資料 12-2

江東区情報化推進プラン（案）

令和2年度～令和6年度

SPORTS & SUPPORTS
KOTO City in TOKYO
スポーツと人情が熱いまち

江東区

目次

第1章　プラン策定にあたって

第1章 プラン策定にあたって

1. プラン策定の趣旨

昨今の情報通信技術（Information and Communication Technology。以下「ICT」といいます。）の発展は目覚ましく、スマートフォン、タブレット端末、ソーシャルメディアなどの普及によってライフスタイルのあらゆる場面に新たなテクノロジーが浸透し、わたしたちの生活において必要不可欠なものとなっています。また、IoT（Internet of Things モノのインターネット）、AI（人工知能）、RPA（Robotic Process Automation　業務自動化ツール）などの最新ITテクノロジーを活用して業務の自動化と効率化を図る動きが急速に広がっています。

こうした社会情勢を踏まえ、国は官民におけるデータ活用の推進と、これにより国民が安心して暮らせる社会・快適な生活環境の実現に寄与することを目的として平成28年12月に「官民データ活用推進基本法」を公布・施行しました。また、新たに「世界最先端IT国家創造宣言・官民データ活用推進基本計画」が閣議決定されました。全ての国民がデジタル技術とデータ利活用の恩恵を享受するとともに、安全で安心な暮らしや豊かさを実感できるデジタル社会の実現に向けた、政府全体のデジタル政策が示されました。このなかで、官民データの利活用には、国と地方公共団体等、各地方公共団体等の施策について、一定の整合性を確保し、官民データを円滑に利活用することが必要不可欠であり、国全体として官民データの利活用が一体的に進むよう、地方公共団体との連携・協力を推進することとしています。

さらに、平成30年１月に「デジタル・ガバメント実行計画」がｅガバメント閣僚会議で決定され、この中で地方公共団体におけるデジタル・ガバメントの推進として地方公共団体における①官民データ活用推進計画の策定②行政手続きのオンライン利用促進③クラウド利用の推進④オープンデータの推進⑤適正な情報セキュリティの確保が掲げられています。

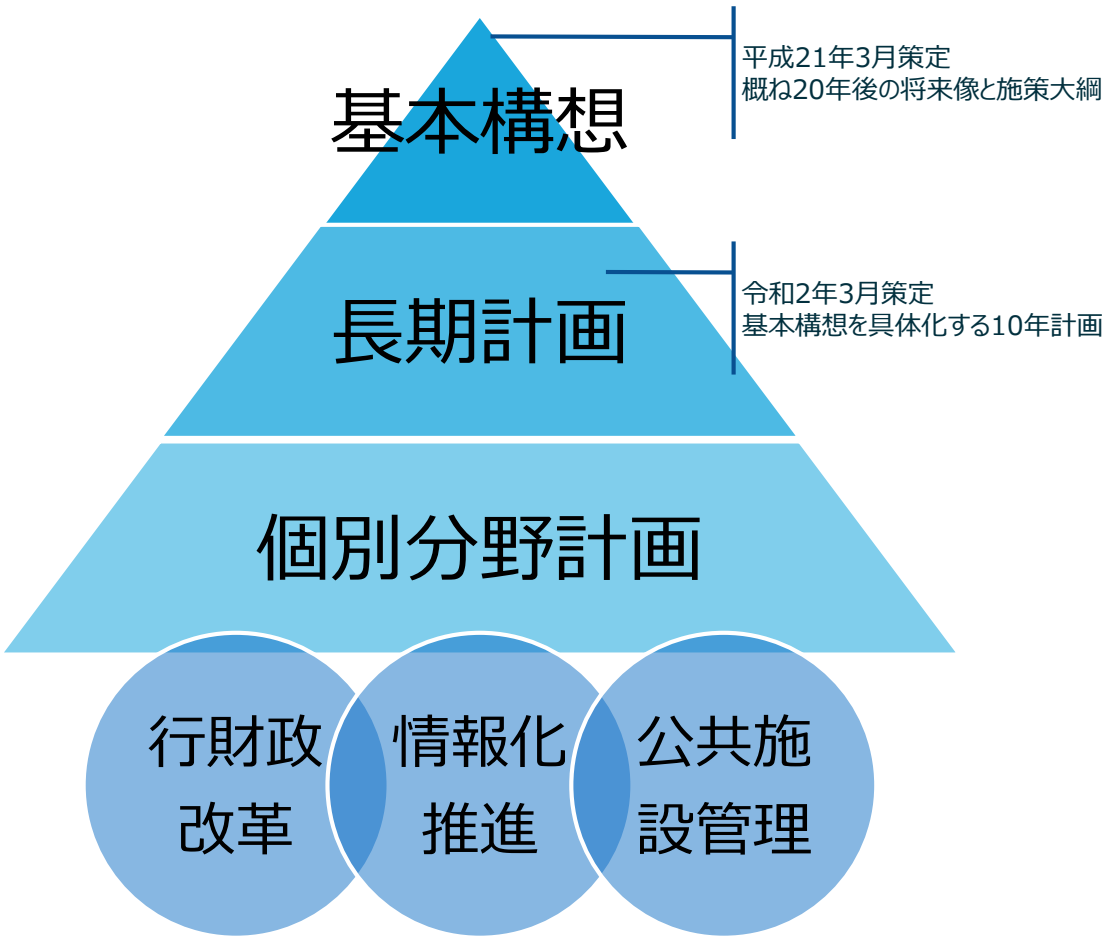
こうしたことから、本区はSociety5.0（※）で実現する社会を見据えて、ICTを利活用し、区民にとって便利で質の高い行政サービスの提供と効率的な行政運営を推進するため江東区官民データ活用推進計画を包含する本プランを策定することとします。

※ Society5.0は、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会で、狩猟社会（Society1.0）、農耕社会（Society2.0）、工業社会（Society3.0）、情報社会（Society4.0）に続く、新たな社会を指します。

2. プランの位置づけ

本プランは、江東区基本構想、江東区長期計画で掲げる区の将来像を情報化の側面から実現するための個別計画であり、情報化の推進に関する方針と方向性、具体の取り組みについて定めるものです。

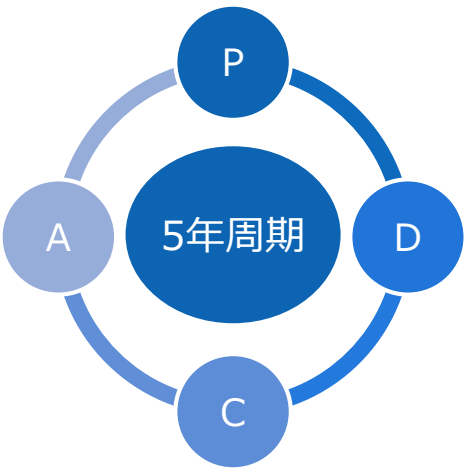
また、官民データ活用推進基本法第9条第3項の規定に基づく「江東区官民データ活用推進計画」として位置づけます。同法が掲げる「行政手続等のオンライン化原則」「オープンデータの促進、データの円滑な流通の促進」「マイナンバーカードの普及・活用」「情報格差の是正」「情報システム改革・業務の見直し」についての取り組みを定めます。



3. プランの期間

本プランの期間は、令和2年度（2020年度）から令和6年度（ 2024年度）までの5ヶ年とします。

PDCAサイクルの考え方に則り、時代背景や経済社会情勢、ICTをとりまく環境の変化、テクノロジーの進化などを踏まえ、必要に応じ見直しを行い、整合性を確保することとします。



第2章　プラン策定の背景

第2章 プラン策定の背景

1. ICTをめぐる社会情勢

ICTの発展は目覚ましく、社会経済のあり方が大きく変化し、個人のライフスタイルの深い層まで新たなテクノロジーが浸透し、より便利で豊かな社会づくりを目指す活動が各方面で展開されています。

個人を取り巻く環境としては、インターネットや移動通信網の高速化・大容量化、フィーチャーフォンからスマートフォンへの移行に伴い、文字によるコミュニケーションからビジュアル（写真や動画）を活用したコミュニケーションへ、また、一方通行、1対1のコミュニケーションだけではなく、「1対他」のコミュニケーションをリアルタイムで行えるようになるなど、個人を取り巻くコミュニケーション、情報発信・情報収集のあり方が大きく変わってきています。

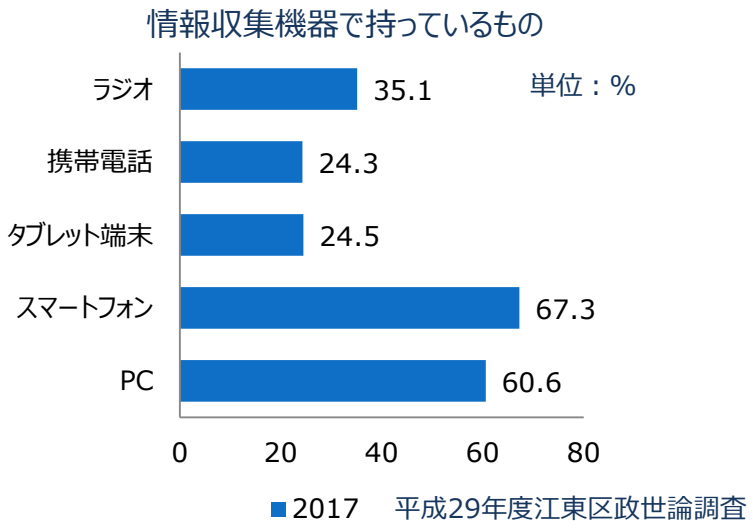
社会を取り巻く環境としては、国の提唱するSociety5.0で実現する社会、2020年に開始される5Gサービスを基盤としたIoTの本格的な普及やAR、VRを用いた新たなサービスの提供が進みつつあります。

また、AIの技術的な進展が進み、生産性の向上やAIを活用した新たなサービスの創出が期待される一方で、AIによる自動化の可能性が70%を超える職業が14%に上るという研究成果も発表されるなど、雇用や働き方に対し大きな変革が生じることも予想されています。

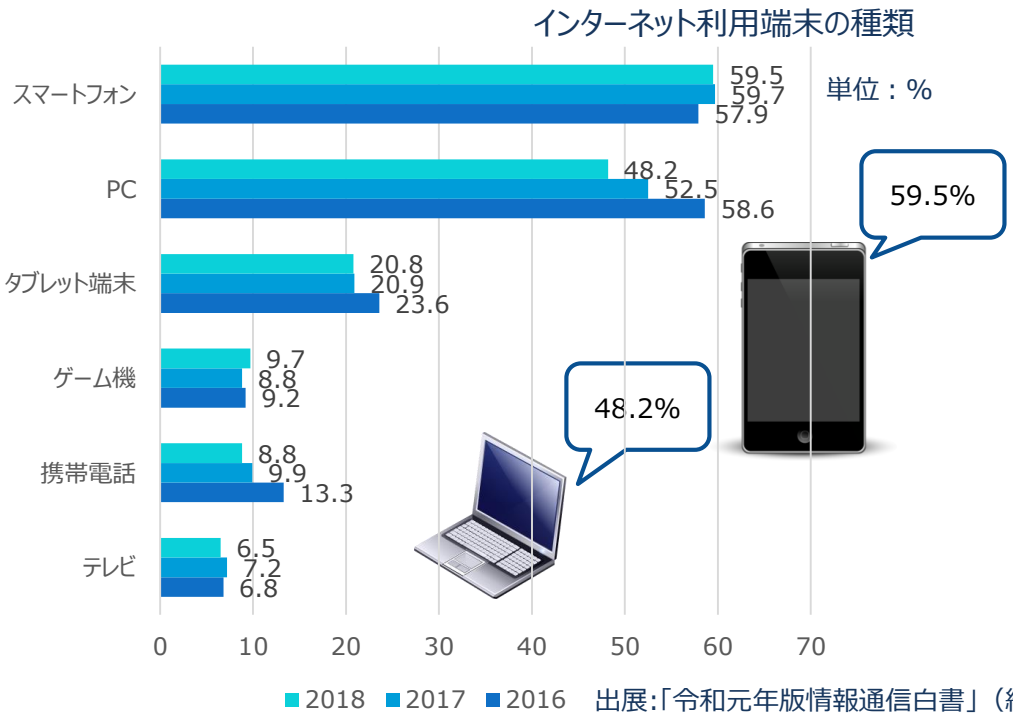
情報システムを取り巻く環境としては、オンプレミス（使用者が管理する施設に設置し、管理運用するシステム形態）によるシステム構築からクラウド環境でのシステム構築、特に、公共部門での利用はまだ進んでいませんが、サーバ機器などのシステムインフラの迅速かつ柔軟な構築の実現や信頼性の向上によって、パブリッククラウド（※）を活用したシステムの構築が急速に進んでいます。

このような柔軟な変更が可能なインフラ環境の実現によって、これまで一般的な開発手法であったウォーターフォール型（工程を順番どおり完成させる確定路線を重視した手法）の開発から、自身を取り巻く環境やユーザの変化、ニーズの変化に柔軟かつ迅速に対応するためにスピード重視型であるアジャイル型の開発手法が普及し、より一層進んできています。

こうした背景を受け、本区においても区民サービスの質の向上、業務の更なる効率化に向けた取り組みを計画的に進めていく必要があります。



平成29年度江東区政世論調査



出展:「令和元年版情報通信白書」（総務省）

※ パブリッククラウド　クラウドコンピューティング（サーバーやアプリケーションなどをネットワーク経由で利用する仕組み）のうち、ユーザーごとに専用のコンピューティング環境を提供する形態（プライベートクラウド）に対して、標準的な環境を不特定多数が共同利用する形で提供する（パブリック）サービスの利用形態をいいます。

2. 国の情報化政策の動向

平成28年12月に「官民データ活用推進基本法」が公布・施行されました。同法では、データ流通環境の整備や行政手続きのオンライン利用の原則化など官民データの活用に資する各種施策の推進が国の取り組みとして義務付けられました。また、国や地方公共団体および事業者の責務を明らかにし、官民データ活用の推進に関する計画の策定を求めています。

平成29年5月には、同法および「高度情報通信ネットワーク社会形成基本法」に基づく取り組みを具現化するものとして、世界最先端IT国家創造宣言・官民データ活用推進基本計画が閣議決定されました。特にIT宣言・官民データ計画の重点分野の一つである電子行政分野における取り組みについては、平成29年5月に「デジタル・ガバメント推進方針」が策定されました。本方針では、本格的に国民・事業者の利便性向上に重点を置き、行政の在り方そのものをデジタル前提で見直すデジタル・ガバメントの実現を目指すこととされています。

