路町 2-8-1	約 0 台
37	高齢者あんしんセンター麹町	一番町 12	約 0 台
38	高齢者総合サポートセンター(かがやきプラザ)	九段南 1-6-10	約 24 台
39	千代田会館(8階　商工観光課、生活衛生課)	九段南 1-6-17	約 77 台
40	児童・家庭支援センター（教育研究所）	神田須田町 1-4-4　PMO 神田須田町	約 14 台

5.8 教育及び引き継に関する事項

(1)　基本事項

受託者は、本業務の完了に先立ち、運用担当者及び関係職員に対し、システムの操作方法、障害対応手順、保守作業手順等に関する教育を実施すること。また教育計画書及び教材を事前に提出し承認を得ること。 さらに、運用開始後の安定稼働を確保するため、引き継ぎ資料(構成管理台帳、設定情報、運用マニュアル、障害対応手順書等)を整備し、関係者への説明を行うこと。引き継ぎ完了後、受託者は確認記録を提出すること。

6. 構成要素の仕様

6.1 クラウドサービスに関する事項

(1)　前提条件

選定するクラウドサービスについては、「政府情報システムのためのセキュリティ評価制度（ISMAP）」に登録されているか、情報セキュリティ管理・運用の基準となる以下のいずれか、または同等の認証を取得し、サービスの信頼性が確認できること。

・ISO/IEC 27017 によるクラウドサービス分野における ISMS 認証取得
・日本セキュリティ監査協会のクラウド情報セキュリティ監査による認定
・SOC2 報告書(Service Organization Control Report)の取得

・クラウドサービスにおいて一定のセキュリティレベルが確保されていることの保証として、クラウドサービスに対する情報セキュリティ監査報告書の内容及び取得・維持している各種認定・認証制度の基準、ガイドライン等について事前に確認し本区に提示すること。
・選定するクラウドサービスは、国内に裁判管轄権があること。
・本サービスを提供する施設等は、必要なセキュリティ及び災害対策等の措置がとられていること。
・選定するクラウドサービスは、地理的に離れた 2 つ以上のリージョンでサービスが提供されており、大規模災害の場合でも別のリージョンへ切り替えが行われること。
・十分な稼働実績を有し、運用の自動化、サービスの高度化、情報セキュリティの強化、新機能の追加等に積極的かつ継続的な投資が行われているクラウドサービスを選定すること。
・クラウドサービスを利用する場合は、本要求水準書に記載されているセキュリティ対策を遵守すること。

(2) 基本事項

・クラウドサービスを使用した時に出力されるログを提供すること。又は、ログ検索機能を提供すること。
・クラウドサービスへのアクセスは機密漏えい防止のため、通信の暗号化を行うこと。
・クラウドサービスの契約終了時、業務データ等の消去を遅滞なく確実に実施すること。
・業務データ等のバックアップは、データの完全性やデータリカバリのコストのバランスを踏まえ、同一クラウドサービスの内部で複数作成すること。
・本業務において導入する全てのクラウドサービスは、全庁ネットワークセキュリティ基盤経由の通信のみに限定できること。ただし、その他の手法により、同等以上のセキュリティレベルの確保ができる場合、この限りではない。
・提案本業務において導入する全てのクラウドサービスは、ユーザ属性及び端末属性により、アクセス範囲の制限が可能であること。

6.2 情報セキュリティに関する事項

(1) 方針

・クラウドサービスの利用や庁外へ持ち出し可能となる業務端末に関して、新たにゼロトラストセキュリティを採用する。ただし、移行期間中に旧全庁 LAN 端末からインターネットへアクセスを行う場合は、境界型(ペリメータ)セキュリティを採用する。
・セキュリティ対策は、「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」、「千代田区情報セキュリティポリシー対策基準」、「個人情報の保護に関する法律」等に示

されるセキュリティ対策事項を参考に実施すること。
・セキュリティインシデントの状況を正確に把握できるよう、適切に分類し報告を行うこと。
・情報漏えいが疑われる、または発生した場合、流出経路の特定等の調査を行い、対策を講じられるようにすること。
・不要な通信は抑制すること。

（2） 認証技術

・利用者が全庁ネットワークセキュリティ基盤を利用する際、アカウントの共有等による不正利用やなりすましを防止するため、多要素認証を行うこと。
・運用担当者が全庁ネットワークセキュリティ基盤のサービスにログインする際においても、多要素認証などセキュリティを担保した方法で、認証を行うこと。
・クラウドサービスを含む各業務システムへのアクセスはシングルサインオンを可能とすること。
・不正にログインしようとする行為を検知及び防止する機能を有すること。
・利用者に付与したアカウントを、その後別の利用者に付与しないこと。
・認証情報を保存する場合に暗号化を行う機能を有すること。

（3） アクセス制御・権限管理

・アカウントはサービスにおける作業者の役割ごと（各種システム操作を含む。）に作成し、作業に必要な権限のみの付与等、目的に応じた適切なアクセス制限、権限管理及び設定を行うこと。
・アクセス制御は拒否を前提とし、必要な通信のみを許可する方針とすること。
・管理者権限を持つアカウントを利用する場合には、管理者としての業務遂行時に限定して利用すること。
・運用管理者が変更になった場合やシステム変更等の理由で不要となった運用管理者等のアカウントは、即時アカウントを削除またはアクセス権を削除し、使い回すことのないようにすること。
・サーバやデータへのアクセスについてはアクセス権限を適切に設定すること。
・ユーザ情報を持つ場合は、人事異動及び組織改編に伴うユーザの一括登録、削除が行えること。ただし、IDaaS 等、外部の認証基盤と同期する場合はこの限りではない。（CSV ファイル等によるユーザの一括登録、削除が行えることを想定している）

（4） ログの取得・管理

・全庁ネットワークセキュリティ基盤で提供するサービスの証跡ログを収集すること。
・内部からの不正操作、誤操作等による情報セキュリティ上の脅威に対応するため、管理者権限操作を含めた証跡ログを取得すること。
・証跡の不当な消去や改ざんを防止するため、証跡に関するアクセス制御機能を備えること。

・不正行為の追跡や情報セキュリティ侵害時において証跡の解析等を容易にするため、正確な時刻に同期する機能を備えること。
・特に指定のない限り、証跡ログの保存期間は全ての機能において、2年以上とし、直近 30 日分はすぐに分析できる状態とすること。
・想定ログ保存システムを整備し、30 日より前のログを格納すること。
・ログの2年保存要件を満たすために「標準保存期間」「アーカイブ／エクスポート」等の多層構えを採用し、コスト効率を重視した方法を提案すること。
（例）標準保存期間はシステム内で保持し、追加のストレージコストを抑制。長期保存は低コストのアーカイブ領域や既存クラウドサービスを活用。
・CSV/JSON 等の標準的なファイル形式でエクスポートし、本区が導入済のクラウドサービス（Box）に保存することも提案に含めること。
・ログファイルの保存形式や圧縮・暗号化方式は事前に区と協議し、運用負荷や追加コストが最小となる方法を選定すること。

（5） 暗号化・電子署名

・外部に送信するデータについては暗号化を行うことで個人情報や機密情報が保護されるように対策を講ずること。
・暗号及び電子署名のアルゴリズムについては、CRYPTREC 暗号リスト（電子政府推奨暗号リスト）から可能な限り、強度の高いアルゴリズムを想定した上で、設計・構築を実施すること。

（6） ソフトウェアに関する脆弱性対策

・本業務において導入する全てのファームウェア、ソフトウェア等に関連するセキュリティホール情報は公開され次第、入手する体制を整えること。
・脆弱性に関する情報が公開された場合、当該脆弱性がもたらすリスクを確認した上で本区へ報告すること。
・セキュリティホール対策の実施に際しては、事前に全庁ネットワークセキュリティ基盤への影響検討、検証作業等を実施し、それらの結果を踏まえて本区との協議により対応を決定すること。ただし、クラウドサービスにおいては、その限りではない。
・機器やソフトウェアはアカウント、パスワード等を初期設定値の状態で運用しないこと。また、推察されやすい安易なユーザアカウント、パスワード等を設定しないこと。
・利用者への提供及び運用に用いるものを除く、不要なプロセス、サービス等は原則停止すること。ただし、クラウドサービスにおいては、その限りではない。

（7） 不正プログラム対策

・本業務において導入するオンプレミスシステムの機器等について、不正プログラムの検知及びその実行の防止の機能を有する対策ソフトウェアを導入すること。ただし、当該電子計算機

で動作可能な不正プログラム対策ソフトウェアが存在しない場合を除く。

（8） セキュリティインシデントへの対応

・セキュリティインシデントが発生した場合に備え、連絡体制・対応手順等を明示して、本区の承認を得ること。

・セキュリティインシデントが発生した場合又はそのおそれがある場合には、速やかに本区へ報告すること。

・セキュリティインシデントに関する問い合わせについて、24 時間 365 日受付可能とすること。

・重大セキュリティインシデント以外のセキュリティインシデントについては、別途定める運用業務の提供時間内において、対応すること。ただし、業務時間内に確認されたインシデントに関しては、重大セキュリティインシデントの判断がつくまで対応すること。

・重大セキュリティインシデントの具体的な定義については、本区と協議の上、決定すること。

6.3 サービスレベルの管理に関する事項

全庁ネットワークセキュリティ基盤について、24 時間 365 日稼動できる体制を確保するものとする。SLA は全庁ネットワークセキュリティ基盤の運用・保守業務開始時点から適応する。なお、運用・保守業務開始の時期は、本区と受託事業者との協議において判断する。なお、サービスレベル基準値を下回った場合、再発を防止することを目的として速やかに改善策を提示すること。

（1） 指標の設定

運用・保守業務の品質の維持・向上を図るため、受託事業者は「8.非機能要件」に記載されている要件を満たす SLA を本区と締結すること。

（2） SLA のモニタリング

受託事業者は SLA の履行状況について報告を月 1 回行うこと。

（3） 改善

・受託事業者は SLA が遵守できているか運用の中で評価し、評価した結果を受けてサービスレベルの改善を本区の承認の下で行っていくこと。

・SLA が遵守できない場合は原因を特定し、報告するとともに、改善策、結果対応について報告すること。

・改善に関する費用は受託事業者が負担すること。

（4） SLA 適用除外条件

以下のいずれかに該当する場合は、上記 SLA の適用外とする。

・公共交通機関の停止、災害による電源供給の停止や通信障害の場合

・本区又は他の事業者の過失及び故意による障害の場合

・受託事業者の瑕疵によらず障害復旧が行えない場合

・受託事業者の瑕疵によらず障害監視が行えない場合

・受託事業者の瑕疵によらず障害通知の受信ができない場合

・区及び受託事業者双方の協議の上、計測の除外とした場合

（5） クラウドサービスの利用

クラウドサービスの稼働率等は各サービスの SLA または SLO に準ずるものとする。なお、各クラウドサービスの SLA または SLO を事前に提示し、本区の承認を得ること。

6.4 ソフトウェアに関する事項

・構成要素単位で記載している要件を満たすソフトウェア構成とすること。

・直観的に操作しやすい UI（ユーザインターフェース）を有し、言語表示は日本語表示を必須とすること。

・快適に操作できるレスポンス（画面遷移通常時3秒以内、集中時 5 秒以内）を確保すること。

・令和 15 年 3 月 31 日までに製品サポートの終了が予定されていない製品の選定を行うこと。また、上記期間までに製品サポートが終了することとなった場合は、受託事業者の責任において、ハードウェアの交換やソフトウェアのバージョンアップ等を実施し、製品サポートを継続すること。

・調達するソフトウェアについては、国、地方自治体又は民間企業における導入・稼働実績等を有し、本区の要件（業務端末数等）に対して動作保証できるものを提供すること。

・ソフトウェアライセンス違反を犯さないように、受託事業者の責任において、調達すること。

・受託事業者が導入するソフトウェアが、本要求水準書どおりの機能を提供できない場合には、本区と協議の上、その代替ソフトウェアを提供すること。

6.5 端末等に関する前提条件

（1） 情報システム課において配布している全庁 LAN 端末（1900 台）

・「IN」から始まる管理番号を付与し、全庁 LAN ネットワークに接続している。

・概ね5年程度で機器更新を行っている。

・OS は、以下のいずれかを利用している。

Microsoft Windows 11 Enterprise（FAT 端末で利用）

Microsoft Windows 10 Enterprise LTSC（VDI 環境で利用）

・Office ソフトは、以下のいずれかを利用している。

Microsoft 365 Apps for enterprise（FAT 端末で利用）

Microsoft Office LTSC Professional Plus 2021（VDI 環境で利用）

（2） デジタル政策課において配布しているモバイルワーク端末（200 台）

Microsoft Windows 10 Enterprise LTSC

ポリシーで動作を制限しており、モバイルワーク用のアプリのみ利用可能

（3） 各課において購入・管理している業務端末

Microsoft Windows 10 Enterprise LTSC

各課にて管理者権限を有しており、アプリケーションのインストール権限を持つ

（4） 各職員の個人端末（BYOD 端末）

・現在は BYOD 端末を許可していないが、リプレース後は導入を検討しているため、適切なセキュリティ対策を実装し提案すること。本区の想定として全庁ネットワークセキュリティ基盤において、セキュリティ確保を行い、Microsoft Teams、Microsoft Outlook の機能を利用する端末として活用する。

・BYOD 端末において、対象とする OS は、以下を想定している。

Apple iOS 最新版

Google Android OS 最新版

6.6 ライセンスの取り扱い

（1） OS

・今後も購入する PC に付属の Microsoft Windows を利用する予定であるが、本契約において Microsoft Windows ライセンス、または Microsoft Windows Enterprise へのアップグレードライセンスの導入を妨げるものではない。

なお、Microsoft Windows ライセンス、または Microsoft Windows Enterprise へのアップグレードライセンスを導入する場合は、全ての職員が常に最新版を利用できることを条件とする。

（2） オフィスソフト

・本区は Microsoft 365（Ms365）を利用しているが、必要に応じて永続版の Microsoft Office を購入し利用する提案を認めるものとする。本契約は Microsoft Office ライセンスの導入を妨げるものではない。 なお、Microsoft Office ライセンスを導入する場合は、全職員が常に Microsoft 365 Apps for enterprise 相当の最新版を利用可能であることを条件とする。

