東大阪市情報セキュリティ基本方針

はじめに

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システムの利用は生活、経済、社会のあらゆる面で拡大しています。一方で、個人情報の漏洩、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たちません。また、自然災害によるシステム障害にも備える必要があります。

本市は、市民の個人情報や行政運営上重要な情報などを多数取り扱っています。また、多くの業務が情報システムやネットワークに依存しています。

したがって、これらの情報資産を様々な脅威から防御することは、市民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠であります。

これらの状況を鑑み、情報セキュリティ基本方針及び情報セキュリティ対策基準よりなる情報セキュリティポリシーを改定し、市民からの信頼を確保し、更に地域に貢献するため、本市における情報資産に対する安全対策を推進するものです。

構成

<table>
<tr><td rowspan="2">東大阪市情報セキュリティポリシー</td><td>情報セキュリティ基本方針</td><td>情報セキュリティ対策における基本的な考え方</td></tr>
<tr><td>情報セキュリティ対策基準</td><td>基本方針に基づく情報システム共通の対策基準</td></tr>
<tr><td colspan="2">情報セキュリティ実施手順</td><td>対策基準を具体的な手順や手続きに展開して、個別の実施事項を定めるもの</td></tr>
</table>

１、目的
２、定義
３、対象とする脅威
４、適用範囲
　（１） 行政機関の範囲
　（２） 情報資産の範囲
５、職員等の遵守義務

６、情報セキュリティ対策
（１） 組織体制
（２） 情報資産の分類と管理
（３） 物理的セキュリティ
（４） 人的セキュリティ
（５） 技術的セキュリティ
（６） 運用
７、情報セキュリティ監査及び自己点検の実施
８、情報セキュリティポリシーの見直し
９、情報セキュリティ対策基準の策定
１０、情報セキュリティ実施手順の策定

東大阪市情報セキュリティ基本方針

１．目的

この方針は、本市の取り扱う情報資産の機密性、完全性、可用性を維持するために、本市の情報セキュリティを確保するための対策について基本的な事項を定めることを目的とする。

２．定義

（省略）

３．対象とする脅威

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) 部外者の侵入、不正アクセス、コンピュータウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏洩・破壊・改ざん・消去等
(2) 情報資産の無断持ち出し、目的外使用、無許可ソフトウエアの使用等の規定違反、プログラム上の欠陥、操作ミス、故障等の非意図的要因による情報資産の漏洩・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) 情報の提供先（外部提供・業務委託先等）からの情報漏洩

４．適用範囲

（1）行政機関の範囲

本基本方針が適用される行政機関は、市長部局、上下水道局、教育委員会、選挙管理委員会、公平委員会、農業委員会、監査委員及び議会事務局とする。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム、これらに関する設備、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（これらを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．職員等の遵守義務

本市の情報を取り扱う職員、臨時職員、非常勤職員(以下「職員等」という)は、情報セキュリティの重要性について共通の認識をもち、業務の遂行にあたって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

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（2）情報資産の分類と管理

本市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講じる。

（3）物理的セキュリティ

サーバー等の管理、情報システムの設置場所、通信回線及び職員等のパソコン並びに記録媒体等の管理について、物理的対策を講じる。

（4）人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めると共に、十分な教育及び啓発を行う等の人的な対策を講じる。

（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。

（6）運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

７．情報セキュリティ監査及び自己点検の実施

情報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．情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシー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、情報セキュリティポリシーを見直す。

９．情報セキュリティ対策基準の策定

上記６，７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

１０．情報セキュリティ実施手順の策定

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の具体的な手順を定めた情報セキュリティ実施手順及び実施計画を策定するものとする。

附則(施行期日)

本基本方針は平成２０年１２月１日から施行する。

＜用語説明＞

・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。

・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。

・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。