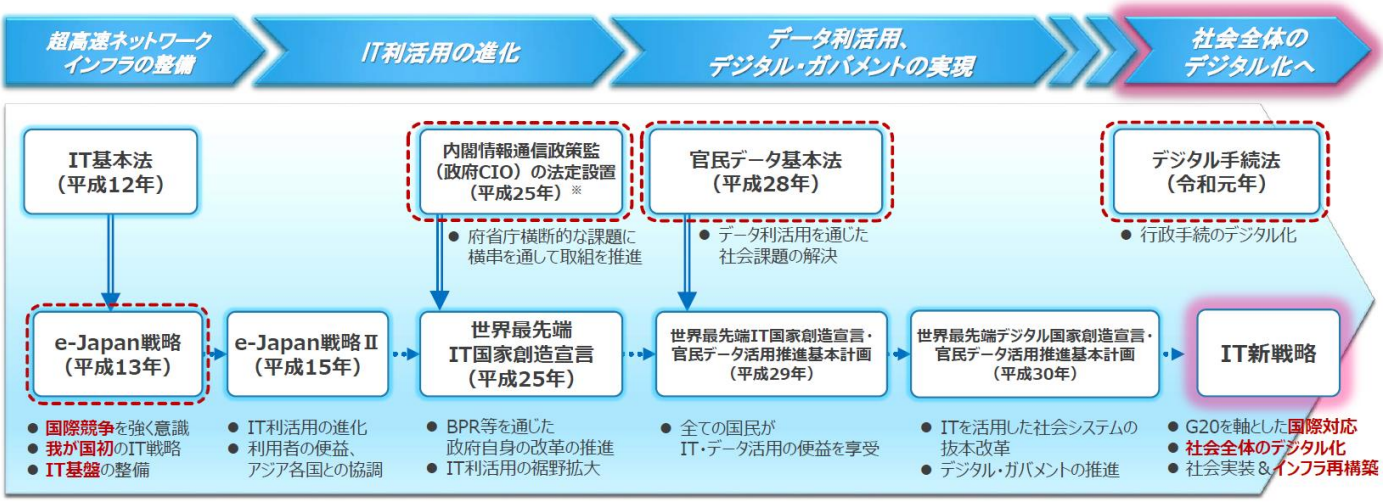
少子化、高齢化の進行や大都市圏への人口の集中、単独世帯や核家族世帯の増加、生産年齢人口の減少、グローバル化の急速な進展など、社会構造は大きく変化しており、これまでの単一的な行政サービスでは、国民一人一人のニーズに応えることが難しくなっています。

一方で、近年目覚ましいICT技術の進展や、マイナンバー制度の導入によって我が国の様々な個人、法人を繋ぐ情報連携基盤の整備が進められています。国民に最適化された行政サービスを提供し、これまでにない新たな価値を提供するための素地が整いつつあります。

こうした背景を受け、官民データ活用推進基本法およびデジタルガバメント推進方針に示された方向性を具体化し、実行することによって、安心、安全かつ公平、公正で豊かな社会を実現するための計画である「デジタル・ガバメント実行計画」が平成30年1月にeガバメント閣僚会議で決定されました。この中で主要施策として、行政手続きにおける①添付書類の撤廃　②オンライン化の徹底　③複数手続のワンストップでの処理　が掲げられています。

さらに、令和元年5月に可決、成立した行政手続きを原則、電子申請に統一する「デジタル手続法（※）」では、行政のデジタル化に関する基本原則として①個々の手続・サービスが一貫してデジタルで完結するデジタルファースト　②一度提出した情報は、二度提出することを不要とするワンスオンリー　③民間サービスを含め、複数の手続き・サービスをワンストップで実現するコネクテッド・ワンストップ　の3つが定められています。

※ 情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律（令和元年法律第16号）



出展:「IT新戦略の概要」（令和元年6月　内閣官房）

3. 都の情報化施策の動向

東京都は、平成28年3月に「東京都における情報通信施策の展開に向けた現況・課題と今後の方向性」を策定しました。その中でICTの概況と都のこれまでのICT利活用状況を整理し、今後の方向性として東京を更なる成熟都市へと高めていくため、ICTを政策実現のツールの一つとして利活用していくとしています。

また、平成29年12月には、都におけるICTの利活用の今後の展開を示す東京都ICT戦略を策定しました。この戦略の基本的な考え方として①都市機能を高めるにあたって、ICTを活用する　②データを活用する　③ICTを活用し、官民連携で行政課題を解決する仕組みを構築する　④民間におけるICT活用を後押しし、生産性向上・新価値創造を図り、東京・日本の成長につなげる　の４つを柱として掲げています。

さらに、令和元年8月に東京都のICT施策として民間企業などと連携して5Gを推進する「TOKYO Data Highway」基本戦略において、5Gネットワークの普及を自治体として早期に構築していく方針が示されました。

4. 江東区における情報化施策の取り組み

本区においては、昭和39年12月にコンピューターを導入して以来これまで、住民基本台帳や住民税等の賦課収納事務といった住民情報に関する基幹系システムの整備や維持管理を進めてきました。また、平成15年2月に庁内LANグループウェアの運用を開始し、財務会計システム、電子決裁システム等の内部情報系システムを整備するなど区民サービスの向上と行政事務の効率化に向けて情報化を着実に進めてきました。

さらに、情報セキュリティ機器の整備や不要なサイトへの接続の制御・管理、LGWAN（行政専用ネットワーク）接続系とインターネット接続系の分割などの対応を図るとともに、業務に係る情報資産のセキュリティ対策が適切に整備および運用されているかの評価・検証を目的とする情報セキュリティ監査およびPIA監査を実施し情報セキュリティ対策を強化してきました。

一方、防災力向上や区民、来訪者および外国人観光客に対する利便性の向上を目的として公衆無線LANの整備を進めてきました。

5. 江東区における情報化施策の課題

ICTをめぐる社会情勢や国・都の情報化施策の動向を踏まえ、本区として今後の情報化施策を推進していく上での課題を次のとおり整理しました。

⑴ ICTを利活用し、人的資源を最大限発揮できる業務改善・事務の効率化が必要です。

⑵ 区民、事業者の利便性向上のためICT利活用とデータの利活用により行政サービスの高度化を推進していく必要があります。

⑶ 安定した業務運営を確保するために低コストで質の高い情報通信基盤の研究・整備に取り組んでいく必要があります。

⑷ サイバーセキュリティを確保し、インシデント発生件数を削減する必要があります。

このような課題に対応するため、ICTを積極的に活用し、行政サービスの高度化、効率化と区民サービスの向上に取り組んでいくことが必要です。

第3章　情報化施策

第3章 情報化施策

1. プランの体系

労働力の不足による職員数の減少など将来懸念される厳しい環境においても、効果的で効率的な行政運営を進め、複雑化かつ多様化する区民ニーズに的確に応えていかなければなりません。そのためにはICTの利活用を推進し、全庁一丸となって業務の効率化や一層の住民サービスの向上を進めていく必要があります。そこで本プランの目指す姿を次のように定め、4つの指針を柱に10の施策を置き、情報化推進の取り組みを進めます。

目指す姿

区民にとって便利で質の高い行政サービスの提供と効率的な行政運営

4つの指針

【指針1】ICTを活用した行政運営の更なる効率化
- [施策1]ICTを活用し業務効率化、生産性を向上させる
- [施策2]業務を自動化する

【指針2】より質の高い行政サービスの提供
- [施策3]区のオープンガバメントを加速する
- [施策4]マイナンバー制度を推進する
- [施策5]学校のICT環境を整備する

【指針3】行政サービスを担う情報インフラの整備・更新
- [施策6]持続可能なシステムにする
- [施策7]Wi-Fiサービスを提供する
- [施策8]情報格差を是正する

【指針4】ICTガバナンスの強化と情報セキュリティの確保
- [施策9]ガバナンスを強化する
- [施策10]セキュリティを強固にする

2. 指針の概要

目指す姿

区民にとって便利で質の高い行政サービスの提供と効率的な行政運営

4つの指針

【指針1】ICTを活用した行政運営の更なる効率化

✓ ICTに係る社会情勢の変化は著しく、RPAやAIなどを活用した業務改善があらゆる分野で進展しています。こういった状況を踏まえ、本区においても、職員数の減少による労働力不足などの将来懸念される厳しい環境下においても持続可能な行政サービスが提供できるよう、ICT技術を活用した業務改善を実施していきます。

【指針2】より質の高い行政サービスの提供

✓ 進化が著しいICT技術を利活用し、区民が行政サービスの利便性向上を実感できるよう取り組みを進めていきます。また、区が保有する行政情報のオープン化を進め、官民の連携によってデータの利活用を行うことで情報化を実感できる環境づくりを進めます。

【指針3】行政サービスを担う情報インフラの整備・更新

✓ 区民サービスを支える基幹系システムは、平成23年度に汎用機からオープンシステムへの再構築を行い、住民サービスの向上、業務改善のためのカスタマイズを施しながら今日まで運用し続けています。本システムを安定的に運用し続けるためには、情報インフラの保守期限を考慮して定期的な更新を行う必要があります。したがって、新たな技術や国、東京都や周辺自治体の動向を注視しつつ情報インフラの整備を行っていきます。

【指針4】ICTガバナンスの強化と情報セキュリティの確保

✓ 区が調達する様々なICT・情報システムについて、セキュリティの確保、サイジングの最適化や無駄の排除といった視点からガバナンスを強化します。また、他区、東京都ほか関係機関との連携を密にし、区民の信頼と付託に応えるべく、更なる情報セキュリティの確保を図ります。

3. 施策と個別施策

【指針1】ICTを活用した行政運営の更なる効率化

【施策1】ICTを活用し業務効率化、生産性を向上させる

（現状）

生産年齢人口（15歳以上65歳未満の人口）の大幅な減少が見込まれている日本において、労働力の確保と生産性の向上は重要な課題となっています。平成31年4月より順次施行されている「働き方改革関連法」に伴い、ICTツールを駆使したオフィス改革に取り組む企業は多くなっています。柔軟な働き方を実現するテレワークやフリーアドレスオフィス、ペーパーレス会議やバーチャル会議など、柔軟な働き方が可能となる環境、より高い生産性を目指した取り組みが拡がっています。

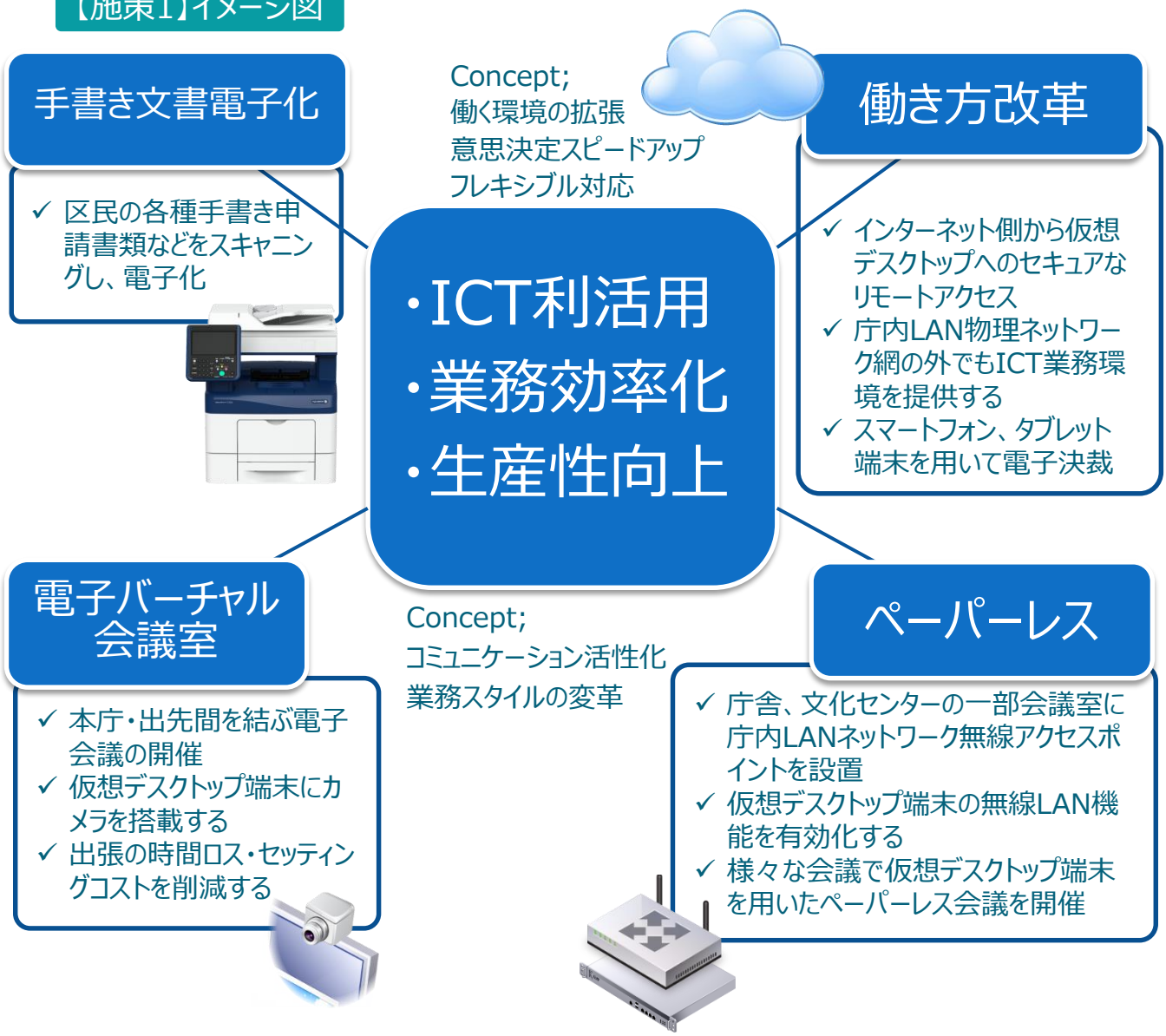
（今後の方針）

本区においてもICT技術を活用して、庁内業務の効率化と生産性の向上につながる取り組みを進めていきます。

分類	機能	ねらい
コミュニケーション活性化	庁内SNS	組織横断型の意見交換
	バーチャル会議	複数の遠隔地を結び時間短縮※
	チャット	リアルタイムな文字会話
業務効率化	電子決裁	決裁プロセスを電子化※
	RPA	ロボットによる業務の一部の自動化※
	プレゼンス管理	在席状況管理※
多様で柔軟な働き方	テレワーク	ワークライフバランスの実現※
	モバイルワーク	すき間時間の有効活用
コスト削減	ファイル共有	情報の蓄積・検索・再利用※
	ペーパーレス化	コスト削減※

※庁内情報系のインフラ・リソースを活用できるプラン

【施策1】イメージ図



【個別施策1】ICTを活用した業務改善、業務の効率化および生産性の向上

テレワーク、モバイルワーク、ペーパーレス会議システム、バーチャル会議システムの導入を検討し、コミュニティの円滑化と情報共有の促進、即時性の向上、意思決定のスピードアップを図ります。

◆ 事業計画

- ペーパーレス会議システムを導入し、活用を進めます。また、バーチャル会議システムの導入を検討していきます。
- 通勤混雑緩和とワークライフバランス推進に向けた検証のため在宅勤務型テレワークを試行実施するとともに、モバイルワークの実施を検討していきます。

【施策2】業務を自動化する

（現状）

近年の技術革新は著しく、ICT技術を活用した業務の自動化については金融業界で先行して導入され、高い効果を発揮したことから、業種を問わず多くの企業・団体においてさまざまな業務を対象に導入されつつあります。自治体においても庁内業務の効率化のため、RPA技術を用いて大量の定型業務、繰り返しのルーティン処理などの単純作業を自動化する取り組みを進めています。

また、AIについても、会議録作成業務や職員の業務支援、保育園入園マッチング支援、市民への情報提供業務など、さまざまな自治体業務において実証実験や実用化が進められています。

（今後の方針）

本区においても、民間事業者や他自治体の取り組みを参考にしながらRPAやAIを活用した業務の自動化に取り組んでいきます。導入にあたっては、ニーズが高く、早期に効果が現れることが見込まれるものから実用化を図っていきます。