（3） 閲覧ブラウザ

情報システム課において配布している全庁 LAN 端末

・ Google Chrome 最新版
・ Microsoft Edge 最新版(既定のブラウザとして設定)

デジタル政策課において配布しているモバイルワーク端末
・ Google Chrome 最新版
・ Microsoft Edge 最新版(既定のブラウザとして設定)

各課において購入・管理している業務端末(個別システム端末)
・ Google Chrome 最新版
・ Microsoft Edge 最新版

6.7 機器設置に関する前提条件

・本区の本庁舎内のラックを使用する場合は以下の要件を満たすこと。
ラックの規格については H2,000mm×W600mm×D900mm(35U)で、うち2ラックが利用可能である。
・利用できる電源容量は、1 ラックあたり 100V, 20A までとする。
・上記を越えるハウジングスペースや電源容量が必要な場合は、追加が可能だが、その際に必要となる費用については、受託事業者の負担とする。
・ラック間の配線は、事業者にて実施すること。
・ラック間の配線は、申請から実施まで 2 週間程度を要するため、余裕をもって設置計画を立てること。

7. 次期システム機能要件

7.1 全庁ネットワークセキュリティ基盤要件

本区では、従来の境界防御型セキュリティモデルでは対応困難な現代の脅威環境に対応するため、「信頼しない、常に検証する」というゼロトラストの考え方をベースに、SASE、IdP、エンドポイントセキュリティ、セキュリティ監視基盤の各要素を組み合わせた統合的なリスク評価・制御機能の実現を目指している。

現行システムでは、ネットワーク境界での防御を前提とした三層分離により一定のセキュリティを確保してきたが、ユーザのアイデンティティ、デバイスの状態、ネットワークの状況、行動履歴等を総合的に評価してアクセス制御を行う仕組みが不足している。このため、高度化するサイバー攻撃や内部脅威、クラウドサービス利用拡大に対する包括的な対策が困難な状況となっている。

本システムでは、ゼロトラストの原則に基づき、すべてのアクセスを信頼せず継続的に検証する仕組みを構築し、アイデンティティを中心とした統合セキュリティ基盤により、リスクベースでの動的なアクセス制御を実現する。これにより、セキュリティレベルの向上と業務効率性の両立

を図る。

横断的な機能要件

・アイデンティティ、デバイス、ネットワーク、行動履歴、外部脅威インテリジェンスなどから総合的にリスク・信頼性を評価できる機能を有すること
・セキュリティ状態、利用パターン、行動履歴、アクセス時刻、場所、ネットワーク環境など
・ユーザ行動・サインインパターンの異常検知（UEBA: エンティティ行動分析）機能を有すること
・リスク・信頼性レベルや指定のコンテキスト条件（アクセス時刻、場所、利用環境など）に応じたアクセス制御機能を有すること

ネットワークセキュリティ（SASE）要件

本システムでは、SASE により自宅等のさまざまな環境からのセキュアで快適なアクセスを実現する。これにより、場所を問わない柔軟な働き方を実現するとともに、セキュリティ運用の効率化を図る。ネットワークセキュリティ基盤（SSE）と広域ネットワーク基盤（SD-WAN）を統合し提供すること。

① **CASB（Cloud Access Security Broker）、SSPM（SaaS Security Posture Management）機能**

- SaaS アプリケーション（Microsoft 365、Box、Zoom、Webex 等）の利用状況可視化機能を有すること
- 許可リスト及び拒否リスト形式でクラウドサービス、またその特定のテナントへのアクセス制御機能を有すること
- 新しいクラウドサービス利用リクエストに対する迅速な制御対応（1 ヶ月程度）を可能とすること
- SaaS アプリケーション（クラウドストレージ含む）へのファイルアップロード、機微データ送信制御機能を有すること
- SaaS アプリケーションのセキュリティ設定誤設定・コンプライアンス違反の自動検知機能を有すること

② **SWG（Secure Web Gateway）、FWaaS（Firewall as a Service）機能**

- SSL/TLS によって暗号化されたトラフィックを含むネットワークトラフィックの検査及びフィルタリング機能を有すること
- 既知脅威（脅威インテリジェンスの活用など）、未知脅威（機械学習技術の活用など）に対する迅速な検知、ブロック機能を有すること（マルウェア及びフィッシング攻撃の検知、ブロックを含む）
- URL カテゴリ及びレピュテーションベースのアクセス制御機能を有すること

- DNS レイヤにおいて、悪意のあるドメインやコマンド＆コントロールサーバ等へのアクセスを事前にブロックし、DNS トンネル等の不正な利用を検知する機能を有すること
- IP アドレス、ポート、プロトコル等のネットワーク条件およびアプリケーション識別に基づき、クラウド上で L3～L7 レベルのアクセス制御を行うファイアウォール機能（FWaaS）を有すること

③ ZTNA（Zero Trust Network Access）機能

- オンプレミス・プライベートクラウドアプリケーション（IaaS, SaaS 問わず）への暗号化された経路でのプライベートな接続機能を有すること
- それらのアプリケーションへのアクセス制御機能、ファイルアップロード、機微データ送信制御機能を有すること

④ ネットワーク接続

- 庁内のネットワーク機器から SASE に接続する集約接続方式（本庁）、エンドポイントからインターネットで直接 SASE に接続する直接接続方式（在宅勤務、モバイル、出張所など）を実現できること
- 同一ユーザの接続場所変更時の自動切り替え機能を有すること
- Windows 端末からの接続機能を有すること
- Chrome、Edge ブラウザでのセキュリティ制御が利用可能であること
- 一部のトラフィックに対する直接インターネット接続機能（一部の通信を SASE 経由から除外するブレイクアウト）を有すること
- Zoom、Webex、Microsoft Teams 等の通信品質が重視されるコミュニケーション SaaS トラフィック
- Amazon Workspaces 等の通信品質が重視される VDI サービストラフィック
- Windows Update 等の大容量アップデート通信のトラフィック
- ブレイクアウト対象サービス・ドメインのトラフィック識別機能、設定・管理機能を有すること

⑤ 管理機能

- 管理コンソールでは IdP と連携した認証認可を実現すること
- ロールまたは属性ベースの権限管理を可能とすること
- セキュリティ監視基盤へのログの出力機能を有すること

エンドポイント管理・セキュリティ要件

本システムでは、EDR（Endpoint Detection and Response）機能を中心とした高度な脅威検知・対応機能と、EMM（Enterprise Mobility Management）機能を中心とした統合的なデバイス管理機能により、ゼロトラストの原則に基づくデバイス信頼性評価とリ

スクベースアクセス制御を実現する。①から⑥については職員が利用する業務 PC（Windows 端末）に関する要件であり、⑦については職員が利用するスマートフォン（iOS, Android 端末）、来庁者がキオスク形式で利用するタブレット（iOS, Android 端末）に関する要件である。VDI に関する要件は 3.15 VDI（LGWAN 系）および 3.16 VDI（個人番号利用事務系）を参照すること。

① 脅威検知・防御機能

- 既知脅威（脅威インテリジェンスの活用など）、未知脅威（機械学習技術の活用など）に対する迅速な検知、ブロック機能を有すること（ランサムウェア、ファイルレス攻撃等の高度な脅威を含む）
- エンドポイント上の活動の継続的監視・記録機能を有すること
- セキュリティインシデントの検知・アラート機能を有すること
- 検知した脅威に対する自動・手動対応機能（隔離、プロセス停止等）を有すること
- インシデント調査のための詳細分析・フォレンジック機能を有すること
  以下①～④の情報は、ダッシュボード上で一覧表示し、フィルタリング・検索・レポート出力が可能であること
  ① ログ収集・可視化
  ユーザのアクセス履歴、アプリ利用状況、ポリシー違反イベントを詳細に記録し、検索・可視化できること。
  ② 脅威検知とアラート
  不審なアクセスやポリシー違反をリアルタイムで検知し、管理者に通知できること。
  ③ ポリシー適用状況の監査
  誰が、いつ、どのリソースにアクセスしたかを追跡可能であること。
  ④ イベントの相互分析
  複数イベントを関連付けて分析し、インシデントの原因および影響範囲を特定できること。
- 行動分析による異常プロセス・攻撃パターンの検知機能を有すること
- プロセス実行チェーンの監視・分析機能を有すること
- 疑わしいプロセス動作の自動検知機能を有すること
- メモリ内攻撃の検知・防御機能を有すること

② 脆弱性管理機能

- エンドポイントの脆弱性スキャン・検知機能を有すること
- 脆弱性の重要度評価・優先度付け機能を有すること
- CVE 情報との連携による脆弱性情報更新機能を有すること
- パッチ適用状況の監視・レポート機能を有すること
- セキュリティ設定の評価・監視機能を有すること

- セキュリティベースラインとの比較・評価機能を有すること
- 設定の逸脱検知・アラート機能を有すること

③ アプリケーション制御機能

（ア）アプリケーション実行制御機能

- 許可リスト方式、拒否リスト方式によるアプリケーション実行制御機能を有すること
- アプリケーションの自動分類・評価機能を有すること
- 実行可能ファイルのデジタル署名検証機能を有すること

（イ）スクリプト実行制御機能

- スクリプト実行制御機能（PowerShell、マクロ等）を有すること
- 悪意のあるスクリプトの検知・ブロック機能を有すること
- スクリプト実行の監視・ログ記録機能を有すること

（ウ）Web ブラウザ制御機能

- ブラウザセキュリティ設定の強制機能を有すること
- 悪意のある Web サイトへのアクセスブロック機能を有すること
- ブラウザ拡張機能の制御・管理機能を有すること
- ダウンロードファイルの検査・制御機能を有すること

④ デバイス制御機能

（ア）外部デバイス制御機能

- 許可リスト方式、拒否リスト方式による USB デバイス・外部メディアの接続制御機能を有すること
- デバイス種別による細かな制御機能を有すること
- 外部デバイス接続の監視・ログ記録機能を有すること

（イ）データ転送制御機能

- 外部メディアへのデータ転送制御・検査機能を有すること
- ファイル種別による転送制御機能を有すること
- 転送データの内容検査・DLP 連携機能を有すること

⑤ データ保護機能

（ア）データ漏洩防止機能

- 機密データの検知・分類機能を有すること
- 機密データの外部送信ブロック機能を有すること
- ファイル・メール・クラウドストレージへのアップロード制御機能を有すること
- データアクセス・操作のログ記録機能を有すること
- データ分類に基づく動的保護機能を有すること

（イ）ファイル暗号化・保護機能

- 機密ファイルの自動暗号化機能を有すること

- ファイルアクセス権限の動的制御機能を有すること
- 暗号化ファイルの利用状況監視機能を有すること

⑥ エンドポイント管理機能

(ア) デバイス認証・登録機能

- デバイス証明書による認証機能を有すること
- ゼロタッチでのセットアップ機能を有すること
- 新規デバイスの検出・登録機能を有すること
- 不正デバイスの検知・ブロック機能を有すること

(イ) コンプライアンス管理機能

- デバイス状態の継続的監視機能を有すること
- デバイスのセキュリティ設定・OS/アプリケーションのバージョン・パッチレベル要件・フルディスク暗号化など
- コンプライアンス違反デバイス(設定したデバイス状態の基準に満たないデバイス)の検知・制限・修復機能を有すること

(ウ) リモート管理機能

- エンドポイントのリモート管理・制御機能を有すること
- リモートでのソフトウェア配布・更新機能を有すること
- リモートでの設定変更・ポリシー適用機能を有すること

⑦ モバイルデバイス管理機能

(ア) デバイス登録・プロビジョニング機能

- iOS/iPadOS/Android デバイスの統合管理機能を有すること
- ゼロタッチ展開機能(Apple DEP/ABM、Android Zero-touch Enrollment 対応)を有すること
- 企業所有デバイス(COBO: Company-Owned Business-Only)の完全管理機能を有すること
- 個人所有デバイス(BYOD: Bring Your Own Device)の業務領域分離管理機能を有すること
- デバイス証明書による認証・登録機能を有すること

(イ) アプリケーション管理機能

- 業務アプリケーションの配布・更新・削除機能を有すること
- アプリストア(App Store、Google Play)からのアプリ配布制御機能を有すること
- 業務アプリケーションの設定自動配布機能を有すること
- アプリケーション実行制御機能(許可リスト・拒否リスト)を有すること
- 個人アプリと業務アプリの分離管理機能を有すること

(ウ) セキュリティ・コンプライアンス機能

- デバイスのセキュリティ設定強制機能を有すること
- パスコード・生体認証要求、画面ロック時間、暗号化要求など
- コンプライアンス違反デバイスの検知・制限機能を有すること
- 脱獄・ルート化デバイスの検知・ブロック機能を有すること
- 紛失・盗難時のリモートワイプ・ロック機能を有すること
- 位置情報追跡機能を有すること

（エ）データ保護機能

- 業務データの暗号化・保護機能を有すること
- 業務データと個人データの分離機能を有すること
- 業務データの外部転送制御機能（コピー・ペースト制限、共有制限等）を有すること
- 業務アプリケーション内データの選択的ワイプ機能を有すること
- スクリーンショット・画面録画制御機能を有すること

（オ）IdP 連携・SaaS アクセス制御機能

- IdP と連携したシングルサインオン（SSO）機能を有すること
- SaaS アプリケーション（Microsoft 365 等）への条件付きアクセス制御機能を有すること
- デバイスコンプライアンス状態に基づく SaaS アクセス制御機能を有すること
- 管理対象アプリケーションからのみ SaaS アクセスを許可する機能を有すること

（カ）ネットワーク関連機能

- Wi-Fi 設定の自動配布機能を有すること
- Wi-Fi ネットワークへの接続制限機能を有すること
- Bluetooth 接続制御機能を有すること

⑧　管理・運用機能

- 全庁エンドポイントの管理状況表示・管理機能を有すること
- エンドポイントセキュリティ状況のリアルタイム可視化機能を有すること
- エンドポイント固有ポリシー配布・管理機能を有すること
- エンドポイント資産情報の管理機能を有すること
- セキュリティ監視基盤へのログの出力機能を有すること
- 管理コンソールでは IdP と連携した認証認可を実現すること
- ロールまたは属性ベースの権限管理を可能とすること

