第１章　情報セキュリティ基本方針

１　目的

戸田市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、外部に漏洩等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これら情報を取り扱う情報システム及び情報を様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。このことが、ひいては、戸田市に対する市民からの信頼の維持向上に寄与するものである。

また､近年のいわゆるＩＴ革命の進展により､電子申請や電子届出が可能となり、電子自治体の実現が期待されているところである。戸田市がこれらに積極的に対応するためには、全てのネットワーク及び情報システムが高度な安全性を有することが前提条件である。

そのため、戸田市の情報資産の**機密性、完全性**及び**可用性**(注１)を維持するための対策、すなわち情報セキュリティ対策を整備するために､「戸田市情報セキュリティポリシー」を定め、その基本的な方針として「情報セキュリティ基本方針」を定めることとする。

「情報セキュリティ基本方針」では、戸田市情報セキュリティポリシーの位置づけ、対象等について定めるものとする。

（注１）

機密性（ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ）

情報にアクセスすることが認可された者だけがアクセスできることを確実にすること

完全性（ｉｎｔｅｇｒｉｔｙ）

情報及び処理の方法の正確さ及び完全である状態を安全防護すること

可用性（ａｖａｉｌａｂｉｌｉｔｙ）

許可された利用者が必要なときに情報にアクセスできることを確実にすること

（「国際標準化機構（ＩＳＯ）（ＩＳＯ７４９８－２：１９８９）」が定めるもの）

２　用語の定義

情報セキュリティポリシーにおける用語については次のように定義する。

①　ネットワーク

戸田市における市長部局、教育委員会、各行政委員会、消防及び上下水道部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）及び、記録媒体で構成され、処理を行う仕組みをいう。

②　情報システム

業務系の電子計算機（業務系におけるネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

③　情報資産

戸田市が作成又は収集し取り扱う情報のうち、資産として守るべき価値があるものをいう。

④　情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

３　位置づけ

情報セキュリティポリシーは、戸田市の所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的に取りまとめたもので、情報セキュリティの頂点に位置するものである。

４　対象範囲

この情報セキュリティポリシーの対象とする範囲は、ネットワーク及び情報システムをはじめとした全ての情報資産である。また、遵守すべき者の範囲は、職員等及び外部委託者とする。

５　情報セキュリティ管理体制

戸田市の情報資産について、幹部職員が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

６　情報資産の分類

情報資産をその重要度に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

７　情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

①　部外者による故意の不正アクセス、不正操作、その他の不正行為による情報資産の持出・盗聴・改ざん・消去、機器及び媒体の盗難等

②　職員等及び部外委託者による意図しない操作、故意の不正アクセス、不正操作、その他の不正行為による情報資産の持出・盗聴・改ざん・消去、機器及び媒体の盗難及び規定外の端末接続によるデータ漏洩等

③　地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

８　情報セキュリティ対策

上記７で示した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・妨害等から保護するために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、職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要 な対策を講ずる。

③　技術及び運用におけるセキュリティ対策

情報資産を外部からの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、ネットワーク管理等の技術面の対策、また、情報システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

9　情報セキュリティ対策基準の策定

上記８の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するもとする。

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を遵守して、情報セキュリティ対策を実施するために、個々の情報資産の対策基準等をそれぞれ定めていく必要がある。

そのため、情報資産に対する脅威及び、情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、所属長等が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティポリシーのうち、「情報セキュリティ対策基準」及び「情報セキュリティ実施手順」は、公にすることにより戸田市の行政運営に支障を及ぼす恐れがあることから、非公開とする。

11　情報セキュリティ監査の実施

　情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を実施する。

12　評価及び見直しの実施

　情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。