【個別施策2】RPAを活用した業務の効率化

職員の日常業務のうち、定型的な業務や単純作業について、可能なものからRPAによる代替を促進し、業務の自動化を図っていきます。これにより職員の負担を軽減し、その余力を創造的な業務などの、より付加価値の高い業務に充てることで、区民サービスの向上につなげます。

OCR_RPAのイメージ

◆事業計画

- AI-OCR（人工知能を活用した帳票読み取りシステム）と、RPAを活用した業務の一部自動化を順次導入していきます。RPAの活用は将来の拡張性を有する施策であるため、令和3年度以降も引き続き業務効率化、業務自動化を実現すべく幅広く取り組んでいきます。

【個別施策3】AIを用いた業務の効率化

次に見られる先行事例を参考に、本区において有用と思われるテクノロジーの導入を順次検討していきます。

- ✓ 保育園入園希望者AIマッチング
- ✓ 問い合わせ自動回答AIチャットボット
- ✓ 多言語AI翻訳サービス
- ✓ 会議録作成AI

◆事業計画

- 個別施策3のAIは、処理に掛かる労力の削減や24時間365日切れ目のないサービスの実現など、区民サービスの向上に資するものの導入、活用に向けて取り組んでいきます。

【指針2】より質の高い行政サービスの提供

【施策3】区のオープンガバメントを加速する ― オープンデータ ―

（現状）

平成28年12月14日に公布施行された官民データ活用推進基本法や国のオープンデータ基本方針、地方公共団体オープンデータガイドライン等を踏まえて、江東区が保有する多種多様なデータを、営利・非営利を問わず誰もが利用できるよう二次利用可能な形で公開しています。

令和2年2月現在でイベント一覧、公共施設一覧、文化財一覧、公衆無線LANアクセスポイントのデータを公開しています。

（今後の方針）

今後、様々な区民ニーズや多様化する地域課題に対応するために、区民・民間事業者と行政が多種多様なデータをオープンデータとしてより広く活用していくことが重要です。このため、ニーズが高く有用なデータから順次積極的に公開していきます。また、オープンデータの利活用を通じて地域問題の解決や新たな事業、新たなサービスの創出など、区民サービスの向上につなげる取り組みを推進していきます。

【個別施策4】オープンデータの利活用

行政の透明性、信頼性の向上をはじめとした多くのメリットを生み出すと考えられる、公共に幅広く有用なデータを二次利用できる形式で積極的に公開します。内容を充実させるため全庁横断的に部署が連携し、東京都オープンデータカタログサイトとも連携した取り組みを推進します。

また、官民連携による調査・分析や課題解決、新たな施策の創出などオープンデータの利活用を検討していきます。

公開するデータのレイアウトは、スケールメリットを考慮し次の2つに準拠します。

- ✓ 推奨データセット（内閣官房情報通信技術（IT）総合戦略室　平成29年12月22日）

※推奨データセット（基本編）①AED設置箇所一覧　②介護サービス事業所一覧　③医療機関一覧　④文化財一覧　⑤観光施設一覧　⑥イベント一覧　⑦公衆無線LANアクセスポイント一覧　⑧公衆トイレ一覧　⑨消防水利施設一覧　⑩指定緊急避難場所一覧　⑪地域・年齢別人口　⑫公共施設一覧　⑬子育て施設一覧　⑭オープンデータ一覧

- ✓ 東京都標準フォーマット

◆事業計画

- 国が公開を推奨するデータセット（上記※）の14の項目について可能なものから順次オープンデータとして公開をしていきます。また、アイデアソン（地域課題を解決するためのアイデアを参加者が議論するもの）などのイベントを活用しオープンデータ利活用の促進を図っていきます。

【個別施策5】統合型GIS（地理情報システム）の利活用

本区の業務で利用する地図は、都市計画、営繕、土木、防災ほか様々な分野で欠かせないツールですが、電子化が進み、電子地図を各分野が個別に定期的に調達している現状があります。これを統合し、地図を重ねて共有することで、行政事務の効率化、コストの低減など多くのメリットが生まれます。

また、統合型GISを元に公式Webサイトで提供できる公開地図を作成すれば、区民サービスの向上が期待されるため、これらを視野に統合型GISの構築を検討していきます。

◆事業計画

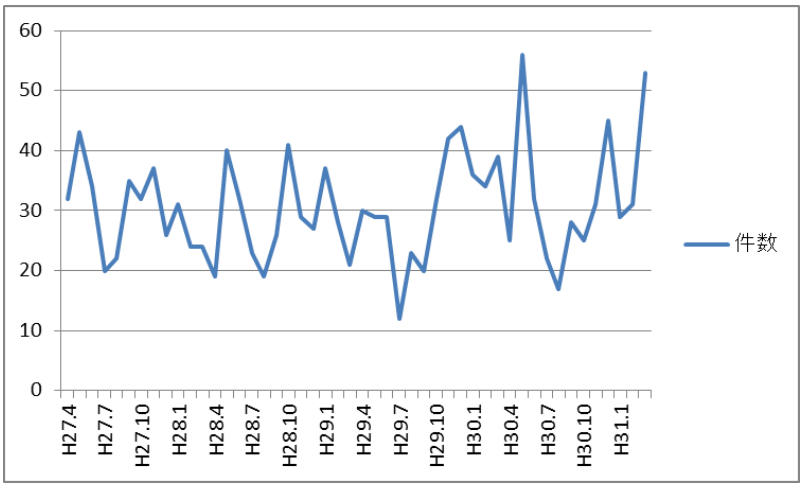
- 統合型GISについて他自治体の取り組みなどを調査研究し、本区の実情に合わせたシステムを早期に構築できるよう早期に検討していきます。

【施策3】区のオープンガバメントを加速する ― 電子申請 ―

（現状）

平成15年2月、都内の都区市町村が1つのシステムを共同利用しつつ、効率的に電子自治体の構築を推進するため、「都区市町村電子自治体共同運営協議会」が設立され、行政手続きの電子化に向け準備、調整を進めました。

平成17年1月、「住民に対する行政サービスの向上並びに行政運営の高度化および効率化」を目的とし、江東区における8つの行政手続きにおいて、電子申請をスタートさせました。以降少しずつ電子申請の対象手続きを追加してきたものの、下図のとおり電子申請件数には顕著な伸びが見られません。



江東区における電子申請利用件数（実績値）

（今後の方針）

官民データ活用推進基本法第10条第1項において、「すぐ使える」「簡単」「便利」な行政サービスを実現するため、行政手続等におけるオンライン化の原則が掲げられています。本区においても行政手続きのオンライン化を拡充していきます。

【個別施策6】電子申請の拡充

電子申請の手続きメニューを増やし、区民サービスの拡充を図ります。また、電子申請の利用促進に向けた自治体間の情報交換、申請手続きを作成できる職員の育成と研修参加の促進を通して、サービスのクオリティが向上するための取り組みを継続して行います。

◆事業計画

- 電子申請の手続きメニュー拡充のため、庁内各部署に電子申請の活用を促し、区民の利便性向上を図ります。また、その担い手となる、電子申請手続きを作成できる職員の育成に取り組んでいきます。

【施策4】マイナンバー制度を推進する

（現状）

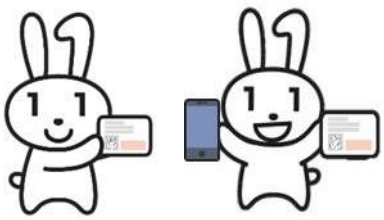
平成28年1月より、社会保障・税・災害対策分野の行政手続きを対象にマイナンバー制度が始まりました。平成29年7月からの試行運用を経て、同年11月から情報提供ネットワークシステムを用いて、国や区市町村等の間で情報連携が開始され、事務手続きにおける書類添付の省略を可能としています。また、ぴったりサービスによる、申請や届出をオンライン上で行えるサービスを、子育ての分野から開始しました。

（今後の方針）

今後、区民がマイナンバー制度のメリットをより享受できるよう、国の方針施策と整合性を図りながら、円滑な情報連携の実施、マイナンバーカードの普及、業務の効率化と区民サービスの向上のための取り組みを推進し、区民の利便性向上を図ります。

【個別施策7】マイナンバーカードの普及促進

国は令和4年度中にほとんどの住民がマイナンバーカードを保有していることを想定しています。本区においても、カードの普及促進に取り組んでいきます。



◆事業計画

- 国のマイナンバーカード普及促進の施策と整合性を図りながら、カードの円滑な交付に引き続き取り組んでいきます。また、区報や区ホームページを通じてマイナンバーカードの普及に向けた広報をしていきます。

【個別施策8】ぴったりサービスの拡充

ぴったりサービスで利用できる電子申請の対象となる手続きメニューを拡充し、区民の利便性向上を図ります。

◆事業計画

- 区民がオンライン上で各種申請や手続きを行える環境整備を推進していきます。これにより、ぴったりサービスを活用した電子申請件数の増加を図っていきます。

【施策5】学校のICT環境を整備する

（現状）

本区では、わかりやすく興味・関心を高める授業づくりと児童・生徒の情報活用能力の育成、校務の効率化による教育の質の向上を目指し、学校のICT環境を整備してきました。

平成28年度には電子黒板を全小中学校の各フロアに1台、平成29年度にはタブレット端末を各校86台整備し、これらと併せて、校内のLAN環境の整備やICT支援員の配置も進めてきました。なお、電子黒板については令和元年度、小学校5・6年生の全普通教室にも整備を行っています。

令和2年度より順次全面実施される新学習指導要領では、情報活用能力を言語能力等と同様に「学習の基盤となる資質・能力」と位置づけるとともに、学校のICT環境整備と、小学校におけるプログラミング教育の必修化などICTを活用した学習活動の充実を明記しています。

新学習指導要領の基本的な考え方である「主体的・対話的で深い学び」を実現し、新しい時代に必要とされる資質・能力を育むために、学校ICT化をさらに加速させることが求められています。

また、近年課題となっている教員の働き方改革の実現に、校務のICT化は必要不可欠となっています。本区では、平成21年度に教員1人1台のパソコンを配付し、平成24年度には成績処理機能を導入して通知表や指導要録を電子化するなど、教員の事務負担軽減に取り組んでいます。

（今後の方針）

新学習指導要領の改訂時期・内容等を踏まえ、「小学校教育情報化推進事業」「中学校教育情報化推進事業」を長期計画の主要事業と位置づけ、学校ICT化を計画的に推進していきます。

また、ハード面の環境整備と並行して、教員のICT活用指導力の強化やICT支援員等による支援の充実など、ソフト面の充実にも取り組んでいきます。

【個別施策9】学校教育における情報化の推進

新学習指導要領の全面実施時期に併せて、小学校では令和2年度、中学校では令和3年度に、タブレット端末や電子黒板、無線LAN等の整備を行います。

◆事業計画

機器等	整備内容
電子黒板	各フロア1台に加え、すべての普通教室に整備
タブレット端末	端末を使用する時数を学年ごとに定め、各校の規模に応じた必要台数を整備。小学5年生以上では週10時間程度、1人1台で使用できる台数を各校に整備
無線LAN環境	普通教室・特別教室に100%整備
ICT支援員	各校に月5.5回派遣

【指針3】行政サービスを担う情報インフラの整備・更新

【施策6】持続可能なシステムにする

（現状）

自治体間で情報システムを集約し、共同利用することでシステム管理運用コストを削減すること、また、自然災害対応力の向上等に資することを目的に、システムに係るハードウェア、ソフトウェア、データを自庁で保有、管理せず、堅牢なデータセンターに設置し、ネットワーク経由でシステムを利用する「自治体クラウド」の取り組みが主に総務省より提唱されています。また、「電子自治体の取り組みを加速するための10の指針（平成26年3月総務省）」においても自治体クラウドの推進が取り上げられているところです。江東区の各業務システムは、平成18年4月に開設した江東区防災センターにサーバーを設置し、概ね5年の間隔で機器を更改しています。

（今後の方針）

ソフトウェア面で自治体クラウドを考察すると、小規模な自治体における共同化であればメリットを生みやすいものの、23区のように人口が数十万人規模の場合、それぞれの区でカスタマイズが施され、文字コードも異なる等の理由から実現が難しい状況にあります。

本区における情報システムのクラウド化は国、東京都や周辺自治体の動向を注視しつつ慎重に進めていきます。

【個別施策10】基幹系業務システムの更改

本区における情報システムのクラウド化は国、東京都や周辺自治体の動向を注視しつつ基幹系業務システムの更改に合わせて検討していきます。

◆事業計画

- 令和2年度に機器更改の調達方針を検討し、令和4年度に機器更改を実施します。クラウド化については継続して検討していきます。

【施策7】Wi-Fiサービスを提供する

（現状）

平成28年度に「江東区公衆無線LAN整備方針」を策定し、この整備方針に基づき平成29年1月に「基本方針」を策定しました。方針では“国、東京都又は他団体等との役割分担を踏まえ、江東区として、通信事業者のインターネット接続ライセンスが無くても、誰でも無償で無線LAN接続端末を用いてインターネットに接続できるサービスを整備し、全庁的に統一した行政サービスの一環として公衆無線LAN環境を展開する”こととしました。

平成29年度、平成30年度はこの基本方針に基づき、災害対策をテーマとし、国の重点施策でもある「災害時における拠点避難所」、外国人などを含む本区を訪れる訪問者向けの施策として「文化･観光施設」、区民が訪れる庁舎・出張所、文化センター、スポーツセンター、図書館、公園などの区内116か所に公衆無線LANを整備（※）しました。 ※整備マップP.34

（今後の方針）

区施設における公衆無線LANの整備は完了しましたが、今後新たな手法による公衆無線LAN環境の整備を検討していきます。

【個別施策11】これからの江東区公衆無線LANの展開

官民連携による自動販売機を用いたフリーWi-Fi整備などの他自治体の取り組みを参考にしながら、より効果的にサービスを拡大する方法について検討していきます。

◆事業計画

- 他自治体のWi-Fi整備の取り組みを調査研究し、本区での活用を検討していきます。

【施策8】情報格差を是正する

（現状）

江東区ホームページでは、「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（※）」に対応することを目的とし、アクセシビリティ（Webの使いやすさ、利用しやすさ）の確保と向上に取り組んできました。

※日本工業標準調査会（JISC)が制定した情報アクセシビリティ向上のための標準規格

また、マイナンバー制度においては、マイナポータル（国が運営するオンラインサービス）へのアクセスにおけるデジタル・ディバイド（情報格差）の解消に向け、マイナポータル用端末を区の業務窓口等に20台配備し、誰しもが使える状態で利用に供しています。

（今後の方針）

本区が展開する各種広報媒体において、引き続きアクセシビリティの向上に取り組むほか、公共サインガイドラインに基づく公共サインの多言語化など、区の様々な区民サービスにおける情報格差の是正に取り組みます。

【個別施策12】ホームページのアクセシビリティ向上

公式ホームページにおけるWebアクセシビリティ（Webの使いやすさ・利用のしやすさ）の確保と向上に取り組んでいきます。

◆事業計画

- 区のホームページが誰にとっても見やすくわかりやすくなるようにすると共に、情報の充実を図ります。

【個別施策13】マイナポータルへのアクセスサポート

マイナポータル利用の専用パソコンを本庁舎各課の窓口に設定しているほか、保健所・保健相談所にも設置し、デジタル・ディバイドの是正に取り組みます。

◆事業計画

- マイナポータル端末の利用率向上のため、マイナポータルで利用可能なサービスや端末設置場所、利用方法等について区報、ホームページで周知を図っていきます。

【指針4】ICTガバナンスの強化と情報セキュリティの確保

【施策9】ガバナンスを強化する

（現状）

ICTガバナンスにおいて本区では、平成29年3月に情報システム部門における「システムライフサイクル・ガイドライン」を策定し、各年度における情報システムに掛かるコストを算出するとともに、費用対効果を検証し、情報システムの利用を継続するかどうかの判断を行うこととしています。