統合認証基盤（IdP）要件

本システムでは、統合認証基盤により一元的な ID 管理を実現し、人事システムとの自動連携、クラウドサービスとのシームレスな認証連携、パスワードレス認証の導入等により、セキュリティの向上と利便性の両立を図る。

① **基本機能**

- 標準認証プロトコル（SAML 2.0、OAuth 2.0、OpenID Connect）によるオンプレミス上のアプリケーション、クラウド上のアプリケーション（IaaS, SaaS 問わず）への SSO 機能を有すること
- セッション状態の監視・可視化機能を有すること
- セッションタイムアウト・自動ログアウト機能を有すること

② **多要素認証・パスワードレス認証機能**

- 複数の認証要素による認証機能を有し、それを強制する機能を有すること
- FIDO2（WebAuthn）による生体認証・デバイス認証機能を有し、それを強制する機能を有すること
- パスワードレス認証機能を有すること
- ユーザ自身による認証要素登録・管理機能を有すること

③ **ユーザライフサイクル管理機能**

- ADMS（ID 統合管理システム）経由での自動ユーザ作成機能を有すること
- 人事情報総合システムからの職員情報（正規職員）自動取り込み機能を有すること
- （人事情報総合システムでの未来日登録によるデータ連携が実現された場合）ユーザ情報の未来日登録が実現できること。
- 教職員・非常勤職員情報の手動配置ファイル対応機能を有すること
- 職員区分（正規職員、指導課、学務課、派遣、委託、会計年度、その他）対応機能を有すること
- 旧姓利用フラグに基づく氏名・メールアドレス自動制御機能を有すること
- 組織変更・異動に伴う自動権限変更機能を有すること
- 退職・異動時の自動アカウント無効化・削除機能を有すること
- ユーザ属性の自動同期・更新機能を有すること

④ **権限管理機能**

- ロールベースアクセス制御（RBAC）機能及び属性ベースアクセス制御（ABAC）に対応できる機能を有すること
- 最小権限原則に基づくロール設計・運用に対応できる機能を有すること
- 権限の一元管理・可視化機能を有すること

⑤ **管理機能**

- 管理コンソールでは IdP 自身と連携した認証認可を実現すること
- ロールまたは属性ベースの権限管理を可能とすること
- セキュリティ監視基盤への認証ログの出力機能を有すること

セキュリティ監視基盤要件

現行システムでは、SOC で EDR とファイアウォールの監視をそれぞれ行っているが、アイデンティティ、エンドポイント、ネットワークを横断的に監視・分析することは実施できていない状況である。本システムでは、各セキュリティ要素から収集したデータを統合分析し、AI・機械学習技術を活用した高度な脅威検知と自動化されたインシデント対応を実現することを目指す。これにより、効率的で効果的なセキュリティ運用を実現する。

① **データ処理基本機能**

- オンプレミス上のアプリケーション、クラウド上のアプリケーション（IaaS, SaaS 問わず）、SASE、IdP、エンドポイントセキュリティからのデータ取り込み機能を有すること
- オンプレミス上のアプリケーション、クラウド上のアプリケーション（IaaS, SaaS 問わず）は今後対象が増加することを想定し、多様なデータ形式・プロトコルに対応すること
- リアルタイムおよびバッチでのデータ収集機能を有すること
- データ収集の可用性・信頼性確保機能を有すること
- 異なるデータソースからのログの統一フォーマット自動変換機能を有すること、また、対応していない製品のログに関してはマニュアル操作によるログの変換が可能なこと
- 共通データモデルによる標準化機能を有すること
- データ間の相関分析・関連付け機能を有すること
- 大容量セキュリティデータの高速検索・分析機能を有すること
- 長期データ保存・アーカイブ機能を有すること
- データ保存コストの最適化を実施できること

② **高度脅威検知・分析機能**

- 既知脅威（脅威インテリジェンスの活用など）、未知脅威（機械学習技術の活用など）に対する迅速な検知機能を有すること
- 統計的手法による異常パターン検知機能を有すること
- 攻撃チェーン・キルチェーン分析機能を有すること
- 複数データソースからの相関分析機能を有すること
- 行動分析による内部脅威検知機能を有すること
- ユーザの異常行動検知機能を有すること
- ダッシュボードにて脅威情報の一元管理機能を有すること、またユーザ/権限ごとで利用可能なダッシュボードを制御可能なこと

③ **インシデント管理・対応機能**

- インシデントの自動生成・分類・優先度付け機能を有すること
- インシデント対応ワークフロー・進捗管理機能を有すること

- 対応履歴の記録・分析機能を有すること
- IdP, SASE, EDR, MDM など他のツールと連携し、検知した脅威に対する自動初期対応ができる機能を有すること
- プレイブック・ワークフローの作成・実行機能を有すること
- インシデントの調査・フォレンジック機能を有すること
- 調査結果の可視化・レポート機能を有すること
- インシデント対応チームとの連携機能（コミュニケーション機能）を有すること

④ 管理機能

- 管理コンソールでは IdP と連携した認証認可を実現すること
- ロールまたは属性ベースの権限管理を可能とすること
- 機能追加・修正は事前通知のうえ、自動で行われること

7.2 ID 統合管理システム

全庁 LAN システムにおいては、ID 統合管理システム（ADMS）が稼働し、各システムのアカウント等を一元管理している。令和5年度の ID 統合管理システム構築により、人事情報総合システムおよび総合行政システムとの ID 連携フローが見直され、NW ドライブマウント経由で取得した人事情報ファイルを取り込み、Active Directory や各種業務システムへ連携する仕組みとなっている。しかし、教職員・非常勤職員等の情報や課代表・プロジェクトメールアドレス等は人事情報総合システムから自動出力されないため、運用担当者による手動配置が必要となっており、職員の作業負荷が高い状況である。また、ID 追加・変更申請についてもワークフローが未整備であり、手作業による対応が求められている。今後は、庁内 ID 管理の統一化、クラウド認証との連携を推進し、効率性・運用性の向上を目指している。

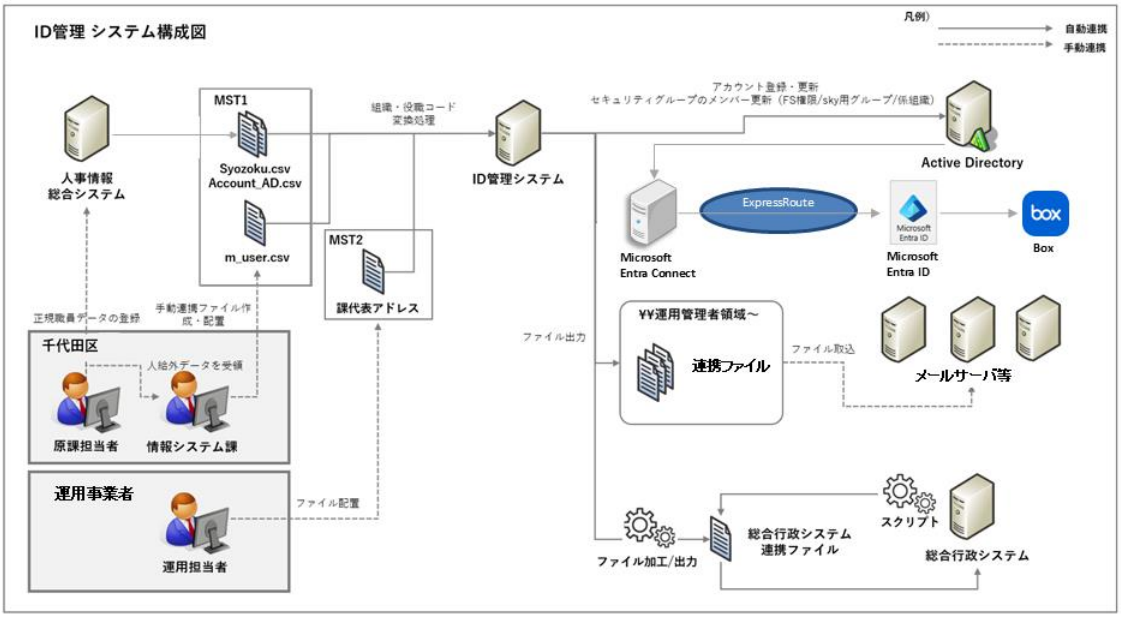
【提案に求める事項】

システム構成上の課題として、人事情報総合システムと ID 統合管理システム（ADMS）、Active Directory、Microsoft Entra ID、Box への連携は自動化されているものの、教職員・非常勤職員等の情報や課代表・プロジェクトメールアドレス等は手動配置が必要であり、ワークフローの整備が求められる。

職員の手作業に基づく課題として、各システムで不足している情報を手入力で補完しているため、作業負荷が高く、ID の新規追加や変更申請から利用管理までに時間を要している。

今後のクラウド利用促進や認証環境の統一化に向けて、庁内認証機能とクラウド認証の連携を実現する仕組みの検討が必要である

現行の ID 連携のイメージを以下に示す



7.3 全庁 LAN システム

職員が業務を行う上で利用するインターネットメール機能、ファイルサーバ（令和 8 年 4 月より Box クラウドサービスに全庁移行予定）等、インターネットアクセス機能、セキュリティ機能を有するインフラシステムの総称である。現行システムでは職員の業務端末はインターネット系であり、LGWAN へは VDI を経由してアクセスしている。現行システムではセキュリティレベルの向上を実現した一方で、異なるネットワーク間で情報のやり取りが必要となるため事務効率性・利便性の低下が発生している。

【提案に求める事項】

・「千代田区情報セキュリティポリシー対策基準」「千代田区_Web サイト構築のための対策基準」「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」及び「地方公共団体における情報セキュリティ監査に関するガイドライン」の対策基準とレベルに準拠する提案であること。

・高度なセキュリティを確保した上での事務効率性・利便性の向上を実現する環境の提供

・将来のワークスタイル、ワークプレイス変革を支援する情報環境の提供

・情報機器端末数は2000台、かつ、外部への持ち運びを重視しモバイル PC を想定している。

以下に現行のシステム機能を示す

現行システム機能概要

（1）インターネット系・LGWAN 系ネットワーク

本ネットワークで以下の機能を提供している。

（ア）電子メール（添付ファイル送付時の上長承認機能、誤送信防止機能）
（イ）仮想化共通基盤システム
（ウ）仮想デスクトップシステム
（エ）認証基盤システム（Active Directory による認証。DHCP・DNS・NTP 等）
（オ）Windows アップデート管理システム
（カ）Windows ライセンス管理システム
（キ）ID 統合管理システム（アカウント等の一元管理）
（ク）シングルサインオンシステム
（ケ）統合ストレージシステム
（コ）ファイル管理システム
（サ）バックアップシステム
（シ）WEB 閲覧用システム（外部 Web 閲覧用プロキシ。ウイルス対策・URL フィルタ）
（ス）プロキシパック公開システム
（セ）クラウドプロキシ（Ms365 接続用負荷分散装置）
（ソ）クラウド認証基盤システム（Ms365 接続時の認証・認可を実施）
（タ）コミュニケーション基盤システム（Ms365）
（チ）大容量ファイル送受信システム
（ツ）ウイルス対策システム
（テ）振る舞い検知システム（EDR）
（ト）ネットワークセキュリティシステム（ネットワーク各系間の通信制御・脅威対策を提供）
（ナ）PC 管理システム（資産管理・ログ収集管理・デバイス管理により利用状況/アクセス状況を把握）
（ニ）ログ管理・解析システム
（ヌ）監視システム（サーバ/ネットワーク機器/仮想基盤の監視・予兆/障害検知・通知）
（ネ）ネットワークシステム（高可用・セキュアなネットワークを提供）
（ノ）認証印刷システム（IC カード認証により印刷/コピー/ファクス/スキャンを制御し情報漏えい防止）
（ハ）遠隔保守環境（運用/他事業者がフレッツ網等を介して遠隔保守可能な環境）
（ヒ）音声系システム（本庁舎の IP 電話、コールセンター中継台、無線 LAN 内線、庁外施設・都防災無線との接続）
（フ）コールセンターシステム（区民問合せの応対履歴管理と公開 FAQ 管理）
（ヘ）サービスデスクシステム（問合せ管理のための運用管理ツール）
（ホ）インターネット系・LGWAN 系ネットワークに接続する主な各課システムを以下に示す
以下の各課等システムの接続インタフェース
・LGWAN システム（LGWAN-ASP システムを含む）
・総合行政システム（財務会計・文書管理・電子決裁）

・人事情報総合システム
・勤怠管理システム
・図書館システム
・防災無線(都)システム
・会館施設予約システム
・人材情報システム
・全国瞬時警報システム(J-ALERT)

(2) 個人番号利用事務系ネットワーク

個人番号利用事務系ネットワークに接続する主な各課システムを以下に示す。

(ア)総合住民情報システム
(イ)住民基本台帳ネットワークシステム
(ウ)戸籍統合システム
(エ)生活保護システム
(オ)手当・医療助成システム
(カ)保育事務システム
(キ)後期高齢者システム
(ク)画像レセプトシステム
(ケ)滞納整理支援システム
(コ)高齢者・相談支援システム
(サ)情報提供ネットワークシステム
(シ)ガバメントクラウドへの接続

7.4 IP 電話システム

現行の IP 電話システムはハードウェアフォンによる有線接続・スマートフォン内線電話で利用しているため人事異動時にサーバ設定、ハードウェアフォン設定等が必要となり、迅速な対応が困難な状況である。また現行システムでは庁内のみ発着信が可能であるため外出時、在宅勤務時の連絡手段として利用できず円滑なコミュニケーションに支障をきたしている。
次期システムでは、柔軟な拡張性と利便性の向上に加え、激甚災害やパンデミック等を想定した BCP 対策として、クラウドサービスの活用も視野に入れ検討を進めている。

【提案に求める事項】
・高品質かつ迅速に住民対応ができる電話環境の提供
・庁舎の電話番号を使用し、どこでも業務継続が可能な電話環境の提供
・電話帳等の管理が、組織階層型(ツリー表示)で表示される機能の提供
・1 つの電話番号で固定電話、業務端末(全庁 LAN 端末)、スマートフォン(BYOD)等で同時鳴

