第３　情報公開と個人情報保護

情報の公表及び提供をはじめとする情報公開は、公正で透明な都政の推進と都民による都政の参加により、開かれた都政を実現するとともに、水道利用者が水道事業の運営に対して的確な判断を行うためにも重要な役割を果たすものである。

当局は、情報公開制度を適正に運用するとともに、水道に関する情報について都民のニーズに的確に応えるため、積極的な情報の公開及び提供に努めている。

１　情報公開

一般に「情報公開」とは、「行政機関が有する情報を住民の請求に応じて提供する全ての制度及び施策」を指すものと考えられている。都では、公文書開示制度をその中の一つとして位置付けている。

都の公文書開示制度は、昭和60年から実施されてきた。しかし、都民に対する説明責任を果たし、行政の公正性の確保と透明性の向上を図るため、都における情報公開を一層推進する必要があること等から、平成12年１月に東京都情報公開条例（平成11年東京都条例第５号）が施行された。

都は、公文書開示制度を適正に運用するのはもちろんのこと、併せて積極的に情報を公表・提供し、都民等のニーズに的確に応えていく必要がある。

なお、平成15年10月には、都民サービス向上のため、インターネットによる公文書の検索と開示請求を行える情報公開用システムの運用を開始した。

また、平成29年７月に東京都情報公開条例が改正され、何人も公文書の開示を請求でき、手数料が改定され、交付文書を電磁記録媒体で交付することが可能となった。

当局の公文書開示請求では、平成21年10月から工事関係の設計書に関する開示請求が大幅に増えたことから平成22年度の決定件数は平成20年度の決定件数に比べて約6.5倍の件数となった。このため、当局では情報公開の一層の推進を図るため、定型的な開示請求である工事設計書については、開示請求によらないＣＤによる情報提供を平成27年４月から開始した。平成28年10月受付分からは、水道局における公文書の開示状況を毎月ホームページで公表している。

表４－13　公文書開示請求の処理状況

（単位　件）

年　度	決定件数	開示	一部開示	非開示		総文書数（開示・一部開示）
				非開示	不存在等	
平成20年度	238	176	54	1	7	331
平成21年度	614	469	135	2	8	822
平成22年度	1,543	1,317	212	0	14	1,693
⋮	⋮	⋮	⋮	⋮	⋮	⋮
平成30年度	1,673	1,391	273	1	8	2,010
令和元年度	1,166	739	420	2	5	1,335
令和２年度	750	452	293	0	5	824

2　個人情報保護

情報公開は、都民にとって、また、当局にとっても重要な役割を果たすものであるが、反面、その取扱いに適正を欠いた場合は、個人の権利利益を侵害するおそれがある。

そこで、都は、個人情報の取扱いの基本的事項を定め、個人の権利利益の侵害を未然に防止するとともに、都民の不安感をなくすために、東京都個人情報の保護に関する条例（平成２年東京都条例第113号）を制定した。

その後、高度情報通信社会の進展等に対応して、個人情報の一層の保護を図るため、①従来の開示・訂正請求権に加えて利用停止請求権を設ける、②職員、受託業務従事者等に対する罰則規定を設けるなど所要の改正（平成17年４月施行）を行った。

3　当局の取組

当局は、両条例上の実施機関として、公文書開示を始めとする情報公開を実施している。サービス推進課に設置する水道局情報コーナー、都民情報ルーム（知事が設置）及び各事業所などで都民等からの公文書開示請求の受付、個人情報の開示、訂正及び利用停止事務並びに各種資料の提供を行っている。

また、ホームページ等により、情報の公開及び提供の総合的な推進を図っている。

4　サイバーセキュリティ向上の取組

（1）　全庁統一のサイバーセキュリティポリシーの策定

今日、インターネットをはじめとする情報通信ネットワークや情報処理システムは、都民生活及び社会経済のあらゆる面で利用が拡大し、必要不可欠な社会基盤となっている。

しかし一方で、世界的規模で生じているサイバーセキュリティに対する脅威が深刻化している。特に、不正アクセスや新たな攻撃手法による重要な情報の漏えい・破壊・改ざんが後を絶たず、サイバー攻撃への対策は重大な課題である。

また、操作ミス等によるシステム障害のほか、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全などにも備える必要がある。

このような状況の中、都は、サイバー攻撃等に対して全庁横断的に取り組むため、平成 28 年４月１日に、「東京都サイバーセキュリティポリシー」を施行した。

その後、クラウドサービス及びテレワーク端末の利用や、外部ネットワークとの分離等、最新のサイバーセキュリティ情勢の変化を踏まえ、平成 31 年４月１日に「東京都サイバーセキュリティポリシー」の全面改正を行い施行した。

（2）東京都サイバーセキュリティポリシーの概要

東京都サイバーセキュリティポリシーは、東京都サイバーセキュリティ基本方針（以下「基本方針」という。）及び東京都サイバーセキュリティ対策基準（以下「対策基準」という。）から構成されている。

基本方針は、サイバーセキュリティ対策の目的、体系等、サイバーセキュリティ対策に対する基本的な考え方を示すものであり、対策基準は、基本方針に基づき、サイバーセキュリティ対策を実施するために必要な遵守事項及び判断基準を具体的に定めたものである。

なお、本ポリシーは、サイバーセキュリティ監査及び自己点検の結果のほか、サイバーセキュリティに関する状況の変化への対応が必要となった場合等には、適宜見直すこととしている。

（3）具体的な対策・取組

具体的な対策・取組は、東京都サイバーセキュリティポリシーに基づく詳細な情報資産の取扱い等を定めた安全管理措置のほか、各情報システムの実施手順を定めたサイバーセキュリティ実施手順に基づき、実施している。

主な対策・取組の内容については、次のとおりである。

ア　組織体制

当局の情報資産について、総合的なサイバーセキュリティ対策を推進するため、サイバーセキュリティ委員会を設置し、局内全体の組織体制を確立している。

また、サイバーセキュリティ対策に関して、各職層における管理者等の役割、権限及び責任を明確化している。

イ　情報資産の分類と管理

対策基準に基づき、当局内各部署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、当該分類の重要度に応じて必要な情報資産の管理を徹底している。

ウ　物理的セキュリティ

サーバ、情報システム室、通信回線、パソコン・外部記録媒体等の情報処理機器類の管理について、設置環境、設置方法、施錠管理、冗長性等の物理的な対策が、対策基準を満たしているかの点検を行っている。

エ　人的セキュリティ

サイバーセキュリティに関し、職員等が遵守すべき事項を明確かつ具体的に定めている。

また、年１回の情報セキュリティ強化月間を実施するとともに、定期的な研修・訓練を行い、職員の意識向上を図っている。

オ　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について、点検を行っている。

カ　サイバーセキュリティ監査及び自己点検等

東京都サイバーセキュリティポリシーの遵守状況を検証するため、定期的及び必要に応じてサイバーセキュリティ監査及び自己点検を実施している。

なお、取り扱う情報資産、規模等から特に重要な情報システムについては、第三者によるサイバーセキュリティ監査（外部委託）を定期的に実施している。