港区議会ホームページリニューアル業務委託仕様書

港区議会事務局

目次

第１章　全体概要

１　件名

港区議会ホームページリニューアル業務委託

２　履行期間

契約締結から令和９年３月３１日まで

３　履行場所

受注者作業場所

４　目的

港区議会ホームページは、ASP サービスによるホームページ管理システム（CMS）にて情報発信を行ってきましたが、情報発信の即時性の確保や利用者ニーズの多様化から、ホームページ機能やアクセシビリティ、自治体 DX を見据えた対応について、より一層の改善が求められるようになっています。

このことから、デジタル化が加速する現在の情勢に合わせて、利用者ニーズに対応できるホームページとするとともに、情報発信機能を充実させ、誰もが使いやすく親しみやすいホームページづくりを目指します。

５　新しいホームページのリニューアル方針

（１）安定した稼働を実現する「いつでも使うことができる」サイトの構築

利用者が知りたいときに知りたい情報をいつでも受け取れる常に安定した環境を提供すること。また、災害発生などの緊急時・非常時でも、迅速かつ安定的な情報発信が可能なシステムを構築する。

（２）高齢者・障害者を含めたすべての利用者が支障なく利用できるホームページ

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、ソフトウェアおよびサービス第 3 部：ウェブコンテンツ)」、「みんなの公共サイト運用モデル（2016 年度改訂版)」等のアクセシビリティに関する規格の要件を満たすものとする。

（３）誰もが目的の情報に簡便かつ快適にたどりつけるホームページ

子どもや若年層も含む幅広い年齢層が使いやすいナビゲーションの配置、わかりやすいサイト内検索機能の強化や利用者の視点に基づいた構造設計など、ユーザビリティに配慮したホームページをめざす。

スマートフォン閲覧も想定して統一感のあるデザインにすること。

（４）コンテンツ作成者・管理者の支援

特に HTML の知識がなくても、職員が容易に「JIS X 8341-3:2016」に準拠したコンテンツが作成できるものとする。また、リンク切れや掲載期間などコンテンツを自動的に管理することで管理担当職員の負担を軽減する。

（５）拡張性の確保及び柔軟性の高い保守運用対応

運用開始後の機能向上やホームページの構造変更等を柔軟に行えるとともに、将来的

なシステムの拡張性を考慮するものとする。また、本業務の受注者は、データのバックアップ、セキュリティパッチ適用等の定期的な保守を実施するとともに、機能向上のための対応を行うものとする。

6　支払方法

契約代金は、すべての業務の履行確認後、受注者からの請求に基づき一括で支払うこととする。

※検証期間には試行運用の実施期間も含むこととし、令和９年３月中の運用保守費用についてはリニューアル業務委託費用に含めること。

第２章　業務概要

1　業務範囲

本業務の範囲は、以下のとおりとする。

（1）ASP サービスの提供及び保守管理
（2）CMS のシステム構築・設定（閲覧・コンテンツ作成整理・管理機能の充実を目的とした計画・設計・環境構築）
（3）カテゴリ分類、掲載内容等のコンサルティング
（4）サイト設計及びトップページほか各ページの企画・デザイン
（5）コンテンツ作成及びコンテンツ移行
（6）操作研修及び各種マニュアル作成
（7）セキュリティ対策の実施・報告
（8）アクセシビリティへの対応
（9）運用保守
(10) 区ホームページにとって有益な独自提案
(11) その他ホームページリニューアルに当たって必要となる業務

2　システム構築の前提条件

本業務において構築するホームページは、以下に示す前提条件を踏まえること。

項番	事項	内容
1	利用時間	システム利用時間は、原則として 24 時間 365 日とする。 ただし、保守等の予定された停止に関しては、その限りではない。
2	対象ホームページ	港区議会ホームページ （https://www.gikai.city.minato.tokyo.jp/　配下） 【移行対象ページ数】 約 500 ページ（約 400MB）
3	ドメイン	ドメインは、現状の港区議会ホームページのドメイン名（gikai.city.minato.tokyo.jp）を引き継ぐこと。
4	CMS 登録ユーザ	・作成者　約 15 ユーザー

	ー数	・承認者　約２ユーザー ・PC　約 15 台
5	クライアント環境	・OS：Windows 11 Pro Office：Office 365 Apps 64bit ・CPU: Corei5 以上 ・メモリ：8GB 以上 ・SSD:256GB 以上 ・ブラウザ：Microsoft Edge、Google Chrome
6	動作環境	・庁内ネットワークに接続されたクライアント端末からブラウザのみで利用可能で、専用ソフトウェアのインストールが不要なシステムである。
7	利用するネットワーク	・本庁舎内幹線：1Gbps ・本庁舎内支線：1Gbps
8	公開用 WEB サーバ	クラウドサーバを利用。下記のスペック以上のものを用意すること ・CPU コア：4 ・メモリ:8GB
9	ウェブページ形式	・生成されるウェブページは、原則として、全て静的に生成されるものとする。ただし、必要に応じて動的に生成されることが最適なウェブページを提案する場合は、別途区議会事務局と協議の上、決定する。

第３章　サイト設計について

1　サイト設計の基本的な考え方・サイト構成

リニューアル方針等を勘案し、システム構築を行うこと。

（1）アクセシビリティ、ユーザービリティ等に配慮したサイト設計を行うこと。

（2）利用者にとっての使いやすさを最優先したナビゲーションメニューや、カテゴリからコンテンツの内容が想像できるカテゴリ分類の設計をすること。

また、利用者が情報を探せなかったときのための救済として、検索方法等などを案内するナビゲーションの設置など、検索性を向上させる仕組みを有すること。

（3）目的とするコンテンツに、原則として 、１～3 クリック、最大 5 クリック程度でたどり着く階層構造とすること。

（4）単一のファイル作成でパソコン、スマートフォンやタブレット端末等異なるデバイスに対して表示内容・操作が最適な状態に変化する設計とすること。特にスマートフォンでの表示・操作の最適化を重視すること。（レスポンシブデザイン可）

（5）すべてのコンテンツにトップページへの リンクを用意すること。

（6）すべてのコンテンツにパンくずリストを自動作成すること。

（7）パソコン向けコンテンツを作成・更新することにより、スマートフォン、タブレッ

ト等の閲覧者の環境に対応したページが自動的に生成されること。

2　デザイン

現行ホームページのコンテンツの現状調査を行い、カテゴリ分類、情報分類、掲載内容等のコンサルティングを行うこと。

リニューアル方針等を勘案し、最適と考えるＰＣ版及びスマートフォン版のデザイン・構造・運用設計を提案・作成すること。構築時にトップページ、目次ページ、詳細ページのデザイン案を作成すること。

なお、デザイン案は２案以上を提案し、発注者と協議の上決定すること。

（1）トップページのデザインや項目などは互いに協力して妥協することなく作成すること。 パソコン、スマートフォン、タブレット等の閲覧者環境の多様化に対応し、各々の環境で適切に港区議会ホームページが表示されるようにすること。

閲覧者の使用する Web ブラウザは以下のものを想定し、これらのブラウザで適切に表示されること。

・Microsoft Edge最新バージョン

・Firefox最新バージョン

・Google Chrome最新バージョン

・iOS Safari最新バージョン

・Android Google Chrome最新バージョン

（2）詳細情報ページおよび分類中間ページは、トップページのデザインとの統一性を確保すること。

（3）カテゴリ分類に基づき、ローカルナビゲーションメニューを配置できること。

（4）緊急時用のトップページ切替機能があること。トップページに緊急情報が表示でき、トップページへの表示、非表示が設定できること。

（5）サイト全体の構造が容易に理解できるサイトマップを配置すること

（6）デザインなどが特殊なテンプレート（FAQなど）は事前に発注者と協議の上、準備すること。

（7）稼働後のトップページレイアウトの変更が容易であること。

（8）トップページほか各ページに関する素材等を作成し、元データを発注者に提供すること。なお、データは一部修正して発注者が利用することができるものとする。

（9）ホームページ制作上の最新技術等の情報提供、提案を行うこと。

(10) レイアウト・アイコン等の配置・配色等を工夫し、掲載されている情報が一目で分かる、利用者が感覚的に探せるデザインにすること。

(11) スマートフォン閲覧者を意識したシンプルで機能的なデザインにすること。

(12) デザインの確認及び移行データ・CMS機能を検証する際は、発注者のパソコンから

確認できる環境を用意すること。

3　テンプレート

作成したデザイン等に基づき、発注者がコンテンツ作成・編集等を行うためのテンプレート設計、開発を行うこと。業務用途に応じた複数のテンプレートを作成すること。

4　独創的な新規コンテンツの提案

リニューアル方針等を勘案し、幅広い世代が議会に関心を持ち、身近に感じてもらうための新たなコンテンツを提案し、作成すること。

第4章　システム構成要件

1　機能要件

機能要件を以下に示す。なお、ＡＳＰサービス等を導入する場合は、セキュリティに配慮した上で、各テンプレートへの埋め込み作業等を行うこと。なお、有償のサービスの導入に係る費用は、見積金額に含めるものとする。

（1）ＣＭＳの機能要件

ア　機能

ＣＭＳに求める機能については、【別紙１】ＣＭＳ機能要件一覧のとおり。

要求要件のうち、【必須機能】の項目については必ず実装すること。ただし、条件どおりの実装が困難な場合は、代替案の提案を可とするが、発注者がその代替案について要求項目を十分に満たすものであると判断した場合のみ、対応可能とする。

【推奨機能】の項目については、必ず満たさなければならないものではないが審査の対象とし、同項目について要件を満たす提案を行った場合は必ず履行すること。

ＣＭＳに関する製品仕様や提案書があれば提出すること。

イ　初期設定

発注者が提供するＣＭＳのユーザー情報、所属等の基本情報等について、受注者が初期設定（マスター登録作業）を行うこと。

（2）検索機能

フリーワード検索、絞り込み等の検索機能を有し、サイト内検索ができること。幅広い世代が使用しやすい検索機能の導入をすること。導入にあたっては、具体的な検索性向上のための機能の提案をすること。ＡＩ技術を活用した方策などがあれば積極的に提案すること。

（3）多言語対応

本ホームページは、日本語のほか、複数（英語、中国語（繁体字・簡体字）、韓国語は、必須とする。）の言語に自動でＡＩ翻訳される仕組みを実装すること。

ＡＳＰサービス等を導入する場合は、以下の要件を満たし、他自治体において、既に導入されているサービスを導入すること。

項番	カテゴリ	要件概要
1	対象ページ	全てのページ。ページ数は限定しない。
2	操作性	閲覧者がソフトウェアのダウンロードやインストールの必要がなく、ホームページ上のボタンをワンクリックするだけで利用可

		能であること。
3	デバイス	パソコン版ホームページだけでなく、スマートフォン版のホームページでも設定した言語に合わせて、自動翻訳できること。
4	その他	地名、人名、組織部署名など固有名詞の誤訳を防ぐため、辞書登録ができること。 文章登録により、事前に用意した翻訳者による翻訳を登録できること。

（4）音声読み上げ機能

ＯＳやソフトウェアによる音声読み上げ機能に対応したコンテンツとすること。

閲覧者の使用する Web ブラウザは以下のものを想定し、これらのブラウザで適切に表示されるとともに、モバイル端末でも、適切に表示されること。

・Microsoft Edge 最新バージョン

・Firefox 最新バージョン

・Google Chrome 最新バージョン

・iOS Safari 最新バージョン

・Android Google Chrome 最新バージョン

（5）アクセス解析機能

発注者が指定する端末からアクセスログが簡単に解析できる機能を提供すること。なおGoogle Analytics 等も可とするが、以下の機能は満たしていること。他有効なシステム等あれば提案すること。

・ 日別・月別等の確認、解析が行えること。

・ 解析結果のデータは CSV ファイル等で容易に保存、出力できること。

・クリック数を日毎・月毎等の確認、解析ができること。

（6）その他

本仕様書に規定のない事項についても、受託者の専門的な知見により、本業務の費用範囲で実現できる効果的なシステムや機能等のオプションがある場合は積極的に提案すること。

2　非機能要件

（1）サーバ等要件

新システムを稼働させるサーバ等の要件を以下に示す。「企画提案書」に対応について具体的内容を記載すること。

項番	カテゴリ	要件概要
1	OS 基本	動作確認がされ、稼働が安定し、稼働日（令和７年４月）から５

		年以上システムサポートが提供される OS を採用すること。
2		修正プログラム適用後のシステム再起動を最小限にできること。
3		過去に発見された脆弱性について、確実に対処されていること。
4		日本語による情報提供ができること。
5	連続運転	安定した連続運転が可能であること（メンテナンス等に要する時間を除き、24 時間稼働状態を維持すること）。
6		業務を停止することなくデータベースのバックアップ等のメンテナンス作業ができ、作業中はレスポンスの低下を招くことのないこと。
7	信頼性	サーバはデータバックアップ方法を採用し、バックアップ作業は毎日自動化されること。
8		サーバや周辺機器が故障した場合、あるいは老朽化に伴うトラブルが発生又は予測された場合には、速やかに現地にて部品交換等の対応ができる体制を確保すること。
9		サーバ等システム運用に係る機器は、公的資格として ISO27001 を取得しているインターネットデータセンター（以下「IDC」という。）に設置すること。
10	その他	インターネットから誰でもアクセスできる領域にデータベースサーバを設置しないこと。
11		WEB サーバ、DB サーバ及びバックアップ装置を含む全ての機器を本区庁舎内に設置せず、IDC を利用した ASP/SaaS 方式とし、機器・ネットワーク回線等の維持管理等一切を受注者が行うものとする。

（2）セキュリティ要件

個人情報保護対策や情報漏えい対策に向けて、セキュリティに十分に配慮された構成であることを求める。セキュリティ要件を以下に示す。「企画提案書」に対応について具体的内容を記載すること。

項番	カテゴリ	要件概要
1	全般	総務省が定める「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」や港区が定める「【別紙２-１】港区情報安全対策指針」及び港区議会が定める「【別紙２-２】港区議会情報安全対策基本方針」に基づき適切に管理運用されていること。
2	認証・アクセス管理	保護対象の情報資産に対し、それを取り扱う権限を持った職員のみがアクセスできるよう理論的対策を講ずること。
3		サイト内の全ページにおいて、常時 SSL 化に対応すること。なお、SSL の更新手続については、受注者が責任を持って行うこと。