また、業務に必要な機器の配備におけるサイジングの最適化に関する取り組みとして、庁内情報系で平成27、30、令和元年度に実施した出力機器更改では、ハードウェア最適化と省エネ・省スペース化を目的として、676台の入出力機器を廃棄の上、複合機を247台導入し、システム最適化と共通化によるコスト抑制、省スペース化および省エネ化を実現しました。

（今後の方針）

ICT調達におけるシステムライフサイクル・ガイドラインを全庁版に改版し、対象を全庁に拡大するとともに、調達する年度の前年度の段階で、見積り徴収におけるシステム全体のサイジング、セキュリティ水準、要件定義の明確さ等が適切であるかをチェックするよう取り組みます。

【個別施策14】ICTガバナンスの強化

システムライフサイクル・ガイドラインを全庁的に適用し、庁内LAN、基幹系各システムだけでなく各課が独自に調達するシステムにおいても、設計、見積り段階からセキュリティ確保の視点で情報システム課がチェックを行う仕組みを構築し、セキュリティ、テクノロジーが得意でないセクションをサポートします。

本区の業務に係る情報資産（情報システムおよび情報システムで取り扱うすべての情報をいいます。例：基幹系システム、庁内LAN、独自システムの機器および各システムで取り扱う個人情報等のデータ）の情報セキュリティ対策が適切に整備および運用されているかを確認し、問題点の確認、改善方法についての検討、助言および指導を行う監査（情報セキュリティ監査、PIA監査）の機能を強化することによって、本区の情報セキュリティレベル向上を図ります。

◆ 事業計画

- 調達仕様や要件定義、設計、構築、試験、運用および資産廃棄まで、一連のICT調達における統一化、標準化を図ります。
- 情報セキュリティ監査、PIA監査の監査項目を適宜見直し、セキュリティの脅威や周囲の状況に対応し監査内容をブラッシュアップします。

【個別施策15】ICT人材の育成

本区では、平成22年10月に「江東区人材育成基本方針」を策定しましたが、約10年が経過したため、令和2年3月に今後の10年を見据えた新たな方針を策定しました。

今後10年を見据えたとき、人口減少社会の到来に伴う労働力不足、人材確保の困難といった厳しい環境下でも持続可能な行政サービスが提供できるよう、AIやRPAを利活用し、定型業務の自動化や事務の効率化を推進することが必要となります。

そこで、新たな方針ではICTなどの専門性を有する人材を育成してくことを盛り込みました。方針に基づいてAIやRPAを利活用できる職員の能力開発と体制の整備を進めていきます。

◆ 事業計画

- ICTを利活用し、業務の効率化や区民サービス向上のために、ICT利活用能力が高い人材の育成に取り組んでいきます。

【施策10】セキュリティを強固にする

（現状）

平成27年4月、番号制度の開始を前に発生した大規模な情報セキュリティインシデントに端を発し、平成28年以降、江東区CSIRTの組織化、インターネットの分離、徹底的な情報持ち出し不可設定など、“情報セキュリティ強靭化”に必要な様々な対策を講じてきました。平成29年6月には、東京都が構築した都区市町村情報セキュリティクラウドに庁内情報系、教育系（校務LAN）、公開系（江東区公式ホームページシステム）をはじめとする主要なインターネット回線が接続し、高度なセキュリティ対策を行っています。

（今後の方針）

区長部局では従来からのセキュリティ監査、自主点検、セキュリティ研修、 OSのアップデートやセキュリティプログラムの適用などのソフト面、運用面の努力を継続することに加え、平成28年度以降に実施したセキュリティ強靭化に係る各施策を継続し、さらに都区市町村で構成するCSIRT連携体制検討部会を中心に各団体CSIRTとの連携の強化を図ります。教育部局では学校版セキュリティポリシーを策定し、教育委員会を含めた区全体としてのレベルアップに向け取り組みます。

【個別施策16】情報セキュリティの確保

都区市町村情報セキュリティクラウド（以下「都SC」といいます。）は、平成29年3月の東京都における先行接続を皮切りに、同年4月より関係する全ての都内区市町村が順次接続し、本区は同年6月3日に接続を完了しました。

また、庁内LANのほか、教職員用校務LANおよび公式HPシステムを都SCに接続し、SOC（※）監視チームにより不正サイト接続防止、攻撃メール添付ファイル接続先のIPブロック、Webサーバーに対するDDoS攻撃の検知およびブロック等一定の成果を上げています。

※SOC Security Operation Centerの略。24時間365日体制でシステム機器や通信を監視し、サイバー攻撃の検知、分析、通知を行う組織

◆ 事業計画

平成29年5月に立ち上がった都区市町村CSIRT連携体制検討部会において、脅威情報やインシデントに関する情報の共有、訓練などを通して、インシデント発生時に速やかに対応できるように取り組みを推進するとし、令和元年以降もこの取り組みが継続されています。本区もこの取り組みに参加し、全体としてセキュリティが確保されるよう連携を図っていきます。

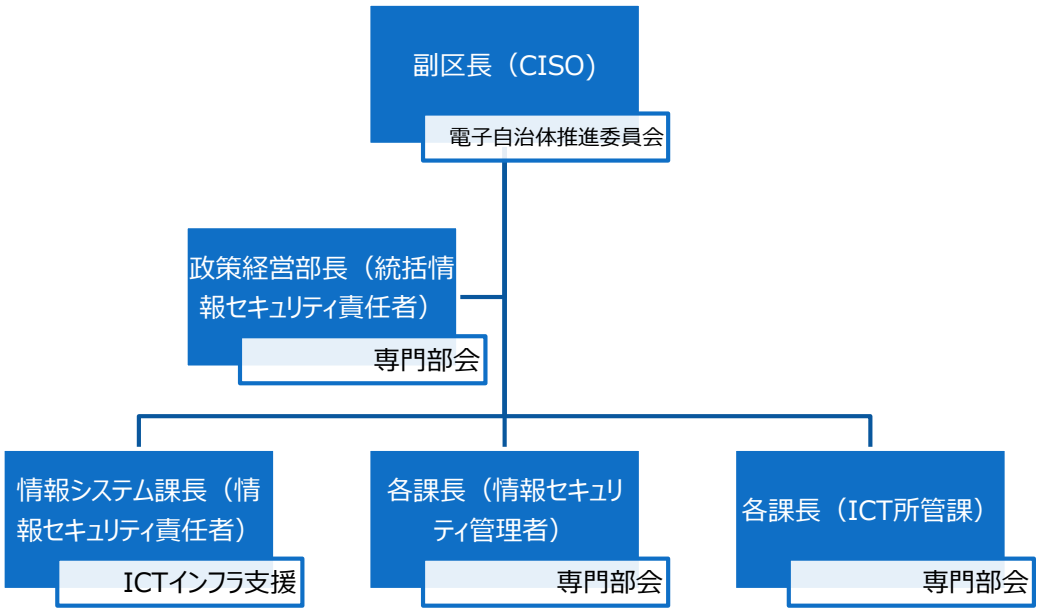
- 学校（学校教育法第1条）では、今後さらにICT化を推し進め、新学習指導要領に対応した高度な学習を全ての学校で展開するに当たり、区長部局とは異なり、教職員や児童生徒を対象とした情報セキュリティ確保策を定めることが不可欠な条件として求められています。これらの背景から、①区長部局CISOを最終権限・責任者とする組織体制の確立、②校務系システムと学習系システムの分離とアクセス制御、③インターネット等の脅威への対策、④外部へ情報を持ち出す際のルールの明確化　を重点に据えた（仮称）江東区教育情報セキュリティ対策基準を策定します。

第4章　推進体制および進捗管理

第4章 推進体制および進捗管理

1. 推進体制

- 本プランを着実に推進するため、庁内組織である江東区電子自治体推進委員会または江東区電子自治体推進委員会専門部会において全庁横断的な体制で取り組みます。また、ICTをとりまく環境の変化やテクノロジーの進化等を踏まえながら、取組内容や手法などの必要な見直しを行います。



2. 進捗管理

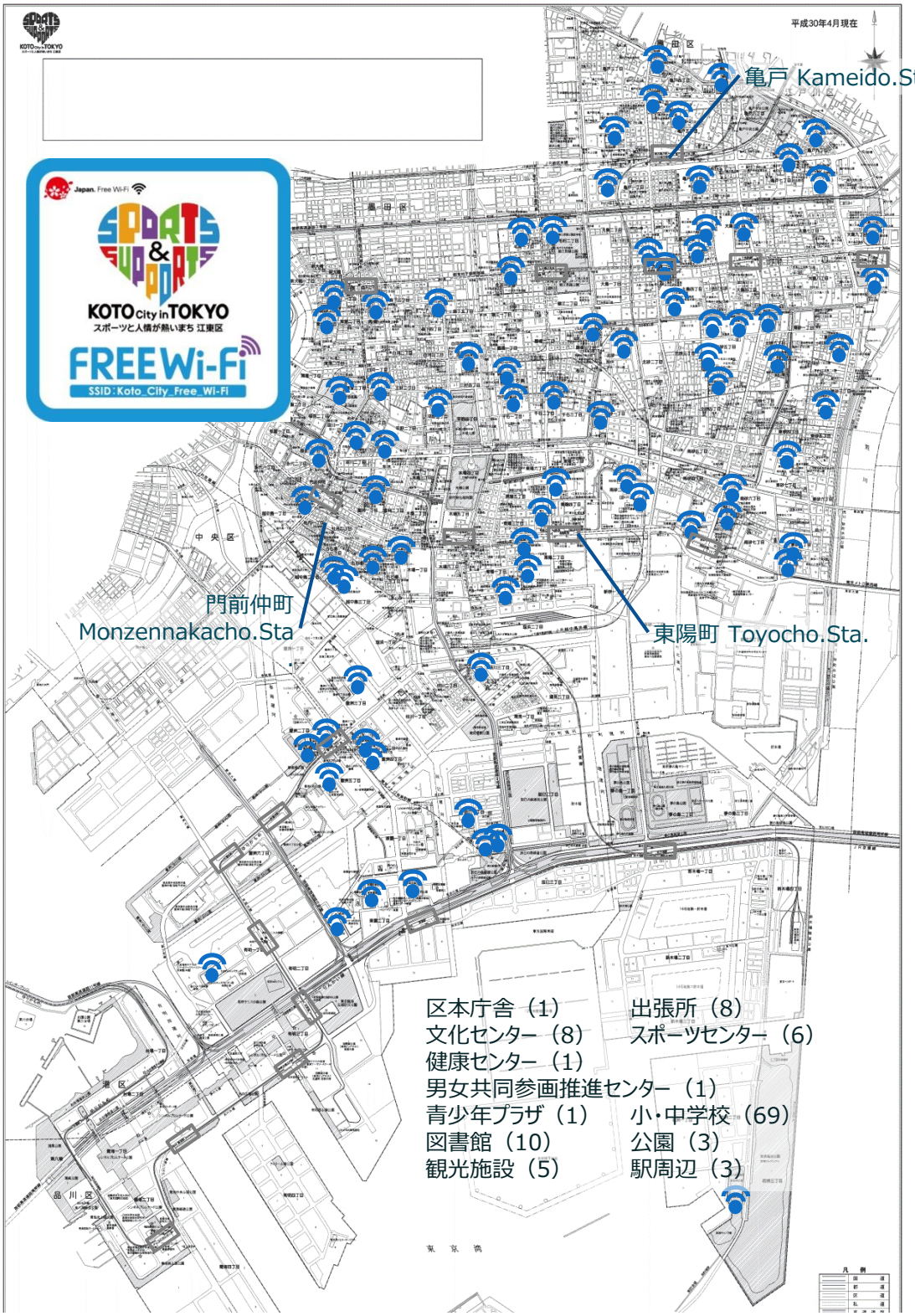
- 各施策・個別施策の進捗管理については、江東区電子自治体推進委員会において行います。進捗状況の報告については、毎年度の行財政改革計画実績版において個別項目「江東区情報化推進プランの推進」のなかで、区議会に報告し、区のホームページに公表します。

資料編

1. 江東区公衆無線LAN整備マップ

Koto city public wireless LAN service

平成31年1月現在、次の拠点に公衆無線LANを整備しています。



2. 江東区情報セキュリティ基本方針

平成16年12月22日
16江政情第142号

改定　平成23年12月8日 23江政情第887号

1　目的

情報システムの高度化・ネットワーク化の進展とともに、情報の改ざん、破壊を目的とした不正アクセスやコンピュータウィルス等の脅威が増大していることから、情報を保護し、情報システムの安全性を確保するためのセキュリティ対策の必要性が一層高まっている。

本区の取り扱う情報資産には、区民の個人情報をはじめ行政運営上重要な情報など、外部に漏洩等した場合は、極めて重大な結果を招く情報が多数含まれている。

このため、本区の個人情報をはじめとする情報資産の機密性（情報へのアクセス権の制御）、完全性（情報及び処理方法の完全性の確保）、可用性（必要なときに情報が利用可能なこと）を維持するための対策を整備するため、江東区情報セキュリティ基本方針を定めることとし、情報セキュリティの確保に最大限取り組むこととする。

2　用語の定義

情報セキュリティ基本方針における用語の意義は、次に定めるところによる。

(1)　電子計算機
ハードウェア及びソフトウェアで構成するコンピュータ及び周辺機器をいう。

(2)　記憶媒体
電子計算機に使用される磁気ディスク、磁気テープ、フロッピーディスク等をいう。

(3)　ネットワーク
コンピュータ相互接続のための通信網及びその構成機器をいう。

(4)　情報システム
電子計算機、記憶媒体及びネットワークで構成される情報処理に用いる仕組みをいう。

(5)　情報資産
情報システム及び情報システムで取り扱うすべての情報をいう。

(6)　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。

3　情報セキュリティ基本方針の適用範囲

情報セキュリティ基本方針の適用範囲は、区の全ての情報資産及び情報資産に接する全ての職員（非常勤職員、臨時職員を含む。）とする。

4　情報資産への脅威

情報資産に対して想定される脅威は、その発生度合や発生した場合の影響を考慮するものとし、次のとおりとする。

(1)　部外者による故意の不正アクセス又は不正操作によるデータやプログラムの持出し・盗聴・改ざん・消去、機器及び記録媒体の盗難等

(2)　職員及び外部委託業者による意図しない操作、故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び記録媒体の盗難、規定外の情報システム接続や操作によるデータ漏洩等

(3)　地震、落雷、火災、水害等の災害並びに事故、故障等による業務の停止

5　情報セキュリティ対策

情報資産を脅威から保護するため、次に定める情報セキュリティ対策を講ずるものとする。

(1)　物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・盗難等から保護するために施設整備等の物理的な対策を講ずる。

(2)　人的セキュリティ対策

情報セキュリティに関する権限や責任を定めるとともに、職員に情報セキュリティポリシーを周知徹底するための教育を実施する等、必要な対策を講ずる。

(3)　技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウィルス対策ソフト導入等の技術面における対策を講ずる。

