

京都市上下水道局情報セキュリティポリシー

目次

第1章 総則（第1条～第3条）

第2章 高度情報化推進のための体制（第4条～第15条）

第3章 情報システムの適正な利用（第16条～第19条）

第4章 情報セキュリティの確保（第20条～第23条）

第5章 雑則（第24条）

附則

第1章 総則

（趣旨）

第1条 京都市上下水道局情報セキュリティポリシー（以下「本ポリシー」という。）は、上下水道局（以下「局」という。）の事務の高度な情報化の推進（以下「高度情報化推進」という。）を図るため、情報システムの適正な利用及び情報セキュリティの確保に関し必要な事項を定めるものとする。

（定義）

第2条 本ポリシーにおいて、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

- (1) 情報システム 電子計算機、ソフトウェア、記録媒体及びネットワーク（電子計算機を相互に接続し、情報を伝送するための設備をいう。）の集合体であって、情報の処理を一体的に行うよう構成されたものをいう。
- (2) 電子情報 電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。）に記録された情報のうち、電子計算機で取り扱うものをいう。

- (3) 入出力帳票 電子計算機に入力するための情報（既に入力された情報の編集、加工、修正、更新、検索又は消去を行うための情報を含む。）が記録された帳票及び電子計算機から出力される帳票をいう。
- (4) 情報資産 情報システム、電子情報、入出力帳票並びに情報システムに係る設計書、仕様書その他情報システムの企画、調達、開発、運用、管理及び評価を行うために必要な書類をいう。
- (5) 情報セキュリティ 情報資産が次のいずれにも該当する状態（機密を要しない情報資産にあつては、イ及びウのいずれにも該当する状態）をいう。
- ア 機密が保持されている状態
 - イ 破壊、改ざん、不正な消去その他の事故（以下「事故」という。）のない状態
 - ウ 必要があるときに利用することができる状態
- (6) 課等 京都市上下水道局組織及び事務処理規程第1条第1項から第5項までに規定する課、課を置かない室、支所及び事業所（課を置く事業所を除く。水道部配水管理事務所及び給水工事事務所にあつては、北部担当及び南部担当をそれぞれ事業所とみなす。以下同じ。）をいう。
- (7) イン트라ネット 局が高度情報化推進のための情報通信基盤として整備したネットワーク及び当該ネットワークに接続した電子計算機等のうち、総務部総務課が管理するものをいう。

（職員の責務）

第3条 職員は、情報システムを利用するに当たっては、法令を遵守するとともに、情報セキュリティを確保するために必要な措置を採らなければならない。

第2章 高度情報化推進のための体制

（会議の開催）

第4条 京都市公営企業管理者上下水道局長は、必要があると認めるときは、高度情報

化推進のための会議を開催するものとする。

(最高高度情報化推進責任者)

第5条 局に、最高高度情報化推進責任者（以下「最高推進責任者」という。）を置く。

2 最高推進責任者は、次長をもって充てる。

3 最高推進責任者は、局の事務の高度情報化推進に係る事務（情報セキュリティの確保に係るものを除く。）の責任者として、次に掲げる事務を統括する。

(1) 局の事務の高度情報化推進に係る計画の企画（情報セキュリティの確保に係るものを除く。）に関すること。

(2) 前号に掲げるもののほか、情報システムの適正な利用に関すること。

(最高情報セキュリティ責任者)

第6条 局に、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、次長をもって充てる。

3 最高情報セキュリティ責任者は、局の情報セキュリティの確保に係る事務の責任者として、次に掲げる事務を統括する。

(1) 情報セキュリティの確保に係る計画の企画に関すること。

(2) 前号に掲げるもののほか、情報セキュリティの確保に関すること。

(情報セキュリティ監理者)

第7条 局に、情報セキュリティ監理者を置く。

2 情報セキュリティ監理者は、監察監をもって充てる。

3 情報セキュリティ監理者は、情報セキュリティを確保するための対策（以下「情報セキュリティ対策」という。）の推進の状況を継続的に監理し、必要があると認めるときは、最高情報セキュリティ責任者に対し、情報セキュリティを確保するために必要な措置を講じるよう勧告する。