動可能な機能の提供

・IP 電話システムの無線化対応（BYOD も含めた検討）、無線利用環境から LTE 等の移動通信システムへの切り替わり時も通話が継続可能な機能の提供

・業務継続性の観点から本庁舎に中継器等を置きクラウドサービスのみを利用するシステムモデルは原則として想定していない。

・出張所等の外部拠点は個別に PBX を導入しビジネスフォンを利用している。現行システムでは VoIP ゲートウェイ（責任分界点）を提供し、外部拠点 PBX と接続し外線内線の利用及び転送を可能

No	激甚災害（パンデミック含む）のリスク	検討案
1	災害時に庁舎に登庁できない	テレワーク環境からも外線・内線の受発信を行う
2	災害時に通信設備の被災リスクへの対策	本庁舎が被災した際でも、区の電話機能を維持する
3	災害時に増大するコールへの対策	増大するコールへの柔軟なスケール変更対応

以下に現行システムの機能を示す

(1) 番号計画

既存の番号計画を踏襲する

(2) 内線番号計画

既存の内線番号計画を踏襲する

(3) 時間外切替機能

代表番号、コールセンター番号の切替時間と着信先の切り替えを行う

(4) 発着信制限機能

以下のサービスクラスを定義し、発信制限および着信制限を行う

サービスクラス

サービスクラス	国際発信	国内発信	内線発信	内線着信
一般（国際可）	○	○	○	○
一般（国際不可）	×	○	○	○
オペレータ	×	○	○	○
内線のみ	×	×	○	○

(5) 発信規制機能

本システムでは特定の番号に対し、発信制限を行う

(6) 内線グループ計画

本システムのサーバでは機能ごとにグループを作成し、そのグループに内線端末を所属させることによって各種グループサービスを提供する。

(ア) パーク保留グループ

パーク保留の範囲を管理するグループ、部署ごとにパーク保留グループを作成する。

(イ) 呼出グループ

外線番号着信時に呼び出すグループ。ダイヤルイン番号ごとにグループを作成する。

(ウ) ピックアップグループ

代理応答の範囲を管理するグループ。部署ごとにピックアップグループを作成する。

(7) 端末設計

本システムで使用する端末はハードウェア、ソフトウェアの両方を検討している。
利便性向上、クラウドサービス利用、災害時のリスク等を踏まえて提案を行うこと。

(8) 緊急通報機能

本システムにおいて、緊急通報(110 番、119 番等)を確実に発信できる機能を有すること。以下の要件を満たすこと。

(ア)発信機能

・緊急通報番号への発信が可能であること。

・発信時に優先制御を行い、他の通話に影響されないこと。

(イ)発信者情報通知

・通報先に対し、発信元の電話番号または識別情報を通知できること。

・必要に応じて、発信元の所在地情報を付加できること。

(ウ)通報経路の冗長化

・ネットワーク障害時に備え、緊急通報が可能な代替経路を確保すること。

(エ)通報記録

・緊急通報の発信日時、発信者、通報先をログとして記録し、一定期間保持できること。

(オ)運用手順

・緊急通報に関する操作手順を利用者向けに明示し、教育資料を提供すること。

(9) 通話録音機能

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。

(ア)録音告知ガイダンス(「この通話は録音されます」等)を設定できる機能を備えること。

(イ)録音データは、暗号化された状態で保存し、一定期間保持できること。

(ウ)録音データの検索・再生・ダウンロードが可能であり、権限管理により利用者を制御できること。

(オ)障害時に備え、録音機能の冗長化またはバックアップ手段を確保すること。

7.5 コールセンターシステム

現行のコールセンターシステムは本庁舎にオンプレミス型で設置されており、コールセンター執務室も本庁舎にあるため、臨時業務用のコールセンター機能の拡充に柔軟に対処できていない課題がある。また将来的に時間外対応やFAQの仕組みについても改善を検討していく。

【提案に求める事項】

・迅速に住民対応できるコールセンター環境の提供

・IP 電話システムと連携し区民と迅速にコミュニケーションが取れる環境の提供

・臨時業務用のコールセンター機能の拡充に柔軟に対処できる環境の提供

(例)コロナ対応コールセンター、ワクチン接種コールセンター等

・IP 電話システムとコールセンターシステム統合によるコスト削減

・激甚災害時(パンデミック含む)の以下のリスクへの対策

No	激甚災害(パンデミック含む)のリスク	検討案
1	災害時に庁舎に出社できない	外部環境からでも適切なセキュリティを確保し、代表番号、外線・内線の受発信を行う
2	災害時に通信設備の被災リスクへの対策	
3	災害時に増大するコールへの対策	増大するコールへの柔軟なスケール変更対応

以下に現行システムの機能を示す

(1) FAQ 及び対応履歴機能システム

区民からの電話、メールでの問い合わせの履歴管理、および区民に公開する FAQ の管理を行うためのシステムである。

(2) PC 中継台システム

区役所 5 階オペレーションルームに着信する「大代表」「コールセンター」「緊急通報」「都区間内線」

「一般内線」の電話取次業務を行うシステム

【クラウドサービス利用の検討】

現行コールセンターシステムはオンプレミスにて本庁舎に設置し、本庁舎にてコールセンター業務を行っているが、コールセンター機能の拡張に柔軟に対応するためクラウドサービスの利用も検討している。

(1) MCS 機能

(ア) FAQ 管理機能

コールセンターの問い合わせから作成した FAQ を管理する

(イ) FAQ データの同期

区民向けに FAQ を公開しているサーバ上に、FAQ データを同期

(ウ) 対応履歴の CSV 出力

コールセンターにて登録された対応履歴を出力する機能

(2) FAQ 管理ツール

(ア) スケジュールの登録・参照

(イ) FAQ 投入用の CSV 作成

(3) ファイル共有機能

コールセンターのスーパーバイザーオペレータが利用するクライアント端末上の OS ユーザが書き込み権限をもつ、共有フォルダを提供する機能

(4) 対応履歴管理

コールセンターの対応内容の履歴管理を提供する機能

(5) メール送受信

本区のドメイン「city.chiyoda.lg.jp」のメールアドレスにてメールの送受信が行える機能

7.6 個別システム対応

庁内には、総合住民情報システムを含めて約 100 の個別システムがあり全庁ネットワーク上で稼働している。個人番号利用事務系、LGWAN 接続系、インターネット接続系の各ネットワーク上に存在している。

（詳細は要求水準書別紙_個別システム一覧を参照）

【提案に求める事項】

・全庁 LAN システムの再構築にあたり、全庁ネットワーク上で稼働している個別システムも含めた全体移行計画の提案を行うこと。

・個別システムの移行は令和9年度予算で実施する計画であるため、個別システムの移行期間は令和9年4月～令和9年12月までとする。
・業務に影響をあたえないよう配慮した移行計画の提案を行うこと。

7.7 既存機器の活用

・無線 AP については、既存機器のリース期間が残っているため、有効活用方法を提案すること。
（詳細は要求水準書別紙_既存無線 AP 一覧を参照）

【提案に求める事項】
・既存機器を有効活用した最適なシステム設計の提案を行うこと

7.8 自治体セキュリティクラウド提供予定機能

令和9年度1月に次期自治体セキュリティクラウドの構築が行われる予定であるが、現時点で、提供される機能の詳細は決定していない。

【提案に求める事項】
今後、動向を見据え、本業務に提案するシステム機能と自治体セキュリティクラウド機能を組み合わせて最適なシステム設計の提案を行うこと。
以下は令和9年度以降に東京都セキュリティクラウドで提供を検討している機能の一覧である。

No	区分	定義
1	監視	・Web サーバ
2		・メールリレーサーバ
3		・プロキシサーバ
4		・外部DNSサービス （IP-VPN 回線の場合のみ）
5	ゲートウェイ	・ファイアウォール
6		・IDS／IPS
7		・マルウェア対策
8		・URLフィルタ
9		・DDoS対策
10	メールセキュリティ対策	・アンチウイルス／スパム対策
11		・振舞い検知
12	Web サーバセキュリティ対策	・WAF
13		・CDN

14	SOC 運用サービス	・ログ収集、分析
15		・イベント監視
16		・マネージドセキュリティサービス
17	対応と復旧	・システム、サービス構成管理
18		・脆弱性情報の入手と対応
19		・障害管理（問題管理、変更管理、復旧対応）
20		・バックアップとリストア
21		・ヘルプデスク機能
22		・定例会等の運営
23		・セキュリティレベルの自己点検
24	情報連携システム	・インシデント管理
25		・情報提供
26		・資料提供
27		・稼働状況
28	回線	・セキュリティクラウド～インターネット網間に回線を提要
29		・セキュリティクラウド～IP-PVN 網間に IP-VPN 接続回線を提供する

7.9 ゼロトラストモデルにおけるセキュリティ運用

次期システムでは、インターネットを活用するシステムモデル（β´モデル）をさらに発展させ、ゼロトラストモデルへの移行を検討している。この移行にあたっては、セキュリティ運用体制の強化が最重要課題であると考えている。IT 技術は区の業務に不可欠な社会インフラとなっており、本区ではクラウドサービスの利用も積極的に推進している。一方で、攻撃者は効率的な攻撃ツールの開発や AI を利用した攻撃など、巧妙かつ多様な攻撃を行っている。区の情報資産を適切に守るためには、平常時にインシデントを未然に防ぐ取り組みと、発生時に迅速かつ適切に対応できる体制の両立が不可欠と考えている。

【提案に求める事項】

・本システムを運用してく上で発生すると想定されるインシデント（Incident）をインシデント影響レベル別に定義（三段階以上のレベルに定義することが望ましい）し、影響レベルごとのセキュリティ運用体制で実現可能な機能の提案を行うこと。

・セキュリティ運用体制の提案には定義した各インシデントの影響レベルに対し、自治体セキュリティクラウドが提供する機能、提案するシステム機能をどのように組み合わせて対応するのかを説明し提案を行うこと、またインシデントの影響レベルの対応が NIST（米国国立標準技術研究所）サイバーセキュリティフレームワーク（NIST CSF）に定義されている「識別（Identify）」「防

御（Protect）」「検知（Detect））「対応（Respond）」「復旧（Recover）」のどのフェーズに該当するかを記載すること。

7.10　セキュアプリント

印刷管理をクラウドサービスとして利用し、ゼロトラスト環境におけるセキュアな複合機運用を実現することで、セキュリティを確保しつつ複合機の利便性を向上させる。

・今回導入する SASE 経由で通信できること。
・特定の接続元からのみ通信を許可できること。
・サービスに接続する複合機のインベントリが管理できること。
・庁内の印刷データおよびスキャンデータを一元的に管理できること。
・本システムの統合認証基盤（IdP）の認証情報を利用して、認証を行えること。
・ユーザ毎に利用権限が設定できること。
・印刷データおよびスキャンデータは暗号化されること。
・印刷データおよびスキャンデータは一定期間経過（8時間）後に自動的に削除されること。
・スキャンデータは既存の Box と連携可能であること。
・スキャンデータは承認された宛先のみに保存（送信）可能であること。
・転送データは暗号化され、保護されること。
・ログ（監査ログ、サービスからの主力ログ）を収集し、関連するシステム（監視システムや分析システム）へ連携（送信）できること。
・管理者権限を持つユーザのみが複合機の設定を変更可能であること。
・インシデントが発生した場合、復旧後にインシデント発生前に登録されたデータを復元できること。
・通常と異なる印刷パターンの検出が行え、それを監視システムへ連携できること。また、異常を検知した場合、利用などを抑止できること。

7.11　VDI（LGWAN 系）

LGWAN に接続された情報システム及びその情報システムで取り扱うデータへのアクセスに専用の VDI を利用し、場所を問わない安全なアクセスと情報資産の保護を実現する。

・特定の接続元からのみ通信を許可できること。
・本システムの統合認証基盤（IdP）の認証情報を利用して、認証を行えること。
・ライフサイクルポリシーにより、保持期間を超過したデータを自動削除ができること。
・承認された端末からのみのアクセスを制限することができること。
・ウイルス対策ソリューションによるウイルス感染の検知が可能であること。
・VDI に接続する PC 機器に接続する周辺機器やデバイスの使用が制御できること。

・転送データは暗号化され、保護されること。
・ログ（監査ログ、サービスからの主力ログ）を収集し、関連するシステム（監視システムや分析システム）へ連携（送信）できること。
・ポリシーを利用して、自動ブロックによるアクセスの遮断ができること。
・保持ポリシーとバージョン履歴機能により、破損または削除されたファイルが復元できること。
・スクリーンショット機能を無効化できること。
・クリップボードを通じたデータのコピーを制限できること。
・ファイルの格納先を限定できること。（Box 等の SaaS を想定）
・VDI は、ガバメントクラウドと同等のセキュリティ対策がなされた安全な環境に構築すること。

7.12　VDI（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータへのアクセスとして、個人番号利用事務に専用の VDI を利用し、場所を問わない安全なアクセスと情報資産の保護を実現する。

・特定の接続元からのみ通信を許可できること。
・本システムの統合認証基盤（IdP）の認証情報を利用して、認証を行えること。
・ライフサイクルポリシーにより、保持期間を超過したデータを自動削除ができること。
・承認された端末からのみのアクセスを制限することができること。
・ウイルス対策ソリューションによるウイルス感染の検知が可能であること。
・VDI に接続する PC 機器に接続する周辺機器やデバイスの使用が制御できること。
・転送データは暗号化され、保護されること。
・ログ（監査ログ、サービスからの主力ログ）を収集し、関連するシステム（監視システムや分析システム）へ連携（送信）できること。
・ポリシーを利用して、自動ブロックによるアクセスの遮断ができること。
・保持ポリシーとバージョン履歴機能により、破損または削除されたファイルが復元できること。
・スクリーンショット機能を無効化できること。
・クリップボードを通じたデータのコピーを制限できること。
・ファイルの格納先を限定できること。（ガバメントクラウド上のオブジェクトストレージを想定）
・VDI は、ガバメントクラウドと同等のセキュリティ対策がなされた安全な環境に構築すること。
・VDI 環境への接続回線は、閉域構成を取るなどして安全な NW 環境を構築すること。