4	ウイルス対策	サーバ、端末等のシステム環境全般において、コンピュータウイルス等の悪意のあるプログラムが侵入できないようウイルス対策を講ずること。
5	改ざん対策	保護対象の情報資産の改ざんを防止するため、通信経路とファイルについて適切な暗号化措置を講ずること。
6		保護対象の情報が改ざんされた場合、速やかに検知が可能であること。
7		保護対象の情報資産の改ざんが発生した場合でも、直ぐに復旧できるように対策を講ずること。
8	不正アクセス対策	外部からの不正アクセスを防止する措置を講ずることで、情報漏えいやサービス停止を発生させないこと。
9		プログラム等を使用した短時間の連続アクセスに対処するため、アクセス制御などの措置を図ること。
10	物理的な盗難への対策	保護対象の情報資産が盗難にあった場合でも、その中の情報が漏えいしない対策を講ずること。
11	インストール等	ソフトウェアのインストール、バージョンアップ等の徹底した管理（一元管理、履歴管理等）を行うこと。
12		保護対象の情報を利用者が必要な時に確実に利用できるシステムの安定稼動対策を講ずること。
13		各種機器・ソフトウェアには適切にセキュリティパッチ、修正プログラム等が適用されていること。最新のプログラムの状態に沿って必要な設定が実施されていること。

（3）システム構成要件

システム構成においては、信頼性や安定性、高性能を求めることとする。「企画提案書」にシステム構成についての具体的内容を記載すること。

項番	カテゴリ	要素名	要件概要
1	システム構成共通	システム形態	事業者がシステムのサービスを提供すること。
2		構成	本システムが要求する性能や稼働率等を踏まえた、最適なサーバ構成とすること。
3			一般的な電源設備（コンセント、電気容量等）に対応していること。
4		性能・品質	区の規模、利用者数、端末数やシステム処理量が十分に考慮され、システムが支障なく動作できること。
5			負荷分散に配慮すること。
6		拡張性	機器やソフトウェアの追加が容易に行えること。
7			業務量（データ量や更新回数等）の増加、端末数の増加が発生した場合でも安定的なレスポンスが確保できること、ハードウェアの追加購入等に係るコストが

			最小限で済み、ソフトウェアの改修が基本的には不要であること等、十分な拡張性が考慮されていること。
8		障害対策	機器の障害発生時においても、業務が継続できるような仕組み（冗長化構成）であること。
9			運用に関する問合せ窓口及び障害受付窓口を用意すること。
１０	運用管理設計	ログ	サーバ等の運用情報は、ログ情報として 7 年程度保持されること。
１１			各種ログ情報については、参照方法や集計方法が提供され、障害の解析に使用できること。
１２			システムの各種ログ情報については、削除処理等のメンテナンスがなされ、システムの動作に影響を及ぼさないよう配慮されていること。
１３			削除処理等のメンテナンスされた過去のログに対し、検索や照会、出力等が可能であること。

（４）アクセシビリティ対応要件

多様な利用環境を想定し、高齢者や障害者を含めた全ての利用者が支障なく利用できるようにすること。

ア　原則、ウェブアクセシビリティに関する日本工業規格「JIS X 8341－3：2016」適合レベル「AA」に準拠するよう構築すること。

イ　全ページのテンプレートヘッダ部分に、文字拡大・背景色変更、音声読み上げ、ふりがな表示の項目ボタンを配置すること

ウ　「JIS X 8341-3:2016」、「みんなの公共サイト運用モデル（2016 年度改訂版）」に基づき、発注者と協議の上、「ウェブアクセシビリティ方針」を策定すること。

エ　アクセシビリティの評価は、総務省から配布されたアクセシビリティ評価ツール（miChecker）を用いた試験を全テンプレート及び主要ページに対して行うこと。「問題あり」や「問題の可能性大」の結果を受け、「問題あり」「問題の可能性大」がなくなるまで修正を行うこと。

また、ホームページ公開後、JIS X 8341-3:2016 のガイドラインに即して同試験結果を報告すること。

３　その他

・サーバについては、CMS・WWW サーバ等を本区外のデータセンターに設置し、受注者において管理・運用・保守を行う ASP または Saas 型とする。

・データセンターについては、【別紙３】データセンター要件の項目をすべて満たすものとする。

・災害時等緊急の場合、発注者以外の場所からでも区議会ホームページの更新が可能となる仕組みを提案すること。

・発注者は、作成や変更を依頼したい内容を業者にメールし、その内容を業者がコン

サルティングによりコンテンツ作成をします。確認用の領域にアップした内容を発注者の端末において職員がチェックし、公開作業を行います。

・CMS サーバのアクセス性能については、複数のユーザーが同時に作業をした際にもストレスなく作業ができること。(同時接続数は最大 14 ユーザーを想定)

・発注者の端末から CMS サーバへのアクセスは、接続元のグローバル IP アドレスにより制限すること。

・発注者の端末から CMS サーバへは、ブラウザを通じて、ID と Password 認証にてログインを行うこと。

・運用するサーバは、クロスサイトスクリプティング等の脆弱性に十分な対策を行うこと。

・セキュリティ対策には万全を期すこと。また、運用するサーバにはウィルス駆除ソフトにより、ウィルスの侵入を防止するとともに、常に最新のパターンファイルをダウンロードする環境を構築すること。

・CMS で作成・公開するページは、SSL 暗号化通信に対応させること。なお、SSL の更新手続きは、受注者が責任を持って行うこと。SSL 使用による費用が発生する場合は、その費用も見積りに含めること。

・登録職員やページ数の増加によるライセンス料金が発生しないこと。(当初ユーザーは 15 人、承認者は２人を想定。事務局内 PC は約 15 台)

・システムの導入後も定期的にリビジョンアップ等により機能強化を行えること。システム運用に係る機器は、データセンターに設置するものとし、その運用主体は ISO 27001 の認定取得企業であること。

・発注者の事務局内 LAN 上で動作するクライアント端末から作成・更新・管理業務が行えること。

第５章　移行要件

１　ホームページ移行

既存システムから新システムへの移行期間は必要期間とし、発注者と協議の上決定すること。

２　データ移行

新ホームページへのデータ移行作業は、原則すべて受注者が実施するものとする。

（１）データ移行範囲

原則、現行のホームページの全ページとする。移行コンテンツは、約 500 ページ（約 400MB）を想定。

（２）データ移行の要件

ア　移行後のコンテンツは、CMS を用いて修正・公開・削除作業が行える状態にすること。

イ　移行する際、アクセシビリティ上の問題が生じた場合は、受注者で修正すること。なお、不要な空白の削除作業や省略された曜日設定など受注者の判断で実施できるものは、全て受注者が行う。

ウ　移行作業にあたっては、発注者職員の負担を最低限に抑える方法を採ること。

（３）データ移行計画書の作成

移行作業の最適な方法、スケジュール、役割分担等を記した「データ移行計画書」を作成し、発注者の承認を得ること。

移行期間中に行われたページの更新分の差分についても、漏れなく反映できるよう、発注者と協議し、移行方法などの計画を立てること。移行期間において発生する差分についても、計画の中で考慮し、「データ移行計画書」に記載すること。

（４）データ移行の検証

データ移行計画書に基づきデータ移行がされているか確認すること。

検査は、ページ内容の移行に不整合がないかを確認するとともに、JIS X 8341-3:2016、総務省「みんなの公共サイト運用モデル（2016 年版）」をはじめとする基準・規定への対応を確認する。対応不十分な事項があった場合は、速やかに修正対応すること。

第６章　運用保守要件

１　業務内容

（１）ホームページの運用・保守業務

ア　港区議会ホームページの運営、技術支援・導入支援・コンサルティング業務

イ　インターネットサーバ環境の提供

外部からの不正アクセスや改ざん等を防ぐため、ウイルス対策、ＩＰＳ（不正侵入防御）、ＷＡＦ（ウェブアプリケーションウォール）など最新のセキュリティ対策を実施すること。

ウ　コンテンツの作成・修正・更新業務など、ホームページの更新は随時実施する。原則、保守時間内に発注者から依頼があったホームページの更新は当日中に対応すること。更新が翌日以降となる場合や保守時間外の緊急的な依頼対応は、発注者と協議の上、更新時間を決定すること。

エ　コンテンツ公開後の確認業務、修正業務、削除業務

オ　議会広報誌 HTML確認業務

カ　コンテンツ緊急アップ業務

キ　リンク切れ等のチェック、修正業務

ク　サイト内検索機能への単語登録業務

ケ　シンプルなリンク機能のメンテナンス業務

コ　アクセシビリティ向上ツールのメンテナンス業務

※委託内容には以下のようなホームページの企画、構成及びコンサルティング等の業務を含むものとする。

サ　サイト共通デザインの作成・修正

シ　インデックスページの作成・追加

ス　ホームページサイトの運営にかかわる支援

セ　ホームページ運営・維持メンテナンスのための技術支援

ソ　アクセスログの分析及び、結果を基にした改善提案

タ　アクセスログを解析し毎月報告すること

チ　セキュリティ監査を受け、その報告をすること

ツ　技術支援・導入支援・コンサルティング業務

(ア)ホームページ作成アドバイス、ホームページ改善案の提示・実施

(イ)サーバ及びシステム再構築時の技術支援・導入支援・データ移行支援

(ウ)ホームページガイドライン修正・更新等業務

テ　ホームページコンテンツ等のメンテナンスに係る業務

(ア)HTMLページコンテンツ等のメンテナンスに係る業務

(イ)新規ページの作成（4頁程度）

(ウ)既存ページの修正（1頁相当）（40頁程度）

(エ)既存ページの修正（1/2頁以上）（60頁程度）

(オ)既存ページの修正（1/2頁未満）（250頁程度）

(カ)既存ページの修正（簡易な修正）（400頁程度）

(キ)新規ページ等追加に伴うリンクの修正（10頁以上）（4件）

(ク)新規ページ等追加に伴うリンクの修正（10頁未満）（20件）

(ケ)サイト内のシステムの保守・管理（12カ月）

(コ)区議会だよりのセットアップ及び動作確認等一式（5回）

(サ)画像の新規作成（2件程度）

(シ)イラスト作成（2件程度）

※データの作成にあたっては、JIS8341-3改正版に準拠するほか、港区アクセシビリティガイドラインを遵守することとする。

（２）障害対応

・障害が発生した場合は、速やかに対応を行うこと。

・セキュリティの脆弱性が発見された場合は、発注者の同意を得た後、修正プログラム、セキュリティパッチの提供、バージョンアップ及び設定変更等の対策を速やかに行うこと。なお、事前に動作確認を行うなど、運用に影響を与えないこと。

・オリジナルのパッケージソフト、オープンソース（OSS）として公開されているパッケージソフトに関わらず、運用保守費用に本対応費用を含めること。

・稼働後も円滑なホームページ運営ができるようにCMS管理者を対象とした問い合わせ窓口の設置などのサポートを行うこと。

・システムに障害が発生した場合のために必要なバックアップを行うこと。なお、バックアップは媒体または別サーバに行い、日次５世代を管理すること。

・システムに障害が発生した場合、迅速に検知するためにシステム監視を行うこと。

・修理は、障害の発見から、平日午前8時30分から午後5時15分内においては1時間以内、夜間及び休日においては2時間以内に着手すること。

２　業務体制

・受注者は、原則として年間を通じて区役所の開庁時間内（午前８時30分～午後５時15分）に業務を行うこと。

ただし、業務履行時間については緊急情報更新業務等、あらかじめ必要と認めた場合は別途協議の上変更するものとする。

・保守業務は、リモートで実施可能とする。

・保守業務対応やシステム障害等の連絡窓口を一本化すること。

・上記問い合わせ窓口は、平日午前8時30分から午後5時15分（土日・祝日を除く）について電話・ファックス・メールでのサポートを行い、回答は、おおむね半日以内に行うこと。なお、サポートは、発注者のサイトを熟知した者が行うこと。業務上の必要性から原則、年間を通じ専任の対応者1名を選出すること。なお、対応者は受注者の正規社員とする。

・保守体制及び連絡先等を明確にした保守体制表を作成し、発注者と受注者の連絡体制や情報発信方法などを具体的に示すこと。

第７章　検査・運用試験

１　検査

（１）デザイン及びテンプレート

デザイン及びテンプレートの検査は、JIS X 8341-3:2016、総務省「みんなの公共サイト運用モデル（2016年版）」をはじめとする基準・規定への対応を確認する。対応不十分な事項があった場合は、速やかに修正対応すること。

（２）CMS導入・設定

受注者によるシステムテスト及びテスト結果に基づく改善が行われ、CMS 導入・設定を完了した段階で、発注者が【別紙１】ＣＭＳ機能要件一覧に基づき実装機能の動作確認を行うとともに、実際の動作を含めた検収を行う。原則として、【別紙１】ＣＭＳ機能要件一覧に示す必須機能(対応可能の回答した推奨機能も含む)全てが稼動できる状態になっていることを条件とする。

２　運用試験

受注者は、発注者の要求どおりに動作すること及び様々なブラウザで正常に表示されることを中心に試験を実施すること。また、試験において発生した障害は、必要に応じて発注者へ報告し、復旧作業及び原因の解明、対策を行うこと。

（１）機能確認試験を実施すること。

（２）CMS 稼動監視試験を実施すること。

（３）システムバックアップとリストア試験を実施すること。

第８章　成果物の納品

１　納品物

（１）構築業務

ア　プロジェクト計画書

イ　システム基本設計書

ウ　デザイン設計書

エ　デザインデータ一式

オ　ネットワーク構成図

カ　データ移行計画書

キ　データ移行確認書

ク　セキュリティ設計書

ケ　操作マニュアル

コ　運用マニュアル

サ　研修資料

シ　障害管理計画

ス　障害時対応マニュアル

セ　緊急時対応マニュアル

ソ　打合せ議事録

タ　その他、打合せにおいて必要となった書類など

（２）運用保守業務

ア　区議会ホームページ及び CMS サーバの保守運営作業実施報告書（月１回）

イ　操作マニュアル

ウ　運用マニュアル

エ　職員研修会資料

オ　アクセスログデータ（月１回）

カ　その他運営に必要なもの

※上記以外のものも発注者と協議の上、必要に応じて成果物を提出する。

２　納品形態

印刷物及び電子媒体（Word、PowerPoint、PDF 形式など）を各１部納品すること。

３　納品期限

書類等納品物は、契約完了日までに納品することとする。各納品物の納品時期については、発注者と協議の上、決定する。

第９章　その他契約条項

１　委託条件

（１）体制

ア　本業務を実施するに当たって、発注者との窓口になる受注者側の責任者を１名指定すること。受注者と発注者との間での貸与資料等の受渡しや返却及び受注者から発注者への各種報告、発注者から受注者への各種報告・指示等は、本責任者との間で実施する。