(高度情報化推進統括者)

第8条 局に、最高推進責任者を補佐するため、高度情報化推進統括者（以下「推進統括者」という。）を置く。

2 推進統括者は、総務部長をもって充てる。

3 推進統括者は、最高推進責任者の命を受け、次に掲げる事務を掌理する。

(1) 高度情報化推進に係る施策及び意見の調整並びに当該施策の実施に関すること（情報セキュリティの確保に係るものを除く）。

(2) 前号に掲げるもののほか、情報システムの適正な利用に関すること。

(情報セキュリティ統括者)

第9条 局に、最高情報セキュリティ責任者を補佐するため、情報セキュリティ統括者を置く。

2 情報セキュリティ統括者は、総務部長をもって充てる。

3 情報セキュリティ統括者は、最高情報セキュリティ責任者の命を受け、情報セキュリティの確保に関する事務を掌理する。

(情報セキュリティ管理責任者)

第10条 局に、情報セキュリティ統括者を補佐するため、情報セキュリティ管理責任者を置く。

2 情報セキュリティ管理責任者は、総務部総務課長をもって充てる。

3 情報セキュリティ管理責任者は、情報セキュリティ統括者の命を受け、情報セキュリティの確保に関する事務を掌理する。

(情報システム管理者)

第11条 情報システムの構築及び運用に係る業務を主管する課等（以下「主管課」という。）に情報システム管理者を置く。

2 情報システム管理者は、主管課の長をもって充てる。

3 情報システム管理者は、主管する情報システムの安定的な運用及び管理に努め、情

報セキュリティを確保するために必要な措置を採らなければならない。

(イントラネット管理者)

第12条 イントラネットを統括管理する情報システム管理者として、総務部総務課にイントラネット管理者を置く。

2 イントラネット管理者は、総務部総務課長をもって充てる。

3 イントラネット管理者は、イントラネットの安定的な運用及び管理に努め、情報セキュリティを確保するために必要な措置を採らなければならない。

(情報セキュリティ管理者)

第13条 課等に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、課等の長をもって充てる。

3 情報セキュリティ管理者は、情報セキュリティを確保するため、これに必要な措置を講じるとともに、所属職員を指導しなければならない。

(情報セキュリティ対策支援員)

第14条 課等に情報セキュリティ対策支援員を置く。

2 情報セキュリティ対策支援員は、所属職員の中から情報セキュリティ管理者が任命する。

3 情報セキュリティ対策支援員は、課等における情報セキュリティ対策に関する事務について、情報セキュリティ管理者を補佐する。

(緊急時即応体制)

第15条 情報セキュリティ統括者は、局が保有する情報資産に係る事故が発生し、又は発生するおそれがある緊急の事態に迅速かつ適切に対応するため、次に掲げる事務を統括する。

(1) 事故の発生等に際し、被害を最小限にとどめ、又は未然に防止するために必要な措置を講じること。

(2) 情報セキュリティ対策に係る他の局等その他関係機関等との連絡及び調整に関すること。

2 次に掲げる者は、情報セキュリティ統括者の指揮に従い、前項各号に掲げる事務に従事する。

(1) 情報セキュリティ管理責任者

(2) 総務部に属する職員であつて、情報セキュリティ統括者が指名する者

第3章 情報システムの適正な利用

(情報システムに係る利用指針等の策定)

第16条 最高推進責任者は、情報システムを効果的かつ効率的に利用するため、次に掲げる事項に係る指針等（以下「利用指針等」という。）を示さなければならない。

(1) 市民の利便性の向上、事務処理の簡素化及び経費の節減に関すること。

(2) 情報システムの仕様書の作成、開発費の積算及び調達方法に関すること。

(3) その他情報システムの適正な利用に関すること。

(情報システムの開発及び改修等に係る審査等)

第17条 情報システム管理者及び課等の長は、当該課等が所管する業務に係る情報システムの開発、改修等をしようとする場合であつて、情報システムを効果的かつ効率的に利用するため推進統括者が必要があると認めるときは、推進統括者の審査を受けなければならない。