(4)　運用における対策

不正なアクセス等から情報セキュリティが侵害されることを防ぐため、ネットワーク監視等の運用面における対策及び緊急事態の発生に備えた危機管理対策を講ずる。

6　情報セキュリティ委員会

情報セキュリティ基本方針の遵守を促進するとともに、情報セキュリティに関する事項について調査検討を行うため、情報セキュリティ委員会を設置する。委員会の構成及び運営は、江東区電子自治体推進委員会において行うものとする。

7　情報セキュリティ対策基準の策定

情報セキュリティ対策を講ずるにあたって必要な基本要件を定めた情報セキュリティ対策基準を策定するものとする。

8　情報セキュリティ実施手順の策定

個々の情報資産の情報セキュリティ対策を実施するため、情報セキュリティ対策基準に基づき情報セキュリティ実施手順を策定するものとする。

9　監査

情報システムの情報セキュリティについて定期的に監査を受けなければならない。

10　情報セキュリティ基本方針の評価・見直し
　情報セキュリティ監査の結果等により、情報セキュリティ基本方針に定める事項及び、情報セキュリティ対策の評価を実施するとともに、情報システムの変更や新たな脅威の発生等、状況の変化に迅速かつ的確に対応するため、必要に応じて情報セキュリティ基本方針の見直しを実施する。

11　関連法規の遵守
　職員は、情報資産の利用にあたり、関連法令を遵守しなければならない。

3.　江東区情報セキュリティ対策基準

平成28年2月5日
27江政情第861号

目次

第1章　総則

（目的）

第1条　この基準は、江東区（以下「区」という。）が江東区情報セキュリティ基本方針（平成16年12月22日16江政情第142号。以下「基本方針」という。）を実施するために必要な事項を定めることにより、区の情報セキュリティを確保することを目的とする。

（定義）

第2条　この基準で使用する用語の意義は、基本方針の例によるほか、次の各号に掲げる区分に応じ、当該各号に定めるところによる。

（1）部　江東区組織条例（昭和50年3月江東区条例第47号）第1条に規定する部をいう。

（2）課　江東区組織規則（昭和48年5月江東区規則第19 号。以下「規則」という。）第7条に規定する課及び室、塩浜福祉園、清掃事務所、江東区保健所処務規程（昭和50年4月江東区訓令甲第38号）第4条に規定する保健相談所、江東区教育委員会事務局処務規則（昭和40年3月江東区教育委員会規則第3号）第2条に規定する課及び室、江東図書館、選挙管理委員会事務局、監査事務局並びに区議会事務局をいう。

（3）職員等　江東区職員定数条例（昭和30年4月江東区条例第1号）第1条に規定する職員、江東区職員の勤務時間、休日、休暇等に関する条例（平成10年3月江東区条例第8号）第2条第3項に規定する再任用短時間勤務職員及び第18条に規定する臨時的に任用される職員並びに江東区非常勤職員の報酬および費用弁償に関する条例（昭和31年11月江東区条例第13号）第1条に規定する非常勤職員をいう。

（4）受託事業者　区が委託する情報システムに係る業務の処理を受託した者（受託した業務に従事していた者を含む。）、派遣職員、公の施設の管理を行う指定管理者及び指定管理者の行う管理業務の従事者をいう。

（5）情報セキュリティに関する事故等　望まない単独若しくは一連の情報セキュリティ事象又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする可能性及び情報セキュリティを脅かす可能性があるものをいう。

（6）端末　情報システムの構成要素である機器のうち、職員等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボード、マウス等の周辺機器を含む。）をいう。

（7）パソコン　端末のうち、その形態を問わず、机の上等に備え置いて業務に使用することを前提とし、移動して使用することを目的としないものをいう。

（8）モバイル端末　端末のうち、その形態を問わず、業務上の必要に応じて移動させて使用することを目的としたものをいう。

(9) 情報セキュリティポリシー　基本方針及び本基準をいう。

(適用範囲)

第3条　この基準の適用範囲は、区の情報資産に接する全ての職員等並びに関係団体及び外部の受託事業者とする。

第2章　組織体制

(最高情報セキュリティ責任者)

第4条　区の保有する全ての情報資産及び情報セキュリティの管理並びに情報セキュリティ対策に関する最終決定権限及びこれらの責任を有する最高責任者として、最高情報セキュリティ責任者を置く。

2　最高情報セキュリティ責任者は、江東区長の職務代理順序に関する規則（平成27年5月江東区規則第51号）に規定する第1順位の副区長をもって充てる。

(統括情報セキュリティ責任者)

第5条　情報セキュリティ対策の適切かつ統一的な実施を管理するとともに、最高情報セキュリティ責任者を補佐する者として、統括情報セキュリティ責任者を置く。

2　統括情報セキュリティ責任者は、政策経営部長をもって充てる。

3　統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

4　統括情報セキュリティ責任者は、区の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、最高情報セキュリティ責任者の指示に従い、最高情報セキュリティ責任者が不在の場合には自らの判断に基づき必要かつ十分な措置を行う権限及び責任を有する。

5　統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、統括情報セキュリティ責任者、情報セキュリティ責任者及び情報セキュリティ管理者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

6　統括情報セキュリティ責任者は、情報セキュリティに関する事故等が発生した際は、最高情報セキュリティ責任者に直ちに報告を行うとともに、回復のための対策を講じなければならない。

(情報セキュリティ責任者)

第6条　区において所管する情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する者として、情報セキュリティ責任者を置く。

2　情報セキュリティ責任者は、政策経営部情報システム課長をもって充てる。

3　情報セキュリティ責任者は、区の情報セキュリティ対策に関する統括的な権限及び責任を有する。

4　情報セキュリティ責任者は、区において所有する情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

(情報セキュリティ管理者)

第7条　課における情報セキュリティ対策に関する権限及び責任を有する者として、情報セキュリティ管理者を置く。

2　情報セキュリティ管理者は、各課の長をもって充てる。ただし、規則第21条に規定する行政機関の独立した管理単位を持つ組織にあっては、当該行政機関が属する課の長による指示のもと、その組織の長が情報セキュリティ管理者の役割及び責務を担うものとする。

3　情報セキュリティ管理者は、その所掌する課において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合は、情報セキュリティ責任者、統括情報セキュリティ責任者及び最高情報セキュリティ責任者へ直ちに報告を行い、指示を仰がなければならない。

（情報システム管理者）

第8条　課において所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する者として、情報システム管理者を置く。

2　情報システム管理者は、前項の情報システムを所管する課の長をもって充てる。

3　情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

4　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持又は管理を行う。

（情報システム担当者）

第9条　情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を、情報システム担当者とする。

（兼務の禁止）

第10条　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

（情報セキュリティに関する統一的な窓口の設置）

第11条　情報セキュリティに関する事故等の統一的な窓口の機能を政策経営部情報システム課（以下「情報システム課」という。）に置く。

2　情報システム課は、最高情報セキュリティ責任者による情報セキュリティ戦略の意思決定が行われた際は、その内容を関係部署等に提供する。

3　情報システム課は、情報セキュリティに関する事故等について情報セキュリティ管理者等から報告を受けた場合は、その状況を確認し、最高情報セキュリティ責任者へ報告する。

4　情報システム課は、情報セキュリティに関する事故等を認知した場合は、その重要度、影響範囲等を勘案し、報道機関への通知、公表対応等について政策経営部広報広聴課と協議しなければならない。

5　情報システム課は、情報セキュリティに関し、関係機関、他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

第3章　情報資産の分類及び管理方法

（情報資産の分類）

第12条　区における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

（1）機密性による情報資産の分類

分類	分類基準	取扱制限
機密性3	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	1 機密性3の情報資産に対する支給された端末以外の端末での作業の原則禁止 2 必要以上の複製及び配布の禁止 3 保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持込みの禁止 4 情報の送信、情報資産の運搬又は提供時における暗号化、パスワード設定及び鍵付きケースへの格納 5 復元不可能な処理を施しての廃棄 6 信頼のできるネットワーク回線の選択 7 外部で情報処理を行う際の安全管理措置の規定 8 電磁的記録媒体及び機密性3の紙媒体の施錠可能な場所への保管
機密性2	行政事務で取り扱う情報資産のうち、機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性1	機密性2又は機密性3の情報資産以外の情報資産	

（2）完全性による情報資産の分類

分類	分類基準	取扱制限
完全性2	行政事務で取り扱う情報資産のうち、改ざん、誤り又は破損により、区民の権利が侵害される又は行政事務の的確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	1 バックアップ及び電子署名の付与 2 外部で情報処理を行う際の安全管理措置の規定 3 電磁的記録媒体の施錠可能な場所への保管
完全性1	完全性2の情報資産以外の情報資産	

(3) 可用性による情報資産の分類

分類	分類基準	取扱制限
可用性2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、区民等の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	1 バックアップ及び指定する時間以内の復旧 2 電磁的記録媒体及び可用性2の紙媒体の施錠可能な場所への保管
可用性1	可用性2の情報資産以外の情報資産	

（管理責任）
第13条　情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。
2　情報セキュリティ管理者は、情報資産が複製又は伝送された場合は、複製等された情報資産も前条の情報資産の分類に基づき管理しなければならない。
（情報資産の分類の表示）
第14条　職員等は、情報資産について、ファイル（ファイル名、ファイルの属性、ヘッダー、フッター等をいう。）、格納する電磁的記録媒体のラベル、文書の隅等に情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。
（情報の作成）
第15条　職員等は、業務上必要のない情報を作成してはならない。
2　情報を作成する者は、情報の作成時に第12条の情報資産の分類に基づき、当該情報の分類及び取扱制限を定めなければならない。
3　情報を作成する者は、作成途上の情報についても、紛失、流出等を防止するとともに、当該情報が不要になった場合は、消去しなければならない。
（情報資産の入手）
第16条　職員等が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。
2　職員等以外の者が作成した情報資産を入手した者は、第12条の情報資産の分類に基づき当該情報の分類と取扱制限を定めなければならない。
3　情報資産を入手した者は、入手した情報資産の分類が不明な場合は、情報セキュリティ管理者に判断を仰がなければならない。
（情報資産の利用）
第17条　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。
2　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。
3　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合は、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。
（情報資産の保管）
第18条　情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

2　情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。
3　情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体及び情報システムのバックアップにより取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。
4　情報セキュリティ管理者又は情報システム管理者は、機密性2以上、完全性2又は可用性2の情報を記録した電磁的記録媒体を保管する場合は、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

（情報資産の運搬）

第19条　車両等により機密性2以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定をする等、情報資産の不正利用を防止するための措置を講じなければならない。
2　機密性2以上の情報資産を運搬する者は、情報セキュリティ管理者の許可を得なければならない。

（情報資産の提供及び公表）

第20条　機密性2以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定をしなければならない。
2　機密性2以上の情報資産を外部に提供する者は、情報セキュリティ管理者の許可を得なければならない。
3　情報セキュリティ管理者は、区民等に公開する情報資産について、完全性を確保しなければならない。

（情報資産の廃棄）

第21条　情報資産を廃棄する者は、情報セキュリティ管理者の許可を得なければならない。
2　機密性2以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合は、電磁的記録媒体の初期化等情報を復元できないように処置した上で廃棄しなければならない。
3　情報資産を廃棄する者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

第4章　物理的セキュリティ

第1節　サーバ等の管理

（機器の取付け）

第22条　情報システム管理者は、サーバ等の機器の取付けを行う場合は、火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等必要な措置を講じなければならない。

（サーバの冗長化）

第23条　情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、区民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。
2　情報システム管理者は、メインサーバに障害が発生した場合は、速やかに冗長化したサーバを起動し、情報システムの運用停止時間を最小限にしなければならない。

（機器の電源）
第24条　情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。
2　情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。
（通信ケーブル等の配線）
第25条　統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するため、配線収納管を使用する等必要な措置を講じなければならない。
2　統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合は、連携して対応しなければならない。
（機器の定期保守及び修理）
第26条　情報システム管理者は、可用性2のサーバ等の機器の定期保守を実施しなければならない。
2　情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合は、内容を消去した状態で行わせなければならない。ただし、内容を消去できない場合は、情報システム管理者は、外部の事業者に故障を修理させるに当たり、修理を委託する事業者との間で守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。
（庁外への機器の設置）
第27条　統括情報セキュリティ責任者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合は、最高情報セキュリティ責任者の承認を得なければならない。
2　統括情報セキュリティ責任者及び情報システム管理者は、前項の規定により庁外に設置した機器の情報セキュリティ対策状況について定期的に確認しなければならない。
（機器の廃棄等）
第28条　情報システム管理者は、機器の廃棄、リース返却等をする場合は、機器内部の記憶装置から全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。
第2節　管理区域（情報システム室等）の管理
（管理区域の構造等）
第29条　統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域（ネットワークの基幹機器又は重要な情報システムを設置し、当該機器等の管理及び運用を行う場所（以下「情報システム室」という。）並びに電磁的記録媒体の保管場所をいう。以下同じ。）から外部に通ずる出入口の設置は必要最小限とし、鍵、監視機能、警報装置等によって許可されていない者の立入りを防止しなければならない。
2　統括情報セキュリティ責任者及び情報システム管理者は、情報システム室内の機器等に転倒、落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

3　統括情報セキュリティ責任者及び情報システム管理者は、管理区域に配置する消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（管理区域の入退室管理等）

第30条　情報システム管理者は、管理区域への入退室を許可された者のみに入退室を制限し、ICカード、指紋認証等の生体認証又は入退室管理簿の記載その他の方法で入退室管理を行わなければならない。

2　職員等及び受託事業者は、管理区域に入室する際は身分証明書等を携帯し、必要に応じ、提示しなければならない。

3　情報システム管理者は、外部からの訪問者が管理区域に入る場合は、必要に応じて立入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と訪問者が判別できる措置を講じなければならない。

（機器等の搬入出）

第31条　情報システム管理者は、搬入する機器等が既存の情報システムに与える影響について、あらかじめ職員等又は受託事業者に確認を行わせなければならない。

2　情報システム管理者は、情報システム室に機器等を搬入出する際は職員等を立ち合わせなければならない。

第3節　通信回線及び通信回線装置の管理

第32条　統括情報セキュリティ責任者は、施設管理部門と連携し、通信回線及び通信回線装置を適切に管理するとともに、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

2　統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

3　統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

4　統括情報セキュリティ責任者は、機密性2以上の情報資産を取り扱う情報システムに通信回線を接続する場合は、必要なセキュリティ水準を検討の上、適切な回線を選択するとともに、必要に応じ、送受信される情報の暗号化を行わなければならない。

5　統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報の破壊、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

6　統括情報セキュリティ責任者は、可用性2の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択するとともに、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

第4節　職員等のパソコン等の管理

第33条　情報システム管理者は、盗難防止のため、執務室等で使用するパソコンのワイヤーによる固定、モバイル端末の使用時以外の施錠管理等の物理的措置を講じなければならない。

2　職員等は、電磁的記録媒体に記録した情報が不要となったときは、速やかに当該情報を消去しなければならない。

3　情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

4　情報システム管理者は、パソコン、モバイル端末等におけるデータの暗号化等の機能を有効に利用し、端末にセキュリティチップが搭載されている場合は当該機能を有効に活用しなければならない。

5　情報システム管理者は、電磁的記録媒体の使用に当たっては、暗号化機能を備える媒体を使用しなければならない。

第5章　人的セキュリティ

第1節　職員等の遵守事項

（機器等の搬入出）

第34条　職員等は、情報セキュリティポリシー及び実施手順を遵守するとともに、情報セキュリティ対策に関して不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