イ　本業務に類似した業務に関する作業実績を有する者が、担当者として携わること。

ウ　受注者は、契約締結後速やかに本委託の実施体制並びにプロジェクトを効果的に推進するためのプロジェクト計画書を定め、発注者への報告、説明を行うこと。

エ　本業務に従事する者を限定させ、業務に従事する者の氏名、所属、連絡先を記載した名簿を契約締結後、速やかに発注者に提出すること。

オ　原則として、業務を履行するメンバーは固定すること。メンバーを交代する場合は、発注者の承諾を得たうえで異動名簿を速やかに提出すること。

カ　受注者は、本契約に基づく業務を第三者に委託する場合、事前に発注者から承認を得ること。この場合において、再委託の内容、再委託先の会社概要、その他再委託先に対する管理方法等を書面により提出すること。

（２）作業の進め方

ア　本件作業を進め方については、本仕様書の内容を基本要件とし、発注者と受注者の協議の上、進めること。

イ　契約日から契約完了日（成果品の納品完了）までの期間に必要となる物品及び役務等は、全て受注者の負担と責任において、供給・実施すること。

ウ　受注者は、本業務実施に当たり、進捗・課題管理・リスク・仕様変更・品質等に係る受注者側のプロジェクト管理を適切に実施し、定期的に一定の様式を定めて発注者に報告、承認を得ること。

エ　受注者は、発注者との打合せ後の議事録について、原則として３営業日以内に作成し、発注者の承認を得ること。

オ　業務履行期間中に法令等の改正や性能を向上させるための技術的な指針等の改訂が発生した場合、発注者と協議の上、迅速に対応すること。

カ　受注者は、設計書等のレビュー、仕様上・設計上発生する問題点の検討・協議・調整等の実施と関連する会議への参加等、必要な作業を行うこと。

２　秘密保持

（１）　本業務により知り得た内容を第三者に漏洩してはならない。

（２）　本業務で作成したデータを第三者へ提供してはならない。

（３） 港区議会ホームページで使用するデータの複写、複製は発注者の依頼によるもの以外行ってはならない。

３　著作権の譲渡等

この契約の履行により作成される成果品の著作権等の取扱いは、次の各号に定めるところによる。ただし、受注者が、この契約の目的を遂行するために発注者に提供する文書、資料及びコンピュータ・プログラム、その他の著作物のうち、この契約以前から受注者が著作権を有していた部分は受注者に留保するものとする。

（１）受注者は、著作権法（昭和４５年法律第４８号）第２１条（複製権）、第２６条の３（貸与権）、第２７条（翻訳権、翻案権等）及び第２８条（二次著作物の利用に関する原著作者の権利）に規定する権利を発注者に無償で譲渡するものとする。ただし、係る成果品についての複製、二次的著作物作成、その他の形式で制限なく自ら利用し、他に利用させることのできる使用権を受注者に留保する。

（２）発注者は、著作権法第２０条（同一性保持権）第２項第３号又は第４号に該当しない場合においても、その使用のために、成果品を改変し、また、任意の著作者名で任意に公表することができるものとする。

（３）受注者は、発注者の書面による事前の同意を得なければ、著作権法第１８条（公表権）及び第１９条（氏名表示権）を行使することができない。

４　受注者の責務

（１）受注者の責務において、区民・業務関係者等に対する安全対策に万全を期し、事故防止に関する必要な措置を講ずること。

（２）受注者は、常に善良なる管理者の注意をもって業務を遂行し、業務の進捗状況について確認の上適宜報告すること。

（３）関係法令等を遵守し、その適用及び運用は受注者の責任において適切に行うこと。

（４）受注者は、この契約の履行に際し知り得た情報を機密情報として扱い、他の目的に使用し、又は第三者に開示、漏えいしてはならない。契約完了後又は解除後も同様とする。

（５）受注者は、本契約の履行に当たり、「港区職員の障害を理由とする差別の解消の推進に関する要綱」の趣旨を踏まえ、適切な対応を図ること。

（６）受注者は、個人情報について、【別紙４】「個人情報等取扱いに関する特記事項」を遵守しなければならないものとする。

（７）受注者は、業務の遂行に際して、【別紙２－１】港区情報安全対策指針及び【別紙２－２】港区議会情報安全対策基本方針を遵守しなければならないものとする。また、受注者は、発注者が実施する、「港区情報安全対策指針」及び「港区議会情報安全対策基本方針」の遵守状況に関する点検作業に対応するものとする。点検作業には、情報セキュリティにおいて問題が発生した場合の検査、あるいはセキュリティ監査等が該当す

る。

（８）受注者は、システム運用管理業務を担当する者の氏名の一覧表を提出すること。

（９）受注者は、「港区職員のハラスメントの防止等に関する要綱」を遵守すること。また、ハラスメントが発生した場合は、発注者と連携して適切に対応すること。

(10）受注者は、本契約の履行に当たり、「港区環境美化の推進および喫煙による迷惑の防止に関する条例」（平成９年港区条例第４２号）第９条に規定するみなとタバコルールを遵守すること。

(11）受注者は、本契約の履行に当たり、基本的人権を尊重し、個人の尊厳を守り、あらゆる差別をなくすために適切な対応を図ること。

(12）受注者は、本契約の履行に当たり、地球温暖化防止のため、省エネルギー対策に努めること。

５ 発注者の追完請求権

（１）受注者が納入する物品、あるいは受注者の作業に契約不適合があるときは、発注者は、受注者に対して相当の期限を定めてその契約不適合の追完を請求し、又は追完に代え、若しくは追完とともに損害の賠償を請求することができる。

（２）前項の規定による契約不適合の追完又は損害賠償の請求は、検査完了日から１年以内に、これを行わなければならない。ただし、検査によって契約不適合を発見することがその性質上合理的にできない場合は、当該契約不適合を知った時から１年以内とする。

６　環境により良い自動車利用について

（１） 本契約の履行に当たって自動車を使用し、又は利用する場合は、都民の健康と安全を確保する環境に関する条例（平成１２年東京都条例第２１５号）の規定に基づき、次の事項を遵守すること。

ア　ディーゼル車規制に適合する自動車であること。

イ　自動車から排出される窒素酸化物及び粒子状物質の特定地域における総量の削減等に関する特別措置法（平成４年法律第７０号）の対策地域内で登録可能な自動車利用に努めること。

（２）電動車を始め、低公害・低燃費な自動車利用に努めること。電動車とは、電気自動車（ＥＶ）、プラグインハイブリッド自動車（ＰＨＶ）、燃料電池自動車（ＦＣ）、ハイブリッド自動車（ＨＶ）の総称を指す。

（３） 適合の確認のために、当該自動車の自動車検査証（車検証）、粒子状物質減少装置装着証明書等の提示又は写しの提出を求められた場合には、速やかに提示し、又は提出すること。

（４）本契約の履行に当たって観光バスを使用する場合は、「観光バスの環境性能表示に関するガイドライン（平成29年３月16日付改正28環改車第790号）」に規定する評価基

準Ａランク以上の車両を供給すること。

７　その他

（１）受注作業中の疑義については発注者に連絡し協議すること。

（２）発注者による立ち入り検査・監査及び調査が必要になった時は、直ちに応ずること。

（３）事故が発生した際は直ちに発注者に報告すること。

（４）発注者の施設等は常に善良なる管理者として注意を払って使用し、本業務以外の目的で使用しないこと。

（５）発注者は本業務履行上の理由により区役所内で業務を行う者又は作業者の変更が必要な場合、事前に受注者へ連絡し協議の上変更することができる。

（６）本仕様書で定められていない事項について疑義が生じた場合は発注者と随時協議すること。

８　連絡先

担当　港区議会事務局議会広報担当　渡邊

TEL 03-3578-2111内線 2920

CMS機能要件一覧表

【要求要件】
必須機能（必ず実装する機能。オプション、カスタマイズ、代替案可）
推奨機能（可能な範囲で実装する機能。オプション、カスタマイズ、代替案可）

大分類	小分類	No.	機能要件	【要求要件】必須/推奨	対応可否	備考/実現方法
CMS（コンテンツ・マネージメント・システム）要件						
システム全般	システム全般	1	システムは庁舎外のデータセンターに設置されたものを利用すること。運用に必要な環境を受託者が全て用意すること。	必須		
		2	区議会事務局の職員端末環境で動作しソフトウェアのインストールの必要がないこと。 インターネット利用環境 OS：Microsoft Windows11 ブラウザ：Microsoft Edge、Google Chrome、FireFox	必須		
		3	導入するCMSは開発ベンダーによる保守が確立された製品とし、脆弱性が発見された際への対応を迅速に行えること。	必須		
		4	都道府県情報セキュリティクラウドの趣旨を理解し、構築時および運用保守期間中において追加費用がかからないこと。	必須		
		5	公開サイトは、特殊な挙動の動的ページを除き、静的HTMLにより構成される仕組みであること。 CMSサーバで生成されたHTMLファイルをWebサーバにアップロードする仕組みであり、更新されるページと関係するページ全てで整合性がを維持できること。	必須		
		6	Webサーバにはサーバ証明書を設置すること。 なお、SSL の導入及び更新手続きについては費用に含み、受託者が責任を持って行うこと。	必須		
		7	ページ編集時や承認時の各操作など、日常的に行う操作については、操作者がストレスを感じない応答時間でのレスポンスを利用期間中確保できるスペックのサーバを提供すること。	必須		
		8	サーバは本団体専用とし、他団体等の影響を受けないこと。	必須		
		9	サービス提供環境におけるサーバ・ネットワーク機器は冗長化をはかること。	必須		
		10	ユーザライセンスは無制限で提供すること。ユーザ数、ページ数等で費用が変わらないこと。	必須		
		11	文字コードはUTF-8であること。	必須		
		12	レスポンシブデザインやリキッドデザインなど、パソコン、スマートフォン、タブレット型端末等機器の種類やサイズに応じて表示内容が最適な状態となること。	必須		
		13	CMSは、定期的にリビジョンアップ等により機能強化を行えるものとすること。	必須		
		14	ページ内のコンテンツ部分を、A4縦サイズで内容が損なわれることなく印刷できること。	推奨		
管理機能	一般	15	ログイン前・後のメインメニュー画面の目立つ位置に、管理者からのお知らせを掲載できること。	推奨		
	ユーザ設定	16	各職員のPC端末から、ユーザIDとパスワードによりシステムへのログイン認証が可能であること。	必須		
		17	ユーザIDを組織（部・課・係等）で割り当てることを想定して、同じユーザIDで同時ログインできること。	必須		
		18	パスワードは、文字数（8文字以上等）と文字種類（英数字混合等）の入力制限ができること。	必須		
		19	管理者は、CMSの管理画面上でユーザー情報（ユーザID・パスワード・権限設定等）の管理（追加・修正・削除）ができること。登録できるユーザ情報の数は上限がないこと、または十分な数を登録できること。	必須		
		20	作成者が自らパスワードを変更できる機能を有すること。	必須		
		21	システム全体の操作権限を持つ管理者用のIDを設定できること。	必須		
		22	ページ作成を行う作成者用のIDとページ承認を行う承認者用のIDを設定できること。	必須		
		23	CMSに登録されているユーザ情報を、CSV等の形式で出力できること。	推奨		
		24	CSV等の形式で作成されたユーザ情報をCMSに取り込めること。	推奨		
		25	複数回ログインを失敗した場合、アカウントを自動的に凍結できること。また管理者によるログイン凍結の解除ができること。	推奨		
		26	アカウントの権限には、管理者・承認者・作成者の3種類あり、ログイン後の画面や使用できる機能・メニューは権限ごとに制限されること。	必須		
	ログ管理	27	ログイン・ログアウトのログを確認できること。	必須		
		28	ページID、操作内容、操作者名、操作日時などの操作ログを確認できること。	必須		
		29	ページ編集に関するログを取得し確認できること。	必須		
		30	ページ単位で更新履歴を保持し、作成者・承認者は過去の操作履歴やその際のコメントを確認できること。	推奨		
	組織変更	31	管理者は、CMSの管理画面上で組織情報（部署名・電話番号・事務分掌等）の管理（追加・修正・削除）が行えること。登録できる組織情報の数は上限がないこと、または十分な数を登録できること。	必須		
		32	各ページに掲載する署名（問い合わせ先）を作成・編集・削除できること。	必須		
		33	ページ下部に表示するお問い合わせ先は、各組織毎に複数の署名を作成することができ、各ページを作成する際に選択できること。	推奨		
		34	組織改編の予約・実行時に、ページ下部に表示される署名（問い合わせ）も自動で更新されること。	推奨		
	緊急時対応	35	災害発生等に緊急情報コンテンツタイトルリストはトップページの目立つ位置に配置できること。	必須		
		36	緊急情報コンテンツは権限を付与された職員が承認者の承認を必要とせずに、最小限の操作で公開し、TOPページ掲載できること。	必須		