7.13　業務端末

セキュリティ機能を備えた業務端末を導入し、本システムにおける情報漏洩リスクを予防しつつ業務効率向上を実現する。

・生体認証、カードリーダー、トークンなどの多要素認証が利用できること。
・BIOS やストレージのアクセス権限を設定できること。
・盗難/紛失時に端末の電源がオフの状態でも遠隔操作でストレージのデータを消去できること。
・端末の廃棄時に端末のデータを復元不能な状態にできること。
・ショルダーハッキング対策として、のぞき見防止フィルタが貼付できる、またはプライバシースクリーン機能が利用できること。
・盗難防止用ロックが取付可能であること。
・盗難または紛失した際に位置情報を利用したデバイスの検索ができること。
・PC のファームウェアに対して NIST SP 800-193 に準拠したセキュリティ対策が実装されていること。

7.14　ガバメントクラウドへの接続

本区は令和 8 年 1 月よりガバメントクラウドの利用を開始している。
本システムのネットワーク更改にあたり、ガバメントクラウド（政府共通クラウド基盤）への接続については、以下の要件を満たすこと。

1. 接続方式

ガバメントクラウドへの接続は、既存の AWS Direct Connect の専用線接続サービスを継続利用し、閉域網による安全な通信経路を確保すること。

2. セキュリティ要件

通信経路は、強度の高い暗号化（例：AES 256、TLS 1.2 以上）を適用し、第三者による盗聴・改ざんを防止すること。
ファイアウォール等のセキュリティ機器を経由し、アクセス制御・通信監視・ログ取得を徹底すること。
ガバメントクラウド接続用ネットワークセグメントは、他の業務系ネットワークと論理的に分離し、不要な通信を遮断すること。
アクセス元端末にはウイルス対策・端末認証・証明書管理等のセキュリティ対策を実施すること。

3. 可用性・運用要件

ガバメントクラウドへ接続する庁内通信回線は冗長構成とし、障害発生時にも業務継続が可

能な設計とすること。
通信品質(帯域・遅延等)は、ガバメントクラウド上の業務要件を満たす十分な性能を確保すること、監視体制を構築し、障害・インシデント発生時には迅速な対応が可能な運用体制とすること。

4. 準拠・遵守事項

総務省「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」および「ガバメントクラウド利用に係る技術要件」等、関連する法令・ガイドラインに準拠すること。
ガバメントクラウド事業者の仕様変更や新たなガイドライン発行時には、速やかに対応策を検討・実施すること。

5. 参考情報(ガバメントクラウド接続状況について)

本区は、ガバメントクラウドへの接続を既に完了しており、標準化対象システムについては全て AWS(Amazon Web Services)環境を利用している。
ガバメントクラウドへの接続は、閉域網専用線(AWS Direct Connect)を活用し、セキュリティ・可用性を確保した構成となっている。
今後のネットワーク更改においても、現行の AWS 環境を前提とし、既存の閉域網接続を維持・最適化することを基本方針とします。

8. 非機能要件

全庁 LAN システムの非機能要件はつぎの通り。
なお、非機能項目の番号は、地方公共団体情報システム非機能要件の標準【第 1.2 版】(非機能要求グレード活用シート)の項番である。

8.1 可用性

「継続性」、「耐障害性」、「災害対策」、「回復性」を考慮し、システムを継続的に利用可能とすること。

項目	要求レベル	非機能項目	備考
RPO(目標復旧地点)	1 営業日前の時点	A.1.3.1	日次バックアップからの復旧
RTO(目標復旧時間)	12 時間以内	A.1.3.2	窓口対応等の重要機能を優先復旧
RLO(目標復旧レベル)	全システム機能の復旧	A.1.3.3	各ソリューションの復旧方針に準拠
システム再開目標(災害時)	1 日以内に再開	A.1.4.1	各ソリューションの復旧方針に準拠
稼働率	99.9%	A.1.5.1	年間累計停止時間 2.9 時間以内
災害対策復旧方針	同一構成で再構築	A.3.1.1	クラウドの地理的冗長性を活用

8.2 性能・拡張性

「業務処理量」、「性能目標値」、「リソース拡張性」、「性能品質保証」を考慮し、システムでの業務処理を通して全体の性能を把握し、将来的なシステム拡張も視野に入れた構成を検討すること。

項目	要求レベル	非機能項目	備考
ユーザ数	契約後別途協議	B.1.1.1	-
同時アクセス数	契約後別途協議	B.1.1.2	-
データ量	契約後別途協議	B.1.1.3	-
オンラインリクエスト数	契約後別途協議	B.1.1.4	-
バッチ処理件数	契約後別途協議	B.1.1.5	-
通常時レスポンス	3 秒以内	B.2.1.4	主要な処理に適用
集中時レスポンス	5 秒以内	B.2.1.5	ピーク時の主要処理に適用
バッチ処理レスポンス	再実行の余裕確保	B.2.2.1 B.2.2.2	通常時・集中時共通

8.3 運用・保守性

「通常運用」、「保守運用」、「障害時運用」を考慮し、その実現のための「体制」や「運用管理方針」などの構成を検討し、安定稼働を可能とすること。

項目	要求レベル	非機能項目	備考
運用時間	24 時間 365 日	C.1.1.1 C.1.1.2	平日・休日共通
マニュアル	通常・保守運用マニュアル提供	C.4.3.1	オンラインドキュメント等含む
外部システム接続	他システムと接続	C.4.5.1	千代田区様他システムとの連携
保守契約	アップデート含む	C.5.2.2	常に最新版を提供
監視情報レベル	リソース監視まで実施	C.1.3.1	死活・エラー・リソース監視
定期報告会	月 1 回	C.5.9.1	障害等報告に関し定例報告
報告内容レベル	障害等報告に加え改善提案含む	C.5.9.2	SOC レポート、性能レポート
問い合わせ窓口	ヘルプデスク	C.6.2.1	重要度に応じた初回応答時間
構成管理	構成管理を実施	C.6.5.1	-
変更管理	変更管理を実施	C.6.6.1	-

項目	要求レベル	非機能項目	備考
リリース管理	リリース管理を実施	C.6.7.1	-

8.4 移行性

「移行時期」、「移行方式」、「移行対象（機器）」、「移行対象（データ）」、「移行計画」を明確に正確にスムーズな移行を可能とすること。

項目	要求レベル	非機能項目	備考
システム停止可能時間	夜間等の利用が少ない時間帯	D.1.1.2	業務影響最小化
作業分担	ユーザ・ベンダー共同実施	D.5.1.1	運用保守時の役割分担参照

8.5 セキュリティ

「アクセス、利用制限」、「データの秘匿」、「不正追跡・監視」等の機能を組み合わせ、「ネットワーク対策」、「マルウェア対策」、「web 対策」、「セキュリティインシデント対応/復旧」を考慮し、かつ千代田区情報セキュリティポリシーに準拠し、本対象システムの安全性の確保をすること。

項目	要求レベル	非機能項目	備考
管理者認証	多要素認証	E.5.1.1	複数回、異なる方式
操作制限	最小権限の原則	E.5.2.1	必要最小限のアクセスのみ許可
伝送データ暗号化	全データ暗号化	E.6.1.1	CRYPTREC 暗号リスト準拠
蓄積データ暗号化	全データ暗号化	E.6.1.2	CRYPTREC 暗号リスト準拠
ログ取得	必要なログを取得	E.7.1.1	ログイン履歴、操作ログ等
監視対象	システム全体	E.7.1.3	ゼロトラスト原則適用
Web 対策	セキュア対策強化	E.10.1.1	セキュアコーディング等

8.6 システム環境・エコロジー

「システム制約条件」、「システム特性」、「適合規格」、「機材設置環境条件」、「環境マネージメント」を考慮し、システムの利用者数や拠点、製品の安全性や環境負荷を抑えるような取り組みをすること。

項目	要求レベル	非機能項目	備考
構築・運用時制約	制約となる庁内基準や法令、条例等	F.1.1.1 F.1.1.2	千代田区セキュリティポリシー、個人情報の保護に関する法律、行政手続

			における特定の個人を識別するための番号の利用等に関する法律　等

9. データセンター要件

9.1 立地要件

（1） 立地要件

- データセンターは、活断層上等の地震被害が発生しやすい地域に立地されていないこと。
- データセンターが建設されている自治体の液状化予測において、液状化発生危険度が低いと評価される区域であること。

（2） 交通アクセス要件

- データセンターまで複数のアクセスルートがあり、有事に孤立する危険性が低いこと。

9.2 建物要件

（1） 耐震構造要件

- データセンターは、1981 年 6 月改正の建築基準法に準拠しており、かつ、耐震性能は東日本大震災級（震度7）の地震による倒壊、崩壊を避ける耐震性能を有していること。
- 鉄骨鉄筋コンクリート造であり、免震構造であること。

（2） 火災対策要件

- データセンターの周囲半径 100 メートル以内に消防法による指定数量以上の危険物製造設備、火薬製造設備、高圧ガス設備がないこと。
- 建築基準法の耐火建築基準・消防法に規定する耐火性能に適合していること。
- データセンターには、火災発生時の消火活動に必要となる消火器、消火栓が設置されていること。

（3） 風水害対策要件

- 津波、高潮、集中豪雨等による出水の被害から、建物及び情報システム等を保護する構造となっていること。

（4） 落雷対策要件

- 雷サージによりネットワークに誘起された異常電圧から情報システム及び電源設備を防護するため、避雷設備及び新接地方式による接地システムが設置されていること。

9.3 建物設備等に係る要件

（1） 電源設備

① 電源室

・電源室はサーバ設置専用室とは独立した部屋にあり、保守管理のためにサーバ設置専用室に立ち入ることがないこと。

② 非常用電源設備

・自家用発電機が用意されており、燃料無補給で1日以上本区の業務継続が可能であること。また、備蓄量を超える継続運転が必要となった場合は、燃料を補給し、運転を継続できることが契約等により保証されていること。

③ 無停電電源装置

・情報システム機器を安定稼動させるため、無停電電源装置(UPS)を設置していること。

・法定点検、工事等によりビル内電力供給が停止している間も機器類を停止することのないこと。

・自家用発電機が動作するまで、蓄電池による 10 分以上の給電が可能であること。

④ 緊急手段

・非常用電源設備が万が一故障した際でも、移動電源車の駆けつけ等、バックアップ体制が契約等により保証されていること。

(2) 空調設備

① 専用性

・サーバ設置専用室の温湿度制御を的確に行うため、空調設備は他の部屋との共用は避け、サーバ設置専用室専用となっていること。

空調能力

・設置機器の増加等に伴う発熱量の増加に対応し、サーバ設置専用室の温湿度を適切に調整する十分な容量の空調設備が確保されていること。

② 温湿度環境

・サーバ設置専用室内の湿温度環境は、温度 20～30℃、湿度 70%以下とすること。

③ 空調予備機

・障害等の発生に備え、サーバ設置専用室の主要な空調設備機器については予備器が設置されており、主要機器が故障の場合でも必要な冷却能力を確保できること。

9.4 サーバ設置専用室に係る要件

(1) 出入口

- 出入口扉は、十分な強度を持つ防火扉等となっていること。
- 履物を区別し、静電靴により静電気・埃対策がされていること。

(2) フロア構造

- 床構造はフリーアクセスフロアとし、ケーブル敷設と空調気流スペースを十分に確保した有効床下スペースであること。
- フリーアクセスフロアの荷重強度が十分にあること。

(3)　天井高

・　必要な温湿度環境を維持するため、フリーアクセスフロア面から天井面まで、十分な高さが確保されていること。

(4)　内装

・　サーバ設置専用室の内装は、不燃材料を使用していること。

(5)　外光対策

・　サーバ設置専用室は、外光の影響を受けない措置が講じられていること。

(6)　防火・火災対策

・　高感度火災検知システム導入または、煙感知器と熱感知器を併用した自動火災報知設備が設置されていること。
・　火災発生時の消火方式としては、水による消火方式は避け、人体への影響が少ない新ガス系消火設備を設置していること。

(7)　漏水・防水対策

・　漏水による情報システム機器への悪影響を防止するため、サーバ設置専用室内には水を使用する設備を設置していないこと。
・　漏水等の恐れのある空調機排水廻り等に漏水検知システムを設置すること。

9.5 セキュリティに係る要件

(1)　監視

・　建物の出入口は、24 時間監視されていること。
・　出入口及び室内は、監視カメラによる 24 時間常時監視がなされていること。

(2)　防犯装置等

・　建物への入退館について、セキュリティ装置により予め設定された入退館資格の識別及び記録、保管を行っていること。
・　入退室については、施錠等の防犯対策を有していること。
・　入退室に当たり、IC カードや生体認証装置により、予め設定された入退室資格の識別及び記録を行っていること。

10. 運用保守要件

10.1　運用保守業務に関する要件

運用保守業務の遂行にあたっては、ITIL（Information Technology Infrastructure Library）や ISO/IEC 20000 等、最新の IT サービスマネジメントのベストプラクティスを参照し、ガバナンス・セキュリティ・効率性・自動化を重視した運用を実施すること。

運用保守業務全体を統括する責任者（サービスマネージャー等）を配置し、24 時間 365 日体制での監視・障害対応・インシデント管理・変更管理・構成管理等を含め、迅速かつ確実な運用体制を構築すること。

運用・保守設計に基づく設計書を作成し、運用実施手順・ルール・エスカレーションフロー等を標準化し、運用保守マニュアル・ナレッジベースとして整備・維持管理すること。

運用保守要件に基づき検討・整理した内容（設計書・運用手順・報告書・改善提案等）は、定期的に本区担当職員へ提示し、必要に応じて協議し承認を得ること。

DX 推進やクラウド活用、ゼロトラストセキュリティ等、最新の技術動向・法令・ガイドラインに適合した運用保守体制とし、継続的な改善（運用自動化、AI 活用等）を図ること。