2　職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

3　最高情報セキュリティ責任者は、機密性2以上、可用性2、完全性2の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

4　職員等は、モバイル端末、電磁的記録媒体等の持ち出し及び外部における情報処理作業について、次の事項を遵守しなければならない。

(1) 区のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合は、情報セキュリティ管理者の許可を得ること。

(2) 外部で情報処理業務を行う場合は、情報セキュリティ管理者の許可を得ること。

(3) 外部で情報処理作業を行う際に私物のパソコンを用いる場合は、情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守すること。

(4) 機密性2以上の情報資産については、私物のパソコンによる情報処理を行わないこと。

5　職員等は、貸与品以外のパソコン、モバイル端末及び電磁的記録媒体の業務利用について、次の事項を遵守しなければならない。

(1) 貸与品以外のパソコン、モバイル端末及び電磁的記録媒体を業務に利用しないこと。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

(2) 外部で情報処理作業を行う際に貸与品以外のパソコン、モバイル端末及び電磁的記録媒体を用いる場合は、情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守すること。

6　情報セキュリティ管理者は、端末等の持ち出し及び持込みについて、記録を作成し、保管しなければならない。

7　職員等は、情報セキュリティ管理者の許可なくパソコン及びモバイル端末のソフトウェアに関するセキュリティ機能の設定を変更してはならない。

8　職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報が閲覧されることがないよう適切な措置を講じなければならない。

9　職員等は、異動、退職等により業務を離れる場合は、利用した情報資産を返却するとともに、以後も業務上知り得た情報を漏らしてはならない。

10　情報セキュリティ管理者は、職員等に対し、採用時に情報セキュリティポリシー等において職員等が遵守すべき内容を理解させるとともに、当該内容を遵守させなければならない。

（非常勤職員及び臨時職員への対応）

第35条　職情報セキュリティ管理者は、職員等のうち非常勤職員及び臨時職員（以下「非常勤職員等」という。）に対し、採用時に必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

2　情報セキュリティ管理者は、非常勤職員等にパソコン又はモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合は、これらを利用できないように措置しなければならない。

（情報セキュリティポリシー等の掲示）

第36条　情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（受託事業者に対する説明）

第37条　情報セキュリティ管理者は、ネットワーク及び情報システムの開発、保守等を受託事業者に発注する場合又は受託事業者が当該業務を別の受託事業者に再委託する場合は、情報セキュリティポリシー等のうち受託事業者が守るべき内容の遵守及びその機密事項の説明をしなければならない。

第2節　研修及び訓練

（情報セキュリティに関する研修及び訓練）

第38条　最高情報セキュリティ責任者は、情報セキュリティに関する研修及び訓練を定期的に実施しなければならない。

（研修計画の策定及び実施）

第39条　最高情報セキュリティ責任者は、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画の策定及びその実施体制の構築を定期的に行わなければならない。

2　統括情報セキュリティ責任者は、新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

（緊急時対応訓練）

第40条　最高情報セキュリティ責任者は、緊急時対応を想定した訓練を定期的に実施しなければならない。

2　前項の訓練に係る計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、効果的に実施できるようにしなければならない。

第3節　情報セキュリティに関する事故等の報告

（庁内からの情報セキュリティに関する事故等の報告）

第41条　職員等は、情報セキュリティに関する事故等を認知した場合は、直ちに情報セキュリティ管理者に報告しなければならない。

2　前項の報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者及び情報システム課に報告しなければならない。

3　統括情報セキュリティ責任者は、第1項において報告を受けた情報セキュリティに関する事故等について、必要に応じ、最高情報セキュリティ責任者に報告しなければならない。

（区民又は外部からの情報セキュリティに関する事故等の報告）
第42条　職員等は、区が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティに関する事故等について、区民又は外部から報告を受けた場合は、直ちに情報セキュリティ管理者に報告しなければならない。
2　前項の報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
3　情報セキュリティ管理者は、第1項において報告を受けた情報セキュリティに関する事故等について、必要に応じ、最高情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない。
4　最高情報セキュリティ責任者は、情報システム等の情報資産に関する情報セキュリティに関する事故等について、区民又は外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。
（情報セキュリティに関する事故等の原因究明、記録及び再発防止等）
第43条　統括情報セキュリティ責任者は、情報セキュリティに関する事故等を引き起こした部門の情報セキュリティ管理者及び情報システム課と連携し、情報セキュリティに関する事故等の原因を究明し、記録を保存するとともに、原因究明結果から再発防止策を検討し、最高情報セキュリティ責任者に報告しなければならない。
2　最高情報セキュリティ責任者は、統括情報セキュリティ責任者から情報セキュリティに関する事故等の報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。
第4節　ID及びパスワードの管理
（ICカード等の取扱い）
第44条　職員等は、自己の管理するICカード等に関し、次の事項を遵守しなければならない。
(1) 認証に用いるICカード等を、職員等間で共有しないこと。
(2) 業務上必要のないときは、ICカード等をカードリーダー又はパソコン等の端末のスロット等から抜いておくこと。
(3) ICカード等を紛失した場合は、速やかに統括情報セキュリティ責任者及び当該ICカードを用いるシステムを所管する情報システム管理者に通報し、指示に従うこと。
2　統括情報セキュリティ責任者及び情報システム管理者は、前項第3号の通報があり次第、当該ICカード等を使用したアクセス等を速やかに停止しなければならない。
3　統括情報セキュリティ責任者及び情報システム管理者は、ICカード等を切り替える場合は、切替え前のカードを回収し、破砕する等復元不可能な処理を行った上で廃棄しなければならない。
（IDの取扱い）
第45条　職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。
(1) 自己が利用しているIDを、他人に利用させないこと。
(2) 共用IDを利用する場合に、当該IDを共用IDの利用者以外に利用させないこと。
（パスワードの取扱い）
第46条　職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。
(1) パスワードは、他者に知られないように管理すること。

(2) パスワードは秘密にし、パスワードの照会等には応じないこと。
(3) パスワードの文字列は、十分な長さとし、推測され難いものにすること。
(4) パスワードが流出したおそれがある場合は、情報セキュリティ管理者への報告及びパスワードの変更を直ちに行うこと。
(5) パスワードは定期的に、又はアクセス回数に基づいて変更し、過去に設定したパスワードを再利用しないこと。
(6) 複数の情報システムを取り扱う職員等は、同一のパスワードを複数の情報システム間で用いないこと。
(7) 仮のパスワードは、最初にログインした時点で変更すること。
(8) 端末にパスワードを記憶させないこと。
(9) 職員等間でパスワードを共有しないこと。

第6章　技術的セキュリティ

第1節　コンピュータ及びネットワークの管理

（ファイルサーバの設定等）

第47条　統括情報セキュリティ責任者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知しなければならない。

2　統括情報セキュリティ責任者は、ファイルサーバを全庁、課及び個人単位で構成し、それぞれの構成単位に適切なアクセス権限を設定しなければならない。

3　情報システム管理者は、区民等の個人情報、人事記録等特定の職員等のみにアクセス権限を制限するデータについて、別途ディレクトリ（論文、数値、図形その他の情報をパソコン、電磁的記録媒体等に保管するための領域をいう。）を作成する等の措置を講じ、同一課であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（バックアップの実施）

第48条　統括情報セキュリティ責任者及び情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策にかかわらず、定期的にバックアップを実施しなければならない。

（他団体との情報システムに関する情報等の交換）

第49条　情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合は、あらかじめその取扱いに関する事項を定め、統括情報セキュリティ責任者及び情報セキュリティ責任者の許可を得なければならない。

（システム管理記録及び作業の確認）

第50条　情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成及び保存しなければならない。

2　統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように当該記録を適切に管理しなければならない。

3　統括情報セキュリティ責任者、情報システム管理者又は情報システム担当者及び契約により操作を認められた受託事業者がシステム変更等の作業を行う場合は、原則として2名以上で作業し、互いにその作業を確認しなければならない。

（情報システム仕様書の管理）

第51条　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図及び情報システム仕様書について、記録媒体にかかわらず、業務上必要とする者以外の者に閲覧され、又は紛失等がないよう、適切に管理しなければならない。

（ログの取得等）
第52条　統括情報セキュリティ責任者及び情報システム管理者は、各種ログ（情報システムに対して行う指示、当該指示に基づき情報システムが実行した処理の内容及び当該処理の結果を時系列に記録したファイルをいう。以下同じ。）及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。
2　統括情報セキュリティ責任者及び情報システム管理者は、ログとして取得する項目、保存期間、取得方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。
3　統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。
（障害記録）
第53条　統括情報セキュリティ責任者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。
（ネットワークの接続制御、経路制御等）
第54条　統括情報セキュリティ責任者は、フィルタリング（情報セキュリティに関する事故等を防ぐためにネットワークの経路上に設けるファイアーウォール（あらかじめ設定された通信規約に基づき許可された電気通信信号を通過させる機能を有する機器又はソフトウェアのうち、インターネットに対応するものをいう。以下同じ。）等により電気通信信号を制御する措置をいう。）及びルーティング（ルータ（ネットワークに接続する機器ごとに設定したＩＰアドレス（ネットワークに接続する機器を識別するための符号をいう。以下同じ。）により、許可された者による通信であることを認証する機器をいう。以下同じ。）により、複数の接続先から特定のＩＰアドレスへ送信する情報を認証し、中継処理する措置をいう。）について、設定の不整合が発生しないように、ファイアーウォール、ルータ等の通信ソフトウェア等を設定しなければならない。
2　情報システム管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。
（外部の者が利用できるシステムの分離等）
第55条　情報システム管理者は、電子申請の汎用受付システム等外部の者が利用できるシステムについて、必要に応じ、他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。
（外部ネットワークとの接続制限等）
第56条　情報システム担当者は、所管するネットワークを外部ネットワークと接続しようとする場合は、情報システム管理者の許可を得なければならない。
2　情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。
3　情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん、システムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

4　統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ（インターネットを利用した公衆による情報の閲覧の用に供されるサーバをいう。）等をインターネットに公開する場合は、庁内ネットワークへの侵入を防御するために、ファイアーウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

5　情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産の機密性、完全性又は可用性を損なう脅威を与えるおそれがある場合は、直ちに統括情報セキュリティ責任者に報告し、了解を得て当該外部ネットワークを物理的に遮断しなければならない。

（複合機のセキュリティ管理）

第57条　情報システム管理者は、複合機（複写の機能に加え、印刷、ファクシミリ送信又はスキャンのうち１以上の機能を有する機械及び印刷の機能に加え、複写、ファクシミリ送信又はスキャンのうち１以上の機能を有する機械をいう。以下同じ。）を調達する場合は、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

2　統括情報セキュリティ責任者は、複合機が備える機能について適切な設定を行うことにより、運用中の複合機に対する情報セキュリティに関する事故等への対策を講じなければならない。

3　統括情報セキュリティ責任者は、複合機の運用を停止する場合は、複合機の持つ電磁的記録媒体の全ての情報を消去し、又は再利用できないようにする対策を講じなければならない。

（特定用途機器のセキュリティ管理）

第58条　統括情報セキュリティ責任者は、特定用途機器（テレビ会議システム、IP電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵しているものをいう。）について、取り扱う情報、利用方法、通信回線への接続形態等により、機密性、完全性又は可用性を損なう脅威を与えるおそれがある場合は、当該機器の特性に応じた対策を実施しなければならない。

（無線LAN及びネットワークの盗聴対策）

第59条　統括情報セキュリティ責任者は、無線LAN（コンピュータを相互に接続する通信手段のうち、無線により接続する通信手段をいう。）の利用を認める場合は、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

2　統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（電子メールのセキュリティ管理）

第60条　統括情報セキュリティ責任者は、権限のない者の利用により、外部から外部へ電子メール転送（電子メールの中継処理をいう。）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

2　統括情報セキュリティ責任者は、大量のスパムメール（多数の電子メールアドレスを自動的に作成する機能を有するプログラムを用いて作成した電子メール及び現に電子メールアドレスとして利用する者がない電子メールアドレスが送信先として大量に含まれる電子メールをいう。）等の受信又は送信を検知した場合は、電子メールサーバの運用を停止しなければならない。

3　統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。
4　統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。
5　統括情報セキュリティ責任者は、情報システムの開発、運用、保守等のため受託事業者による電子メールアドレスの利用について、受託事業者との間で利用方法を取り決めなければならない。
6　統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等により、情報システム上措置しなければならない。

（電子メールの利用制限）

第61条　職員等は、自動転送機能を用いて、電子メールを転送してはならない。
2　職員等は、業務上必要のない送信先に電子メールを送信してはならない。
3　職員等は、複数人に電子メールを送信する場合は、必要がある場合を除き、他の送信先の電子メールアドレスを非開示にしなければならない。
4　職員等は、重要な電子メールを誤送信した場合は、直ちに情報セキュリティ管理者に報告しなければならない。
5　職員等は、ウェブで利用できるフリーメール（利用者が自己の情報を提供すること又は契約を締結することを条件に、特定のウェブサイトの運営者が、自己の運営するウェブサイトへアクセスさせることによって利用することができる電子メールアドレスを利用者に提供し、当該電子メールを利用させるサービスをいう。）、ネットワークストレージサービス（利用者が自己の情報を提供すること又は契約を締結することを条件に、特定のウェブサイトの運営者が、論文、数値、図形その他の情報を保管するための領域を利用者に提供するサービスをいう。）等を使用してはならない。

（電子署名、暗号化）

第62条　職員等は、情報資産の分類により定めた取扱制限に基づき、外部に送るデータの機密性又は完全性を確保することが必要な場合は、最高情報セキュリティ責任者が定めた電子署名、暗号化又はパスワード設定等のセキュリティ対策を講じて送信しなければならない。
2　職員等は、暗号化を行う場合は、最高情報セキュリティ責任者が別に定める方法以外の方法を用いてはならない。
3　職員等は、暗号化を行う場合は、最高情報セキュリティ責任者が別に定めた方法で暗号のための鍵を管理しなければならない。
4　最高情報セキュリティ責任者は、電子署名の正当性を検証するための情報又は手段を、区において所管する情報システムにあっては情報セキュリティ管理者へ、課において所管する情報システムにあっては情報システム管理者へ安全に提供しなければならない。

（無許可ソフトウェアの導入等の禁止）

第63条　職員等は、パソコン及びモバイル端末に無断でソフトウェアを導入してはならない。
2　職員等は、業務上の必要がある場合は、情報システム管理者の許可を得て、ソフトウェアを導入することができる。

3　前項の許可を受けたソフトウェアを導入する際は、情報セキュリティ管理者又は情報システム管理者は、当該ソフトウェアのライセンスを管理しなければならない。

4　職員等は、不正にソフトウェアをコピーし、及び利用してはならない。

（機器構成の変更の制限）

第64条　職員等は、パソコン及びモバイル端末に対し機器の改造、増設又は交換を行ってはならない。

2　職員等は、業務上、パソコン及びモバイル端末に対し機器の改造、増設又は交換を行う必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

（無許可でのネットワーク接続の禁止）

第65条　職員等は、統括情報セキュリティ責任者の許可なくパソコン及びモバイル端末をネットワークに接続してはならない。

（業務目的以外でのウェブ閲覧の禁止）

第66条　職員等は、業務以外の目的でウェブを閲覧してはならない。

2　統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

第2節　アクセス制御

（アクセス制御等）

第67条　統括情報セキュリティ責任者又は情報システム管理者は、所属するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制御しなければならない。