CMS機能要件一覧表

【要求要件】
必須機能（必ず実装する機能。オプション、カスタマイズ、代替案可）
推奨機能（可能な範囲で実装する機能。オプション、カスタマイズ、代替案可）

大分類	小分類	No.	機能要件	【要求要件】必須/推奨	対応可否	備考/実現方法
		37	災害発生等の緊急時には、権限を付与された職員が最小限の操作でトップページ全体のデザインをテキスト中心のデザインに切り替えられること。	必須		
		38	緊急情報と関連したイベントの中止情報などは「必須なお知らせ」として、権限を付与されたユーザーが承認を必要とせずトップページの目立つ位置に公開できること。	推奨		
		39	緊急情報の編集においては、CMSの各種ページと同様の操作方法で同等の機能を活用できること。（時系列で管理したり、更新日時を自動で表示したりできること。）	推奨		
ワークフロー	承認ルート	40	作成者は、ページ作成のみで承認は行えないこと。	必須		
		41	コンテンツ作成から公開に至るまでの承認ルートとして、作成者（作成、確認依頼、保存）→承認者（所属長が公開依頼、差戻）→公開者（管理者が公開承認、差戻）とする機能があること。（2段階承認の設定）	必須		
		42	管理者は、組織改変等に伴う承認ワークフローの変更が容易に行えること。	推奨		
		43	承認者が不在の時、代理承認などの手段によってコンテンツを公開することができること。（代決権限の設定）	必須		
	作成・編集作業	44	作成途中にコンテンツを一時保存でき、再ログイン後に途中段階から編集が再開できること。	推奨		
		45	自身が管理している作成中のページや承認依頼中のページを一覧で表示する機能があること。	推奨		
		46	自身が管理している公開終了間近のページをワンクリックで一覧表示できること。	推奨		
		47	承認依頼中のページを作成者自らがキャンセルし、内容を再編集できること。（作成者による承認依頼の差戻、引き戻しができ、修正等ができること。）	推奨		
		48	作成中は、他の利用者が同一のコンテンツを編集できないよう自動ロックすること。	必須		
		49	作成者からの承認依頼がメール等によって承認者に自動的に送信されること。	推奨		
	承認作業	50	内容確認のため、ページのプレビューが可能であること。（本ページからのリンク先ページも目視確認ができること。）	必須		
		51	承認者による差し戻しができ、差し戻し時にはコメントを付記できること。メールにより差し戻しがあったことを通知するメールが送信できること。	推奨		
		52	承認者は、作成者と同様に申請されたコンテンツの修正・編集・アクセシビリティチェックが可能であること。	必須		
		53	一定期間承認処理がされないページについて、自動的に催促メールを送信できること。	推奨		
		54	管理者は複数のページを一括して承認できること。	推奨		
		55	管理者は、承認者の承認を必要とせずにページを即時公開できること。	必須		
		56	承認者がページ承認時に変更箇所があった場合、変更箇所を視覚的に確認できること。	推奨		
編集機能	ヘルプ	57	職員が円滑にホームページの作成を行えるように、専用のオンラインマニュアルの参照ができること。	必須		
	全般	58	CMSの操作・ページ作成には、ソースの編集を一切必要としないこと。	必須		
		59	トップページを除く全ページにパンくずリストを自動生成すること。	必須		
		60	サイトマップを編集できること。	必須		
	テンプレート	61	テンプレートを利用したページ作成が可能であること。	推奨		
		62	所属ごとに利用できるテンプレートを制限できること。	推奨		
		63	テンプレートは所属の担当者が作成・登録することができ、所属内だけで利用できること。	推奨		
		64	管理可能なテンプレート数に上限がないこと。	推奨		
		65	管理者は、全ての部署で使用できるテンプレートの新規作成・登録ができること。	推奨		
	CMS内検索機能	66	管理コンテンツ状態（「作成中」「公開中」「公開終了」等）で検索抽出できること。 他の検索条件と組み合わせて検索抽出できること。	必須		
		67	フリーキーワードにて全文検索できること。他の検索条件と組み合わせて検索できること。	必須		
		68	検索で抽出されたコンテンツリストをCSV形式で出力できること。	推奨		
		69	ページタイトル、ページIDを検索対象としてキーワード検索できること。他の検索条件と組み合わせて検索できること。	推奨		
		70	作成者（課・係）で検索ができること。他の検索条件と組み合わせて検索できること。	必須		
		71	コンテンツ管理編集画面では、担当者の所属部署で管理するページのみが対象となり、公開前の他部署で作成中のページは検索対象にはならないこと。（採用情報、施行前の施策等）	推奨		
		72	検索結果一覧には「タイトル」「作成者」「状態（作成中・公開・公開終了）」「公開期間」「最終更新日」等が表示されること。	推奨		
		73	検索結果の一覧画面でページの容量（ページデータサイズ、添付ファイルサイズ）を確認できること。 またサイズの昇順・降順で並び替えることができること。	推奨		

CMS機能要件一覧表

【要求要件】
必須機能（必ず実装する機能。オプション、カスタマイズ、代替案可）
推奨機能（可能な範囲で実装する機能。オプション、カスタマイズ、代替案可）

大分類	小分類	No.	機能要件	【要求要件】必須/推奨	対応可否	備考/実現方法
		74	特定の日本語キーワードが含まれる語句を検索し、一括置換できること。	推奨		
		75	検索結果より、該当するページを選択してページの編集ができること。	推奨		
	コンテンツ作成	76	ページデザインは、スタイルシートで管理され、作成者がデザインを意識することなくページ作成ができること。	推奨		
		77	コンテンツデータの入力フォームは、見出し、テキスト、画像、ファイルリンク、表などの掲載データごとにパーツ化されていること。	推奨		
		78	ページ単位にてメニューボタンが備わっており、ページの作成・編集・削除、コピー、プレビューを操作できること。	推奨		
		79	ページの状況（公開中、非公開、承認中、一時保存など）をわかりやすく表示されること。	必須		
		80	ページ作成時に、新着情報への表示、イベントカレンダーへの表示、公開日・終了日の設定、カテゴリへの掲載等の公開に関する各種設定を行うことができること。	推奨		
		81	内容確認のため、公開時と同じ状態でページ全体のプレビューが可能であること（本ページからのリンク先（内部リンク・外部リンク共に）ページも目視確認ができること）。	推奨		
		82	未来の日時を指定することで、指定した日時におけるサイト全体をプレビューできること。	推奨		
		83	CMS内で、公開イメージをA4縦サイズで印刷可能なファイルで形式で出力できること。	推奨		
		84	公開ページ全体イメージを画像として出力・保存できること。	推奨		
		85	ページの作成日（更新があった場合は更新日）は自動で表示されること。また、任意の日時に設定できること。	必須		
		86	ページ編集時に必須入力箇所が表示できること。また、必須入力箇所が未入力であった場合は、そのまま公開許可申請処理が行えないこと。	推奨		
		87	予め管理者が登録したサイト内で使用を禁止する用語を入力した場合、エラーとなり登録できない、もしくは適切な表記へ自動変換する機能を有すること。（例：子供→子ども）	必須		
		88	ページの作成時に誤った操作をした場合、簡易な操作で直前の状態に戻せる機能を備えること。	必須		
		89	トップページの新着表示の可否を選択できること。	推奨		
		90	Microsoft Word・Excelとの互換性を持ち、入力一般、及び表の作成の際にはコピーアンドペーストが可能であること。また、その際不要なタグ・非推奨タグは削除できる機能を有すること。	推奨		
		91	既定項目については、プルダウンやチェックボックス等で選択できること。	推奨		
		92	ページ作成時、担当所属名・連絡先（問い合わせフォーム）等の署名が組織情報に基づき自動的に入力されること。	推奨		
		93	HTMLの知識がない職員でも、簡単な操作で表が作成できること。行、列の追加や削除、見出し（列・行）セルの設定、幅のパーセント指定などが、HTMLソースを直接編集することなく、簡単な操作で編集できること。	必須		
		94	管理者のみHTMLソースの直接編集が可能であること。	推奨		
		95	コンテンツをコピーし、編集するなど、転用が可能であること。	必須		
		96	作成したコンテンツの保存・削除が可能であること。	必須		
		97	ゴミ箱機能を備え、削除を行っても一定期間、完全削除されないこと。（作成者・承認者はページをゴミ箱に移動でき、管理者または受託者はゴミ箱内のページを空にできること。）	推奨		
	ウェブアクセシビリティ	98	コンテンツの作成・編集時にアクセシビリティチェックができること。	必須		
		99	公開許可申請時に、アクセシビリティチェックにより不適切な入力があり「エラー」が表示された場合、指摘箇所を修正しなければ、公開許可申請処理が行えないこと。	必須		
		100	アクセシビリティチェック結果画面から指摘事項が表示され、理由と修正方法が表示されること。	必須		
		101	ウェブアクセシビリティチェックは、チェックボタンのクリック等1回の操作で集約してエラー及び警告一覧が表示されること。	必須		
		102	HTML言語を意識することなく、h1属性（見出し）を付けることができること。また見出し順序のチェックが行われること。	推奨		
		103	HTML言語を意識することなく、alt属性（代替テキスト）を付けることができること。	推奨		
		104	alt属性について未入力や具体的でない単語を入れた場合は画像を登録できないこと。未入力の場合は、警告を表示すること。 例：「画像」のみ入力し登録しようとした場合	推奨		
		105	アクセシビリティ上、使用できない単語を自動変換する単語辞書と、使用に関して注意喚起する単語辞書を分けて登録できること。	推奨		
		106	上記について、運用開始後でも管理者がメンテナンス（追加・変更・削除）できること。	推奨		
		107	HTML言語を意識することなく、表の見出しやキャプションを簡単に設定できること。	推奨		

CMS機能要件一覧表

【要求要件】
必須機能（必ず実装する機能。オプション、カスタマイズ、代替案可）
推奨機能（可能な範囲で実装する機能。オプション、カスタマイズ、代替案可）

大分類	小分類	No.	機能要件	【要求要件】必須/推奨	対応可否	備考/実現方法
		108	表の幅はパーセント指定で設定できること。	必須		
		109	表の幅は固定値（ピクセル）でも設定できること。	推奨		
		110	全角英数字は、半角英数字へ自動置き換えできること。	必須		
		111	半角カナは、全角カナへ自動置き換えできること。	必須		
		112	機種依存文字を自動置き換え、及び警告表示が可能であること。機種依存文字及び置き換え文字について、一般的な内容で提案及び初期設定すること。	推奨		
		113	上記について、運用開始後でも管理者がメンテナンス（追加・変更・削除）できること。	推奨		
		114	日付と時間表記等を市が定めるルールに従い、自動置き換え及び警告表示できること。（例：2015/4/1→2015年4月1日、（月）→（月曜日）、13:30→午後1時30分）	推奨		
		115	色覚異常の特性に応じた掲載画像の見え方チェックが可能で、チェックにより不適切の場合は、画像の色遣いの変換が可能なこと。	推奨		
		116	画像化された文字を掲載しようとする際に、背景色と文字色のコントラストチェックができること。	推奨		
	公開設定	117	ページ作成時にURLを任意に設定できること。設定しない場合はシステムが自動で割り振ること。	必須		
		118	コンテンツの公開・終了期間の設定が、日時・時間単位で可能なこと。	必須		
		119	公開期間を「無期限」とする設定が容易にできること。	必須		
		120	公開期間が終了したHTMLや使用した関連ファイル等は、Webサーバから自動的に削除されること。	推奨		
		121	公開期間が終了したページは、CMSサーバには非公開状態として保存され再利用できること。	推奨		
		122	緊急情報などのコンテンツについては、即時公開（5分以内）が可能であること。	必須		
		123	公開期間の設定において公開日時・終了日時を一定間隔で設定でき、公開できること。	推奨		
		124	ページの公開日（更新があった場合は更新日）は自動で表示されること。また、任意の日時に設定できること。	必須		
		125	公開中のコンテンツを修正し、上書きの日時を予約指定する機能があること。 例：2月1日に公開中ページを修正し、修正した内容を3月1日に公開（2月中は元の内容で公開）	推奨		
	画像	126	画像を簡単な操作で配置できること。また、同一ページ内に掲載数の制限なく複数配置できること。	必須		
		127	CMSにてアップロードされた画像ファイルを任意のサイズにリサイズ及びトリミングなどができること。	必須		
		128	定められた大きさ以上の画像を登録する場合、自動的にリサイズされること。	推奨		
		129	英数字以外のファイル名を登録できないこと。	推奨		
		130	同一ファイル名でアップロードした際に、上書き登録かファイル名を変更するかの警告を表示し選択できること。	必須		
		131	管理者は全課で使用できる画像などを登録できる共有フォルダに登録できること。	推奨		
		132	作成者が共用で使用できる画像をキーワード検索できること。	推奨		
		133	画像にリンクを設定できること。	必須		
		134	掲載画像の一部にモザイク処理を追加できること。	推奨		
		135	画像の回転操作ができること。	必須		
		136	登録できる画像のファイル種別（JPEG、GIF、PNGのみ等）を制限できること。	推奨		
	イベント情報	137	コンテンツの作成時の操作の流れで、イベントカレンダーへの表示設定が行えること。	推奨		
		138	イベントカレンダ上に掲載するイベント記事を利用者はカテゴリ等で絞り込み表示検索ができること。	推奨		
		139	イベントカレンダーに表示されるイベント記事タイトル付近に、参加申込の要不要、申込期間を表示できること。	推奨		
		140	イベント開催日は複数日指定や期間指定ができること。	推奨		
		141	不定期開催のイベントについて、カレンダーに表示設定できること。	推奨		
	リンク管理	142	情報量が多いページの編集時に、同一ページ内の「見出し」位置に移動するページ内リンクを簡単に表示できること。（アンカー機能）	推奨		
		143	上記ページ内リンクに表示させるリンクリストは、見出しのレベル単位で表示の有無を制御できること。	推奨		
		144	内部リンクは、サイトツリーから選択するなど、アドレス入力やファイル名指定の必要がなく設定できること。	推奨		
		145	外部リンクは、「（外部リンク）」などの文言もしくはアイコンが自動的に設定されること。	推奨		