2 推進統括者は、必要があると認めるときは、情報システム管理者及び課等の長に対し、情報システムの開発、改修等の進行状況について報告を求めることができる。

(推進統括者の指導等)

第18条 推進統括者は、前条第1項の審査の結果、その開発、改修等が利用指針等に照らして適当でないとき、情報システム管理者及び課等の長に対し、情報システムを適正に利用するために必要な指導又は助言を行うものとする。

2 情報システム管理者及び課等の長は、前項の指導又は助言を受けたときは、情報システムの見直しその他の必要な措置を採らなければならない。

(情報システムの運用等に係る報告)

第19条 推進統括者は、必要があると認めるときは、情報システム管理者に対し、情報システムの運用及び管理の状況について報告を求めることができる。

2 情報システム管理者は、前項の規定により報告を求められたときは、利用指針等に基づき、主管する情報システムの適正性について評価を行うとともに、その結果を推進統括者に報告しなければならない。

3 推進統括者は、前項の報告を取りまとめ、これに意見を付して、最高推進責任者に報告しなければならない。

第4章 情報セキュリティの確保

(情報セキュリティ対策基準の策定)

第20条 最高情報セキュリティ責任者は、局の保有する情報資産を適切に管理し、事故を防止するため、電子情報を保護するための対策その他の情報セキュリティ対策に関する基準（以下「情報セキュリティ対策基準」という。）を策定しなければならない。

(事故発生時の対応)

第21条 情報セキュリティ管理者及び情報システム管理者は、事故が発生したときは、直ちにその状況を調査するとともに、その事故の内容を情報セキュリティ管理責任者に報告しなければならない。

2 情報セキュリティ管理責任者は、前項の報告を受けたときは、情報セキュリティ管理者及び情報システム管理者に対し、必要な指示をするとともに、直ちに情報セキュリティ統括者に報告しなければならない。

3 情報セキュリティ統括者は、前項の報告を受けたときは、軽易な事故を除き、直ち

に最高情報セキュリティ責任者及び情報セキュリティ監理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、前項の報告を受けたときは、情報セキュリティ統括者に対し、事故の再発を防止するために必要な措置を講じるよう指示しなければならない。

(実施状況の監査)

第22条 情報セキュリティ統括者は、課等における情報セキュリティ対策の実施状況について、毎年1回以上、監査を行わなければならない。

- 2 情報セキュリティ統括者は、最高情報セキュリティ責任者に対し、前項の監査の結果を報告しなければならない。

(情報セキュリティ対策基準の見直し)

第23条 最高情報セキュリティ責任者は、情報セキュリティ対策の実施状況、情報通信技術の進歩その他の社会情勢の変化を踏まえ、必要があると認めるときは、情報セキュリティ対策基準の見直しを行わなければならない。

第5章 雑則

(補則)

第24条 本ポリシーにおいて別に定めることとされている事項及び本ポリシーの施行に関し必要な事項は、次長が定める。

附 則

本ポリシーは、決定の日から実施する。(平成14年8月22日決定)

附 則

本ポリシーは、決定の日から実施する。(平成16年4月1日決定)

附 則

本ポリシーは、決定の日から実施する。(平成19年12月6日決定)

附 則

本ポリシーは、決定の日から実施する。(平成21年4月1日決定)

附 則

本ポリシーは、決定の日から実施する。(平成22年4月1日決定)

附 則

本ポリシーは、決定の日から実施する。(平成25年4月1日決定)

附 則

本ポリシーは、決定の日から実施する。(平成28年12月28日決定)

附 則

本ポリシーは、平成30年4月1日から実施する。(平成30年3月30日決定)

附 則

本ポリシーは、平成31年4月1日から実施する。(平成31年3月29日決定)

附 則

本ポリシーは、決定の日から実施する。(令和3年4月1日決定)

附 則

本ポリシーは、決定の日から実施する。(令和4年4月1日決定)

附 則

本ポリシーは、決定の日から実施する。(令和5年4月1日決定)

附 則

本ポリシーは、決定の日から実施する。(令和6年4月1日決定)

附 則

本ポリシーは、決定の日から実施する。(令和7年4月1日決定)