10.2　運用保守時の役割分担

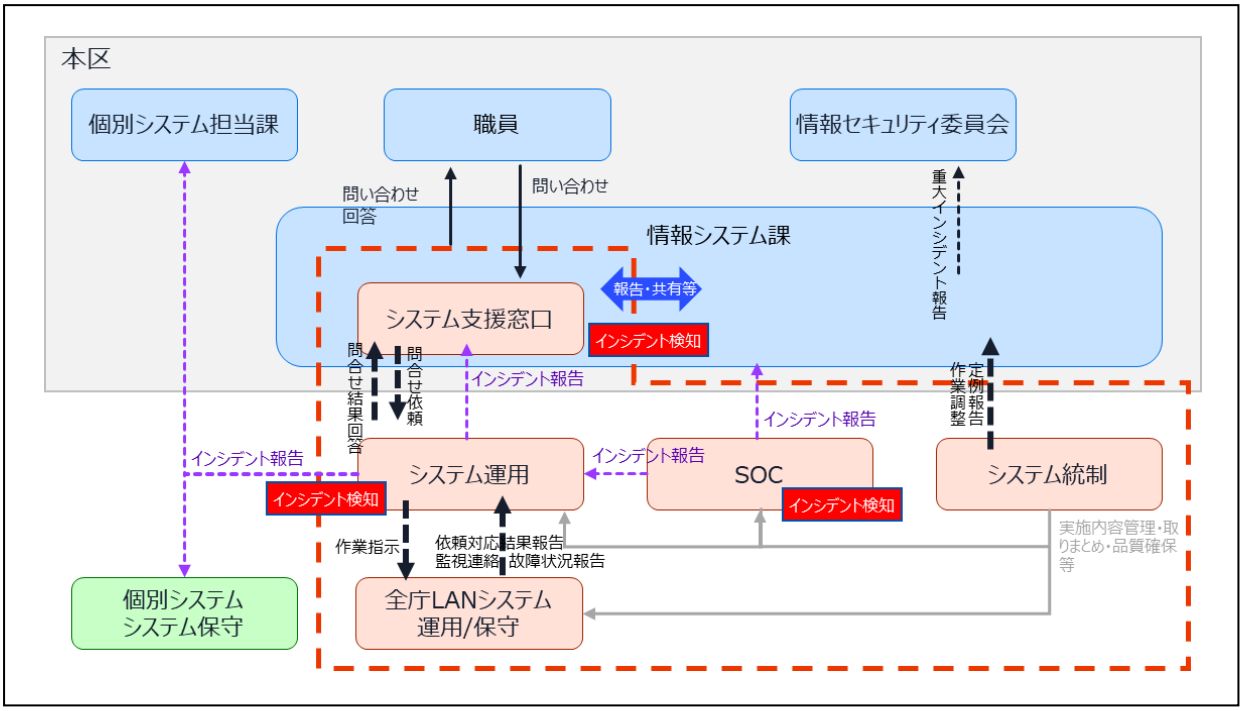
運用保守業務の実施体制は、以下を想定している。

運用保守時の役割分担

区分	名称	主な役割
受託者	システム支援窓口	・ 全庁 LAN に関する各種問い合わせ等を業務時間（原則平日 8:30～17:15）に、本区担当職員とともに受け付ける。 ・ 本区担当職員の支援として、問い合わせ内容の分析、関係者への依頼、インシデント発生状況確認、システム運用、SOC、システム統括、各システム保守とのやり取りの窓口として活動する。 ・ インシデント発生時は、システムの稼働状況を速やかに確認・把握し、本区担当職員へ連絡等を実施する。 ・ 本区担当職員との緊密な連携が必要となるため、常駐等すぐに連絡・対応が取れる体制とする。
受託者	システム運用	・ NOC（ネットワークオペレーションセンター）として、システムの稼働状況とセキュリティを 24 時間 365 日体制で監視し、障害やサイバー攻撃の予兆を早期に検知する ・ インシデント発生時は、内容を分析・把握を行う。 ・ インシデントが個別システムに関連する場合は、システム支援窓口、本区担当職員、該当の個別システム担当課及び該当の個別システム保守事業者に連絡を行う。 ・ 業務影響が発生している場合は原因特定と迅速な復旧対応を行い、影響範囲確認、関係者連絡、応急処置による業務継続確保を実施。 ・ インシデントの重要度・緊急度に応じた優先順位付け、

区分	名称	主な役割
		エスカレーション実行、復旧状況報告、対応履歴の一元管理により、システムの安定稼働の維持を図る。 ・ SOC（セキュリティ・オペレーション・センター）、システム統括と連携し、システム支援窓口に必要な情報等を提供する。
受託者	SOC	・ 専門ツールで 24 時間 365 日セキュリティを監視・分析する ・ セキュリティインシデント検知時は脅威を分析し、本区担当職員、システム支援窓口及びシステム運用へ報告する。 ・ 必要に応じてシステム運用・システム統括へ対応等を指示する。 ・ 最新の脅威情報や監視状況を定期的（月次等）に報告する。
受託者	システム統括	・ 運用保守計画を策定すると共に、定期報告や実績分析に基づいた継続的な業務改善を推進する。 ・ システムのライフサイクル全体を見据え、計画的かつ安定的なサービス提供を実現し、その品質を維持・向上させる司令塔としての役割を担う。 ・ システムの変更管理・構成管理・ドキュメント保守を一元的に行い、IT ガバナンスを徹底する。 ・ システム運用が実施する作業内容や連絡手順の整備や改善等を実施する。
受託者	全庁 LAN システム運用保守	・ 庁舎内設備や全庁 LAN システムを構成する機器等（サービス利用含む）の運用・保守を実施する。
千代田区	政策経営部 情報システム課 （本区担当職員）	・ 全庁 LAN システムの維持管理、千代田区職員から全庁 LAN や端末に関する対応を行う。 ・ 区（教育委員会、委託事業者、指定管理者を含む）全体の情報セキュリティに関する統一窓口（CSIRT としての対応を含む）となる。
千代田区	職員	・ 全庁 LAN を利用して業務を実施する職員
千代田区	個別システム担当課	・ 全庁 LAN 以外の個別業務システムを維持管理する課（職員含む）
外部関係者	個別システム保守事業者	・ 担当システムの安定した稼働を維持するため、定期的なメンテナンス・アップデート・不具合修正を実施する ・ 担当システムに関係するインシデントが発生した場合は、システム運用等からの連絡を受けて対処・対応を行う。

運用保守体制



10.3　運用計画

運用保守を実施するために、運用計画として以下の内容を実施すること。

運用保守計画

運用・保守の設計で検討した内容を踏まえて、以下の要件が含まれる形で運用保守計画書の確定版を作成すること。

① **作業概要**

- 監視、運用・保守作業の対象範囲、管理対象、作業概要等を記載すること。

② **作業体制に関する事項**

- 運用・保守業務を実施するための体制について、管理体制図、本件受託者の要員（責任者、作業者、役割分担）、連絡手段等について記載し、全体的な運用管理体制を明確にすること。

③ **スケジュールに関する事項**

- プロジェクト計画書及び本要求水準書に基づき、運用・保守を行う上で基本とする作業内容、関係するほかの作業工程、そのスケジュール等について記載すること。
- 日次、週次、月次等の定型的な業務について、作業内容を記載すること。また、複数回発生した非定型業務の報告及びその定形業務化（手順書の作成等）の提案を含めること。

・　年次の作業内容には、運用業務の中で発生した運用上の課題、作業量の多い作業等について整理報告し、その改善（例えば自動化等）の提案を行う作業、システム運用継続計画の見直し作業、運用保守計画書の見直し作業を含めること。

④　成果物に関する事項

・　運用・保守業務にて納品する成果物の内容、担当者、納品期限、納品方法、納品部数等について記載する。

⑤　運用・保守形態、環境等

・　運用において採用する運用形態（オンサイト、リモート等）、運用にて利用する環境（本番環境、検証環境、研修用の環境等の有無）等を記載すること。

⑥　管理対象

・　受託者は本業務で開発する【次期リプレース対象のシステム】及びドキュメントについて保守を行うこと。

⑦　クラウドサービスの利用

・　運用作業、運用手順及び運用管理用のソフトウェアも含め、可能な限り統一化を図るとともに、自動化された機能及びクラウドサービスが提供する機能等を利用し、運用に係る役務を可能な限り効率化すること。

・　利用しているクラウドサービスの機能や性能等に変更が発生した場合、受託者側でクラウドサービスの変更に伴う影響を確認し、対応が必要な場合は、原則対応すること。ただし、変更規模が大きい又は影響範囲が広い場合は本区担当職員と協議の上対応を検討・実施すること。

⑧　サービスレベル

・　運用・保守業務で達成目標とするサービスレベル項目及びサービスレベルを本区担当職員が協議の上、決定すること。

・　運用におけるリソース使用状況に基づき、毎年のリソース計画を策定する。月間の運用実績を評価し、達成状況が目標に満たない場合はその要因の分析を行うとともに、サービスレベル達成状況の改善に向けた対応策を提案すること。

運用保守実施要領

運用保守計画の内容を踏まえて、以下の要件が含まれる形で、運用保守実施要領の確定版を作成すること。

①　コミュニケーション管理

・　運用・保守業務を実施する上で必要となるコミュニケーション手段について、会議体（会議体　名称、開催目的、開催スケジュール、出席者、報告内容等）、インシデント発生時　の報告ルート等について記載し、効率的かつ円滑なコミュニケーションを実現すること。

✓　インシデント復旧の進捗状況の伝達範囲と内容を含んだコミュニケーション計画を策定すること。

② 体制管理

- 運用・保守に携わる事業者における作業体制の管理手法等について記載する。

③ 作業管理

- 運用・保守作業及びその品質の管理手法等について記載する。

④ リスク管理

- 運用・保守における作業を阻害する可能性のあるリスクを適切に管理するため、リスク認識の手法、リスクの管理手法、顕在時の対応手順等について記載すること。
- 再委託先や関係先を含めて業務遂行上のサプライチェーンリスクの評価方法を定め、計画を策定すること。

⑤ 課題管理

- 運用・保守において解決すべき問題について、発生時の対応手順、管理手法等について記載すること。
- 運用保守業務のナレッジ管理として、外部サービス等を利用してナレッジを蓄積する仕組みを整備し、速やかな分析が実施できる環境を整備すること。

⑥ システム構成管理

- 運用・保守における情報システムの構成（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、施設・区域、公開ドメイン等）の管理手法等について記載すること。
- 運用・保守における情報システムは、原則コンフィデンシャルコンピューティングの技術を用いた構成とすること。
- 運用・保守業務のアカウント管理において、IdP での特権を一元管理する管理手法を記載すること。
- 情報システムを構成する要素（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等）の下記内容を明確にすること。
- 利用範囲（ユーザ、システム）の定義
- データの種類、ライフサイクルの定義
- 連携するコンポーネント（SASE、IdP、API でアクセスするシステム、等）のアクセス管理手法、インベントリ管理手法
- 構成要素（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、施設・区域、公開ドメイン等）に対する組織内デバイスからの利用に係る管理手法

⑦ 変更管理

- 運用・保守により発生する変更内容について、管理対象、変更手順、管理手法等について記載すること。
- 運用・保守業務の実施にあたり、個別にソフトウェアを導入する場合は脆弱性対策を含めた維持管理計画を策定して記載すること。

⑧　情報セキュリティ対策

- 平常時のセキュリティ運用として、継続的な脆弱性管理、構成管理及び変更管理を行い、不正アクセス等のセキュリティ脅威に対する監視運用を行うための具体的な方法を記載すること。
- 運用・保守業務の実施にあたり、運用保守業務で導入するツール類について、導入時及び継続的にセキュリティ対策を実施する具体的な方法を記載すること。
- SIEM 等によるセキュリティ総合監視を実施する仕組みを導入すること。
- 構成要素（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等）の設定に対する継続したリスク確認の具体的な方法を記載すること。
- 構成要素（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等）を安全に利用するための方法に関するトレーニングについて記載すること。
- 外部サービス上でのデータの機密性保持のためのデータ管理手法を記載すること。
- 外部サービスを外部組織と共有して利用するためのアクセス管理手法、共有データの管理手法を記載すること。
- また、セキュリティインシデント発生に備えた体制や手順、発生時の被害極小化、速やかなサービス復旧を行うための具体的な方法を記載すること。
- 想定されるインシデントとその影響範囲を事前に整理し、具体的な対応プロセスの整備すること。
- 業務サービス等の定常状況を鑑み、復旧の判断基準を事前に定義にして記載すること。
- 復旧作業を速やかに実施できるよう、行動計画を作成して記載すること。
- 復旧作業に必要となる連絡先等を含めた体制を整備して記載すること。
- インシデントの発生可能性を評価するための具体的な手順を記載すること。
- インシデント発生時の緊急措置を実行するための具体的な手順を記載すること。
- インシデント発生後のシステムの利用復旧計画及び手順を記載すること。
- インシデント発生時、端末の盗難/紛失時の対応ルールを具体的に記載すること。

10.4　運用業務

運用業務として、以下の内容を実施すること。

システム監視・管理

①　システム監視・管理

- 本システムの運用状況を監視し、障害の発生またはその兆候を検知するとともに、障害を検知した際には重要性等で分類した上で、メールなどにより自動で通知する仕組みを構築すること。

- ✓ ジョブ監視
- ✓ 死活監視
- ✓ 性能監視
- ✓ リソース監視
- ✓ 障害監視
- ✓ ログ監視(監視対象のログを監視し、特定の文字列パターンと一致した場合に障害とする方式)
  - ✧ クラウドサービスのアクセスログ、共有活動、ダウンロード活動の監視すること。
  - ✧ ハードウェアのイベントログ、BIOS 設定変更などの監視すること。
- ✓ セキュリティ監視
  - ✧ 取得ログやセキュリティ製品のアラート等を用いて、不正アクセスやマルウェア感染等のセキュリティ脅威により引き起こされる異常な状態の監視等を行い、セキュリティインシデントやその兆候を早期に検知すること。
  - ✧ 検知されたセキュリティアラートや障害通知について、緊急度と影響度に基づいて優先順位を決定し、初期調査により真の脅威か誤検知かを判定した上で、攻撃の種類、影響範囲、被害の可能性を評価して対応方針を決定し、適切な対応チームや専門チームにエスカレーションすること。
  - ✧ ダッシュボードにより、下記の情報を一覧形式、数値、もしくはグラフによる時系列形式で表示すること。
    - 重大なセキュリティイベント一覧、件数
    - アクティブなセキュリティアラート件数
    - 過去の攻撃試行回数および攻撃元(時間単位が変更可能なこと)
    - 脅威傾向
    - 最も狙われているアセット
- ✓ クラウドの構成監視(クラウドサービスを構成する要素を監視する方式)
- ✓ 外形監視(本システムを利用するユーザと同じ方法でアクセスし正常に動作しているか監視する方式)
- ✓ コスト管理
  - ✧ ・従量課金でのサービスについて、計画値(予算額)との乖離がないかを管理すること。
  - ✧ ・予算額に対する利用状況監視や、利用金額の閾値監視等にて、予算超過の兆候を検知すること。