CMS機能要件一覧表

【要求要件】
必須機能（必ず実装する機能。オプション、カスタマイズ、代替案可）
推奨機能（可能な範囲で実装する機能。オプション、カスタマイズ、代替案可）

大分類	小分類	No.	機能要件	【要求要件】必須/推奨	対応可否	備考/実現方法
		146	CMS内で作成中・承認中のページにリンクを貼ることができること。リンクを貼る方法はリストやプレビューから選択する方式であること。	推奨		
		147	内部リンクは、システムが自動的に管理し、リンク先ページが非公開時、ページ削除時、カテゴリ移動時にリンク切れを発生させないこと。	必須		
		148	CMSに登録されている全ページに対してリンクチェックが実行でき、ページごとにリンク切れチェック結果が確認できること。	必須		
		149	作成者は編集中ページがサイト内の別ページからリンク設定されているページ一覧を確認できること。（被リンク一覧表示）]	推奨		
		150	新規に作成したページのアドレスは公開前に確認できること。	必須		
		151	リンクのテキストに適切ではない可能性のあるテキスト（「ここをクリック」など）が含まれていないかチェックできること。	推奨		
		152	公開が終了したページに対して他のページからリンクされている場合、公開が終了した時点で自動的にリンク設定が削除されること。（閲覧者がクリックしてリンク先がない状態が発生しないこと）	推奨		
		153	上記の場合、編集画面からはリンクが切れていることを検知し、ページ所管課に通知されること。	推奨		
	ファイル管理	154	ページファイル名は自動で付与されること。	推奨		
		155	添付ファイルを掲載する際は、ファイルの種類（アイコンと名称）とファイル容量が自動的に表示されること。（例：掲載文の文頭にはアイコンが表示され、文末にはファイル名と容量が自動的に表示されること。）	推奨		
		156	ページにPDF等の各種ファイル（Microsoft Word・Excel、PDFは必須）が添付できること。	必須		
		157	ページに添付できるファイルの種類・容量を制限できること。また、添付ファイルの種類・容量が制限の範囲外である場合はアップロードできないこと。	必須		
		158	添付ファイルをCMSに一括でアップロードできること。	必須		
		159	添付ファイルの閲覧にソフトが必要な場合には、自動的に閲覧方法などが表示されること。PDFをリンクした場合、AdobeReaderのダウンロードを促す案内が自動で挿入されること。	必須		
		160	同名のファイルをアップロードしようとした場合は警告を表示すること。その際、アップロード画面からファイル名称を変更してアップロードできること。ただし、自動でファイル名を付与する場合は警告が表示されなくても可能とすること。	推奨		
		161	添付するファイルをアップロードした際に、CMS編集画面上でファイルの中身をプレビューできること。	必須		
	地図機能	162	外部API（GoogleMapsなど）を利用した地図機能を、住所の入力、緯度・経度情報の入力等の容易な作業で表示・利用できること。	必須		
		163	GoogleMapを活用するうえで別途経費が必要となる場合は、CMSの利用料に含めること。	必須		
		164	地図に複数のポイントを設定できること。	必須		
	RSS配信	165	サイト内の全ページでRSS配信ができること。	推奨		
		166	カテゴリごとの新着情報をRSSフォーマットで出力できること。	推奨		
	ソーシャルメディア連携	167	全てのページにXの「ポスト」ボタンやFacebookの「いいね」ボタン等のSNS連携ボタンを設置でき、作成者で表示非表示が制御できること。	推奨		
		168	更新情報をSNSに連携投稿できること。	推奨		
		169	複数のSNSアカウントに対して、複数の連携設定が行えること。	推奨		
		170	連携投稿の停止・開始を管理画面から制御できること。	推奨		
		171	自動投稿配信が失敗した際のエラーを確認できること。	推奨		
	スマートフォン・タブレット等	172	レスポンシブウェブデザインにより閲覧者の端末画面の解像度に合わせて最適化され表示できること。	必須		
公開ホームページ	閲覧環境	173	サポート期間内で標準的なブラウザ（Safari、Google Chrome、Firefox、Edge）で支障なく閲覧できること。	必須		
		174	すべてのページをSSL通信により表示させること。	必須		
	イベントカレンダー	175	イベントカレンダーは月単位で表示できること。	推奨		
		176	イベントは月ごと日ごとのリスト表示もできること。	推奨		
		177	カテゴリごとに絞り込んでイベントカレンダーを表示できること。	推奨		
		178	イベントカレンダーを開いた当日に開催しているイベントを目立つ位置にわかりやすく表示できること。	推奨		
		179	日付やカテゴリ、施設やキーワードなど、イベントページにある情報を指定してイベント検索ができること。	推奨		
	FAQ機能	180	よくある質問（FAQ）ページが集約された専用FAQサイトが作れること。	必須		
		181	FAQコンテンツはカテゴリにより分類され、キーワードによる検索が可能であること。	必須		

CMS機能要件一覧表

【要求要件】
必須機能（必ず実装する機能。オプション、カスタマイズ、代替案可）
推奨機能（可能な範囲で実装する機能。オプション、カスタマイズ、代替案可）

大分類	小分類	No.	機能要件	【要求要件】必須/推奨	対応可否	備考/実現方法
		182	キーワード検索結果は更新日の昇順・降順など並び替え、よく見られている順での並び替えができること。	推奨		
		183	よく見られているFAQの一覧をFAQサイトに掲載できること	必須		
		184	よくある質問には、関連ページへのリンクや問い合わせ先を容易に設定できること。	必須		
	アクセス解析	185	アクセス解析が可能であること。	必須		
		186	検索されたキーワード、閲覧者の接続ポイント（都道府県）を解析及び集計できること。	推奨		
		187	集計結果を数値およびグラフで表示できること。	推奨		
		188	CSVファイル等で出力可能であること。	必須		
	ウェブアクセシビリティ対応	189	閲覧者がキーボード操作のみでサイトを利用できること。	必須		
		190	閲覧者が任意に文字の拡大を制御できること。	必須		
	閲覧支援	191	外国語自動翻訳機能を公開ページで提供できること。翻訳は、英語、中国語（簡体語・繁体語）、韓国語、とする。	必須		
	ページ表示	192	トップページの目立つ位置に画像等を複数掲載したスライドショーが表示できること。また画像は、職員が簡単に変更でき、差し替えについて表示期間の予約ができること。	推奨		
		193	上記のスライドショーは、閲覧者が表示を制御できること。	推奨		
		194	各ページの同じ位置にグローバルナビゲーションを自動的に生成できること。	必須		
		195	カテゴリーページは、配下に情報がない場合、非表示にできること。	推奨		
		196	カテゴリの名称変更等があったときは、それに紐づくコンテンツ及びパンくずリストも同時に変更すること。	必須		
		197	パンくずリストは、そのページの掲載場所と実際に閲覧者が表示した履歴を自動表示できること。	必須		
		198	閲覧コンテンツが複数のカテゴリに掲載設定されている場合、ページの下部に「別ルート」が自動表示されること。	推奨		
		199	複数のカテゴリに掲載設定されている内容が同一のコンテンツは、URLが同じで、アクセス解析時に集約された集計が行えること。	推奨		
		200	閲覧コンテンツの同じカテゴリ・階層内にあるコンテンツへのリンクを表示するローカルナビゲーションを自動的に生成できること。	推奨		
		201	新着情報、おすすめ情報等の「特定情報」は、各カテゴリページにも配置できること。	推奨		
		202	トップページや主要なページに、「特定情報」（お知らせ・新着情報・イベント情報等）のリンクを一覧で表示できること。	推奨		
		203	トップページの目立つ位置に、災害情報、緊急情報等のリンクリスト（テキスト表示・詳細ページへのリンク）を表示できること。	必須		
		204	新着情報など一覧ページに表示させるサムネイル画像を登録できること。	推奨		
	サイト内検索	205	各ページの見やすい位置にサイト内キーワード検索機能を表示できること。	必須		
		206	サイト内の全文検索機能を有すること。	必須		
		207	定期的にサイト内のクロールを実施し、最新情報が検索対象となること。	必須		
		208	広告の出ないサイト内検索を提供できること。	必須		

港区情報安全対策指針

（個人情報等を守るための事務処理指針）

平成１５年（２００３年）８月

港　　区

令和５年（２０２３年）９月改定版

港区平和都市宣言

かけがえのない美しい地球を守り、世界の恒久平和を願う人びとの心は一つであり、いつまでも変わることはありません。

私たちも真の平和を望みながら、文化や伝統を守り、生きがいに満ちたまちづくりに努めています。

このふれあいのある郷土、美しい大地をこれから生まれ育つこどもたちに伝えることは私たちの務めです。

私たちは、我が国が『非核三原則』を堅持することを求めるとともに、ここに広く核兵器の廃絶を訴え、心から平和の願いをこめて港区が平和都市であることを宣言します。

昭和６０年８月１５日

港　　区

港 区 情 報 安 全 対 策 指 針

目　　次

港区情報安全対策基本方針

（平成１５年８月１５日
１５港政情第３１２号）

改正　平成 22 年 3 月 21 日 21 港総情第 2973 号
改正　平成 27 年 6 月 1 日 27 港総情第 1378 号
改正　平成 28 年 4 月 1 日 27 港総情第 6454 号
改正　平成 31 年 4 月 1 日 30 港総情第 4563 号
改正　令和 2 年 4 月 1 日 31 港総情第 4410 号
改正　令和 4 年 9 月 1 日 4 港総情第 1933 号
改正　令和 5 年 4 月 1 日 4 港総情第 4687 号

１　基本的考え方

インターネットに代表される高度情報通信ネットワーク社会の進展は、私たちの生活や仕事、人と人とのコミュニケーションに大きな変化をもたらしています。ネットワーク化の促進によって、誰もが様々な情報にいつでもどこからでも容易にアクセスできるようになり、私たちの暮らしはより便利に、より快適になるものと期待されています。

区は、急速に進歩する情報技術を積極的に活用することにより、区民に様々な行政サービスをスピーディに提供し、区政情報の提供・公開と区民の区政参加を促進するデジタル環境の構築に取り組んでいます。また、国や他の自治体等とのネットワークシステムに参加し、より密接な連携・協力関係のもとで、新たな区民サービスを展開していきます。

行政サービスの高度情報化は、区と区民との新しい関係を創り出し、区民サービスの一層の向上や効率化の促進など大きな効果が期待されます。その反面、情報の改ざん・漏えいを目的とする不正アクセスや、コンピュータの機能を麻痺させるコンピュータウイルスの侵入等、安全で安定した行政サービスを脅かす存在が増加しています。

情報システムの障害はもとより、個人情報の改ざん・漏えい等は絶対にあってはならないことです。区民が安心して行政サービスを利用するためには、個人情報や区の情報システムが安全に管理されていることが不可欠です。

区は、行政サービスの情報化の推進にあたって、個人情報の保護を最優先とした適切な安全管理のもとに、区が収集・蓄積した情報を様々な脅威から守ります。

さらにネットワークシステムの一員として、区民に対してはもちろんのこと、国や他の自治体等へ、ネットワークを通じて脅威を及ぼさないよう適切な措置を講じ、システム全体の社会的信頼の確保に取り組みます。

区は、こうした基本的な考え方に基づいて、体系的、総合的かつ継続的な情報セキュリティ対策を実施し、区が保有する情報資産（情報システム及び情報システムで記録・処理される情報等）及び一定の手続きのもとに区の情報システムに接続する職員個人が所有する携帯情報端末を適切に保護することにより、区民から信頼される安全なデジタル環境を実現しま

す。

2　港区情報安全対策指針の位置付け

区は、情報セキュリティ対策に関する方針、行動指針等を次のように体系的に整備します。

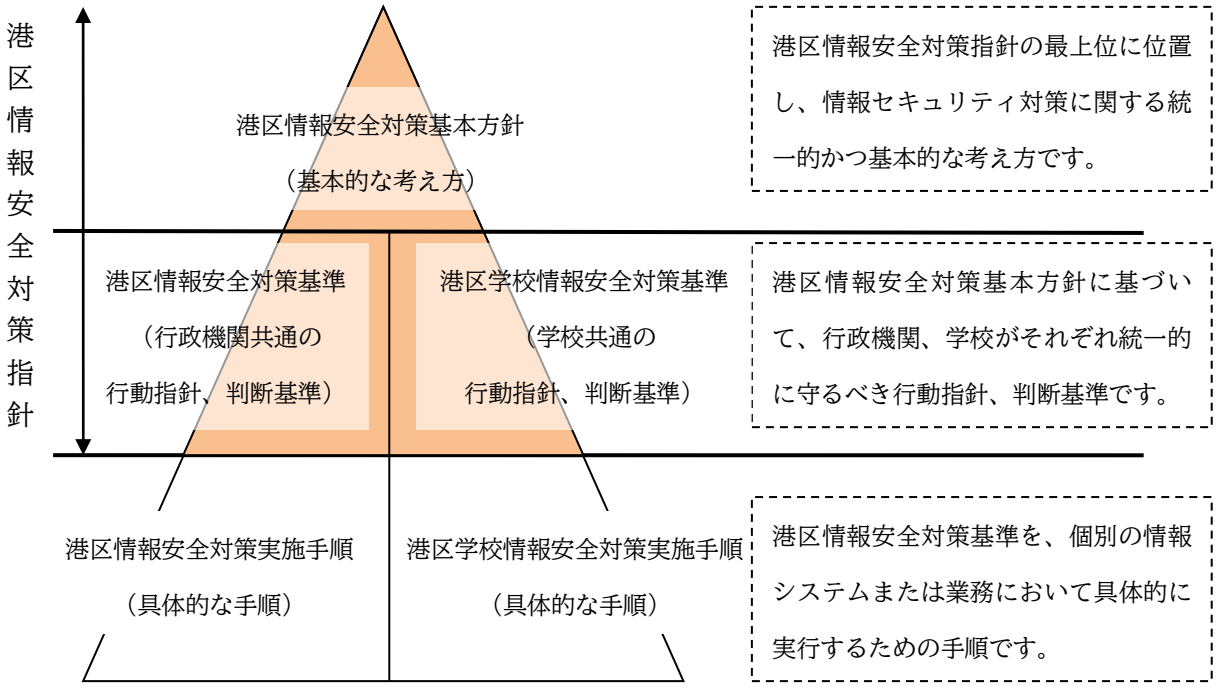

図　情報セキュリティ対策の体系的な整備

3　対象範囲

この方針の対象範囲は、区が保有する情報資産及び建物・関連設備並びに情報資産を取り扱う職員、指定管理者及び受託事業者（以下「職員等」といいます。）とします。

4　情報セキュリティ対策の実施

区は、情報資産を安全に保護するため、全庁的な推進体制を整備し、次のとおりに総合的かつ継続的に情報セキュリティ対策を実施します。

（１）法令等の遵守

個人情報の保護及び情報セキュリティの確保については、法律、条例、規則等を守ります。

（２）脅威の認識

情報資産の不正利用、情報の漏えい等の危険性をもたらす脅威を次のように捉えます。

１）故意による脅威（不正アクセス、情報の改ざん・漏えい等）

２）過失による脅威（誤操作等）

３）故障による脅威（機器の故障等）

４）災害による脅威（地震、火災、水害、落雷等）

（３）総合的な情報セキュリティ対策

様々な脅威から情報資産を保護するため、次の情報セキュリティ対策を実施します。

１）人的な情報セキュリティ対策

職員等の情報セキュリティに関する責任の明確化及び行動指針の遵守による対策

２）技術的な情報セキュリティ対策

情報システムへの不正アクセス、コンピュータウイルス等から保護するための対策

３）物理的な情報セキュリティ対策

情報システムの設置されている場所への不正な立ち入り、機器の損傷等から保護するための対策

（４）監査及び点検

港区情報安全対策指針の遵守状況を確認するために、監査の体制を明確に定めて、監査及び点検を行います。

（５）評価及び見直し

情報資産を取り巻く環境の変化に適切に対応していくため、港区情報安全対策指針の評価及び見直しを行います。

５　職員等の義務

職員等は、情報セキュリティの重要性を認識し、業務の遂行にあたって港区情報安全対策指針を守る義務があります。港区情報安全対策指針に違反した場合は、法令及び港区職員の懲戒処分に関する指針に基づき、処罰等又は懲戒処分の対象となります。