（利用者IDの取扱い）

第68条　統括情報セキュリティ責任者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職等に伴う利用者IDの取扱い等の方法を定めなければならない。

2　職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

3　統括情報セキュリティ責任者及び情報システム管理者は、退職した職員等の管理するIDが抹消されていない等利用されていないIDが放置されないよう、人事管理部門と連携し、点検しなければならない。

（特権を付与されたIDの管理等）

第69条　統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該ID及びパスワードの漏えい等が発生しないよう、厳重に管理しなければならない。

2　統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者（次項において「代行者」という。）は、統括情報セキュリティ責任者及び情報システム管理者が指名し、かつ、最高情報セキュリティ責任者が認めた者でなければならない。

3　最高情報セキュリティ責任者は、代行者を認めた場合は、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

4　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたID及びパスワードの変更を受託事業者に行わせてはならない。

（職員等による外部からのアクセス等の制限）

第70条　職員等が外部のパソコン等から区が管理するネットワーク又は情報システムにアクセス（以下「外部からのアクセス」という。）をする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

2　統括情報セキュリティ責任者は、外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

3　統括情報セキュリティ責任者は、外部からのアクセスを認める場合は、情報システム上利用者の本人確認を行う機能を確保しなければならない。

4　統括情報セキュリティ責任者は、外部からのアクセスを認める場合は、通信途上の盗聴等を防御するために暗号化等の措置を講じなければならない。

5　統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合は、セキュリティ確保のために必要な措置を講じなければならない。

6　職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内ネットワークに接続する場合は、接続する前に、当該モバイル端末がコンピュータウイルスに感染していないこと、当該モバイル端末のパッチ（機器（ソフトウェアを含む。）の開発者又は製造者が、自ら又は外部からの指摘によって機器の欠陥又はぜい弱性を覚知し、当該欠陥又はぜい弱性を標的にした攻撃を防御するために公開する修正プログラム又は追加プログラムをいう。以下同じ。）の適用状況等を確認しなければならない。

7　統括情報セキュリティ責任者は、公衆通信回線（公衆無線LAN等をいう。）の庁外通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のID及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ICカード等をいう。以下同じ。）による認証に加えて、通信内容の暗号化等情報セキュリティ確保のために必要な措置を講じなければならない。

（自動識別の設定）

第71条　統括情報セキュリティ責任者及び情報システム管理者は、区が管理するネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（ログイン時の表示等）

第72条　情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定、ログイン及びログアウト時刻の表示等により、正当なアクセス権限を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

（パスワードに関する情報の管理）

第73条　統括情報セキュリティ責任者又は情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。

2　情報システム管理者は、その所管する情報システムに、オペレーティングシステム等によるパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

3　統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

（特権による接続時間の制限）

第74条　情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

第3節　システム開発、導入、保守等

（情報システムの調達）

第75条　統括情報セキュリティ責任者又は情報システム管理者は、情報システムの開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

2　統括情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウェアの調達に当たっては、あらかじめ当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（情報システムの開発）

第76条　情報システム管理者は、情報システムの開発の責任者及び作業者を特定するとともに、情報システムの開発のための規程を確立しなければならない。

2　情報システム管理者は、情報システムの開発の責任者及び作業者が使用するIDを管理し、当該開発完了後、開発用のIDを削除しなければならない。

3　情報システム管理者は、情報システムの開発の責任者及び作業者のアクセス権限を設定しなければならない。

4　情報システム管理者は、情報システムの開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

5　情報システム管理者は、開発しようとしている情報システムに利用を認めたソフトウェア以外のソフトウェアが導入されている場合は、当該ソフトウェアを情報システムから削除しなければならない。

（情報システムの導入）

第77条　情報システム管理者は、情報システムの開発、保守及び情報システムのテスト環境と運用環境を分離しなければならない。

2　情報システム管理者は、情報システムの開発、保守及び情報システムのテスト環境から運用環境への移行について、情報システムの開発時及び保守計画の策定時に手順を明確にしなければならない。

3　情報システム管理者は、前項に規定する移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

4　情報システム管理者は、情報システムを導入する場合は、導入する情報システム及びサービスの可用性が確保されていることを確認した上で導入しなければならない。

5　情報システム管理者は、新たに情報システムを導入する場合は、既に稼動している情報システムに接続する前に十分な試験を行わなければならない。

6　情報システム管理者は、運用テストを行う場合は、あらかじめ擬似環境による操作確認を行わなければならない。

7　情報システム管理者は、個人情報及び機密性の高いデータをテストデータに使用してはならない。

8　情報システム管理者は、開発した情報システムについて受入れテストを行う場合は、開発した組織及び導入する組織がそれぞれ独立したテストを行わなければならない。

（システム開発及び保守に関する資料等の整備及び保管）

第78条　情報システム管理者は、情報システムの開発及び保守に関連する資料並びに情報システムの関連文書を適切に整備及び保管しなければならない。

2　情報システム管理者は、テスト結果を一定期間保管しなければならない。

3　情報システム管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

（情報システムにおける入出力データの正確性の確保）

第79条　情報システム管理者は、情報システムに入力されるデータについて、範囲及び妥当性のチェック機能並びに不正な文字列等の入力を除外する機能を組み込むように情報システムを設計しなければならない。

2　情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合は、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

3　情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（情報システムの変更管理）

第80条　情報システム管理者は、情報システムを変更した場合は、プログラム仕様書等の変更履歴を作成しなければならない。

（開発及び保守用のソフトウェアの更新等）

第81条　情報システム管理者は、開発及び保守用のソフトウェア等を更新し、又はパッチを適用する場合は、他の情報システムとの整合性を確認しなければならない。

（システム更新又は統合時の検証等）

第82条　情報システム管理者は、情報システムの更新又は統合を行う場合は、リスク管理体制の構築、移行基準の明確化及び更新又は統合後の業務運営体制の検証を行わなければならない。

第4節　不正プログラム対策

（統括情報セキュリティ責任者の措置事項）

第83条　統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

(1) 外部ネットワークから受信したファイルは、コンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止すること。

(2) 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止すること。

(3) コンピュータウイルス等の不正プログラムの情報を収集し、必要に応じ、職員等に対して注意喚起すること。

(4) 区が管理するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させること。

(5) 不正プログラム対策ソフトウェア及び当該ソフトウェアのパターンファイルは、常に最新の状態に保つこと。
(6) パッチ、バージョンアップ等の開発元のサポートが終了したソフトウェアを使用させないこと。

(情報システム管理者の措置事項)

第84条　情報システム管理者は、不正プログラム対策として、次の事項を措置しなければならない。

(1) 所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させること。
(2) 前号により常駐させるソフトウェア及び当該ソフトウェアのパターンファイルは、常に最新の状態に保つこと。
(3) インターネットに接続していない情報システムにおいて、電磁的記録媒体を使用する場合は、コンピュータウイルス等の感染を防止するため、区が管理している媒体以外の媒体を職員等に使用させないこと。
(4) 前号の場合において、不正プログラムの感染及び侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施すること。

(職員等の遵守事項)

第85条　職員等は、不正プログラム対策として、次の事項を遵守しなければならない。

(1) パソコン及びモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更しないこと。
(2) 外部からデータ又はソフトウェアを導入する場合は、必ず不正プログラム対策ソフトウェアによるチェックを行うこと。
(3) 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除すること。
(4) 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施すること。
(5) 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行うこと。
(6) 統括情報セキュリティ責任者が提供するウイルス情報を、常に確認すること。
(7) コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、次の対応を行うこと。

ア　パソコンの場合　　LANケーブルの即時取り外し
イ　モバイル端末の場合　　即時の利用中止及び通信を行わない設定への変更

(専門家の支援体制)

第86条　統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生する場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

第5節　不正アクセス対策

(統括情報セキュリティ責任者の措置事項)

第87条　統括情報セキュリティ責任者は、不正アクセス対策として、次の事項を措置しなければならない。

(1) 使用されていないポートを閉鎖すること。

(2) 不要なサービスについて、機能を削除又は停止すること。
(3) 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう設定すること。
(4) 重要なシステムの設定を行ったファイルについて、定期的に当該ファイルの改ざんの有無を検査すること。
(5) 情報システム課と連携し、監視、通知、外部への連絡及び適切な対応等を実施できる体制並びに連絡網を構築すること。

(攻撃の予告)

第88条　最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合は、関係機関と連絡を密にして情報の収集に努めるとともに、情報システムの停止を含む必要な措置を講じなければならない。

(記録の保存)

第89条　最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律（平成11年法律第128号）に違反する等の犯罪の可能性がある場合は、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

(内部からの攻撃)

第90条　統括情報セキュリティ責任者及び情報システム管理者は、職員等及び受託事業者が使用している端末からの庁内のサーバ等に対する攻撃及び外部のサイトに対する攻撃を監視しなければならない。

(職員等による不正アクセス)

第91条　統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを発見した場合は、速やかに当該職員等が所属する課の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

(サービス不能攻撃)

第92条　統括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を常に講じなければならない。

(攻撃の予告)

第93条　統括情報セキュリティ責任者及び情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育及び自動再生無効化等の入口対策を講ずるとともに、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

第6節　セキュリティ情報の収集

(ソフトウェアのぜい弱性に関する情報収集、共有、ソフトウェアの更新等)

第94条　統括情報セキュリティ責任者及び情報システム管理者は、ソフトウェアのぜい弱性に関する情報を収集し、必要に応じ、関係者間で共有するとともに、当該ソフトウェアのぜい弱性の緊急度に応じてソフトウェアの更新等の対策を実施しなければならない。

(不正プログラム等のセキュリティ情報の収集及び周知)

第95条　統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じて、対応方法について職員等に周知しなければならない。

第7章　運用
第1節　情報システムの監視
（情報システムの常時監視等）
第96条　統括情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。
2　統括情報セキュリティ責任者及び情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。
3　統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続する情報システムを常時監視しなければならない。
第2節　情報セキュリティポリシーの遵守状況の確認
（遵守状況の確認及び対処）
第97条　情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合は、速やかに最高情報セキュリティ責任者及び統括情報セキュリティ責任者に報告しなければならない。
2　最高情報セキュリティ責任者は、前項の報告を受けた問題について、適切かつ速やかに対処しなければならない。
3　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク、サーバ等の情報システム設定等における情報セキュリティポリシーの遵守状況について定期的に確認を行い、問題が発生した場合は、適切かつ速やかに対処しなければならない。
（パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査）
第98条　最高情報セキュリティ責任者及び最高情報セキュリティ責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メール等の送受信記録等の利用状況を調査することができる。
（職員等の報告義務）
第99条　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合は、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告しなければならない。
2　前項の違反行為が情報セキュリティ上重大な影響を及ぼすと統括情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。
第3節　侵害時の対応等
（緊急時対応計画の策定）
第100条　情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合は、速やかに最高情報セキュリティ責任者及び統括情報セキュリティ責任者に報告しなければならない。
（緊急時対応計画に盛り込むべき内容）
第101条　前条の緊急時対応計画には、次の事項を定めるものとする。
(1) 関係者の連絡先
(2) 発生した事案に係る報告すべき事項
(3) 発生した事案への対応措置
(4) 再発防止措置の策定

（業務継続計画との整合性確保）
第102条　情報セキュリティ委員会は、自然災害、大規模又は広範囲にわたる疾病等に備えて区が別に策定する業務継続計画と情報セキュリティポリシーとの整合性を確保しなければならない。
（緊急時対応計画の見直し）
第103条　情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化、組織体制の変動等を考慮し、必要に応じて緊急時対応計画を見直すものとする。
（許可を得た例外措置）
第104条　情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規程を遵守することが困難な状況において、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用することについて合理的な理由がある場合は、最高情報セキュリティ責任者の許可を得て、例外措置を行うことができる。
（緊急時の例外措置）
第105条　情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合に例外措置を行ったときは、事後速やかに最高情報セキュリティ責任者に報告しなければならない。
（例外措置の申請書の管理）
第106条　最高情報セキュリティ責任者は、例外措置の記録を適切に保管し、定期的に申請状況を確認しなければならない。
第5節　法令遵守
第107条　職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。
(1) 地方公務員法（昭和25年法律第261号）
(2) 著作権法（昭和45年法律第48号）
(3) 不正アクセス行為の禁止等に関する法律
(4) 個人情報の保護に関する法律（平成15年法律第57号）
(5) 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）
(6) 江東区個人情報保護条例（平成10年3月江東区条例第10号）
(7) 江東区電子計算組織管理運営に関する規則（平成10年12月江東区規則第59号）
第6節　懲戒処分等
（懲戒処分）
第108条　情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じ、地方公務員法による懲戒処分の対象とする。
（違反時の対応）
第109条　職員等の情報セキュリティポリシーに違反する行動を確認した場合は、次の措置を講じなければならない。
(1) 統括情報セキュリティ責任者が違反を確認した場合は、速やかに当該職員等が所属する課の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。
(2) 情報システム管理者等が違反を確認した場合は、速やかに統括情報セキュリティ責任者及び当該職員等が所属する課の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

(3) 情報セキュリティ管理者の指導によっても違反する行動が改善されない場合は、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止又は剥奪することができる。
(4) 統括情報セキュリティ責任者は、前項の措置を行った場合は、速やかに最高情報セキュリティ責任者及び当該職員等が所属する課の情報セキュリティ管理者に措置の内容を通知しなければならない。

第8章　外部サービスの利用

第1節　外部委託

（外部委託事業者の選定基準）

第110条　情報セキュリティ管理者は、外部委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

2　情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして事業者を選定しなければならない。

3　情報セキュリティ管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

（契約項目）

第111条　契約担当者（江東区契約事務規則（昭和39年3月江東区規則第11号）第2条第5号の契約担当者をいう。）又は情報セキュリティ管理者は、情報システムの運用、保守等を外部委託する場合は、外部委託事業者との間で必要に応じ次の情報セキュリティ要件を明記した契約を締結しなければならない。

(1) 情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
(2) 外部委託事業者の責任者、委託内容、作業者及び作業場所の特定
(3) 提供されるサービスレベルの保証
(4) 外部委託事業者にアクセスを許可する情報の種類、範囲及びアクセス方法
(5) 外部委託事業者の従業員に対する教育の実施
(6) 提供された情報の目的外利用及び受託者以外の者への提供の禁止
(7) 業務上知り得た情報の守秘義務
(8) 再委託に関する制限事項の遵守
(9) 委託業務終了時の情報資産の返還、廃棄等
(10) 委託業務の定期報告及び緊急時報告義務
(11) 区による監査又は検査
(12) 区による情報セキュリティに関する事故等発生時の公表
(13) 情報セキュリティポリシーが遵守されなかった場合の損害賠償等の規定

（確認、措置等）

第112条　情報セキュリティ管理者は、外部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定期的に確認し、セキュリティ対策が確保されていない場合は、前条の契約に基づき措置するとともに、その内容を統括情報セキュリティ責任者に報告し、内容の重要度に応じて最高情報セキュリティ責任者に報告しなければならない。

第2節　約款による外部サービスの利用

（約款による外部サービスの利用に係る規定の整備）

第113条　情報セキュリティ管理者は、次の事項を含む約款による外部サービスの利用に関する規定を整備しなければならない。

(1) 約款によるサービスを利用してよい範囲
(2) 業務により利用する約款による外部サービス
(3) 利用手続及び運用手順

2　情報セキュリティ管理者は、前項の外部サービスの利用に関する規定において、機密性2以上の情報が取り扱われないようにしなければならない。

(約款による外部サービスの利用における対策の実施)