② **ジョブ管理**

- 本システムで実行される各種バッチジョブ、データ処理ジョブ、定期実行ジョブの統合管理を行い、ジョブの実行状況、依存関係、リソース使用状況を一元的に監視・制御する仕組みを構築すること。

③ **ログ管理**

- システム全体で生成される各種ログファイルを統合的に収集、保管、分析し、システムの動作状況把握、障害原因調査、セキュリティ監査、コンプライアンス対応を支援する包括的なログ管理の仕組みを構築すること。
- 構成要素(ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等)の活動ログを定期的にレビューし、異常なアクティビティやポリシー違反を検知するための監視体制を確立し、ログの保管期間とアクセス制御を定義すること。
- 包括的なログ管理の仕組みを用いて、統合分析し、異常パターンの検知、性能ボトルネックの特定、セキュリティ脅威の早期発見を実施すること。
- 新たな SaaS アプリケーションの追加や監視内容の改善等により必要となるログ収集項目の追加(変更)設定を実施し、既存ログ管理の仕組みへ統合を行うこと。
- 定義されたログ保管ポリシーに従い、長期保管対象ログのアーカイブを実施すること。アクセス頻度等を考慮した最適配置を行い、確実な長期保管を実現すること。

④ **監視設定**

- 各種監視結果を定期的に集計・分析し、監視方法や閾値、通知の見直し等が必要な場合は、本区担当職員の承認を得た上でこれに係る設計を行い、対応を実施すること。
- システムサイジングについても定期的に分析を行い、本区担当職員の承認を得た上で見直すこと。
- リソース監視の状況を踏まえたリソースの増強(スケーリング)を実施すること。
- 監視結果の定期的集計・分析結果の反映や新たな不正アクセス・マルウェア感染等の異常検知の向上を目指し、新たな脅威パターンに対応するカスタムルールの追加・変更設定を継続的に実施すること。

システム構成管理

本システムに係る全ての構成品目について、適切な構成管理を実施すること。

① **アカウント・アクセス管理**

- 連携するコンポーネント(SASE、ID フェデレーションする IdP、API でアクセスするシステム等)のインベントリの管理し維持すること。
- 構成要素(ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等)のユーザ・グループの権限マッピングの整備し、管理を実施すること。

- 組織内デバイスにおける外部サービスの利用手続を整備し、利用状況の管理を実施すること
- 外部サービスを外部と共有して利用する際の承認プロセスを整備すること。
- アカウントの利用状況の棚卸を実施すること。実施するタイミングは、年 1 回程度を想定しているが、具体的な時期については本区担当職員と協議の上、決定すること。
- システム運用保守用 ID は、個人に紐づく一意の識別子を持ち、共有 ID の使用は原則禁止とすること。特権 ID の使用においては、二要素認証を必須とし、適切な管理を行うこと。
- システムの運用保守に使用する ID は、業務に必要な最小限の権限を付与すること。また、定期的な権限の見直しを実施し、不要な権限は速やかに削除すること。
- 変更作業を行う ID（特権 ID 含む）は、使用時間の制限や特定の端末からのみアクセス可能とする制御を実装すること。
- すべての ID の使用について、アクセスログを取得し、改ざん防止措置を講じること。ログには最低限、使用者、使用時刻、アクセス先、実行操作を記録すること。
- 緊急時における特権 ID 使用の手順を明確化し、事後の承認プロセスを定めること。
- ID の付与・変更・削除は、承認プロセスを経た上で実施し、その記録を保管すること。ID 管理状況について定期的な監査を実施し、管理体制の有効性を検証すること。退職者や異動者の ID について、速やかな無効化手順を確立すること。

② システム構成管理

- システム構成管理対象を特定し、管理レベルを定めること。なお、システム構成管理対象は、本システムを構成するクラウドサービス、ソフトウェア（製品名、開発元、バージョン、ライセンス、依存関係等）、アプリケーション、通信回線、公開ドメインのほか、本システムの運用・保守に係る全てのドキュメント及びデータとすること。ただし、本システムの外部から提供を受けるものであり、運用・保守において変更を行わないものは、システム構成管理の対象外とする。
- システム構成管理対象の変更について、変更履歴を追跡可能であること。
- 本番環境・検証環境の維持管理を行うこと。
- SASE 経由でのアクセス制御を実現するため、認証基盤連携、ユーザ・グループ管理、ネットワークアクセス制御、セキュリティポリシー実装、アプリケーションアクセス制御等を実施すること。
- 構成要素（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等）に対し、新たな脆弱性情報がないかの収集を行い、定期的に報告すること。

・ 構成要素（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等）の新機能のリリースを調査し、定期的に報告すること。

③ バックアップ・リストア

・ システムバックアップ、データバックアップを取得すること。

・ 必要に応じてシステムリストア、データリストアを実施すること。

④ パッチ適用

・ パッチ適用にむけて、CVE（Common Vulnerabilities and Exposures）データベース、ベンダーセキュリティ情報、JPCERT/CC アラートの定期的な確認を実施して影響度と CVSS スコアに基づく優先度評価を行うとともに、システムインベントリと照合して影響を受けるコンポーネント（OS、ミドルウェア、アプリケーション、ライブラリ）を特定し、業務への影響度を評価してパッチ適用対象を決定すること。

・ 本番環境へのパッチ適用に先立ち、本番環境と同等構成の検証環境でパッチ適用を実施し、システム機能の正常性確認、既存機能への影響評価、パフォーマンス検証を行うこと。必要に応じて関係システムの影響有無（互換性確認等）を実施し、検証結果を文書化して承認プロセスを経た上で本番適用の可否を決定すること。

・ 適用するパッチの重要度や緊急度に応じて、システム負荷やユーザ利用状況を考慮し、実施スケジュールを計画し、本区担当職員と協議の上、決定すること。

・ パッチ適用は、適用後の予期せぬ不具合の発生時に迅速に対応できるよう、設定ファイルの保存、ロールバック手順書の準備を実施し、問題発生時の迅速な復旧体制を確保し、実施すること。

・ パッチ適用後は、稼働状況などを確認し、問題ないことを確認すること。また、適用結果を取りまとめて報告し、記録を管理すること。

⑤ バージョンアップ対応

・ 構成要素（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等）の新バージョンが出た場合、機能追加、仕様変更、廃止機能、依存関係の変更を特定し、バージョンアップの必要について検討すること。検討結果を、本区担当職員へ報告すること。

・ バージョンアップを実施する場合は、変更管理手順に従い必要な作業を実施すること。

変更・リリース管理

① 問題管理

・ 重大な影響を与えるインシデントや将来的に重大なインシデントに発展する可能性がある問題について影響評価を行った上で、緊急度及び優先度を定め、根本原因の調査及び解決策の立案を行うこと。

② **変更管理**

- 課題管理機能の活用を前提として、適切な変更管理を実施すること。
- 構成要素を追加、変更又は廃棄する場合は、変更依頼書を起票すること。
- 機密情報の不要な公開等の意図しないセキュリティインシデントを防止するため、本システムの設定変更等に当たっては、情報セキュリティ関連の設定に影響しないことを確認すること。

③ **リリース管理**

- 本区担当職員とリリース作業の日程、作業内容、依頼事項等の調整を行い、実施の計画をリリース計画書に記載すること。
- リリースを実施した際、リリースに関する情報を「リリース管理台帳」にて管理すること。
- 「リリース管理台帳」には項目として、「実施計画の内容」「リリーステストの実施有無及び結果」「リリース時期」「各種レビューの実施有無及び結果」「リリース内容」を管理し、履歴を確認すること。上記以外の項目で履歴情報等の管理が必要な項目についても、管理する仕組みとすること。

障害対応・インシデント管理

① **障害対応**

- 障害発生時は、発生から解決までの一連の作業（受付、問題判別、業者間調整、調査解析、修復方法の検討、障害原因への対処、再発防止・品質向上作業、報告書作成・報告実施、環境（本番環境・検証環境等）反映）を行うこと。
- 個別システムにおいて障害が発生し、業務影響が発生した場合においても、個別システム担当が実施する原因調査、代替策、解決策の検討及び処置を必要に応じて支援すること。
- 激甚災害が発生した場合に、業務継続（業務復旧）が可能となるよう準備し、発生時には速やかに対応すること。

② **インシデント管理**

- システム障害と想定されるインシデント連絡を受け付けた際、別途、本区担当職員より指示する担当者へ速やかにエスカレーションすること。関係者との応答内容の記録を残すこと。
- インシデント発生後、インシデントからの復旧と運用能力回復のための活動を実施する際に、内部および外部に向けた状況共有・報告を行う体制を整備すること。
- 運用開始後、本区担当職員でよりインシデント状況を確認できるダッシュボードにて、さらなる詳細情報の確認要望等がある場合は、ダッシュボードの更新にむけた技術支援を行うこと。

③　**情報セキュリティインシデント対応**

- 情報セキュリティインシデントが発生した場合は、「運用保守実施要領」等に定めた手順に従ってインシデント対応を行うこと。対応に当たっては、本区担当職員、関係事業者と適宜調整の上で対応を行うこと。
- 手順には、情報セキュリティインシデント発生時の緊急措置の実行、インシデント発生後のデータ復元や利用復旧の実施を含めること。
- 情報セキュリティインシデント発生後のデータ復元手順の定期的なテストを実施すること。
- 情報セキュリティインシデント対応手順の実効性を担保するため、定期的にインシデント対応手順の見直しやインシデント対応訓練を実施すること。
- UEBA（User and Entity Behavior Analytics）システムでの誤検知を減らすため、業務上正当な行動パターンと異常行動の区別方法を利用者へ指導できるよう支援し、ルール調整やホワイトリスト設定の手法を提示すること。

利用者支援

①　**ヘルプデスク業務**

- 本システムの利用方法に関する問い合わせの受付からクローズまでを一元管理するヘルプデスクをシステム支援窓口もしくはシステム運用に設け、本システム利用者からの問い合わせを受け付けること。
- ヘルプデスク担当者のスケジューリング等の運営を適切に行うこと。
- ヘルプデスク担当者による対応手順、サービスレベル等を統一するため、ヘルプデスク運用マニュアルを作成し、本区担当職員の承認を得ること。
- ヘルプデスク運営の中で FAQ は適宜追加、更新等、メンテナンスを行うこと。
- ヘルプデスク要員は以下の要件を満たすものが担当すること。なお、1 名で満たすことが望ましいが、複数名で満たすことも可とする。その場合は、最も経験を有する者をリーダとして、そのものが本区担当職員との窓口を担うこと。
- 本システムと同等規模のネットワークシステムでのヘルプデスク経験（2 年以上）
- 自治体（行政機関可）または大規模組織でのユーザサポート経験（1 年以上）
- 複数の関係者（運用チーム、保守ベンダー等）との調整経験
- 組織所有の Windows 端末及びモバイルデバイスの整備・保守に関する経験
- ヘルプデスク業務における対応履歴の管理・報告業務や FAQ 作成・管理の経験
- インシデント管理、セキュリティインシデント対応に関する知見

②　**業務支援**

- 受け付けた問い合わせは、質問、インシデント、サービス要求、作業依頼等に分類した上で、対応日時、問い合わせ元、内容、回答状況等とともに記録すること。なお、具体的な運用方法については、本システムの設計開始以降に改めて検討する。

- 問い合わせ記録は受付件数、問い合わせ者情報、問い合わせ内容、回答率、回答に要した期間、回答内容等を適切な粒度で整理した上で、定期的に問題発生状況を分析すること。分析結果を踏まえ、回答時間の短縮や回答内容の分かりやすさ向上等、必要な対策を検討し、本区担当職員と協議の上、実施すること。
- 問い合わせで把握した問題については、運用改善を実施する際の参考情報となるよう整理すること。
- 運用・保守の計画及び実施状況について、本区担当職員の定める報告様式に従って取りまとめ、本区担当職員に報告を行うこと。（原則、月次での報告）
- 利用する SaaS アプリケーションにおいて、利用するユーザに応じたセキュリティポリシーとアクセス制御の設定を実施すること。

③　ユーザアカウント管理

- 外部サービス（IdP）と連携して管理するアカウントの定期的な棚卸しとメンテナンスを行うこと。
- 構成要素（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等）と連携するユーザ・グループの権限マッピングの定期的な棚卸しとメンテナンスを行うこと。

10.5　保守業務

保守業務として、以下の内容を実施すること。

- 問い合わせの受付時間は、運用保守実施要領に記載の通りとする。ただし、本区担当職員が緊急かつ業務に支障を来すと判断した場合はこの限りではない。
- 受け付けた問い合わせをインシデントとして管理し、インシデントのクローズまで、対応を継続すること。
- 障害について対応したときは、障害報告書を作成し、本区担当職員に報告すること。
- 激甚災害が発生した場合に、速やかな業務復旧が可能となるよう対応計画を整備し、定期的な確認をすること。

クラウドサービス保守

クラウドサービスの保守として以下を実施すること。

①　役割分担の整理

役割分担を行う際に以下の点に留意すること。

- 保守業務の設計に際し、受託者の責任範囲及びクラウドサービスを含めた関連事業者間の役割分担を整理すること。
- 本システムがクラウドサービス上で稼働することを踏まえ、各業者間の役割分担を考慮した上で、運用・保守設計を行うこと。

② **クラウドサービスの利用**

クラウドサービスを利用する際に以下の点に留意すること。

- 保守設計を実施する上で、クラウドサービスの標準機能を可能な限り活用すること。
- クラウドサービスによる自動化等により、省力化を実施すること。
- 運用・保守実施要領、運用・保守計画書及び運用・保守手順書については、クラウドサービスが提供する各サービスを活用することにより、作業のみならずドキュメント類についても効率的に作成すること。
- 利用するクラウドサービスにおいて、提供サービスの仕様上必要となるアップデートパッチの適用やメンテナンス等の対応に際して、本システムへの影響度に鑑み、本区担当職員と協議の上対応を行うこと。または、自動適用を行う等の対応が可能となるよう、必要な仕組み（検知、適用、等）を準備すること。