港区情報安全対策基準

（平成１５年８月１５日
１５港政情第３１２号）

改正　平成17年4月　1日 17港政情第　14号
改正　平成18年3月 22日 17港政情第　703号
改正　平成19年4月　1日 19港総情第　　1号
改正　平成19年6月　1日 19港総情第　616号
改正　平成22年3月 21日 21港総情第 2973号
改正　平成22年4月　1日 22港総情第　308号
改正　平成24年5月　1日 24港総情第 1618号
改正　平成27年6月　1日 27港総情第 1378号
改正　平成28年4月　1日 27港総情第 6454号
改正　平成31年4月　1日 30港総情第 4563号
改正　令和2年4月　1日 31港総情第 4410号
改正　令和4年9月　1日　4港総情第 1933号
改正　令和5年4月　1日　4港総情第 4687号
改正　令和5年9月　1日　5港企情第 1195号

港区情報安全対策基準とは、港区情報安全対策基本方針に基づいて、区が保有する情報資産[*1]を故意、過失、故障及び災害の脅威から保護し、区民から信頼されるデジタル環境を実現するための情報セキュリティ対策に関する基準です。

なお、区立の幼稚園、小学校及び中学校が保有する情報資産については、港区学校情報安全対策基準によります。

１　対象範囲

港区情報安全対策基準が対象とする行政機関の範囲は、港区総合支所及び部の設置等に関する条例(平成１７年港区条例第６２号)に規定する総合支所及び部並びに防災危機管理室、みなと保健所、会計室、教育委員会事務局、選挙管理委員会事務局、監査事務局及び区議会事務局とします。

２　管理体制

全庁的な情報セキュリティ推進体制は、次のとおりです。

（１）セキュリティ統括責任者

① セキュリティ統括責任者は、情報資産の情報セキュリティ対策を統括する最高責任者とし、副区長（企画経営部を担任する者）をもって充てます。

② セキュリティ統括責任者は、情報セキュリティ対策に関する責任体制、継続的な監視体制、監査体制を整備し、情報資産の適切な管理に努めます。

（２）セキュリティ副統括責任者

① セキュリティ副統括責任者は、セキュリティ統括責任者を補佐する者とし、デジ

*1 情報資産：ハードウェア・ソフトウェア・ネットワークで構成される情報システム、情報システム・外部記録媒体等に記録されたデータ、情報システムで処理された入出力データの総称をいいます。

タル改革担当部長をもって充てます。

② セキュリティ副統括責任者は、セキュリティ統括責任者に事故あるときはその職務を代理します。

（３）システム統括管理者

① システム統括管理者は、情報資産の適切な情報セキュリティ対策を実施する者とし、情報政策課長をもって充てます。

② システム統括管理者は、情報資産の情報セキュリティを確保するため、次の事項を実施します。

・庁内の主要なネットワーク*2 の管理運営
・庁内の主要な情報システム*3 の管理運営
・情報セキュリティに関する調査及び研究
・情報セキュリティ確保に関する措置
・情報セキュリティに関する啓発及び研修
・セキュリティ責任者への情報セキュリティに関する指導及び助言
・その他必要な事項

（４）システム管理者

① システム管理者は、情報システムの開発、変更、運用等について責任を有する者とし、その情報システムを設置する課等の長をもって充てます。なお、情報政策課が所管する情報システムについては、システム統括管理者が兼任します。

② システム管理者は、所管する情報システムについて、適切な管理運営を行うため、港区情報安全対策実施手順等の策定、評価及び見直しを実施します。

（５）セキュリティ責任者

① セキュリティ責任者は、情報資産を利用する課等の長をもって充てます。なお、情報システムを設置する課等においては、システム管理者が兼任します。

② セキュリティ責任者は、システム管理者と相互調整を図り、課等の情報資産の情報セキュリティを確保するため、次の事項を実施します。

・港区情報安全対策指針、港区情報安全対策実施手順等の運用状況の確認
・課等に設置する情報システム関連機器の監視
・職員等への啓発及び教育
・情報セキュリティに関する欠陥、事故等の報告
・その他必要な事項

*2 庁内の主要なネットワーク：情報政策課が所管する内部情報系ネットワークをいいます。
*3 庁内の主要な情報システム：内部情報系ネットワークを利用する行政情報システム等をいいます。

（６）兼務の禁止

① 情報セキュリティ対策の実施において、承認又は許可の申請を行う者と承認又は許可をする者は、原則として同じ者が兼務しない体制とします。

（７）港区情報システムセキュリティ会議

① セキュリティ統括責任者は、港区情報システムセキュリティ会議を招集します。

② 港区情報システムセキュリティ会議は、セキュリティ統括責任者、セキュリティ副統括責任者、システム統括管理者及びセキュリティ統括責任者が指名する者をもって組織します。

③ 港区情報システムセキュリティ会議の庶務は、情報政策課が行います。

④ 港区情報システムセキュリティ会議は、情報セキュリティの継続的な確保を図るため、次の事項を決定します。

・港区情報安全対策指針の評価及び見直し
・情報システムの情報セキュリティ対策の評価及び見直し
・セキュリティ監査の実施
・緊急時における措置
・港区情報安全対策指針に対する重大な違反に関する調査及び再発防止策
・職員等への計画的な教育など、港区情報安全対策指針の運用に関する事項
・その他必要な事項

⑤ 港区情報システムセキュリティ会議の決定事項は、庁議等を通じて総合支所長、部長、室長、所長、次長、局長に速やかに伝達します。

（８）情報セキュリティに関する欠陥、事故等の統一的な窓口（ＣＳＩＲＴ：Computer Security　Incident Response Team、以下「ＣＳＩＲＴ」という。）

① セキュリティ責任者は、情報セキュリティに関する欠陥、事故等について、その状況をＣＳＩＲＴに報告します。

② システム統括管理者は、情報セキュリティに関して、必要に応じて関係機関や他の地方公共団体のＣＳＩＲＴの機能を有する部署、外部の事業者等との情報共有、通知・公表等を行います。

3　情報の分類と管理

（1）情報の分類

① 区が保有する情報は、次の重要性分類に従って分類します。

レベル３	・個人情報 ・法令又は条例の定めにより守秘義務を課されている区政情報（上記個人情報を除きます。） ・法人その他の団体に関する情報であって、公開することにより当該団体の利益を害するおそれのある情報 ・情報システムに関するパスワード及びシステム設定情報
レベル２	公開することにより区の事務事業の執行に重大な影響を及ぼす情報
レベル１	上記以外の区政情報

（2）管理責任

① セキュリティ責任者は、課等で収集及び作成した情報を管理する責任を有します。

（3）アクセス権限の設定

① セキュリティ責任者は、情報の分類に従いアクセス権限を定めます。

② コンピュータ*4 に情報を保存する場合は、アクセス制御された場所に保存します。

③ レベル３及び２の情報について、複製、外部記録媒体*5 を用いた送付、ネットワークを通じた送信を行う場合は、セキュリティ責任者の承認を得たうえで行います。

（4）複製物の管理

① セキュリティ責任者の承認を得て複製した情報は、複製元の情報と同様の管理を実施します。

② 障害や緊急時の発生に備えて、情報のバックアップデータを取得します。なお、バックアップデータは、必要に応じて災害対策を施した場所に保管します。

（5）外部記録媒体の管理

① レベル３及び２の情報を記録した外部記録媒体は、施錠可能な場所に保管します。なお、持ち運びの容易な保管庫等に保管する場合は、保管庫を盗難等から保護します。

② 外部記録媒体の保管状況を記録します。

③ レベル３及び２の情報を記録した外部記録媒体を搬送する場合は、職員等が行うとともに、物理的な保護措置を実施します。また、搬送した日時、搬送先等を記録します。

④ レベル３及び２の情報を記録した外部記録媒体を廃棄する場合は、セキュリティ責任者の承認を得たうえで行います。

*4 コンピュータ：情報を電磁的に処理、蓄積等する機器で、サーバー及びパソコン、携帯情報端末等の端末装置をいいます。

*5 外部記録媒体：磁気テープ、光ディスク、USBメモリ等の記録媒体をいいます。

⑤ 外部記録媒体を廃棄する場合は、初期化処理だけではなく、必ず破壊等を行い、情報漏えいを防ぎます。

（６）入出力データの管理

① レベル３及び２の情報に関する入出力データ（申請書、出力帳票、印刷物等）は、施錠可能な場所に保管します。なお、持ち運びの容易な保管庫等に保管する場合は、保管庫を盗難等から保護します。

② 入出力データの保管状況を記録します。

③ レベル３及び２の情報に関する入出力データを搬送する場合は、職員等が行うとともに、物理的な保護措置を実施します。また、搬送した日時、搬送先等を記録します。

④ レベル３及び２の情報に関する入出力データを廃棄する場合は、セキュリティ責任者の承認を得たうえで、必ず焼却や溶解処分、シュレッダー処理等を行い、情報漏えいを防ぎます。

４　人的な情報セキュリティ対策

（１）職員等の責務

１）港区情報安全対策指針の遵守

① 情報資産の取り扱いにあたっては、関連法令等を守ります。

② 港区情報安全対策指針及び港区情報安全対策実施手順等を守ります。

③ 港区情報安全対策指針及び港区情報安全対策実施手順等について不明な点等がある場合は、速やかにセキュリティ責任者に報告し、指示等を仰ぎます。

④ 職務中だけでなく、異動、退職等により職務を離れた場合も、知り得た情報の秘密を守ります。

２）目的外利用の禁止

① 情報資産を職務上の目的だけに使用します。

② 不正アクセス又はそれに類する行為を行いません。

③ 個人の所有するコンピュータ、外部記録媒体等を職務に使用することは、原則禁止とします。ただし、例外的に使用する場合は、システム統括管理者の承認を得ることとします。

３）情報資産の適切な取り扱い

① 第三者による不正使用、盗難等から情報資産を保護します。特に、コンピュータ

等から離れる場合は、情報システムのロック、サインアウト*6 等を行います。

② コンピュータの改造又は機器の増設を行う場合は、システム管理者の承認を得たうえで行います。

③ コンピュータにソフトウェアを導入する場合は、システム管理者の承認を得たうえで行います。

④ 情報資産を庁舎外に持ち出す場合は、セキュリティ責任者の承認を得たうえで行います。なお、庁舎外で作業する場合は、利用する情報資産の管理責任を自らが負うことを自覚し、港区情報安全対策指針及び港区情報安全対策実施手順等を遵守します。

４）パスワード等の管理

① パスワード、IC カード等を他人に使用されないように各個人が責任を持って管理します。

② IC カードの紛失等があった場合は、当該 IC カードの利用、保管、返却、廃棄等に責任をもつシステム管理者に報告します。

③ パスワードは、英数（大・小文字）、記号等を用いて他人に推測されにくいものを設定し、使い回したり、他人に教えたりしません。

５）欠陥・事故の報告義務

① 情報システムの欠陥、誤動作又は港区情報安全対策指針に対する違反行為等を発見した場合又は住民等外部からの報告があった場合は、セキュリティ責任者に報告し、指示等を仰ぎます。

（２）教育・訓練

① セキュリティ副統括責任者は、職員等に個人情報の保護及び港区情報安全対策指針に関する研修を受講させます。

② システム管理者は、情報システムの開発、保守、運用等に携わる職員等に、担当者として必要な研修を受講させます。

③ セキュリティ統括責任者は、情報資産への脅威及び緊急時の対応を想定した訓練を定期的に実施します。

*6 サインアウト：コンピュータや情報システム等にアクセス可能な状態を終了することをいいます。
アクセス可能な状態にすることをサインインといいます。

5　技術的な情報セキュリティ対策

（1）コンピュータの管理

1）担当者の指名

① システム管理者は、コンピュータの運用管理を行う職員等を指名します。

② コンピュータの運用管理を行う職員等は、複数かつ必要最小限とします。

③ セキュリティ責任者は、コンピュータの管理を行う職員等を指名します。

2）機器管理

① システム管理者は、コンピュータに管理番号を付与し、その設置場所等を記録します。

② システム管理者は、コンピュータの設置状況等を定期的に点検します。

（2）ネットワークの管理

1）担当者の指名

① システム管理者は、ネットワークの運用管理を行う職員等を指名します。

② ネットワークの運用管理を行う職員等は、複数かつ必要最小限とします。

2）構成管理

① システム管理者は、最新のネットワーク構成状況を把握します。

② システム管理者は、ネットワーク機器の設置場所及びネットワーク配線の経路を記録します。

③ システム管理者は、ネットワーク機器の設定情報を改ざんされないようにアクセス制御により管理します。

④ システム管理者は、ネットワーク機器の設定情報のバックアップを取得します。

⑤ システム管理者は、ネットワークに通信回線を使用する場合、継続的な運用を可能とする通信回線を選択し、必要に応じて通信回線を冗長構成にする等の措置を講じます。

3）構成変更

① 庁内の主要なネットワークへの新規接続や構成変更を行う場合は、システム統括管理者の承認を得たうえで行います。

4）無線 LAN

① 庁内のネットワークに無線 LAN （Local Area Network）*7 を利用する場合は、解読が困難な暗号化及び認証技術を使用します。

*7 無線LAN（Local Area Network）：ケーブル線の代わりに無線通信を利用してデータの送受信を行う仕組みをいいます。

（３）情報システムの管理

１）担当者の指名

① システム管理者は、情報システムの運用管理を行う職員等を指名します。

② 情報システムの運用管理を行う職員等は、複数かつ必要最小限とします。

２）運用管理

① システム管理者は、情報システムを構成するソフトウェア等のバックアップを取得します。

② システム管理者は、情報システムごとに操作手順書を作成し、常備します。

③ システム管理者は、情報システムごとに操作の承認手続きを定めます。

④ システム管理者は、実施した作業の記録を作成し、適切に保管します。

３）ソフトウェア管理

① システム管理者は、コンピュータへのソフトウェアの導入状況を把握します。

② ソフトウェアを導入する場合は、正規のライセンスを取得します。

③ 導入するソフトウェアは、業務上必要なものに限ります。

④ ソフトウェアを使用する場合は、使用許諾条件等の定められた条件を守ります。

（４）外部とのシステム結合

１）外部ネットワークとの接続

① 庁内の主要なネットワークと外部のネットワークを接続する場合は、港区情報システムセキュリティ会議の承認に基づき実施します。また、庁内の主要なネットワーク以外のネットワークと外部のネットワークを接続する場合は、システム統括管理者の承認に基づき実施します。なお、個人情報を処理する情報システムと外部の情報システムを結合する場合は、港区個人情報の保護に関する法律施行条例に規定する手続きをとります。