第114条　職員等は、利用するサービスの約款その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

第3節　ソーシャルメディアサービスの利用

(ソーシャルメディアサービス運用手順等)

第115条　情報セキュリティ管理者は、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（インターネット上で展開される情報メディアのあり方で、組織又は個人による情報発信、個人間のコミュニケーション、人の結びつきを利用した情報流通等の社会的な要素を含んだメディアのことをいう。以下同じ。）を利用する場合は、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(1) 区のアカウントによる情報発信が、実際の区のものであることを明らかにするために、区の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法によりなりすまし対策を行うこと。
(2) パスワード、認証のためのコード等の認証情報及びこれを記録した媒体等を適切に管理する等の方法により不正アクセス対策を行うこと。

2　機密性2以上の情報は、ソーシャルメディアサービスで発信してはならない。

3　情報セキュリティ管理者は、利用するソーシャルメディアサービスごとに責任者を定めなければならない。

第9章　評価及び見直し

第1節　監査

(監査の実施方法)

第116条　最高情報セキュリティ責任者は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

(監査を行う者の要件)

第117条　情報セキュリティ監査統括責任者は、監査を実施する場合は、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

2　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

(監査実施計画の立案及び実施への協力)

第118条　情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

2　被監査部門は、監査の実施に協力しなければならない。

(外部委託事業者に対する監査)

第119条　情報セキュリティ監査統括責任者は、区が委託する事業を対象として、その受託事業者及び受託事業者が再委託する場合はその再委託受託事業者を含めて、情報セキュリティポリシーの遵守について定期的に監査を行わなければならない。

（報告）
第120条　情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。
（保管）
第121条　情報セキュリティ監査統括責任者は、監査の実施を通じて収集した監査証拠及び監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。
（監査結果への対応）
第122条　最高情報セキュリティ責任者は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対応を指示するとともに、指摘事項を所管していない情報セキュリティ管理者に対し、同種の課題又は問題点がある可能性が高い場合は、当該課題又は問題点の有無を確認させなければならない。
（情報セキュリティポリシー及び関係規程等の見直し等への活用）
第123条　情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規程等の見直しその他情報セキュリティ対策の見直し時に活用するものとする。
第2節　自主点検
（自主点検の実施方法）
第124条　統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自主点検を実施しなければならない。
2　情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する課における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自主点検を行わなければならない。
（報告）
第125条　統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、自主点検結果及び自主点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。
（自主点検結果の活用）
第126条　職員等は、自主点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。
2　情報セキュリティ委員会は、点検結果を情報セキュリティポリシー及び関係規程等の見直しその他情報セキュリティ対策の見直し時に活用しなければならない。

第3節　情報セキュリティポリシー及び関係規程等の見直し
（評価及び改善等）
第127条　情報セキュリティ委員会は、情報セキュリティ監査及び自主点検の結果並びに情報セキュリティに関する社会状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認める場合は、改善を行うものとする。
附　則
この基準は、平成28年2月5日から施行する。

4. 江東区電子自治体推進委員会設置要綱

平成27年8月21日
27江政情第546号

（設置）
第1条　江東区における情報政策の基本指針を定めるとともに、情報政策の総合調整及び推進を図るため、江東区電子自治体推進委員会（以下「委員会」という。）を設置する。
（所掌事務）
第2条　委員会は、次の事項を所掌する。
(1) 情報政策の基本指針に関すること。
(2) 情報政策の総合調整及び推進に関すること。
(3) 情報セキュリティ対策及び情報セキュリティに関する事故等の対応に関すること。
(4) 前３号に掲げるもののほか、区長が必要と認める事項
2　本会にワーキンググループ（以下「WG」という。）を置く。
(1) WGにWG会長を置き、政策経営部情報システム課長をもって充てる。
(2) WGの会員は、検討内容に応じて、専門部会が選任する。
（組織）
第3条　委員会は、委員長、副委員長及び委員をもって構成する。
2　委員長は、政策経営部を担任する副区長（以下「政策経営部担任副区長」という。）をもって充てる。
3　副委員長は、政策経営部担任副区長以外の副区長及び教育長をもって充てる。
4　委員は、別表に掲げる者をもって充てる。
（運営）
第4条　委員長は、必要に応じて委員会を招集し、会務を総理する。
2　副委員長は、委員長を補佐し、委員長に事故があるとき又は委員長が欠けたときは、委員長があらかじめ指名する副委員長がその職務を代理する。
3　委員長は、必要があると認めるときは、委員以外の者の出席を求め、又は他の方法で意見を聴くことができる。
4　委員は、別表に掲げる者をもって充てる。
（専門部会）
第5条　委員長は、必要に応じて専門部会を置くことができる。
2　専門部会は、委員会が指定する事項を調査及び検討する。
3　専門部会長及び専門部会の部会員は、委員長が指名する。
4　専門部会長は、必要に応じて専門部会を招集し、会務を総理する。
5　専門部会長は、必要があると認めるときは、専門部会に部会員以外の者の出席を求め、又は他の方法で意見を聴くことができる。
（庶務）
第6条　委員会の庶務は、政策経営部情報システム課において処理する。
（委任）
第7条　この要綱に定めるもののほか、必要な事項は、委員長が別に定める。
附　則
この要綱は、平成27年8月24日から施行する。
別表(第3条関係)

政策経営部長、総務部長、地域振興部長、区民部長、福祉部長、福祉推進担当部長、生活支援部長、健康部長、こども未来部長、環境清掃部長、都市整備部長、土木部長、会計管理室長、教育委員会事務局次長、選挙管理委員会事務局長、監査事務局長、区議会事務局長、企画課長、財政課長、広報広聴課長、情報システム課長、総務課長、職員課長

5. 江東区電子自治体推進委員会専門部会設置要領

平成31年2月1日
30江政情第1761号

（目的）
第1条　この要領は、江東区電子自治体推進委員会設置要綱（平成27年8月21日付け27江政情第546号）第5条に基づき、別に定める「江東区情報化推進プラン（以下「推進プラン」という。）」に関し必要な事項を調査及び検討し、その結果を踏まえ推進プランを策定及び実施し、将来に向けた展開を含め、総合的にこれらを推進する専門部会（以下「本会」という。）を設置することを目的とする。
（組織）
第2条　本会は、専門部会長（以下「部会長」という。）、副専門部会長（以下「副部会長」という。）及び部会員をもって構成する。
(1) 部会長は、政策経営部長をもって充てる。
(2) 副部会長は、政策経営部情報システム課長をもって充てる。
(3) 部会員は、別表に掲げる者をもって充てる。
2　本会にワーキンググループ（以下「WG」という。）を置く。
(1) WGにWG会長を置き、政策経営部情報システム課長をもって充てる。
(2) WGの会員は、検討内容に応じて、専門部会が選任する。
（運営）
第3条　部会長は、必要に応じて本会を招集し、会務を総理する。
2　副部会長は、部会長を補佐し、部会長が欠けたときは、その職務を代理する。
3　WG会長は、必要に応じてWGを招集し、WG会務を総理する。
（所掌事項）
第4条　本会は、次に掲げる事項を所掌する。
(1) 推進プランの策定及び実施に関すること。
(2) 推進プランの調整及び推進に関すること。
2　WGは、次に掲げる事項を所掌する。
(1) 推進プランの策定及び実施に必要な個別具体の検討、推進プランの補完に関すること。
(2) 推進プランの調整及び推進に必要な個別具体の検討及び将来性を考慮した推進プランの補完に関すること。
（委任）
第5条　この要領に定めるもののほか、必要な事項は、委員長が別に定める。
別表（第２条第１号関係）
企画課長、財政課長、広報広聴課長、情報システム課長、総務課長、職員課長、経理課長、地域振興課長、区民課長、福祉課長、医療保険課長、健康推進課長、こども家庭支援課長、温暖化対策課長、都市計画課長、管理課長、庶務課長

6. 用語の解説

◆ AI

- Artificial Intelligenceの略。この言葉に明確な定義はありませんが、このテクノロジーの起源は、人の神経網の仕組みに着目し学習するモデルで1958年に米で提唱された「パーセプトロン」と、これを発展させた「ニューラルネットワーク」であると言われています。

- 「ニューラルネットワーク」の考え方を用いて、人の学習機構に倣い多層的に学習するコンピューターの研究は、「深層学習（Deep Learning）」と呼ばれ、これを基盤とした音声認識、画像認識の精度が飛躍的に向上しています。

- 私たちの暮らしに浸透しつつある製品としては、GoogleやAmazon等が商品化しているAIスピーカー（音声を認識し、指示を実行するパーソナルアシスタント機能を持つ製品）が一般的ですが、音声認識、画像認識の技術を用いて自治体業務に活かす分野としては「保育所入所マッチング」（保育園入園申請者から寄せられる様々な要望を最大限実現するための入園割当て業務）、「戸籍業務審査支援」（法務省の過去の判断基準を検索し、戸籍届出内容の審査を支援する業務）等の実証、導入事例があります。

◆ ICT

- Information and Communication Technologyの略。情報通信技術と訳されており、IT（Information Technology）にCommunication（通信）を加え、情報機器、テクノロジーといった概念に情報の処理、共有、利活用といった幅広い意味を持たせて使われます。

◆ RPA

- Robotic Process Automationの略。農業、工業等の一次産業から製造業、サービス業、ホワイトカラーの様々な分野までにおける定型的な業務の遂行をロボットに置き換え、超少子高齢化社会における労働力不足の補完、人にしかできない創造的な業務への注力等が期待されています。

- 先行自治体の導入事例としては、各種印刷業務、電子申告審査業務等におけるRPA代行事例等があります。

◆ IoT

- Internet of Thingsの略。電車、自動車や航空機、工場やビル、冷蔵庫や洗濯機、農地や牧場の牛など、あらゆるものをネットワークに接続することで、様々な知識や情報が共有され、それぞれの最新状態を示すデータを集め分析した結果から、より最適な状態に導くようにフィードバックを返すという、一連の流れを指します。

- 今までにない新たな価値を生み出すことで、経済の発展と社会的な課題の解決が期待されています。

◆ 5Gサービス

- 「G」はGeneration（世代）の頭文字で、第5世代移動通信システムを言います。移動通信は1980年代の1G（アナログ無線）→1990年代後半の2G（デジタル無線）→2000年から始まった3G（国際標準として規格化したIMT-2000）→2012年以降の4G（高速化技術＝LTE（Lomg-Term-Evolution)を用いた高速通信へと進化を遂げ、2020年以降にサービスを展開する10Gbpsの超高速無線通信サービスを略して5Gと呼称しています。

◆ AR,VR

- AR（Augmented Reality）は、拡張現実といった意味です。CG等で作るデジタルコンテンツを現実世界に加え、あたかもコンテンツが傍にいるかのような表現で現実を「拡張」する技術をいいます。

- VR（Virtual Reality）は、仮想現実といった意味です。ディスプレイに表示する人工的な仮想空間に自分があたかも存在するように体験できる仕組みを提供するものです。

◆ LGWAN

- LGWANは総合行政ネットワーク（Local Government Wide Area Network）の略称で、地方公共団体の組織内ネットワークを相互に接続し、地方公共団体間のコミュニケーションの円滑化、情報の共有による情報の高度利用を図ることを目的とした、高度なセキュリティを維持した行政専用の閉域ネットワークです。

◆ CMSシステム

- Content Management Systemの略。Webサイトを構成するコンテント（ページを構成する要素、基礎レイアウト、ページの連携・遷移構造等の創造や管理を指します。）を統合管理するシステムをいいます。

- Webサイトを作成する際のHTML言語やタグ等の専門知識を要さずに、複数の組織が横断的に統一化されたデザインのページを視覚的かつ容易に作成できるよう、様々なツールを提供します。

◆ OCR

- Optical Character Recognition（光学文字認識）の略。文字が記された紙媒体をスキャナーで読み取った生成物（画像）をもとに、文字をデジタル文字コードに変換するソフトウェアをいいます。

◆ PIA監査

- 江東区が特定個人情報を業務で取り扱うにあたり、情報セキュリティを確保するための対策の一つとして監査を受けることを評価書において表明しており、この評価書に基づき、業務が適切に行われているかをチェックするために行っているのがPIA監査です。

◆ アクセシビリティ

- モノやインフラ、サービス等の使いやすさ、利用しやすさを意味する言葉です。ホームページのクオリティ（品質）を議論する上でのアクセシビリティとは、視覚障害を持つ閲覧者にもより多くの情報を伝えられるページ作りがなされているか、閲覧者が必要な情報を取得できるまでのプロセスを省力化する配慮がなされているか、といった情報提供のバリアフリーを目指す視点でクオリティの高低を判断します。この判断には国際基準（WCAG2.1）やJIS規格（JIS X 8341-3:2016　8341は「優しい」の意)等により公正・公平に判断することができます。

◆ 庁内LAN

- 江東区で全職員が用いる庁内情報系ネットワークシステムの閉域LAN（Local Area Network）を組み合わせた造語で、全職員が日々の業務で利用する仮想デスクトップPC、ファイルを共有管理するNAS、グループウェアや業務効率化アプリケーション、これらを繋ぐネットワーク機器、セキュリティ機器等の総体を表す用語です。

◆ CSIRT

- Computer Security Incident Response Teamの略。組織で発生するインシデントに対応することを目的とする組織たチームを意味します。国内においては国際連携CSIRTとしてJPSIRT/CCが活動しているほか、各企業、団体ごとにチームを立ち上げ、インシデント即応体制を整える活動を行っています。

- 地方自治体におけるCSIRT設立の動きは、マイナンバー制度の本格運用を目前に控えた平成27年5月に日本年金機構が標的型攻撃を受け、大量の個人情報漏洩インシデントが発生したことに端を発し、自治体セキュリティ強靭化対策の推進、自治体セキュリティポリシーガイドラインの改訂とともに各団体において設立が進められております。

- 横断的な取り組みとしては、J-LISが平成30年10月に自治体CSIRT協議会を設立し、各団体におけるCSIRTの機能強化、自治体間連携等を目的として活動しています。

◆ 地域BWA

- BWA＝Broadband Wireless Accessの略。平成20年に、WIMAX方式を用いてデジタル・ディバイド（ICT利用者と非利用者間格差）を解消し、地域の福祉を向上させることを目的として総務省が構築した電気通信事業をいいます。

- 平成26年10月電波法改正により、WIMAX方式にLTEをベースとしたAXGP方式を加え、通信の高速化を実現しました。制度には、免許制であること、携帯電話事業者が参入できないこと、一市町村に一つのサービスであることといった特徴があります。

参考文献

- 内閣府「地理空間情報活用推進基本計画」（平成29年3月24日閣議決定）
- 内閣府「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画」（令和元年6月14日閣議決定）
- 内閣府「デジタルガバメント推進方針」（平成29年5月30日IT本部・官民データ活用推進戦略会議決定）
- 内閣府「デジタルガバメント実行計画」（令和元年12月20日閣議決定）
- 総務省「令和元年版情報通信白書」（令和元年7月）
- 東京都「東京都における情報通信施策の展開に向けた現状・課題と今後の方向性」（平成28年3月31日）
- 東京都「東京都ICT戦略」（平成29年12月22日）
- 東京都「TOKYO Data Highway 基本戦略」（令和元年8月29日）

江東区情報化推進プラン

発行　江東区政策経営部情報システム課