③ **クラウドサービスの保守**

クラウドサービスの保守として以下を実施すること。

- 利用しているクラウドサービスにおいて脆弱性及び不具合が確認された場合は、その対応について本区担当職員と協議し、パッチ適用要否を判断すること。
- クラウドサービスにおいてバージョンアップ等の情報が公開された場合には、バージョンアップに伴う影響調査を実施した上で、本区担当職員と協議し、適用等の可否を決定すること。なお、実施することとなったバージョンアップに伴う機器・サービス等の停止は計画停止に準ずるものとして扱う。また、バージョンアップに起因して改修が必要な場合には、対応について別途本区担当職員と協議すること。
- クラウドサービスで利用している環境の最新化や更新は、原則として IaC（Infrastructure as Code）を活用しコードを変更し、変更後のコードを実行することにより実施すること。
- 修正パッチ適用やバージョンアップ等を行う場合には、事前に検証環境において本システムの運用に影響が生じないことを十分に検証し、環境更新の事前評価を実施すること。

ソフトウェア保守

ソフトウェアの保守として以下を実施すること。

① **ソフトウェア最新化**

- 本システムを構成する全てのソフトウェアについて、製品不具合や情報セキュリティに関する脆弱性を修正するため、本区担当職員と協議の上、ソフトウェアを最新化すること。なお、ソフトウェアの最新化に当たっては、本システムのシステム構成等に考慮すること。

② 修正プログラムの適用

修正プログラム適用の際は以下の点に留意すること。

- 情報セキュリティや安定稼働の観点から緊急性が高いと考えられる修正プログラムについては、緊急適用を計画すること。緊急性が低い修正プログラムについては、定期保守作業の中での適用を計画すること。
- 使用しているクラウドサービスの内容に変更が発生する際には、クラウドサービスより提供する情報を元に本システムへの影響範囲を調査の上、修正プログラムの適用可否を本区担当職員へ報告すること。適用が必要と判断された場合、クラウドサービスより提供されるソフトウェアに対する修正プログラムの適用作業を実施すること。

③ 検証・デプロイ

検証・デプロイを行う際は以下の点に留意すること。

- ソフトウェア保守に当たっては、事前に検証環境で本システムの運用に影響が生じないことを十分に検証すること。
- ソフトウェア保守に伴い、本システムの安定稼働に影響が生じる事態が予測される場合、本区担当職員の指示に基づいてデプロイ実施の是非を判断すること。

④ 設計書への反映

- ソフトウェア保守によりソフトウェア構成に変更が生じた場合、設計書等へ変更内容を反映すること。

⑤ 保守条件の決定

- 保守条件は、「製品の導入や使用方法」、「製品の互換性や相互操作性」、「製品資料の解釈」、「構成サンプルの提供」、「修正策の情報提供」、「製品プログラム、製品コードに起因する障害」等の保守が提供されることを想定しているが、最終的な保守条件は、本区担当職員と調整の上、運用・保守設計において決定すること。

⑥ 脆弱性管理

ソフトウェアに関する脆弱性に対処するために、以下の対応を行うこと。

- 脆弱性管理の方針を定めた脆弱性管理基準を、運用・保守設計において本区担当職員と調整の上で作成し、運用すること。脆弱性管理基準には、以下の項目を含めること。
  - ✓ 個別対応の要否判断の基準
  - ✓ 定期アップデート規則
  - ✓ ソフトウェア採用判断の基準
  - ✓ 脆弱性管理の対象と管理方式
- 脆弱性に対処する手順を定めた脆弱性管理手順を、運用・保守設計において本区担当職員と調整の上で作成し、運用すること。脆弱性管理手順には以下の項目を含めること。

- ✓ ソフトウェア構成の管理
- ✓ 脅威情報の収集、自システムへの影響分析
- ✓ リスクに応じた脆弱性対応及び定期アップデート

アプリケーション保守

アプリケーションの保守として以下を実施すること。

① インシデント管理

- 運用管理・監視等作業におけるインシデント管理と適切な連携を図ること。

② 是正保守

- アプリケーションに起因した障害発生時、監査指摘事項への対応時等、アプリケーションの是正が必要な場合に、是正保守を行うこと。

③ 適応保守

- OS、ブラウザ、ミドルウェア等のバージョンアップ対応等、利用環境の変更への対応が必要な場合、アプリケーションに係る適応保守を行うこと。

④ 予防保守

- 本サービスのアプリケーションに潜在的な問題が発見され、当該問題除去を目的とした変更が必要な場合又はアプリケーションコンポーネントについて新たに脆弱性が報告された場合に、予防保守を行うこと。

⑤ 改善措置

上記②～④に伴う改善措置を実施する際には以下の点に留意すること。

- 区民等の利用者に影響がある保守作業を実施する場合は、アプリケーション保守の実施効果、現在及び将来の利用者に対する影響の分析を行うこと。
- アプリケーションに係る機能性、信頼性、使用性、効率性、保守性、移植性等の改善が必要な場合に、対処を行うこと。
- Web 解析結果に基づき、本サービスのユーザインタフェースについて、ユーザビリティ又は UX に関する課題を識別した場合、課題解決に資する是正保守、予防保守を行うこと。
- Web サーバ、データベース等について、運用改善の結果を踏まえ、必要に応じて稼働環境の改善等に伴う設定変更を実施すること。

⑥ 根本原因の分析

根本原因を分析する際に以下の点に留意すること。

- 是正保守及び予防保守の実施に当たり、障害、監査指摘、潜在する問題等に係る根本原因の分析を行うこと。

⑦ 検証

- 修正したアプリケーションを本番環境へ展開(デブロイ)する前に、修正が適切に実施されているか否かについて検証環境において検証すること。

⑧　ドキュメントの修正

・　アプリケーション保守に伴い、ドキュメント（設計書、マニュアル等）の修正を要する場合は、速やかに修正を行うこと。なお、改修等に伴い画面等に発生する変更が軽微な場合は、ドキュメントの更新方針等について別途本区担当職員と協議すること。

ハードウェア保守

ハードウェアの保守として以下を実施すること。

①　インシデント管理

・　運用管理・監視等作業におけるインシデント管理と適切な連携を図ること。

②　適応保守

・　ファームウェア、BIOS 等のバージョンアップ対応等、利用環境の変更への対応が必要な場合、ハードウェアに係る適応保守を行うこと。

③　改善措置

・　ハードウェアの交換が必要な場合は、手順に従い交換を実施すること。

④　デバイス管理

・　デバイスの登録・プロビジョニング管理、アプリケーションの配布・更新・削除管理、および紛失・盗難時のリモートワイプ・ロック対応を含むモバイルデバイスのライフサイクル全般にわたる一元的な管理を実施すること。

軽微な修正

運用・保守の期間中に必要となる軽微な改修として以下を実施すること。

・　運用・保守の期間中に、利用者からの要望対応、不具合の改善、環境変化への対応等の目的で軽微な改修を行うことを想定している。改修への対応工数（必要に応じて教育訓練等を含む）として、相応の作業を見込むこと。
・　個々の改修に当たっては、改修範囲、影響範囲等を分析して必要工数を事前に見積もった上で、本区担当職員の承認を得た上で作業を実施すること。
・　月次の定期報告において、個々の改修の実施状況（工数の消化状況等）について報告すること。また、改修が必要と考えられる事項が受託者においてある場合は積極的な提案を行うこと。
・　個々の改修が完了した後に、工数実績を提示すること。また、計画工数と実績工数の差異を分析した上で、その後の改修案件のおける見積精度向上と改修生産性向上に努めること。

10.6　継続的改善

運用保守業務の品質向上とコスト低減を実現するため、以下の内容を実施すること。

保守実績評価

保守実績の評価として以下を実施すること。

- 本システムの運営に関わる関係者間で本システムの保守に係る情報や問題認識を共有し、保守業務の品質を継続的に維持・向上させること。
- 本システムが使用するアプリケーション、クラウドサービス、ソフトウェア等の保守実施状況について、日々の保守業務の中で収集する定量的な管理指標を定め、本区担当職員と合意すること。
- ログ解析機能等を活用し、指標値の収集、評価及び管理を効率的に行うこと。
- 管理指標の達成状況を評価し、未達の場合は原因分析を行い、改善措置を検討すること。また、これらの実績、評価、改善措置について、定期報告すること。

運用改善

運用保守業務の改善として以下を実施すること。

- 運用・保守業務で発生する課題とその対応履歴の蓄積・分析を行い、業務等の改善を定期的に実施すること。
- 構成要素（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等）の利用状況を分析し、改善計画を策定するプロセスを整備すること。
- 構成要素（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等）の活動ログの定期的なレビューを実施すること。
- ログ解析機能、Web 解析機能の活用を前提として、モニタリング及び運用過程を通じて得られた利用状況を分析することにより、ライフサイクルコスト低減の観点から、利用するクラウドサービスの所要量及びソフトウェアライセンスの削減可能性を検討すること。また、利用状況の実績、評価、コスト削減可能性について、定期報告すること。
- セキュリティ監視において、偽陽性イベントを抑止する案を検討して提示すること。
- セキュリティインシデント対応における、新機能の適用可否の検討・提案を実施すること。
- 運用保守業務の改善として、人的ミスの軽減や省力化の観点からオペレーション等の自動化の検討・提案を行うこと。

訓練・監査

訓練・監査として以下を実施すること。

- 構成要素（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等）のリスクアセスメントを実施すること。
- 復旧作業を速やかに実施できるように、行動計画に基づく訓練を実施すること。
- 復旧計画に含まれる体制のなかで、連絡先の定期的な見直しを実施すること。
- 取得しているバックアップが利用可能であること、バックアップから復旧が可能であることを、定期的に手順を含めて確認すること。

- ID 管理において、特権 ID 全てのパスワードが変更可能であることを検証し、変更時の影響範囲を整理すること。
- 本区が定期的に実施する監査(セキュリティ監査やシステム監査等)の対応を行うこと。対応にあたり、監査人等から必要となる証跡等を求められた場合は提出すること。また、監査指摘事項に対し、対応計画の立案し、本区担当職員へ報告すること。対応計画に基づき是正対応を実施し、その進捗や結果を本区担当職員へ報告すること。

教育

- 構成要素(ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、等)の安全な利用方法についてトレーニングを実施すること。

10.7 報告・ドキュメント管理

運用保守業務の維持管理として、以下の内容を実施すること。

定期報告

運用保守に関連する活動内容の報告として、以下を実施すること。それぞれの報告の周期は本区担当職員と協議により決定すること。なお、重要事項は協議の決定周期によらず、随時報告すること。

- システム運用状況(システムの稼働状況と管理指標の実績、リソース使用状況とリソース計画の進捗、サービスレベルの達成状況と未達の場合の改善措置、各種監視(死活監視、性能監視、リソース監視、障害監視、ログ監視)の結果等)
- インシデント・課題(問題)管理(発生したインシデントの状況と対応結果、問い合わせ内容の分析結果、課題(問題)の発生状況と対応状況等)
- セキュリティ関連(セキュリティ監視における発生した脅威の分析結果と対応状況、最新の脅威情報や監視状況、セキュリティアラートや障害通知の検知・対応状況等)
- 構成管理・変更管理(システム構成の変更状況、パッチ適用・アップデート状況、ソフトウェアライセンスの利用状況等)
- ヘルプデスク活動(問い合わせ状況、問い合わせ内容の分析結果、活動計画等)
- 運用保守改善(運用保守業務の改善提案と実施状況、コスト削減施策の検討状況と効果等)

ドキュメント保守

設計・開発関連ドキュメント及び運用・保守関連ドキュメントが、受託者の契約期間において、最新の状態であるよう維持・更新等を行うこと。

11. 成果物と納入方法

11.1 基本事項

- 各種成果物は製本版と電子データにて提出すること。
- 提出方法については、本区と協議し提出すること。

11.2　最終納入成果物

・ 本システムの構築・導入業務においての最終納入成果物の対象を以下に示す。なお、成果物は、各工程途中においても必ず本区に提出し、随時本区と協議しながらまとめること。

成果物	納期
プロジェクト計画書	契約締結後、本区と協議の上速やかに提出
議事録	原則、会議開催後 5 営業日以内
進捗報告書	定例会時
課題管理表	定例会時
要件定義書	要件定義工程完了時
品質管理計画書	プロジェクト開始時
各種設計書 （基本設計書、詳細設計書、テスト設計書、システム移行・データ移行設計書、運用・保守設計書）その他、本区が必要とする書類	工程完了時
テスト結果報告書	工程完了時
各種手順書（各工程での実装時に必要な手順書類）	各工程実施時
各種マニュアルなど	各種研修実施時
システム運用マニュアル	各種研修実施時
個人情報の保護に関する誓約書	プロジェクト開始時

本システムの運用保守業務において納入成果物の対象は以下に示す。

成果物	納期
運用保守計画書	毎年 4 月末
議事録	原則、会議開催後 5 営業日以内
定例報告資料	月次定例報告会時
問い合わせ一覧	随時
問題点・課題一覧	随時
改版ドキュメント一式	随時
障害管理台帳	随時
変更・リリース管理台帳	随時
構成管理台帳	随時
保守作業報告書	随時

※随時納入としたものについても、年度末に一式を製本し納入すること

11.3　納入場所

・ 〒102-8688　千代田区九段南１−２−１
　千代田区役所　政策経営部情報システム課

11.4　その他留意事項

（1）作業場所

・ 本業務は事前に本区担当職員と協議を行い、許可を受けた場所でのみ実施すること。なお、作業場所は受託者の責任と負担において用意すること。

（2）その他支援

・ 受託者は、調整事項等が発生した場合、本区担当職員と協議すること。また、必要となる調整作業を支援すること。
・ 本区担当職員から本システムに係る技術的な助言を求められた際は、速やかに対応し書面、又は、電子メールによる回答を行うこと。また、受託者は、本システム構築に必要な技術動向、製品動向等の情報を積極的に提供すること。