２）総合行政ネットワークとの接続

① 総合行政ネットワークに関する諸規定に基づき、適切に接続及び運用します。

３）住民基本台帳ネットワークシステムとの接続

① 法令等に基づき、適切に接続及び運用します。

（５）アクセス制御

１）コンピュータアクセス制御

① システム管理者は、不正アクセスを防ぐため、コンピュータについて次の事項を実施します。

・起動時にユーザーを認証する機能を設けます。

・利用できるコンピュータ機能を必要最小限にします。

2）ネットワークアクセス制御

① システム管理者は、ネットワークのアクセス経路を制御し、ネットワーク機器の設定を適切に維持・管理します。

② システム管理者は、ネットワーク及びネットワーク機能ごとにアクセス可能な者を定めるとともに、未使用ポートの閉鎖、不要なサービス機能の削除又は停止等、不必要なネットワーク機能へのアクセスを防ぐ対策を実施します。

③ システム管理者は、庁内のネットワークと外部のネットワークの間には、ファイアウォール*8を設置するなど、必要な対策を実施します。

④ 庁内のネットワークと外部のネットワークの接続点の数は、必要最小限にします。

3）情報システムアクセス制御

① セキュリティ責任者は、情報及び情報システムに対する職員等のアクセス権限を定めます。

② システム管理者は、情報システムにユーザーを認証する機能を設け、サインイン手順を定めます。

③ システム管理者は、情報システムごとにユーザー登録、抹消等の手続きを定めます。

④ システム管理者は、セキュリティ責任者からユーザー登録、変更等の申請を受けた場合は、直ちに情報システムに反映します。

⑤ システム管理者は、必要なアクセス制限を行うとともに、例外的な使用を行う場合の申請・承認の手続きを定めます。

⑥ 職員等がテレワークにより外部から情報システムを利用又は情報を閲覧する場合は、人事課が定めるテレワークの諸規定に則り実施します。

4）システム上の管理者権限*9

① システム管理者は、情報システム、ネットワーク機器及びサーバー等について、システム上の管理者権限の付与、変更等の手続きを定めます。

② システム上の管理者権限の変更があった場合は、パスワード等を直ちに変更します。

5）パスワードの管理

① システム管理者は、情報システムで使用するユーザーID・パスワードを厳重に管理します。

6）IC カードの管理

*8 ファイアウォール：庁内のコンピュータやネットワークが外部から侵入されることを防ぐための仕組みをいいます。

*9 システム上の管理者権限：情報システム、ネットワーク機器及びサーバー等において、システム上の設定を行うことのできる管理者用の権限をいいます。

① システム管理者は、IC カードの利用、保管、返却、廃棄等における取扱方法を定め、厳重に管理します。

② システム管理者は、IC カードの紛失等の報告があった場合は、当該 IC カードを使用した情報システムへのアクセス等をただちに停止します。

7）アクセスログ*10 の取得・分析

① システム管理者は、アクセスログを取得すべき情報システム等を定め、記録機能を設けます。

② システム管理者は、アクセスログを一定期間保存するとともに、改ざん、漏えい等の防止策を実施します。

③ システム管理者は、不正アクセス等の状況を調査するため、アクセスログを必要に応じて分析します。

（6）不正アクセス対策

① システム管理者は、内部及び外部への不正アクセスを防ぐため、技術的な検査を実施します。

② システム管理者は、重要な情報システムの設定に関するファイル、インターネットに公開しているファイル等について、その改ざんの有無を確認します。

③ システム管理者は、セキュリティホール*11 等、情報セキュリティ対策に関する情報の収集に努め、速やかに必要な対応を実施します。

④ システム管理者は、標的型攻撃*12 による内部への侵入防止及び侵入した攻撃を早期検知するため、情報セキュリティ教育及び技術的対策を実施します。

⑤ インターネットに公開するウェブサイトにおいては、転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を実施します。

（7）コンピュータウイルス*13 対策

1）コンピュータウイルスの検査

① システム管理者は、ウイルス対策を必要とするコンピュータにウイルス対策ソフトを導入し、ウイルス検査を実施します。また、ウイルス対策ソフトを適切に更新します。

② システム統括管理者は、庁内の主要なネットワークにつながるコンピュータにおいて外部記録媒体の利用を制限します。

③ システム統括管理者は、インターネットとの接続点にウイルス対策ソフトを導入

*10 アクセスログ：情報システム等にアクセスした者、日時、処理内容等を記録したものをいいます。
*11 セキュリティホール：コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことをいいます。
*12 標的型攻撃：機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃のことをいいます。

し、ウイルス検査を実施します。

④ 職員等は、外部からデータ又はソフトウェアを取り入れる場合は、必ずウイルス検査を実施します。また、電子メール等で送付元が不明なファイル等、不審なメールを受信した場合は、速やかに削除します。なお、不審なメールの受信状況はシステム管理者に報告します。

2）コンピュータウイルス発見時の対応

① 職員等は、ウイルス検査によりコンピュータウイルス感染を検知した場合は、システム管理者に直ちに報告します。

② システム管理者は、ＣＳＩＲＴへ状況を報告するとともに、被害状況に応じて、感染経路の特定、被害拡大の防止、修復措置等を実施します。

（8）情報システム構築・保守等の対策

1）情報システムの開発・導入・変更

① システム管理者は、情報システムの開発、導入、変更を行う場合は、情報セキュリティ対策及び稼動中の情報システムへの影響を十分に検証します。

② システム管理者は、情報システムを変更する場合は、必要なときに変更前の状態に復旧できるようにします。

③ システム管理者は、システム障害を防止するため、作業内容について記録を作成し、適切に保管します。

④ システム管理者は、ソフトウェア等を購入する場合は、次の事項を満たす製品を選定します。

・港区情報安全対策指針に定める運用が可能であり､情報セキュリティ上問題がないこと

・購入先又は開発元の事業者の連絡先が明らかなものであること

・製品に関する更新情報の提供が受けられバージョンアップ等の対応が可能であること

2）情報システムの保守

① システム管理者は、情報システムの保守を適切に行い、情報セキュリティに重大な影響を及ぼす内容を発見したときは、速やかに対応します。

② システム管理者は、情報システムの保守を行う場合は、不具合及び他の情報システムへの影響を十分に検証したうえで作業を実施します。

3）設計書等の管理

*13 コンピュータウイルス：コンピュータのソフトウェアに侵入し、その中のデータやプログラムを破壊する悪意をもって作られたプログラムをいいます。

① システム管理者は、情報システムの開発、変更等に関する記録（設計書等）を作成します。

② システム管理者は、設計書等を適切に管理し、最新の状態を保ちます。また、閲覧を制限します。

（９）障害対応

① 必要に応じて情報システムの可用性を確保するため、情報システムを多重化する等の対策を実施します。

② 情報システムには、障害等の発生を検知できる機能を必要に応じて設けます。

③ システム管理者は、情報システムごとに障害発生時の対応手順を定めます。

④ システム管理者は、障害発生時において、その発生原因及び対応の記録を作成し、保管します。また、再発防止策を検討及び実施します。

（１０）電子メールの利用制限

① セキュリティ責任者は、情報資産の不正な持ち出しを防止するため、電子メールの利用及びセキュリティ管理について、必要な手続きを定めます。

（１１）Web 会議サービス*14 の利用時の対策

① システム統括管理者は、Web 会議を適切に利用するための必要な手続きを定めます。

（１２）ソーシャルメディアサービスの利用

① 港区が管理するアカウントでソーシャルメディアサービスを利用する場合、セキュリティ責任者はソーシャルメディアサービス運用にあたっての手順等を定めます。

*14 Web会議サービス：専用のアプリケーションやWebブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいいます。

6　物理的な情報セキュリティ対策

（1）入退管理

① システム統括管理者は、管理区域*15 に許可した者以外が立ち入らないよう入退管理を実施します。

② システム管理者は、事務室や管理区域に許可したもの以外が立ち入らないよう入退管理を実施します。

（2）搬入出物の管理

① 事務室や管理区域への搬入出物については、業務上必要なものに制限し、事務室や管理区域のセキュリティ責任者の承認を得たうえで搬入出します。

（3）作業の監視

① システム統括管理者が指定する管理区域には、監視カメラを設置し、監視を行います。

② 職員等以外の者が事務室や管理区域へ立ち入る場合は、事務室や管理区域のセキュリティ責任者の承認を得たうえで行います。

③ 職員等以外の者が管理区域で作業を行う場合は、職員等が立会うなど、必要な対策を実施します。

（4）不正行為の防止

① システム管理者は、コンピュータやネットワーク機器について、盗難等を防ぐための対策を実施します。

② システム管理者は、ネットワーク配線について、傍受又は損傷等を防ぐための対策を実施します。

③ 職員等以外の者が利用できる情報システムのコンピュータについては、その設置環境に応じて盗難防止策や不正使用防止策を実施します。

（5）災害対策

① セキュリティ統括責任者は、管理区域の構造や内装について、その状況に応じて災害対策を実施します。

② システム管理者は、コンピュータやネットワーク機器について、その設置環境に応じて災害対策を実施します。

（6）電源の確保

① システム管理者は、コンピュータやネットワーク機器について、停電等による影響を受けないように予備電源を確保するなど、必要な対策を実施します。

*15 管理区域：コンピュータや重要なネットワーク機器等の設置場所のことをいいます。

（７）機器の保守

① システム管理者は、コンピュータやネットワーク機器の保守を実施します。

② コンピュータ等の機器を修理等のために庁舎外に搬出する場合は、情報漏えいを防ぐ措置を実施します。

（８）機器の廃棄

① コンピュータ等の機器を廃棄やリース返却等する場合は、機器内部の記憶装置の初期化処理だけではなく、必ず記録領域の消磁や記憶装置の物理破壊等によるデータ復元が不可能な措置を行い、情報漏えいを防ぎます。

７　指定管理者の管理

（１）選定

① 港区情報安全対策指針を遵守できる指定管理者を選択します。

（２）協定

① 指定管理業務の業務主管課のセキュリティ責任者は、指定管理者と協定を締結する際、守秘義務、港区情報安全対策指針の遵守義務、違反時の措置等を明記します。

（３）指定管理業務に関する情報資産の保護措置

① 指定管理業務の業務主管課のセキュリティ責任者は、指定管理業務に関する情報資産について、情報セキュリティを確保するために必要な人的、技術的、物理的対策を、指定管理者に実施させます。

（４）検査

① セキュリティ統括責任者は、指定管理者に対して、港区情報安全対策指針が遵守されていることを点検します。

（５）指定管理者の情報システムの利用

① システム統括管理者は、指定管理者が指定管理業務遂行のために指定管理者の情報システムを用いる場合は、次の事項を確認した上で承認します。

・港区が所管するコンピュータ、ネットワークと接続しないこと。

・港区情報安全対策指針が遵守できること。

（６）指定管理者の情報資産の受入れ

① システム統括管理者は、指定管理者が指定管理業務と直接関係のない指定管理者のコンピュータ等の情報資産を指定管理施設内に持ち込む場合は、次の事項を確

認した上で承認します。

・港区情報安全対策指針が遵守できること。

8　業務委託の管理

（1）委託先の選定

① 港区情報安全対策指針を遵守できる委託事業者を選択します。

（2）委託先との契約

① システム管理者は、情報システムの開発、保守、運用等を業務委託する場合は、守秘義務、港区情報安全対策指針の遵守義務、違反時の措置等を明記した契約等を締結します。

（3）委託業務に関する情報資産の保護措置

① セキュリティ責任者は、委託業務に関する情報資産について、情報セキュリティを確保するために必要な人的、技術的、物理的対策を実施します。

（4）委託先に関する点検

① セキュリティ責任者は、委託先において港区情報安全対策指針が遵守されていることを点検します。

（5）指定管理業務の委託先の管理

① 指定管理者が、指定管理業務の一部を外部委託する際は、8業務委託の管理の第1項から第4項までを準用します。

9　クラウドサービスの利用

（1）クラウドサービス[*16]の選定

① システム管理者は、「港区情報安全対策実施手順」に従い、クラウドサービスを選定します。

（2）クラウドサービスの契約

① システム管理者は、クラウドサービスの契約等を締結する場合は、「港区情報安全対策実施手順」に従い、締結を行います。

（3）クラウドサービスに対する情報セキュリティ対策

① セキュリティ責任者は、クラウドサービスにおいて利用する情報資産について、「港区情報安全対策実施手順」に従い、情報セキュリティを確保するための対策を行います。

（４）クラウドサービスの運用

① セキュリティ責任者は、利用するクラウドサービスにおいて、「港区情報安全対策実施手順」に従い、運用されていることを確認します。

１０　港区情報安全対策指針の運用

（１）監査の実施

① セキュリティ統括責任者は、情報安全対策指針の遵守状況について監査を実施します。なお、セキュリティ監査に関する具体的な実施事項は、システム統括管理者が定めます。

② セキュリティ統括責任者は、専門知識を有する者が監査を実施する体制とします。

③ 監査を受ける者とその監査を実施する者は、原則として同じ者が兼務しない体制とします。

④ セキュリティ統括責任者は、システム統括管理者の報告を受けて、評価、指摘、改善します。

⑤ システム統括管理者は、セキュリティ監査に関して、次の事項を実施します。

・監査計画書の作成
・監査の実施
・監査報告書の作成
・改善計画書の作成
・改善計画書の実施

⑥ セキュリティ責任者は、セキュリティ統括責任者によるセキュリティ監査の評価結果、指摘事項に関して、速やかに改善します。

（２）点検の実施

① セキュリティ責任者は、課等における港区情報安全対策指針及び港区情報安全対策実施手順等の遵守状況を点検し、その結果に応じて改善します。

（３）情報資産の利用状況等調査の実施

① セキュリティ統括責任者及びセキュリティ統括責任者が指名した者は、情報資産の保護及び不正な取り扱いの防止を目的とする場合は、その運用管理状況や利用状況を調査することができます。

② 調査は、ログの取得、分析、送受信中のデータ取得、分析、記録の確認等の手段により行います。

*16 クラウドサービス：事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するもの（ソフトウェアやデータ等を、インターネットを通じ必要に応じて利用者に提供するサービス等）をいいます。

（４）緊急時対応

① セキュリティ統括責任者は、緊急時の連絡体制を整備します。

② ＣＳＩＲＴは、情報資産への侵害が発生した場合は、速やかに発生原因を調査し、対応します。状況により、セキュリティ統括責任者は、港区情報システムセキュリティ会議を招集し、再発防止策を検討及び実施します。

③ システム統括管理者は、情報資産への侵害が発生した場合は、ネットワークを物理的に遮断するなど、被害拡大の防止策を実施します。

④ 情報資産への侵害があった場合は、国や他の自治体等と連携し、適切に対応します。また、犯罪のおそれがある場合は、速やかに警察に通報します。

（５）港区情報安全対策指針の掲示

① セキュリティ統括責任者は、職員等が常に港区情報安全対策指針を閲覧できるように掲示します。

１１　港区情報安全対策指針の評価及び見直し

セキュリティ統括責任者は、情報資産を取り巻く環境の変化やセキュリティ監査の指摘に応じて、継続的に必要な評価及び見直しを行い、区民から信頼されるデジタル環境を実現するための情報セキュリティ対策を実施します。

港区議会
情報安全対策基本方針

（個人情報等を守るための事務処理指針）

令和８年（２０２６年）１月

港　区　議　会

港区平和都市宣言

かけがえのない美しい地球を守り、世界の恒久平和を願う人びとの心は一つであり、いつまでも変わることはありません。

私たちも真の平和を望みながら、文化や伝統を守り、生きがいに満ちたまちづくりに努めています。

このふれあいのある郷土、美しい大地をこれから生まれ育つこどもたちに伝えることは私たちの務めです。

私たちは、我が国が『非核三原則』を堅持することを求めるとともに、ここに広く核兵器の廃絶を訴え、心から平和の願いをこめて港区が平和都市であることを宣言します。

昭和６０年８月１５日

港　　区

港 区 議 会 情 報 安 全 対 策 基 本 方 針

目　　次

令和８年１月３０日
７港議第２０１４号

港区議会情報安全対策基本方針

１　基本的考え方

港区議会情報安全対策基本方針（以下「基本方針」という。）は、港区議会（以下「議会」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、議会が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

また、基本方針は、地方自治法の一部を改正する法律（令和６年法律第６５号）による改正後の地方自治法第２４４条の６第１項で定めるサイバーセキリティを確保するための方針に位置付けるものとする。

なお、港区議会議員（以下「議員」という。）個人が、議員活動の中で取得した情報資産は、基本方針の対象外とする。

２　定義

（１）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（３）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（４）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（５）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（６）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情

報にアクセスできる状態を確保することをいう。

（７）無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

３　対象とする脅威

港区議会事務局職員(以下「事務局職員」という。)は、情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３）地震、落雷、火災等の災害によるサービス及び業務の停止等

（４）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

４　適用範囲

（１）対象者

この方針の対象は、議会が保有する情報資産を取り扱う議員及び事務局職員とします。

（２）情報資産の範囲

基本方針では議会が保有する以下の情報資産を対象とします。

① ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

② ネットワーク及び情報システムで取り扱う情報（印刷した文書を含む。）

③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

５　遵守義務

議員及び事務局職員は、情報セキュリティの重要性について共通の認識を持ち、業務の

遂行に当たって基本方針及び「港区議会タブレット端末使用基準」等の議会で策定した情報セキュリティに関する個別の基準（以下「個別基準」という。）を遵守しなければならない。

6　情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１）組織体制

議会が保有する情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（２）情報資産の分類と管理

議会の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３）物理的セキュリティ

サーバ、情報システム室、通信回線及びパソコン等の管理について、物理的な対策を講じる。

（４）人的セキュリティ

情報セキュリティに関し、議員及び事務局職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

ア　情報資産の持ち出し

・議会が保有する情報資産は、区及び議会が貸与する端末以外へ転送しない。

イ　ソフトウェアの仕様

・区及び議会から貸与された端末で、無許可のソフトウェアや外部サービスを利用しない。

ウ　内部不正の対策

・区及び議会から貸与された端末は、議会関係者以外が閲覧できない環境で利用する。

エ　機器廃棄

・コンピュータ等の機器を廃棄やリース返却等する場合は、機器内部の記憶装置の初期化処理だけではなく、必ず記録領域の消磁や記憶装置の物理破壊等によるデータ復元が不可能な措置を行うこと。

（５）技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等

の技術的対策を講じる。

ア　不正アクセス

・不正アクセスを防ぐため、端末利用時はユーザー認証を行う。

・不正に操作された恐れがある場合はアクセスログ･操作ログ等を調査･分析する。

イ　ウイルス対策

・コンピュータには、ウイルス対策ソフトを導入する。

・ウイルス対策ソフトの実行ファイルやパターンファイルは、最新のバージョンに更新する。

（６）業務継続計画

ア　地震、落雷、火災等の災害によるサービス及び業務の停止等の対策

・港区業務継続計画に従い対応する。

・システムが停止した場合、事務局が契約事業者へ連絡し復旧対応を行う。

イ　大規模･広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等の対策

・港区業務継続計画に従い対応する。

ウ　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等の対策

・港区業務継続計画に従い対応する。

（７）運用

情報システムの監視、基本方針や個別基準の遵守状況の確認、業務委託を行う際のセキュリティ確保等、運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（８）業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用する

ソーシャルメディアサービスごとの責任者を定める。

（９）評価・見直し

基本方針や個別基準の遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。基本方針や個別基準の見直しが必要な場合は、適宜見直しを行う。

７　情報セキュリティ監査及び自己点検の実施

事務局職員は、基本方針や個別基準の遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

８　基本方針等の見直し

事務局職員は、情報セキュリティ監査及び自己点検の結果、基本方針や個別基準の見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、基本方針や個別基準を見直す。

９　情報セキュリティ対策基準の策定

議会は、上記６、７及び８に規定する対策等を実施するために、必要に応じて具体的な遵守事項及び判断基準等を情報セキュリティ対策基準として策定する。

１０　情報セキュリティ実施手順の策定

議会は、区の情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するために、必要に応じて具体的な手順を定めた情報セキュリティ実施手順を策定する。

なお、議会の情報セキュリティ実施手順は、公にすることにより議会運営に重大な支障を及ぼすおそれがあることから非公開とする。

データセンター要件

下記データセンター要件はすべて満たすこと。

番号	要　件
1	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以上の危険物製造設備、危険物貯蔵設備がなく、隣接建物から延焼防止策がとられていること。
2	日本国内に所在し、港区役所から直線距離で30km以上離れた場所に位置すること。
3	建築基準法の規定する耐震構造建築物とし、同法に規定する耐火性能を有し、防火対策及び水の被害を防止する措置が施されていること。
4	震度7クラスの地震発生時にもサービス提供可能な耐震又は免震構造であること。
5	避雷設備及び内部雷保護システムに対応した雷対策を講じていること。
6	自動火災報知設備、消火設備、非常照明設備が設置されていること。
7	建物の出入り口に防犯対策が講じられていること。
8	情報セキュリティマネジメントシステム（ISO/IEC27001）適合性評価制度の認定を受けていること。
9	データセンターは24時間365日の監視体制で、入退室者を識別・記録できるセキュリティ設備（ICカード等）により、許可された者のみが入館できるよう、入退館が管理されていること。
10	区議会事務局が必要とする場合に、区議会事務局担当職員の建物への入館を許可すること。
11	「インターネットへの接続は1G／bps以上の回線を有し、異なるキャリアにより冗長化されていること。」
12	サーバルームのラックは、鍵付きラックを使用すること。
13	サーバルームの出入り口は、非常口を除き、階段、廊下等建物共用部から直接入れない位置に設けていること。
14	サーバルームの出入り口には、生体認証や磁気カード認証による入退室管理システムを設置し、不正侵入等に対する監視及び管理処置等の防止措置が施されていること。
15	サーバルームは、設置機器に影響を与えないよう、水を使用しない不活性ガスの消火設備を設置していること。
16	屋外側の窓、外壁、天井及び床からの水の浸入が無いこと。
17	サーバルーム内には監視カメラが設置され、サーバルーム内を監視及び記録することができること。
18	室内の環境は、腐食性ガス、振動、塵埃が発生しないこと。
19	防湿、防塵対策が施されていること。
20	サーバルームの電源設備容量は、機器の負荷を考慮して余裕を持たせること。
21	自家発電設備等の予備電源供給が可能なこと。
22	24時間365日電源の安定供給が可能であること。
23	無停電対策として電源が冗長化されており、無停電電源装置が設置されていること。
24	予備電源供給として自家発電設備を利用する場合、商用電力の供給停止から1分以内（この間は無停電電源装置から電力供給）に電力が供給できること。
25	自家発電設備は、24時間以上の運転が可能であること。
26	サーバルームの受電容量に十分な非常用自家発電設備等が設置されていること。
27	サーバルームには、非常用照明及び誘導灯が設置されていること。
28	サーバルームには、室内の負荷発熱に対応した空調能力のある24時間365日連続運転が可能な複数台の空調機が設置されていること。
29	サーバルームには、専用の空調システムにより、温度及び湿度が一定に保たれるような設備が備わっていること。
30	温度、湿度は機器等の安定稼働に影響を及ぼさないよう保たれていること。
31	使用するデータセンターは、過去5年以内に政府機関・地方公共団体のCMSの稼働実績があること。

仕様書別紙４

個人情報等取扱いに関する特記事項

令和５年４月１日改正

（基本的事項）

第１条　受注者は、個人情報の保護の重要性を認識し、この契約による事務を処理するための個人情報の取扱いに当たっては、個人情報の保護に関する法律（平成１５年法律第５７号）、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（平成２５年法律第２７号）、港区個人情報の保護に関する法律施行条例（令和４年港区条例第５３号）及び港区議会の個人情報の保護に関する条例（令和４年港区条例第６７号）を遵守し、個人情報を適正に取り扱わなければならない。

（秘密保持等の義務）

第２条　受注者は、この契約により受託した事務に関して知り得た個人情報をみだりに他人に知らせてはならない。契約期間満了後又は契約解除後も同様とする。

２　受注者は、この契約により受託した事務に従事する者及び従事した者にも、前項の義務を遵守させなければならない。

（目的外利用等の禁止）

第３条　受注者は、この契約により受託した事務に係る個人情報を委託された事務以外の用途に利用してはならない。

２　受注者は、この契約により受託した事務に係る個人情報を第三者に提供し、又は譲渡してはならない。

（再委託）

第４条　受注者は、この契約により受託した事務の一部を第三者に再委託する必要がある場合は、あらかじめ発注者に通知し、承諾を得なければならない。

２　受注者は、この契約により受託した事務について前項の規定により第三者に再委託する場合は、この契約により求められる安全管理措置と同等の措置を講ずることができる事業者を再委託先とし、この契約と同等の安全管理措置を義務付ける再委託契約を結ばなければならない。また、受注者は再委託先に対して適切な監督を行い、発注者の求めに応じて、その状況を報告しなければならない。

３　前２項の規定は、再委託先が受注者の子会社（会社法（平成１７ 年法律第８６ 号）第２条第１項第３号に規定する子会社をいう。）である場合も同様とする。

（複写、複製等の禁止）

第５条　受注者は、この契約により受託した事務に係る個人情報を発注者の許可なく複写し、又は複製してはならない。

２　受注者は、この契約により受託した事務の範囲を越えて、個人情報の加工、再生等をしてはならない。

（個人情報の安全管理措置）

第６条　受注者は、個人情報の漏えい、滅失及び毀損の防止その他の個人情報の安全な管理のために必要な措置を講じなければならない。

（事故発生時等における報告及び対応の義務）

第７条　受注者は、個人情報の漏えいその他の個人情報の保護に関する事故が生じたとき、又は生ずるおそれがあることを知ったときは、直ちに発注者に通知し、当該事故の解決に努めるとともに、遅滞なくその状況を書面をもって発注者に報告しなければならない。また、受注者は、情報セキュリティにおいて問題が発生した場合は、検査、セキュリティ監査等の実地調査に対応しなければならない。

（返還及び廃棄の義務）

第８条　受注者は、この契約により受託した事務が完了したとき又はこの契約が解除されたときは、受託した事務に係る個人情報を速やかに発注者に返還しなければならない。

２　前項の規定にかかわらず、受注者は、当該個人情報を発注者の指示に基づき廃棄するときは、第三者の利用に供されることのないよう、電磁的記録媒体の物理的な破壊、消去、溶解、裁断その他当該個人情報を判読不可能とするために必要な措置を講じなければならない。

（契約の解除、公表措置及び損害賠償義務）

第９条　発注者は、受注者が個人情報等取扱いに関する特記事項に掲げる義務に違反し、又は義務を怠った場合は、この契約を解除することができる。

２　前項の場合において、発注者は、その事実を公表することができる。

３　第一項の場合において、発注者が損害を受けたときは、受注者はその損害を賠償しなければならない。契約期間満了後も同様とする。

（監査・検査への協力等）

第１０条　発注者は、受注者がこの契約により受託した事務の処理に伴う個人情報の取扱いについて、個人情報等取扱いに関する特記事項に基づき、必要な措置を講じていることを確認するため、受注者に報告を求めることができる。

２　発注者は、受注者に通知し、個人情報の管理状況について監査・検査を実施することができる。再委託先についても同様とする。

（第１１条から第１６条までの条文は、「特定個人情報（※）」の取扱業務を委託する契約のみ）

（特定個人情報管理体制の整備）

第１１条　受注者は、委託業務を統括管理する部署に特定個人情報保護管理責任者を置き、委託業務を実行する部署に特定個人情報保護責任者を置か

なければならない。
（特定個人情報を取り扱う従業者の明確化）
第１２条　受注者は、特定個人情報を取り扱う従業者及びその役割を指定し、事前に従業者名簿を発注者へ提出しなければならない。
（従業者への教育訓練及び監督）
第１３条　受注者は従業者に対して、委託業務を行うために必要な教育及び訓練を実施し、継続的に監督するとともに、秘密保持契約を締結する等の人的安全管理措置を講じなければならない。
（持出しの禁止）
第１４条　受注者は、この契約により受託した事務に係る特定個人情報を指定された区域から持出ししてはならない。
（契約内容の遵守状況についての報告）
第１５条　受注者は、契約内容の遵守状況、特定個人情報の安全管理体制等を書面で報告しなければならない。
（安全管理措置の改善）
第１６条　受注者及び発注者は、第９条に基づく監査・検査の結果及び前条に基づく委託業務の遵守状況等についての報告を踏まえ、委託業務における特定個人情報の安全管理措置の改善要否を協議し、改善が必要と判断した場合は双方協力のうえ対応しなければならない。
※「特定個人情報」とは、「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（平成２５年法律第２７号）」第２条第８項に規定する特定個人情報をいう。

（以下の条文は、該当する契約のみ）
（電磁的記録媒体の保管）
第１７条　受注者は、この契約により受託した事務に係る個人情報を記録した電磁的記録媒体を施錠して保管しなければならない。
（電磁的記録媒体の搬送）
第１８条　受注者は、この契約により受託した事務に係る個人情報を記録した電磁的記録媒体を持ち出す場合は、電磁的記録の暗号化処理又はこれと同等以上の保護措置を施し、専用ケース等に入れて施錠した上で、安全対策を施して搬送しなければならない。